NETOP™ REMOTE CONTROL

Mobile | Embedded™

Remote Support for Mobile & Embedded Systems

User's Guide - Host

Version 9.5

Netop

Please send any comments to:
Netop Business Solutions A/S
Bregnerodvej 127
DK-3460 Birkerod
Denmark
Fax: Int +45 45 90 25 26
E-mail: info@netop.com
Internet: www.netop.com

The document is optimized for double-sided printing.

Contents

1 Features

Netop Mobile & Embedded comprises Netop's solutions for mobile computers and mobile technology computers embedded in equipment.

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 currently includes this module:

- Netop Mobile Host: Enables the mobile device to be remote controlled and interacted with in other ways from a computer running Netop Guest.

Note

Netop Guest is a Netop Remote Control product family module, which can remote control and interact with a computer running a Netop Host or extended Host or Netop Mobile Host.

Netop Mobile features include:

- Remote control
- Other sessions
- Security
- Operating systems
- Communication devices

1.1 Remote control

Remote control is the Netop Mobile key feature. It enables the user of a computer running Netop Guest to display a skin of the mobile device and work in it using the Netop Guest computer keyboard and mouse.

Netop Mobile Hosts can transfer information about their button layout to Windows Guests enabling Netop Guest users to see the button layout by means of a clickable bitmap. This is called a skin.

If you run a remote control session, you can see the Host device and execute commands on the Host device by clicking buttons on the applied skin. Devices may have more than one skin definition depending on its state, for example slide out keyboard, portrait and landscape orientation etc.

Every time the device changes state, the Host sends updated skin information to the Netop Guest. If the Netop Guest does not have the skin that is needed for a remote control session with a particular Host, it attempts to collect a suitable skin from the Skin Repository Server. If the necessary skin is not available, the Netop Guest uses a default skin.

You can configure Netop Mobile Host Guest Access Security to limit the remote control options of a connected Netop Guest.

See also

Sessions

Netop Mobile Host Manager

1.2 Other sessions

Netop Mobile offers these other session options:

- **File Transfer** enables the user of a computer running Netop Guest to transfer files and directories between the mobile device and the Netop Guest computer.
- **Chat** enables the user of a computer running Netop Guest to run a typed text based dialog with a user of the mobile device.
- **Request Help** enables the user of a mobile device or, on certain events, Netop Mobile Host to request help from a Netop Guest that offers help services. The Netop Guest user will typically respond by starting a remote control session.
- **Run Program** enables the user of a computer running Netop Guest to run a program that is installed on the mobile device.
- **Send Message** enables the user of a computer running Netop Guest to send a text message which will pop up on the mobile device display.
- **Get Inventory** enables the user of a computer running Netop Guest to collect available mobile device hardware and software information.
- **Netop Script** enables the user of a computer running Netop Guest to run a Netop script on the mobile device.
- **Remote Management** enables the user of a computer running Netop Guest to manage the Netop Mobile Host.

You can configure **Guest Access Security** on the Netop Mobile Host to limit other session options of a connected Netop Guest.

See also

Netop Mobile Host
Netop Mobile Host Manager
Sessions

1.3 Security

Netop Mobile security includes:

- **Guest Access Security**: You can configure the Netop Mobile 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 Mobile Host to use it to centrally authenticate and assign individual roles to connecting Netop Guests.
- **Logging**: You can configure the Netop Mobile Host to log selected Netop events locally, in Netop Security Management and by Window Messages.

Note
Netop Security Management belongs to the Netop Remote Control product family.

See also

Netop Mobile Host
Netop authentication
Netop Mobile Host Manager
Roles
Netop Security Server authentication

1.4 Operating systems

Netop Mobile currently supports these mobile device operating systems:

- Windows CE 4.2
- Windows CE 5
- Windows CE 6
- Windows Pocket PC 2003
- Windows Mobile 5
- Windows Mobile 6
- Windows Mobile 6.1
- Windows Mobile 6.5

1.5 Communication devices

Netop Mobile currently supports these communication devices:

- WebConnect
- TCP/IP (UDP)
- TCP/IP (TCP)

Note
Netop Mobile does not support modem communication or communication using WAP.

See also

Netop communication

2 Netop Mobile Host

The Netop Mobile Host enables the mobile device to be remote controlled and interacted with in other ways from a computer running Netop Guest.

A newly installed Netop Mobile Host will use the default configuration. If Netop Mobile Host 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. However, the Netop Mobile Host can also be run in stealth mode. The mobile device user will then have no access to the options. The user of a stealth mode Netop Mobile Host can request help by a help request hotkey.

2.1 First load

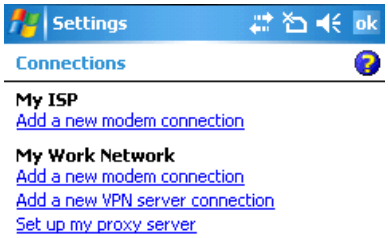
When the Netop Mobile Host has been installed, tap **Start > Programs > Netop Host** to open the **Netop Host** display license display:

In the **License Key** field, specify your Netop Mobile Host license number and tap **OK** to load the Netop Mobile Host and open the Netop Host display.

Before the mobile device can communicate via MS Connection Manager, you need to configure how it should connect. See Dial-up connection setup.

2.1.1 Dial-up connection setup

The dial-up feature of Netop Mobile uses the built-in Connection Manager to establish a dial-up connection. However, the Connection Manager also handles WIFI and VPN connections.



