



NETOP®

RemoteControl

Secure Remote Management and Support

31 March 2017

Copyright© 1981-2017 Netop Business Solutions A/S. All Rights Reserved.
Portions used under license from third parties.
Please send any comments to:

Netop Business Solutions A/S
Bregnerodvej 127
DK-3460 Birkerød
Denmark
E-mail: info@netop.com
Internet: www.netop.com

Netop™ is a trademark of Netop Business Solutions A/S. All other products mentioned in this document are trademarks of their respective manufacturers. Netop Business Solutions A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice. Netop Business Solutions A/S retains the copyright to this document.

The document is optimized for double-sided printing.

Contents

1 Overview	4
1.1 Remote Control modules	4
1.2 Security	4
1.3 Communication profiles	5
2 Managing Hosts	6
2.1 Start and end a remote control session	6
2.2 Use Netop phonebook to manage connections	7
2.2.1 Edit phonebook records	8
2.2.2 Protect your phonebook record files with a password	9
2.2.3 Organize your phonebook	9
2.2.4 Export and import phonebook data	10
2.2.5 Add a phonebook reference	11
2.2.6 Use Remote Desktop from the Netop phonebook	11
2.3 Keyboard, mouse and display during remote control	11
2.4 Generate a Host inventory	12
2.4.1 Process Host computer inventory information	12
2.5 Monitor Hosts	13
2.6 Execute system control commands on a Host computer	14
2.7 Perform Remote Management tasks	15
2.7.1 Management pane	15
2.7.2 Disk Drives	16
2.7.3 Event Viewer	16
2.7.4 Task Manager	17
2.7.5 Registry	17
2.7.6 Services	17
2.7.7 Shared Folders	19
2.7.8 Inventory	20
2.7.9 Command Console	20
2.7.10 System Control	20
2.7.11 Local Users and Groups	20
2.7.12 Integrate third party applications	22
2.7.13 Netop Sessions	23
2.8 Create and run a script	24
2.9 Use Intel vPro from Netop Remote Control	26
2.9.1 Log on to the vPro Console	27
2.9.2 vPro Console	29
2.10 Tunnel	33
2.10.1 Predefine local ports for the tunnel	34
2.10.2 Open tunnel session	34
2.11 Run a remote program	35
2.12 Transfer files	36
2.13 Log events	38
2.14 Record sessions	39
2.14.1 Play back session recordings	39
2.15 Use a skin to see the Host button layout	40

2.16	Multisession Support	40
3	Getting remote support	41
3.1	Request help	41
3.2	Notification	41
3.3	Communicate with Guest users	42
3.4	End a remote control session from a Host computer	43
4	Providing remote support	44
4.1	Set up Help Request on Guest and Host	44
4.2	Respond to a help request	46
4.3	Run a multi Guest session	46
4.4	Send special keystrokes	47
4.5	Use clipboard commands	48
4.6	Communicate with Host users	49
4.7	Send or receive print jobs	50
4.7.1	Redirect a print job	51
4.8	Share your screen	51
4.9	Netop Screen Video	52
4.10	Netop Marker Utility	53
5	Dialog box help	55
5.1	Guest dialog boxes	55
5.1.1	Advanced audio settings	55
5.1.2	Advanced Help Service	55
5.1.3	Advanced inventory option	56
5.1.4	Advanced TCP/IP Configuration	57
5.1.5	Advanced Video	58
5.1.6	Communication Profile Edit	59
5.1.7	Communication Profile Setup	65
5.1.8	Connect to Host	65
5.1.8.1	Connection Properties	66
5.1.9	Inventory	75
5.1.10	Name Not Found	76
5.1.11	Custom Inventory Items	77
5.1.12	Global Settings	77
5.1.13	IP Broadcast List	79
5.1.14	Log Setup	80
5.1.14.1	Available Netop log event codes and arguments - Guest	84
5.1.14.2	Available Netop log event codes and arguments - Host	87
5.1.15	Netop File Manager Options	94
5.1.16	Modem	97
5.1.17	Modem Configuration	98
5.1.18	Novell Network Numbers	98
5.1.19	Program Options	99
5.1.20	Run	112
5.1.21	Script	112
5.1.22	Send Message	114
5.2	Host dialog boxes	115
5.2.1	Advanced Help Request Options	115

5.2.2	Allowed ISDN Numbers	115
5.2.3	Directory Service	116
5.2.4	Guest Access Security	117
5.2.5	Guest Profile	125
5.2.6	Help Providers	126
5.2.7	Help Request	126
5.2.8	Maintenance Password	127
5.2.9	Program Options	128
5.2.10	Select Directory Services Users or Groups	137
Index	138

1 Overview

1.1 Remote Control modules

Netop Remote Control comprises the following modules:

- **Netop Guest:** Enables the computer user to remote control and interact with another computer running a Netop Host or extended Host.
- **Netop Host:** Enables the computer to be remote controlled and interacted with from a computer running a Netop Guest.
- **Netop WebConnect:** A secure web-based service consisting of a Connection Manager that serves as a meeting hub for Netop Guests and Hosts, and at least one Connection Server that routes the traffic between Guests and Hosts. The Connection Server is an extended Host. This is available as a hosted service or as an on-premise application.
- **Netop WebConnect 3:** A secure web-based service consisting of a Connection Manager that serves as a meeting hub for Netop Guests and Hosts, and at least one Connection Server that routes the traffic between Guests and Hosts. The Connection Server is an extended Host. This is available as a hosted service or as an on-premise application. WebConnect 3.0 has improved security.
- **Netop Portal:** A browser-based interface allowing the users to manage Guest authentication and authorization, view connected devices and do remote sessions using a lightweight support console which does not require any kind of installation.
- **Netop Browser Based Support Console:** A browser based interface for the Guest, allowing the supporters to remote control devices, no install required.
- **Netop Security Server:** An extended Host that uses a central database to manage Guest authentication and authorization across the network. It also provides centralized logging capabilities and extended authentication methods including RSA.
- **Netop Gateway:** An extended Host that can route Netop traffic between different communication devices. Netop Gateway can receive Netop communication that uses one communication device and send it using another communication device. This ability enables Netop Gateway to provide communication between Netop modules that use mutually incompatible communication devices, typically to connect Netop modules inside a network or terminal server environment with Netop modules outside a network or terminal server environment.
- **Netop Name Server:** An extended Host that can connect Netop modules across segmented networks. Netop Name Server resolves Netop names into IP addresses, which can be used for connecting across any TCP/IP network including the Internet.