To display the Connection Manager, tap **Start** and select **Settings**. In **Settings**, choose the **Connections** tab and then tap the **Connections** icon.

Every Windows Mobile device uses two standard connections called **My ISP** and **My Work Network** by default.

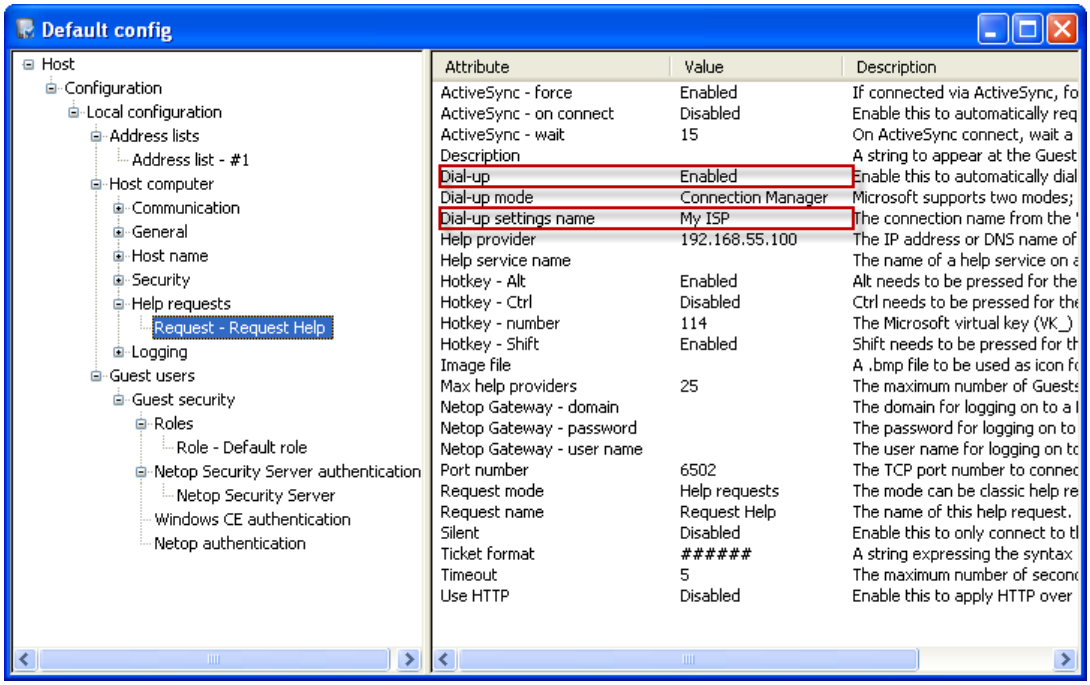
Each of these can be, in principle at least, any type of connection to an IP network – modem, WiFi, IR, Bluetooth or VPN. In practice, however, the **My ISP** usually connects to the Internet via a modem, WiFi, and so on, and the **My Work Network** is usually a VPN connection. The reason for this is that a VPN connection does not include any specification for a physical way of connecting to anything. It assumes that there is already a routable Internet connection to the VPN server that you specify and simply uses this to construct a secure "pipe" through the Internet to your private network.

To configure the "dial-up" connection, please refer to the documentation that came with your device or consult your ISP or Tech Support depending on whether you are setting up an Internet connection or a VPN connection.

Netop Mobile Host dial-up

In Netop Mobile Host Manager, configure the Mobile Host for dial-up.

The two settings framed in red below are the relevant settings.



Dial-up: If enabled, Netop Mobile will establish a network connection through the Connection Manager when using the issuing of a Help Request. If disabled, dial-up will be prohibited.

Dial-up settings name: Usually **My ISP** or **My Work Network**, but it can also be the name of a specific connection defined in the Connection Manager if you have defined multiple connections.

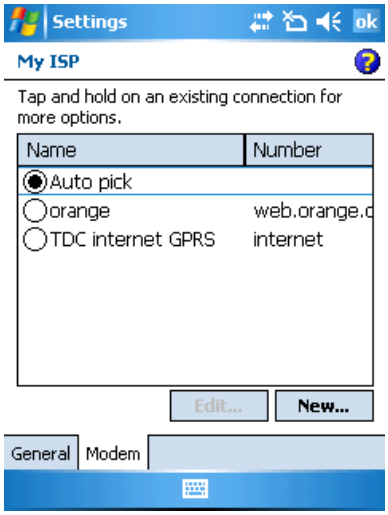
If **Dial-up** is enabled and **Dial-up settings name** is set to **My ISP** and you have a configuration like the one above, **TDC Internet GPRS** will always be used.

See also

Request help from a dial-up connected mobile device.

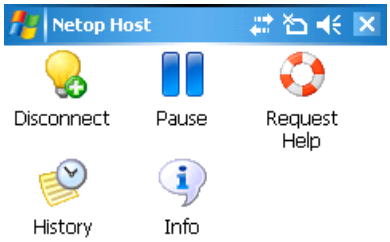
Change connection type

If you would like Netop Mobile to use another connection, set the dial-up setting **Name** to the preferred name, for example **orange**.



2.2 Netop Host display

This is the mobile device **Netop Host** display:



If the Netop Mobile 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. See Icons below.
- If the **General** branch **Startup** parameter **Load at Boot** attribute has been disabled in the Netop Mobile Host Manager.

  In these cases, tap **Start > Netop Host or Start > Programs > Netop Host** to display the **Netop Host** display.
- If the Netop Mobile Host has been configured to run in stealth mode. See Administrator options.

Icons

The **Netop Host Home** display contains the following icons:

 Running	The light bulb icon indicates the Host communication status. If Host communication is enabled, the bulb is yellow with the label **Running.** If Host communication is disabled, the bulb is gray with the label **Paused** or in transition **Opening** or **Closing**. If a Netop Guest is connected, the bulb is yellow with a green dot with a white **+** (plus) and the label **Connected**.
 Pause	Tap this icon to enable/disable Host communication. If Host communication is enabled, the icon shows two vertical blue bars and the label **Pause**. If Host communication is disabled, the icon shows a blue triangle pointing to the right and the label **Run**. **Note** Disabling Host communication will disconnect Netop Guest.
 Request Help	By default, one life belt icon with the label **Request Help** is displayed. If multiple help request options have been configured in the **Help request** parameters in the Netop Mobile Host Manager, multiple life belt icons with different labels will be displayed. Tap a life belt icon to request help. While connecting to the help provider Netop Guest, the label will be **Opening**. When the help request has been delivered, the life belt icon will display a red X and the label **Cancel Help**. Click this icon to cancel the help request. When the help provider Netop Guest connects in response to the help request, the life belt icon will become disabled. On disconnect, the help request icon will be enabled again. **See also** Request help from a Guest offering help Help requests
 History	Click the document and clock icon with the label **History** to see a list of Netop Guest **Connect** (lightning) and **Disconnect** (red X) events since the Netop Mobile Host was last started. Click **<-Home** at the top of the display or click the **Home** button on the menu bar to return to the **Home** display.
 Info	Click the information balloon icon with the label **Info** to display the name, IP address, regional settings language and possibly other details of the Netop Mobile Host. Click **<- Home** at the top of the display or click the **Home** button on the menu bar to return to the **Home** display. **Notes** The displayed Netop Mobile Host name and IP address will be enabled only if the Host communication status is Running or Connected.

Menu bar

This is the **Netop Host** display menu bar:

If the **History** or **Info** display is open, tap **Home** to return to the **Home** display.

Tap **Menu** to display the Host menu, which provides access to exiting and restarting the Host, viewing **About** information and tracing.

You must typically restart Netop Mobile Host to apply Netop Mobile Host Manager configuration changes.

Tapping the **Trace** command allows you to save a debug trace file named netophost.txt in the mobile device root directory. It is a plain text record of recent communication events that may be requested by Netop support to diagnose communication problems. Its interpretation requires Netop expertise.

See also

Netop Mobile Host Manager

2.3 Connectivity

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**: A standard configuration of the TCP/IP communication device.
- **TCP**: 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 Mobile Host directly or alternatively, the end user can request help to initiate a session with the Netop Guest.

Remote sessions can also be initiated and established through ActiveSync when the mobile device is docked.

See also

Netop Mobile Host Manager
Change the configuration using the configuration panel
Netop communication
Request help from a Guest offering help services

2.4 Request help from a Guest offering help services

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

- tapping the icon panel **Request Help** icon.
- keying the **Request** parameter specified hotkey.

The Netop Guest user will typically respond by starting a remote control session.

You can configure a **Request** parameter for these alternative functionalities:

- On ActiveSync connection to a desktop computer, Netop Mobile Host will request help from a specified Netop Guest help service to enable this Netop Guest only to connect.
- On ActiveSync connection to a desktop computer, Netop Mobile Host will connect to a specified Netop Gateway to enable different Netop Guests to connect to it.

Notes

Netop Gateway is a Netop Remote Control extended Host that can route communication between different communication profiles. See the Netop Remote Control Administrator's Guide, Netop Gateway.

Warning

Enabling multiple Guests to connect to Netop Mobile Host entails security hazards.

See also

Help requests
Sessions

2.5 Sessions

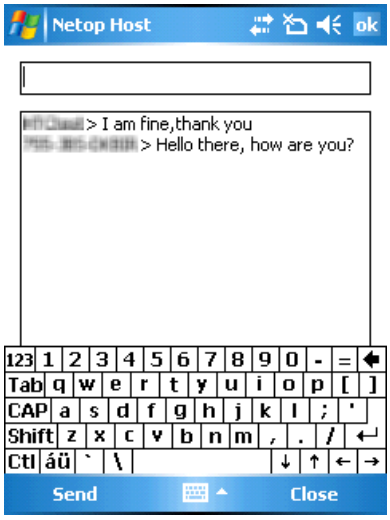
A Netop Guest can connect to the Netop Mobile Host to run the following types of sessions:

- **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 Mobile Host can control a remote control session only by configuring selected actions to be denied. See Roles.

- **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 Mobile Host can control a file transfer session only by configuring selected actions to be denied. See Roles.

- **Chat**: Will replace the **Netop Host** display with this **Chat** display:



In the field at the top, enter your chat contribution. Tap **Send** on the menu bar to send it.

The pane below the field at the top will display the chat dialog with later contributions above earlier contributions. Your contributions will be preceded by the Netop Mobile Host name. Netop Guest user contributions will be preceded by *root* if **System Authentication** is applied or by the Netop Guest name if **Netop Authentication** or **Security Server Authentication** is applied.

Tap **OK** on the title bar at the top or **Close** on the menu bar at the bottom to end the chat session and go to the **Home** display. The Netop Guest user can also end the chat session.

See also

Windows CE authentication
Netop authentication
Security server authentication

2.6 Actions

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 Mobile 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 Mobile 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.