See also

The Netop Remote Control Administrator's Guide for further information about the Security Server, the Gateway and the Name Server.

The Netop WebConnect Installation Guide for further information about the WebConnect Connection Server.

1.2 Security

You can prevent changes to the installed Netop Remote Control modules by using a maintenance password and even hide the Host module from the end user via the stealth mode feature.

- The **Guest Access Security** functions of the Host can protect against unauthorized access and limit the actions available to the Guest:
 - Upon connection to the Host, the Guest can be authenticated against their Windows logon credentials.
 - Security roles can be defined on the Host which dictate what remote control actions the authenticated Guest can perform.

- The policy functions can determine how the Host behaves before, during and after the remote control session, including notification, confirm access and illegal connection attempts.
- The communication between Netop modules can be encrypted using different methods depending on the environment.
- Audit trails including all remote control events and physical session recordings can be centrally maintained.
- All Netop Remote Control modules can log Netop events locally and centrally in a Netop log.
- You can protect the Guest and Host setup with a maintenance password.

See also

[Guest Access Security](#)

[Program Options](#) (Encryption tab and Smart Card tab)

Administrator's Guide

1.3 Communication profiles

For Netop modules to be able to communicate with each other, you need to define a communication profile. A communication profile is a specific configuration of a communication device.

A communication device is a Netop adaptation of a generally available communication protocol or a Netop proprietary communication protocol.

A newly installed Netop module includes default communication profiles. You typically need to modify the default communication profiles or create communication profiles to optimize communication in your environment.

NOTE: Communication profiles are stored in the Netop configuration file (`comprof.ndb`), which is typically located in the folder `C:\Documents and Settings\\Application Data\Netop\Netop Remote Control\`. For more information about Netop configuration files, see the [Netop Knowledgebase](#).

See also

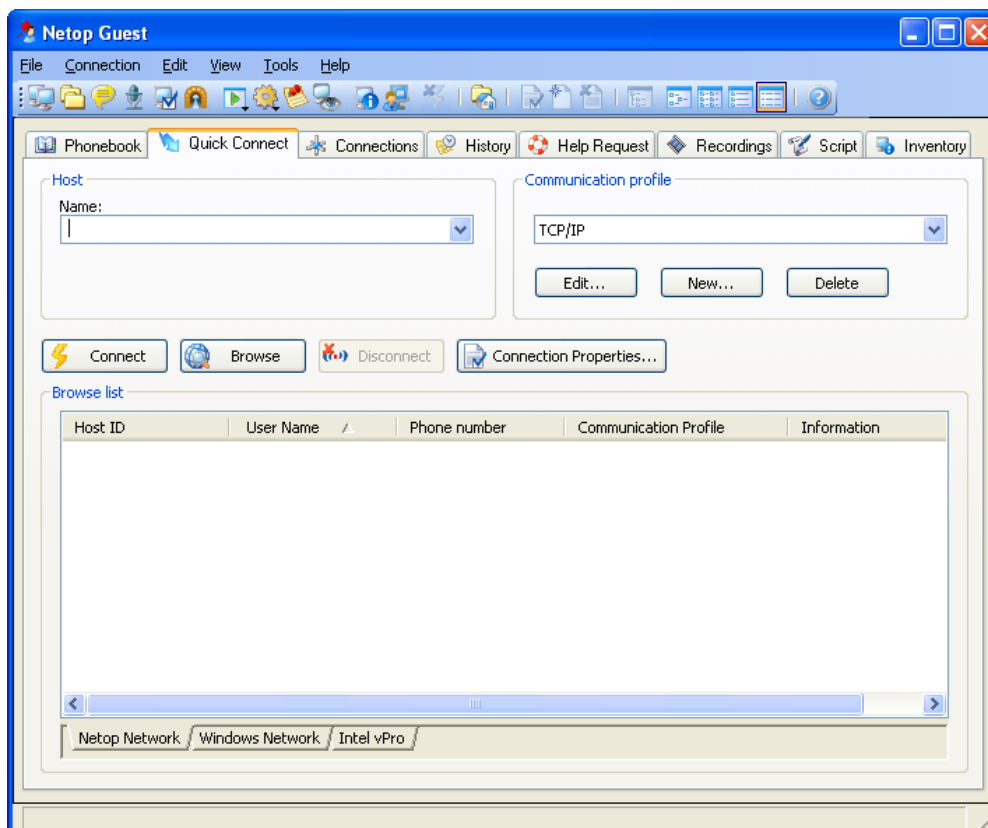
[Communication Profiles](#)

2 Managing Hosts

2.1 Start and end a remote control session

You can connect and start a remote control session in several ways.

Before starting a remote control session, specify a communication profile corresponding to a communication profile (default is TCP/IP = UDP) enabled on the Host in the **Communication Profile** section of the **Quick Connect** tab.