See also

Roles

2.7 Administrator options

Administrators will typically install and configure Netop Mobile Hosts to ensure protection of organizational resources.

You can reconfigure Netop Mobile Host by creating a configuration .xml file in Netop Mobile Host Manager and install it on a mobile device connected by ActiveSync or copy it to the Netop Mobile Host files on the mobile device. To apply configuration changes, restart Netop Mobile Host from the **Restart** command of the **Netop Host** display **Menu**.

Windows mobile technology does not enable full configuration protection. To discourage configuration changes by the mobile device user, run Netop Mobile Host in stealth mode to disable displaying the **Netop Host** display.

To run Netop Mobile Host in stealth mode, add this key to the mobile device registry:

```
Local Device\HKEY_CURRENT_USER\Software\Netop\NetopHost\View\Stealth=1
```

Note
Windows mobile registry editor utilities are available for download from the Internet.

Modify Netop Mobile Host user interface text

You can modify Netop Mobile Host user interface text, typically translate it into another language, by adding stringtable files to the **Netop Host** directory of the mobile device.

Netop Mobile Host stringtable files specify modifications by contents in the following format:

```
<?xml version="1.0" encoding="utf-8"?>
<stringtable>
  <string hint="<Original string 1>" value="<New string 1>"/>
  <string hint="<Original string 2>" value="<New string 2>"/>



  .
  .
  <string hint="<Original string n>" value="<New string n>"/>
</stringtable>
```

`<Original string x>` represents an original string of characters.

`<New string x>` represents the modified string of characters.

Name a Netop Mobile Host stringtable file STHOST_<Language code>.XML using a Windows three- or two-letter language code, e.g. STHOST_GER.XML, to apply it by the regional settings of the mobile device which are indicated in the **Language** detail of the **Info** display.

Name a Netop Mobile Host stringtable file STHOSTCE.XML to apply it regardless of the regional settings of the mobile device.

Note
An applicable three-letter language code stringtable file will have priority over an applicable two-letter language code stringtable file which will have priority over a CE stringtable file.

Control Netop Mobile Host by WM_COPYDATA messages

The **Logging** branch **Logging to window messaging** parameter in the Netop Mobile Host Manager enables data exchange with other mobile device applications by WM_COPYDATA messages.

Note
WM_COPYDATA messages are explained in http://msdn.microsoft.com/en-us/library/ms649011(VS.85).aspx

This enables controlling the Netop Mobile Host user interface from the user interface of another mobile device application, e.g. your own mobile device application.

This is the COPYDATASTRUCT structure of Netop Mobile Host WM_COPYDATA messages:

```
typedef struct _ExtMess
{
  char pass[32]; (Max 31 UTF-8 characters that identify the message as a Netop
  Mobile Host WM_COPYDATA message - NULL terminated)
  int cmd; (4 bytes outgoing command or event number)
  char text[1]; (Unlimited number of optional encoding characters that provide
  arguments to the command or event - NULL terminated)
}
ExtMess;
```

Note
To enable Netop Mobile Host to exchange WM_COPYDATA messages, you must set up the **Logging** branch **Log to window messaging** parameter in the Netop Mobile Host Manager.

You can send WM_COPYDATA messages to Netop Mobile Host to execute these commands:

Number	Command	Effect
0	WP_TEST	The Netop Mobile Host will return a ChatMessage event if this command is received successfully.
1	WP_EXIT	Exit the Netop Mobile Host as specified in a command argument (no argument: immediately).
2	WP_EXIT_NOW	Exit the Netop Mobile Host immediately.
3	WP_EXIT_ON_IDLE	Exit the Netop Mobile Host when unconnected.
4	WP_PAUSE	Disable Netop Mobile Host communication.
5	WP_START	Enable Netop Mobile Host communication.
6	WP_RESTART	Disable and enable Netop Mobile Host communication.
7	WP_SEND_CHATMSG	Send the chat contribution specified in a command argument from the Netop Mobile Host.

8	WP_HIDE	Hide the Netop Mobile Host user interface.
9	WP_SHOW	Display the Netop Mobile Host user interface if hidden.
10	WP_REQUEST_HELP	Request help from the Netop Mobile Host.
11	WP_CANCEL_HELP	Cancel a pending Netop Mobile Host help request.

Example

This code example is provided without guarantee or support to assist you in creating your own code:

```
void CDialogSubclass::OnBnClickedButtonSend()
{
  HWND hWnd = ::FindWindow(NULL, L"NetopHost");
  COPYDATASTRUCT copydata;
  ExtMess *extmess;
  BOOL used;
  int n;
  if (!hWnd)
  {
    AfxMessageBox(L"No NetopHost running");
    return;
  }
  UpdateData(TRUE);
  n = 256; (32 bytes pass, 4 bytes command, 220 bytes left for text)
  extmess = (ExtMess*)malloc(n);
  if (!extmess)
  {
    AfxMessageBox(L"Out of memory");
    return;
  }
  memset(extmess, 0, n);
```

This code fills in the CMD field with the selection from the combo box:

```
  DWORD wparam = m_combo_cmd_ctrl.GetCurSel();
  extmess->cmd = wparam;
```

This code converts the text from the upper edit field to ANSI and sends it as pass:

```
  WideCharToMultiByte(CP_ACP, 0, m_edit_pass.GetBuffer(1), -1, extmess-
  >pass, 32, "?", &used);
```

This code converts the text from the lower edit field to ANSI and sends it as text:

```
  WideCharToMultiByte(CP_ACP, 0, m_edit_txt.GetBuffer(1), -1, extmess-
  >text, 220, "?", &used);
```

This code fills in the COPYDATASTRUCT and sends the command to the Netop Mobile Host. The same value is also stored in the ((ExtMess*)copydata.lpData)->cmd member:

```
  copydata.dwData = wparam;
  copydata.cbData = n;
  copydata.lpData = extmess;
  ::SendMessage(hWnd, WM_COPYDATA, (WPARAM)this->m_hWnd, (LPARAM)©data);
  free(extmess);
}
```

Netop Mobile Host

Netop Mobile Host can detect these events and return WM_COPYDATA messages about them:

Number	Event	Explanation
145	Starthost	The Netop Mobile Host enabled communication.
146	Stophost	The Netop Mobile Host disabled communication.
147	RequestHelp	The Netop Mobile Host requested help.
148	CancelHelp	The Netop Mobile Host canceled a pending help request.
149	StartSession	A session with the Netop Mobile Host was started.
150	StopSession	A session with the Netop Mobile Host was stopped.
151	PasswordRejected	The Netop Mobile Host rejected a wrong Guest access password.
152	LoginRejected	The Netop Mobile Host rejected a Guest logon attempt.
153	ConfirmAccessDenied	The Netop Mobile Host denied Guest access.
154	HostTimeout	A Guest connect attempt to the Netop Mobile Host timed out.
155	StartRc	A remote control session with the Netop Mobile Host started.
156	StopRc	A remote control session with the Netop Mobile Host stopped.
157	StartChat	A chat session with the Netop Mobile Host started.
158	StopChat	A chat session with the Netop Mobile Host stopped.
159	StartNfm	A file transfer session with the Netop Mobile Host started.
160	StopNfm	A file transfer session with the Netop Mobile Host stopped.
161	SendFile	A file transfer session sent a file to the Netop Mobile Host.
162	RecvFile	A file transfer session received a file from the Netop Mobile Host.
185	RequestHelpPending	A Netop Mobile Host help request was acknowledged.
186	RequestHelpNoConnect	A Netop Mobile Host help request did not connect to any help provider.
187	RequestHelpNoAnswer	A Netop Mobile Host help request help connected to a help provider that did not acknowledge.
188	ChatMessage	The Netop Mobile Host received or sent a chat message specified in an argument.
189	Message_Displayed	The Netop Mobile Host displayed a Netop message specified in an argument.
190	Inventory_Delivered	The Netop Mobile Host delivered its inventory to a Guest.

Example

This code example is provided without guarantee or support to assist you in creating your own code:

```
LRESULT CDialogSubclass::WindowProc(UINT message, WPARAM wParam, LPARAM
lParam)
{
  switch(message)
  {
    case WM_COPYDATA:
    {
    COPYDATASTRUCT *pcds = (COPYDATASTRUCT*)lParam;
    ExtMess* extmess = pcds ? (ExtMess*)pcds->lpData : NULL;
    bool passok = false;
    char *text = NULL;
    if (!extmess)
    {
      m_list_in_ctrl.InsertString(0, L"NULL message");
    }
    else
    {
      char ctxt[256];
      WCHAR wtxt[256];
```

This code is not a strong password check but only a filter for mistakes if `(!strcmp (extmess->pass, "mypass"))`:

```
      {
        passok = true;
      }
```

This code is a very simple buffer overflow guard which assumes that the rest takes max. 64 bytes of `ctxt`:

```
      text = extmess->text;
      if (strlen(text) > 256 - 64) text = "overflow";
      sprintf(ctxt, "%s %d %s %s", passok ? "Ok": "!!", extmess->cmd,
      extmess->pass, extmess->text);
      MultiByteToWideChar(CP_ACP, 0, ctxt, -1, wtxt, 256);
      m_list_in_ctrl.InsertString(0, wtxt);
      }
    }
    return TRUE;
    default: break;
  }
  return CDialog::WindowProc(message, wParam, lParam);
}
```

Note

Example C++ code for Windows Mobile 5 is included in the exevent2.zip file which is included with Netop Mobile Host installation files.