Start a remote control session from the Guest window Quick Connect tab

1. On the **Quick Connect** tab, in the **Host** section, specify a Host name or address as required by the selected communication profile.
2. Click the **Connect** button to connect and start a remote control session.

Alternatively, click a toolbar button or select a command on the **Connection** menu to connect and start a session.

Typically, a Netop logon window is displayed prompting you to log on to the Host.

3. Type your credentials to log on.

When you have logged on to the Host, the session starts.

Connections will be displayed on the **Connections** tab. You can change session type or execute action commands by right-clicking a Host on the **Connections** tab.

Other ways to connect from the Quick Connect tab

1. Click the **Browse** button (Applies only when using profiles that use UDP and WebConnect).
2. Select one or multiple Hosts in the **Browse list** (**Netop Network** tab).
3. Click the **Connect** button.

Alternatively, click a toolbar button or select a command on the **Connection** menu to connect and start a session.

Typically, a Netop logon window is displayed prompting you to log on to the Host.

4. Type your credentials to log on.

When you have logged on to the Host, the session starts.

or

1. Click the **Windows Network** tab at the bottom of the window.
2. In the **Windows Network list** navigate to and select one or multiple Hosts.
3. Click the **Connect** button.

Alternatively, click a toolbar button or select a command on the **Connection** menu to connect and start a session.

Typically, a Netop logon window is displayed prompting you to log on to the Host.

4. Type your credentials to log on.

When you have logged on to the Host, the session starts.

Start a remote control session from other Guest window tabs

1. On the **Phonebook** tab, **History** tab, or **Help Request** tab, select one or multiple Hosts.
2. Click a toolbar button or select a command on the **Connection** menu to connect and start a session.

Typically, a Netop logon window is displayed prompting you to log on to the Host.

3. Type your credentials to log on.


When you have logged on to the Host, the session starts.

Phonebook	Stores Host records that you have created or saved from the Quick Connect tab or History tab.
History	Stores records of previous Host connections.
Help Request	Displays a list of pending Host help requests.

See also

[Save connection information in the phonebook](#)

End a remote control session

- In the **Remote Control** window of the Guest, click the  **Disconnect** button on the toolbar.

Alternatively, click the  **Remote Control** button on the toolbar.

or

- In the **Guest** window, select the connection on the **Connections** tab.

Click the **Disconnect** button on the toolbar.

Alternatively, select **Disconnect** on the **Connection** menu.

The Host user can also end the session by selecting **Disconnect** on the **Session** menu.

2.2 Use Netop phonebook to manage connections

You can save connection information as records in the Netop phonebook for later use.

The phonebook works much like a personal quick-dial telephone directory with the communication

profile needed to connect and passwords.

Passwords will be encrypted by a secure algorithm.

Phonebook records are saved as files with the extension `dwc` in `C:\Documents and Settings\\Application Data\Netop\Netop Remote Control\Guest\PhBook`. The `dwc` files are `xml` format files whose contents can be viewed in any text editor.

From the Quick Connect tab

1. You can add connection information to the phonebook by right-clicking a Host record in the pane in lower part of the **Guest** window and selecting **Add to Phonebook** after having browsed for Hosts.
2. In the displayed dialog box select the phonebook folder in which you want to save the information and click **OK**.

or

1. You can copy connection information to the phonebook by right-clicking a Host record in the pane in the lower part of the **Guest** window and selecting **Copy** after having browsed for Hosts.
2. Click the **Phonebook** tab, right-click the folder in the left pane in which you want to save the information, and select **Paste**.

The Host record will be displayed in the right pane of the **Phonebook** tab.


From the History tab

1. You can add connection information to the phonebook by right-clicking a Host record in the right pane of the **History** tab and selecting **Copy**.
2. Click the **Phonebook** tab, right-click the folder in the left pane in which you want to save the information, and select **Paste**.

The Host record will be displayed in the right pane of the **Phonebook** tab.

Create phonebook records on the Phonebook tab

To create a phonebook record from scratch

1. Click the  **Phonebook Entry** button on the toolbar.
Alternatively, select **New > Phonebook Entry** on the **Edit** menu.
The **Connection Properties** dialog box is displayed.
2. Fill in the fields in **Connection Properties** with the necessary information and click **OK**.


See also

[Connection Properties](#)
[Start and end a remote control session](#)

2.2.1 Edit phonebook records

If you want to edit a phonebook record and change information such as the specified communication profile or the Host credentials, you can do that in **Connection Properties**.

To edit a phonebook record

1. Select the phonebook record in the right pane of the **Phonebook** tab.
2. Click the  **Connection Properties** button on the toolbar.

Alternatively, select **Connection Properties** on the **Edit** menu.

The **Connection Properties** dialog box is displayed.

3. Edit the information and click **OK**.

You can move phonebook records between the **Phonebook** root folder and user-created folders using drag-and-drop.

See also

[Connection Properties](#)

2.2.2 Protect your phonebook record files with a password

To protect your phonebook record files (`dwc`), you can specify a password for each file in **Connection Properties**. This is useful, for example, if the file is part of a shared company phonebook and will be used by everyone in your company.

You can specify that the password should be entered every time someone wants to use or edit the file, or you can specify that the password should be entered only to edit the file.

To specify a password for a phonebook record file

1. Select the phonebook record in the right pane of the **Phonebook** tab.

2. Click the  **Connection Properties** button on the toolbar.

3. Click the **Protect Item** tab.

4. Specify a password and confirm it.

If you want the password *only* to apply to editing, select the **Connect without password** check box.

5. Click **OK**.

See also

[Connection Properties](#)

2.2.3 Organize your phonebook

You can create new folders in the phonebook to organize your connection information and make it easier to find the Host that you want to connect to.

For example, create folders and name them according to departments in your company.

To create a new folder

1. On the **Edit** menu, select **New > Folder**.

2. Enter a name for the folder

3. Click **OK**.

Alternatively, right-click and create a folder using the shortcut menu.

To create a new subfolder

1. In the left pane, select the folder in which you want to create a subfolder.

2. On the **Edit** menu, select **New > Folder**.

3. Enter a name for the folder

4. Click **OK**.

Alternatively, right-click the folder in which you want to create a subfolder, and create a folder using the shortcut menu.

You can use drag-and-drop to rearrange your folders.

2.2.4 Export and import phonebook data

You can export and import phonebook data in a comma separated values (`csv`) file. This is useful for example if you want to copy phonebook data from one computer to another.

You can also populate the phonebook using existing data from another system, for example by importing data from Active Directory.

Scripts can use the phonebook data to call Hosts.

Export phonebook data

1. Select a folder in the left pane of the **Phonebook** tab or select one or multiple phonebook records in the right pane.
2. On the **File** menu, select **Export**.
3. In the displayed dialog box, specify the path to and name of the `csv` file that you want to save the phonebook records to.

If you specify only a file name, the export file will be saved to the folder in which the Netop Guest is installed.

4. Select the **Export Passwords** check box if you want to include passwords for the phonebook records in the `csv` file.
5. Click **OK**.

You cannot export all **Connection Properties** properties for a phonebook record. This applies to the properties on the **Display** tab, the **Keyboard/Mouse** tab, the **Compression/Encryption** tab, the **Desktop** tab, and the **Record** tab, but you can specify these properties when importing.


Csv file syntax

The `csv` file is a plain text file. For each phonebook record, the file contains a line of values separated by commas according to this syntax:

```
<Folder path>,<Description>,<Phone number>,<Name>,<Comment>,<Communication profile>,<Host logon name>,<Host logon password>,<Host logon domain>,<Gateway logon name>,<Gateway logon password>,<Gateway logon domain>,<Protect item password>,<Wake on LAN MAC address>,<Logon credentials flags>,<Custom application description>,<Custom application command line>
```

Passwords will be encrypted as 64-digit hexadecimal checksums with the prefix `ENCRYPTED:`.

Import phonebook data

1. On the **File** menu, select **Import to Phonebook**.
2. Specify the path to and name of the `csv` file that you want to import.
3. Click the  **Connection Properties** button if you want to specify **Display** tab properties, **Keyboard/Mouse** tab properties, **Compression/Encryption** tab properties, **Desktop** tab properties, and **Record** tab properties.
4. Click **OK**.

2.2.5 Add a phonebook reference

You can add a phonebook reference in the Guest phonebook. A phonebook reference will link to a folder containing phonebook records (`dwc` files), for instance a phonebook shared by multiple users.

To add a phonebook reference

1. Right-click in the left pane of the **Phonebook** tab and select **Add Phonebook reference**.
2. In the **Add Phonebook Reference** dialog box, specify the folder containing phonebook records that you want to link to.

You can browse for the folder by clicking the button next to the **Folder** field.

3. Click **OK**.

A phonebook reference to a folder containing phonebook records will be displayed in the left pane of the **Phonebook** tab, and the records will be displayed in the right pane.

You can edit the phonebook reference by right-clicking the reference and selecting **Edit Phonebook reference**.

2.2.6 Use Remote Desktop from the Netop phonebook

The Netop phonebook provides access to using Remote Desktop functionality. This means that you can use one tool for all your remote control sessions.

For information about configuration of RDP (Remote Desktop Protocol), please see Microsoft documentation.

To create a Remote Desktop entry in the phonebook

1. Right-click the right pane of the **Phonebook** tab and select **New > Remote Desktop Entry**. The **Remote Desktop Connection** dialog box opens.
2. On the **General** tab, specify logon settings and a `.rdp` file to be used for the entry.


A Remote Desktop entry will be created and displayed in the records pane of the **Phonebook** tab together with a pseudo communication profile.


Use the Remote Desktop phonebook entry you created to start a remote desktop session.

For information about the use of Remote Desktop, click the **Help** button in the **Remote Desktop Connection** dialog box.

2.3 Keyboard, mouse and display during remote control

By default the Guest and the Host share the keyboard and mouse control during remote control.

If allowed by the **Guest Access Security** settings on the Host, you can block the Host user from using the keyboard and mouse. To do so, click the  **Lock Keyboard and Mouse** button on the toolbar in the **Remote Control** window.

You can also blank the Host screen, if allowed by the **Guest Access Security** settings on the Host, so that what is going on on the Host computer cannot be seen by anyone. To do so, click the  **Blank Display** button on the toolbar.

NOTE: While Blank Display works with most Host computers, the design of some display adapters prevents applying it.

Typically, these two functions are used together, for example if you are carrying out maintenance work on an unattended Host computer or working on your office computer from home, and you do not want anyone passing by to see what you are doing or to interfere.

In the Guest **Connection Properties**, on the **Startup** tab, you can specify that the Host computer screen should be blanked and the keyboard and mouse should be locked on the Host computer from

the start when you establish a connection to the Host.

See also

[Guest Access Security Connection Properties](#) (Keyboard/Mouse tab)

2.4 Generate a Host inventory

If allowed by the **Guest Access Security** settings on the Host, you can generate an inventory of Host computer hardware and software. The inventory will be displayed on the **Inventory** tab of the Guest.

Define what you want the Host inventory summary to contain

1. On the **Tools** menu, select **Program Options**.
2. Click the **Inventory** tab, select/clear selection of elements on the **Summary view** list, and click **OK**.

Generate a Host inventory

1. On one of the **Guest** window tabs, select the Host computer for which you want to generate an inventory.

The Guest can connect and generate an inventory from the **Quick Connect** tab, the **Phonebook** tab or the **History** tab.