See also

Netop Mobile Host Manager
Sessions
Actions

3 Netop Mobile Host Manager

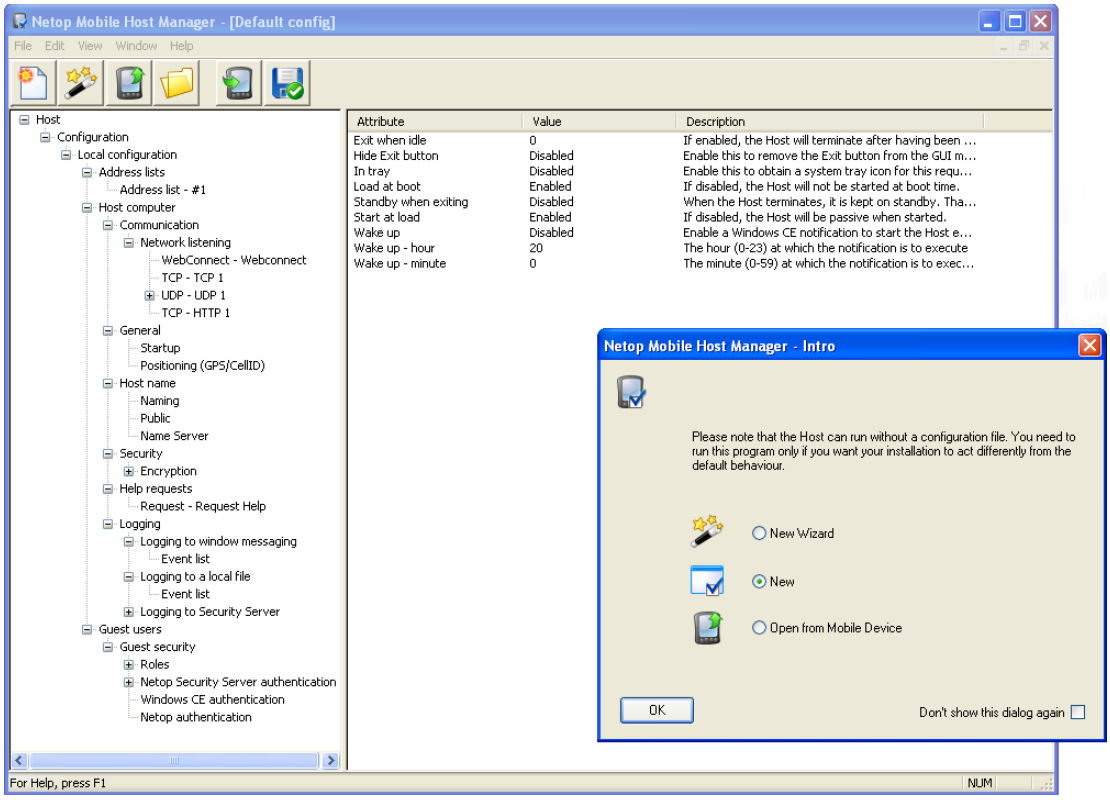
A newly installed Netop Mobile Host will use the default configuration.

You can customize the configuration from Netop Mobile Host Manager on a desktop computer. You can install a customized configuration by connecting the mobile device to the desktop computer by Microsoft ActiveSync. Alternatively, you can copy the netophost.xml file created by Netop Mobile Host Manager to the **Netop Host** directory of the mobile device.

Note

To apply configuration changes, you must restart the Netop Mobile Host.

On the desktop computer, click **Start > All Programs > Netop Mobile Host Manager** to load Netop Mobile Host Manager and display the **Intro** window on top.



If you do not want to see the **Intro** window again, you can hide it using the **Intro** command 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 Mobile Host on a mobile device connected to the desktop computer by ActiveSync in the configuration panel of the **Netop Mobile Host Manager** window.

Don't show this dialog again: Select this check box to not display the **Intro** window when loading Netop Mobile Host Manager on the computer the next time. You can reverse this selection from the **Intro** command on the **View** menu.

Note

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

See also

Menu bar
Toolbar
Change the configuration using the configuration wizard
Change the configuration using the configuration panel

3.1 Menu bar

The **Netop Mobile Host Manager** window 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.

See also

Toolbar
Configuration panel
Change the configuration using the configuration wizard
Change the configuration using the configuration panel

3.2 Toolbar

The **Netop Mobile Host Manager** window toolbar contains the following buttons:

	**Create a new default configuration**: Click this button to open the **Default Configuration** window the configuration panel or make it the active window if already open. Alternatively, select the **New** command on the **File** menu or press CTRL+N.
	**Create a new configuration using a wizard dialog**: Click this button to display the configuration wizard. Alternatively, select the **New Wizard** command on the **File** menu or press CTRL+W.

	**Open the configuration in effect on the mobile device**: Click this button to open a **Mobile Device** window in the configuration panel, if a mobile device using a customized Netop Mobile Host configuration is connected to the desktop computer by ActiveSync. Alternatively, select the **Open from Mobile Device** command on the **File** menu.
	**Open a configuration from an existing local disk file**: Click this button to open a customized configuration file (.xml) in the configuration panel. Alternatively, select the **Open** command on the **File** menu or press CTRL+O.
	**Make the configuration effective on the mobile device**: 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. Alternatively, select the **Save to Mobile Device** command on the **File** menu.
	**Save the active configuration to a file with a new name**: 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. Alternatively, select the **Save** command on the **File** menu or press CTRL+S. Otherwise select the **Save As** command on the **File** menu to save with a specified file name in a selected desktop computer directory.