2. Click the  **Get Inventory** button on the toolbar.

Alternatively, select **Get Inventory** on the **Connection** menu.

or

- If already connected to a Host, in the **Remote Control** window, click the **Get Inventory** button on the toolbar.

The inventory as defined on the **Inventory** tab in **Program Options** is displayed on the **Inventory** tab in the **Guest** window.

See also

[Program Options](#) (Inventory tab)
[Process Host computer inventory information](#)

2.4.1 Process Host computer inventory information

You can use Host computer inventory information to get an overview.

In addition to this you can specify an external program to be executed after an inventory scan has completed. Inventory data are saved in `xml` files, and you might for example want to import the data to a database where it can be further analyzed.

You can also specify custom inventory items that you want to include when generating inventories, that is items not included in the list of inventory items on the **Inventory** tab in Program Options.

You might for example want to check what version of a certain program is installed on a number of Host computers. If you know the registry key for the program version in question, you can specify a custom inventory item for the registry key. You can then generate inventories telling you what version of the program is installed.

Specify a program to run after inventory scan

1. On the **Tools** menu, select **Program Options**.

2. Click the **Inventory** tab, and click the **Advanced** button.
3. In the **Advanced inventory option** dialog box, specify whether you want to run a program after generating an inventory for each Host or after generating inventories for all Hosts for which you choose to generate inventories.

In the **File name** field, specify the program file name. Click the **Browse** button to find the program.

Then click **OK**.

When you generate Host inventories, the specified program will run automatically afterwards as specified.

Specify custom inventory items

You can retrieve additional information during the inventory scan, such as environment variables, registry keys, file information etc.

1. On the **Tools** menu, select **Program Options**.
2. Click the **Inventory** tab, and click the **Advanced** button.
3. In the **Advanced inventory option** dialog box, click the **Add** button.
4. In the **Custom Inventory Items** dialog box, enter a name for the custom inventory item.
Select item type on the **Item Type** list, for example **Registry key**, and fill in all fields for the selected item type as necessary.

Then click **OK**.

The custom inventory item you created is displayed in the **Custom Inventory Items** pane in the **Advanced inventory option** dialog box. From here you can edit or delete it.

NOTE: The pane contents are stored in the Netop configuration file `InvCuItm.xml`, which is typically located here: `C:\Documents and Settings\\Application Data\Netop\Netop Remote Control\Guest`.

2.5 Monitor Hosts


If the **Guest Access Security** settings on the Hosts allow remote control, the Guest can sequentially monitor the computer screen images of multiple Hosts and toggle between monitor mode and remote control mode.

During monitoring most Guest toolbar buttons will be disabled, and the Guest will have no keyboard and mouse control on the Host computer.


If you discover during monitoring that you need to do something on the Host being monitored, switch to remote control mode using the **Monitor/Remote Control** toggle button in the monitor toolbox. Not all remote control functionality, however, will be available.

Each Host will be monitored for a specified number of seconds. Specify the monitor interval in **Tools > Program Options > Monitor**.

On the Host, monitoring will appear as multiple short remote control sessions.









While in a remote control session, you can dynamically change the host monitor to be displayed on the screen by clicking the **Monitors**  icon from the main menu and selecting the desired monitor.

To start monitoring Hosts

1. Select Hosts on the **Quick Connect** tab, the **Phonebook** tab or the **History** tab.
2. Click the  **Monitor** button on the toolbar to start connecting to the first selected Host.

Alternatively, select **Monitor** on the **Connection** menu.

3. If prompted by the Host, enter logon information to log on to the Host.
You will now see the first Host computer.
4. The monitor toolbox will be displayed. Use the tools to control the monitoring.

Button	Description
	End monitoring.
	Continue countdown after Hold.
	Hold countdown.
	Monitor the previous Host.
	Monitor the next Host.
	Switch between monitor and remote control mode. The button will display a remote control icon in monitor mode and a monitor icon in remote control mode.
	Switch between window and full screen. The button will display a window to full screen icon in window mode and a full screen to window icon in full screen mode.
	Display a list of monitored Hosts. Use it to select a specific Host to monitor.

NOTE: The Guest cannot monitor a Host computer with which it runs a remote control session.

2.6 Execute system control commands on a Host computer

If allowed by the **Guest Access Security** settings on the Host, the Guest can execute system control commands on Host computers.

To execute a system control command on a Host computer

1. On one of the **Guest** window tabs, select the Host computer that you want to connect to and execute a system control command on.

The Guest can connect and execute a system control command from the **Quick Connect** tab, the **Phonebook** tab or the **History** tab in the **Guest** window.

2. Click the  **Execute Command** button on the toolbar.

Alternatively, select the **Execute Command** on the **Connection** menu.

or

- When already connected, in the **Remote Control** window, click the **Execute Command** button on the toolbar.

Execute Command will display a menu from which you can select the following commands:

Command	Note
Log Off	

Command	Note
Restart	
Shut Down	
Lock Workstation	You can lock only Host computers running on Windows NT and later (2000, XP, 2003, 2008, Vista, and 7) operating systems.
Wake on LAN	Select Wake on LAN to start selected Host computers whose Wake on LAN MAC Address is specified on the Connect tab in the Connection Properties window. NOTE: You can only use this command for Host computers that support this.

See also

[Guest Access Security](#)

2.7 Perform Remote Management tasks


If allowed by the **Guest Access Security** settings on the Host, the Guest can use **Remote Management** to manage the Host.

For the Host computer you can access the **Disk drives**, **Event Viewer**, **Task Manager**, **Registry**, **Services**, **Shared Folders**, **Inventory**, **Command Console**, **System Control** and **Local Users and Groups**.