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

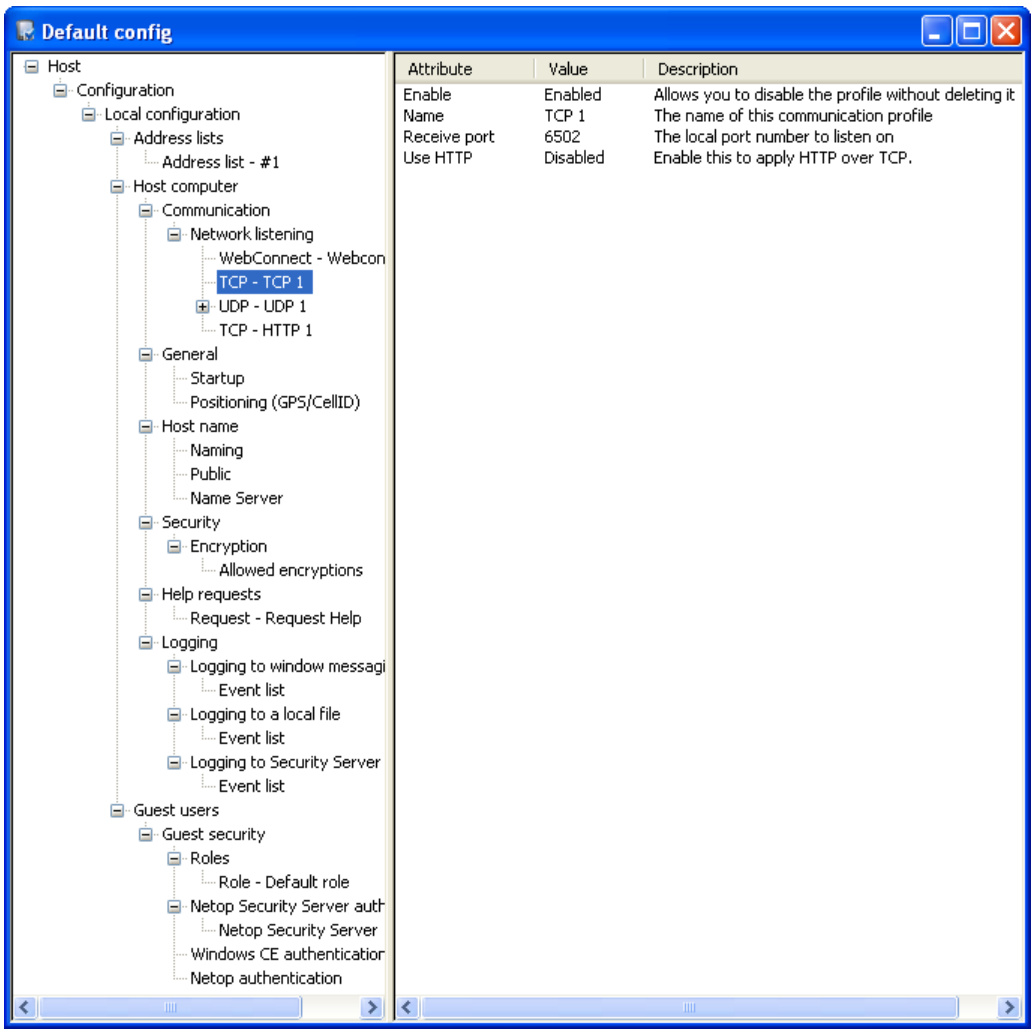
See also

Menu bar
Configuration panel
Change the configuration using the configuration wizard

3.3 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:



Address lists branch

Use the Address lists branch parameters to create address lists and specify computer addresses.

Note

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

Host computer branch

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.

Guest users branch

The **Guest users** branch contains all authentication parameters used when a Guest logs on to the Host.

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.

See also

Menu bar
Toolbar
Change the configuration using the configuration panel

3.3.1 Netop communication

Netop modules 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 Mobile 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.

See also

Netop Remote Control User's Guide

Netop WebConnect Installation Guide

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.

See also

Help requests

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.

See also

Help requests

3.3.2 Security (Host computer)

The **Security** branch specifies Host protection configuration.

Netop Mobile 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.

Netop 6.x/5.x 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.
No encryption	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.
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
Keyboard	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.
Data integrity and keyboard	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.
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.
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.

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**.

3.3.3 Help requests

The **Help requests** branch specifies Host help request configurations.

You can configure **Request** parameters to:

- **Request help from a network connected mobile device**

  Configure the following attributes:

  - **Help provider**
  - **Port number** (Send Port)
  - **Request mode**
  - **Description** (optional)

Request help from an ActiveSync connected mobile device

Configure 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

Configure 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

Configure 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, configure the following attributes:

- **Netop Gateway - user name**
- **Netop Gateway - password**
- **Netop Gateway - domain**

To enable help request by a hotkey (keystroke combination), configure these attributes:

- **Hotkey - Alt**
- **Hotkey - Ctrl**
- **Hotkey - Shift**
- **Hotkey - number**

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

To limit the search for help provider Netop Guests, configure the following attributes:

- **Max help providers**
- **Timeout** (Seconds)

To encapsulate a help request in HTTP to facilitate firewall passage, configure these attributes:

- **Use HTTP** (Enabled)
- **Port number** (80)

To request help when a mobile device becomes connected by ActiveSync, configure this attribute:

- **ActiveSync - on connect** (Enabled)

3.3.4 Roles

The **Roles** branch specifies the Host role configuration. It expands into one **Role** parameter.

Netop Mobile 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.

3.3.5 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.

See also

Roles

3.3.6 Windows CE authentication

The **Windows CE authentication** parameter has no attributes. It uses the mobile device's system password.

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

See also

Roles

3.3.7 Netop Security Server authentication

The **Netop Security Server Authentication** branch specifies the Host Security Server authentication configuration.

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

Netop Mobile 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 Mobile 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.