The window section called **Netop Sessions** provides access to a few basic remote control session types, **Remote Control**, **File Transfer**, **Chat** and **Audio-Video Chat**, which you can use while remote managing the Host.

Other third party programs can be installed in their own window section. On the **File** menu, click **Third Party Program Integration**. The first step is to add your own window section, and the next step is to add shortcuts to relevant programs.

To start a remote management session with a Host

1. On one of the **Guest** window tabs, select the Host that you want to connect to and run a remote management session with.
2. Click the  **Remote Management** button on the toolbar to start a remote management session with the selected Host.

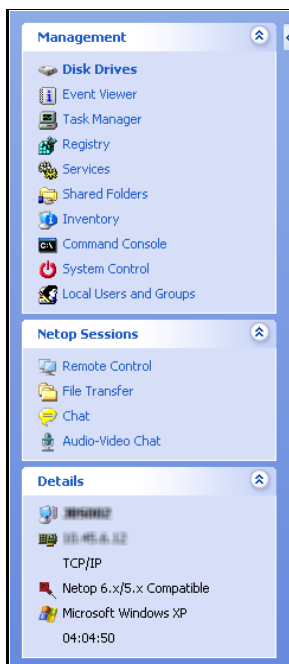
Alternatively, select **Remote Management** on the **Connection** menu.

The **Remote Management** window is displayed.

Nothing is displayed on the Host computer.

2.7.1 Management pane

When you have started a remote management session with a Host, you see the **Remote Management** window. The **Remote Management** window contains a pane on the left providing access to available management tools in three or more sections.



Management

The first section provides access to the **Management** tools. The tools are also available from the **Management** menu, which is added to the Netop Remote Management menu bar when a remote management session is started.

For details about each tool, see the relevant topic below.

Netop Sessions

The second section provides access to the **Netop Sessions** commands. For a brief overview of the command, see [Netop Sessions](#)

Details

The third section is informational only and displays the following information:

- The Host ID
- The Host computer ID or MAC address
- The Guest communication profile
- The encryption type icon and name
- The Host computer operating system
- The remote management session duration in this format: HH:MM:SS

2.7.2 Disk Drives

Click **Disk Drives** in the **Management** section to display available Host computer disk drives and their properties.

Use the **Disk Drives** tool to get an overview of the available disk space on a remote controlled computer.

Viewing options are available from the **Disk Drives** menu and from the shortcut menu that opens when you right-click the data panel.

2.7.3 Event Viewer

Click **Event Viewer** in the **Management** section to display Windows event logs of the Host computer.

Use the **Event Viewer** tool to:

- View and change log properties.
- View the properties of an event record and copy them to the clipboard.
- Clear logs.
- Save a log on the Guest or Host computer.
- Open a log saved on the Guest or Host computer to view it.

NOTE: Only Windows NT and later versions (2000, XP, 2003, 2008, Vista, and 7) record event logs. Consequently, the Event Viewer command is enabled only if the Host computer runs on a Windows NT or later operating system.

Like the Windows Event Viewer, the **Event Viewer** tool includes three categories of information: **Application**, **Security** and **System**.

The fourth tab named **File** can display a saved event log.

The following commands are available from the **Event Viewer** menu and from the shortcut menu that opens when you right-click the data panel:

Command	Description
Open	Opens an event log that was previously saved using the Save command. Event log files have extension .evt. NOTE: Opening a saved event log overwrites any previous File tab contents.
Save	Saves an event log as a file in a specified location. The file must have extension .evt.
Clear	Clears the Application, Security, or System event log from Windows. Before the event log is cleared, you can choose to save the information to a log file for later inspection. The log file should be saved with extension .evt.
Refresh	Retrieves new data from the Host computer to refresh the tab display.
Log Properties	Opens the properties window for the Application, Security or System log file. You can view and change log size and filter properties.
Event Properties	Displays properties for the selected event. Use the up and down arrows to scroll through the list of events. Click the Copy button to copy the record properties to the clipboard.

2.7.4 Task Manager

Click **Task Manager** in the **Management** section to display lists of applications and processes that are running on the Host computer.

The **Task Manager** tool works like the **Windows Task Manager**, only on a remote controlled computer. The tool can be used to view and control applications and end processes, and to view the computer load and process threads.

2.7.5 Registry

Click **Registry** in the **Management** section to open the Windows registry on the Host computer.

The **Registry** tool works like the **Windows Registry Editor**, only on a remote controlled computer.

About Windows registry

The Windows registry stores the configuration of the Windows operating system in a structured database. The registry 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. The registry settings should be modified with caution as erroneous data entries can make the computer malfunction.

Refer to the Windows Registry Editor help for details about entries and how to modify them.

2.7.6 Services

Click **Services** in the **Management** section to display a list of services that are running on the Host computer. *Services* are programs that can run in the background, that is not displaying on the desktop, to support operating system or application functionalities.

The **Services** tool enables you to start, stop, pause, resume and restart Host computer services, to

add and remove services and to change the properties of services.

Note: Only Windows NT and later (NT, 2000, XP, 2003, 2008, Vista, and 7) can manage services. Consequently, the `Services` command is enabled only if the Host computer runs on a Windows NT or later operating system.

The following commands are available from the **Services** menu and from the shortcut menu that opens when you right-click the data panel:

Command	Description
Add...	Adds a service on the Host computer. Follow the instructions in the wizard that opens.
Remove	<p>Deletes a service.</p> <p>When a Services record is deleted, the service status and startup type change to "Stopped" and "Disabled". When the application that uses the service is unloaded, the record is removed.</p> <p>NOTE: Deleting a Services record and removing the service will affect dependent services. Dependencies are shown on the Dependencies tab on the Properties dialog box: Right-click and select Properties on the shortcut menu.</p>
Restart	<p>Stops and starts the service.</p> <p>NOTE: Stopping, pausing or restarting a service may affect dependent services. Dependencies are shown on the Dependencies tab on the Properties dialog box: Right-click and select Properties on the shortcut menu.</p>
Refresh	Retrieve new information from the Host computer to refresh the displayed information.
Properties	<p>Displays properties for the service on three tab pages.</p> <p>NOTE: Do not change service properties unless you know exactly what you are doing. Keep notes of changes to enable restoring properties if changes cause an unexpected behavior.</p> <p>General tab</p> <p>Use the Startup type field to change the way the service starts.</p> <p>NOTE: If you change Startup type to "Disabled", a service which has already been started or paused does not change its status, but when it is stopped, it can no longer be started.</p> <p>Use the Start, Stop, Pause and Resume buttons to control the service.</p> <p>The Start parameters field is enabled when a service is "Stopped". Specify any parameters like command line options to be used when the service is started.</p> <p>NOTE: Start parameters are not saved. A backslash (\) is interpreted as an <code>ESCAPE</code> character. Specify two backslashes for each backslash in a parameter.</p>

Log On tab

Use the **Log on as** options to specify how to log on to a service using a different account.

- Use **Local System account** to log on as a local system account that has extensive rights on the Host computer, but no rights on other computers (typically the default selection).
- Use **This account** to log on as a specific user and specify the user credentials in the fields.

To specify that the selected Host computer service should use the Local Service account, type `NT AUTHORITY\LocalService`. To specify that it should use the Network Service account, specify `NT AUTHORITY\NetworkService`. Do not specify a password for these accounts; both of them have built-in passwords.

Dependencies tab

Displays dependencies and dependents. You cannot change dependencies on this tab.

2.7.7 Shared Folders

Click **Shared Folders** in the **Management** section to view and manage agent computer shared resources and view and disconnect shared resource sessions and shared file connections.

Shares tab

Special shares, typically with \$ as the last character in the share name, are created automatically as hidden resources by the operating system for administrative and system use.

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

These special shares may appear on the **Shares** tab:

<Drive letter>\$	Enables Guests 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 inter program communication by named pipes. <code>IPC\$</code> is used during remote administration of a computer and when viewing a computer's shared resources and cannot be deleted.
NETLOGON	Required on domain controllers. Removing it causes a loss of functionality on domain client computers.
SYSVOL	Required on domain controllers. Removing it causes a loss of functionality on domain client computers.
PRINT\$	Used during remote administration of printers.
FAX\$	A server folder that is used by clients when sending a fax. It stores temporary fax files and fax cover pages.

2.7.8 Inventory

Click **Inventory** in the **Management** section for an overview of the Host computer inventory of hardware and software.

2.7.9 Command Console

Click **Command Console** in the **Management** section to open a command prompt window on the Host computer. This corresponds to clicking **Run** on the Windows **Start** menu and typing `cmd` but have the command prompt window display the *Host computer*, not the Guest.

Before the command prompt window opens, you will be required to enter credentials (user name, password and domain) that are valid on the Host computer.

2.7.10 System Control

Click **System Control** in the **Management** section to control the Host computer status.

System Control allows you to:

- Lock the computer (Windows NT, 2000, XP, 2003, 2008, Vista and 7 only)
- Log off the user
- Restart the computer
- Shut down the computer.

Before any of these actions are performed, you can choose to warn the user by displaying a message, for example:

`Computer updates need to be implemented and you will be logged off in a few minutes. Please save your work and close any open program.`

Use the **Options** section to specify whether the user is to be warned and to specify the number of seconds between prompting the user and executing the action selected under **Action to Perform**.

Allow user to cancel	Generally, you cannot cancel a system control command. However, selecting this option enables the Abort button on the pop-up message, and the user is allowed to cancel the command.
Close open programs without saving data	Normally data is saved before the selected system control command is executed. Select this option to close any open programs without saving data.

2.7.11 Local Users and Groups

Click **Local Users and Groups** in the **Management** section to manage users and groups on the Host computer.

With **Local Users and Groups**, you can:

- Add new users and groups.
- View and edit properties of existing local users and groups.
- Set user passwords.
- Rename or delete users and groups.

Users tab

The **Users** tab contains the list of users of the Host computer.

The shortcut menu has these commands:

Command	Description
New User	Select this command to add a new user. In the New User dialog box, type the appropriate information and select or clear the selection of options related to password and account. Click Create , and then click Close .
Set Password	Select this command to change the selected user's password.
Delete	Select this command to delete the selected user. NOTE: When you need to remove a user account, it is a good idea to disable the account first. When you are certain that disabling the account has not caused a problem, you can safely delete it. To disable the account, select Account is disabled in the Properties dialog box. A deleted user account cannot be recovered. The built-in Administrator and Guest accounts cannot be deleted.
Rename	Select this command to rename the selected user. Type a new name and press Enter to save. NOTE: Because it retains its security identifier, a renamed user account retains all its other properties, such as its description, password, group memberships, user environment profile, account information, and any assigned permissions and rights. A user name cannot be identical to any other user or group name of the computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following: " / \ [] : ; = , + * ? < > . A user name cannot consist solely of periods (.) or spaces.
Refresh F5	Select this command to retrieve new data from the Host computer and refresh the tab display.
Properties	Select this command to view and change properties for a user account. When a user has been created with the New User command, the user must be added to a group. This is done on the Member Of tab in the properties dialog box. NOTE: Adding users to the Administrators group will give them unlimited access rights.

Groups tab

The **Groups** tab contains the list of groups of the Host computer.

The shortcut menu has these commands:

Command	Description
New Group	Select this command to add a new group.