See also

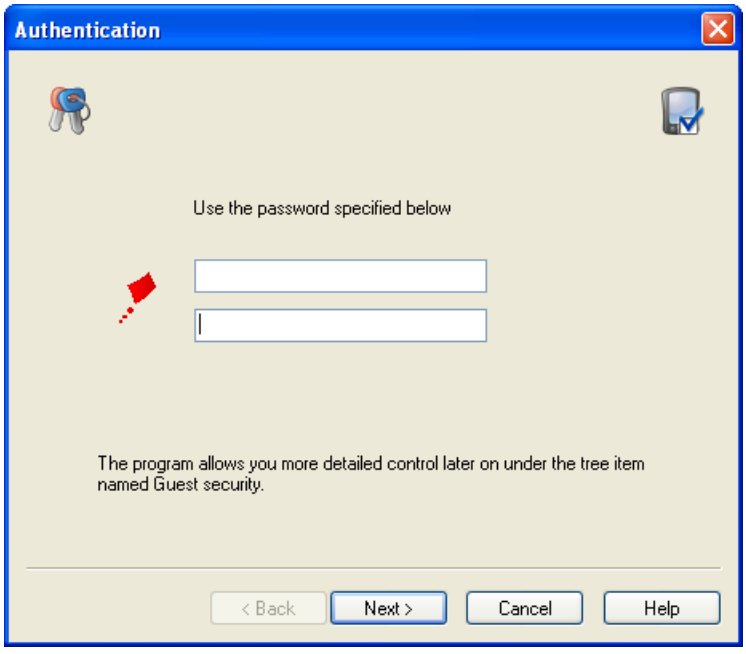
Roles

3.4 Change the 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 the **New Wizard** option 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, select the **New Wizard** command on the **File** menu, or press CTRL+W.



The **Authentication** page allows you to configure a Guest Access Security password.

Use the password specified below: Request the password specified in the fields below from connecting Netop Guests. 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** to display this window:

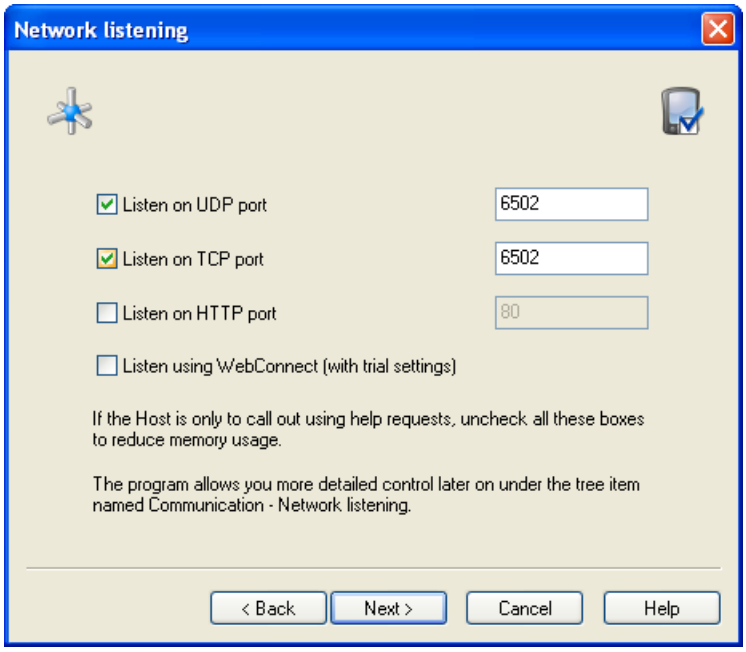
The **Authorization** page allows you to configure the role that will initially apply to connecting Netop Guests.

Select one of these options:

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** to display this window:



The **Network Listening** page allows you to configure communication profiles by which to communicate with the Netop Guest.

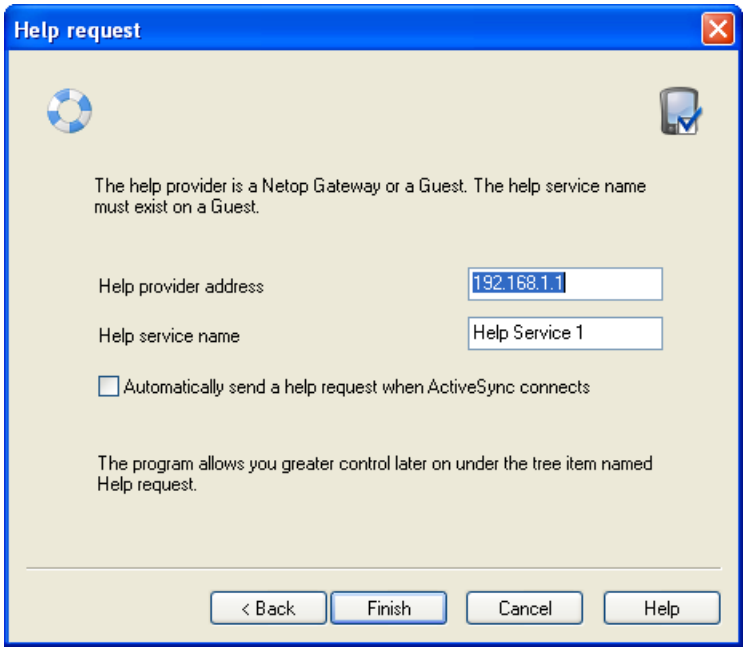
Listen on UDP port: Leave this check box selected to enable a communication profile that uses the TCP/IP communication device with the receive port number specified in the field (default: selected, 6502).

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** to display this window:



The **Help Request** page allows you to 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: 192.186.1.1).

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).

Click **Back** to return to previous configuration wizard pages to change your specifications.

Click **Finish** to end the configuration wizard and display a NetopHost1 configuration window according to your specifications in the configuration panel of the **Netop Mobile Host Manager** window.

See also
Roles
Help requests
Windows CE authentication
Netop authentication
Netop communication

3.5 Change the configuration using the configuration panel

Netop Mobile Host Manager includes a basic configuration named Default config. You can view its parameters in the **Default config** window using the **New** command on the **File** menu or the **Create a new default configuration** button on the toolbar.

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. The **OK** button will be enabled if the specification in the active element in the window is valid.
3. Click the **OK** button to confirm the change and close the attribute window.

See also

Configuration panel
Toolbar

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

V

W