	<p>In the New Group dialog box, type the appropriate information and click Add to add existing users to the group. Click Create, and then click Close.</p> <p>NOTE: A local group name cannot be identical to any other group or user name on the computer being administered. It can contain up to 256 uppercase or lowercase characters, except for the following: " / \ [] : ; = , + * ? < > . A group name cannot consist solely of periods (.) or spaces.</p>
Delete	<p>Select this command to delete the selected group.</p> <p>NOTES:</p> <ul style="list-style-type: none"> • The following built-in groups cannot be deleted: Administrators, Backup Operators, Power Users, Users, Guests, Replicator. • A deleted group cannot be recovered. • Deleting a local group removes only the group; it does not delete the user accounts and global groups that were members of that group. • If you delete a group and then create another group with the same group name, you must set new permissions for the new group; it will not inherit the permissions that were granted to the old group.
Rename	<p>Select this command to rename the selected group. Type a new name and press Enter to save.</p> <p>NOTE: Because it retains its security identifier, a renamed group retains all its other properties, such as its description and members. A group name cannot be identical to any other user or group name of the computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following: " / \ [] : ; = , + * ? < > . A group name cannot consist solely of periods (.) or spaces.</p>
Refresh F5	<p>Select this command to retrieve new data from the Host computer and refresh the tab display.</p>
Properties	<p>Select this command to add and remove users from the group.</p>

2.7.12 Integrate third party applications

If there are applications that you use frequently in connection with remote management, you can create your own section in the left pane of the **Remote Management** window and add commands to open any third party application.

The user defined section in the left pane of the **Remote Management** window is added beneath the **Management** section; see illustration and description in [Management pane](#). Within the user defined section, the third party applications can be added beneath user-defined group headings like for example **Utilities** or **Tools**.

Add a third party application

1. On the **File** menu, click **Third Party Program Integration**.
2. Click **Add Section** to create the section and give it a name, for example **My own section**.
Note that the section will not appear until one or more programs have been added.
3. Select a section and click **Add Program**.

4. In the **Add Program** dialog box, click the **Browse** button to locate the executable.
The **Working Folder** field is updated automatically.
5. Click **OK** to add the program and close the dialog box.

Optional parameters

In addition to specifying the name of the executable, optional parameters can also be specified.

Parameter Name	Description
Display Name	Define the program name to be shown in the new section. If this parameter is not set, the name of the executable (for example: <code>excel.exe</code>) is shown.
Display Name	Define the text to be displayed when the mouse pointer rests on the program name. If this parameter is not set, the name of the executable (for example: <code>excel.exe</code>) is shown.
Command Line	Define the program parameters that should be passed to the program when it is started. The following built-in parameters can be used: <ul style="list-style-type: none"> • %%CN - Host Computer Name • %%CD - Host Computer Domain • %%LU - Host Logged in User • %%LD - Host Logged in Domain • %%IA - Host IP Address • %%MA - Host MAC Address
Working Folder	Select the folder for the program to store its data. If this parameter is not set, the folder where the executable is located is used.
Run As	Select how the program window will be displayed: Normal Window , Minimized , Maximized , Hidden .

TIP: Any program that is installed on the Guest computer and can react to command line executions can be integrated. To view any necessary command line parameters you can open the program properties dialog box: Right-click the program on Windows' **Start** menu and then click **Properties**.

2.7.13 Netop Sessions

The following commands are available in the **Netop Sessions** section:

Command	Description
Remote Control	Start/stop a remote control session with the connected Host.
File Transfer	Start/stop a file transfer session with the connected Host.
Chat	Start/stop a chat session with the connected Host.
Audio-Video Chat	Start/stop an audio-video chat session with the connected Host.

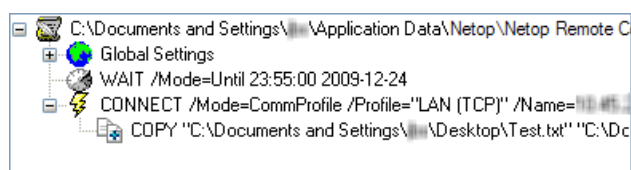
NOTE: Start **Audio-Video Chat** will be disabled if the Guest and Host computers are not both interactive audio enabled or if the Guest is engaged in another audio session. The **Guest Access Security** settings on the Host may deny a Guest starting a session.

2.8 Create and run a script

A script is a user specified command structure that can execute a task, for example an unattended scheduled file transfer.

You create the script in the **Script** dialog box as a tree structure consisting of:

- **Global Settings**, such as overwrite/delete settings, error handling and log file settings etc.
- One or multiple commands, for example a **Wait** command and a **Connect** command to connect to a Host.
- One or multiple commands, for example **Copy**, **Delete**, **Synch**, or **Inventory**, which will be executed on the Host after connection.



The following example describes how to create a script that copies a file from the Guest to a Host on a specified date and time.

To create this script

1. Click the **Script** tab to display the tab.
2. On the **Edit** menu, select **New > Script** to display the **Script** dialog box.
3. In the **File name** field, enter a name for your script, for example "Copy document".
If you do not specify a file type extension, the script will get the file type extension `.dws`.
4. Click the **Open Script** button and click **Yes** to start a new script.
The **Global Settings** dialog box is displayed.
5. In the **Global Settings** dialog box, specify settings for the script. You might for example want to review the **Overwrite/Delete** settings and the **Log File** settings.
When you are satisfied with the global settings, click **OK** to close the dialog box.
6. In the **Comment** field, enter a comment about the script, which will be displayed on the **Script** tab in the **Guest** window.
7. Select **Global Settings** in the tree structure in the upper pane of the dialog box, and click the **Add** button. Select **Wait** on the menu.
8. In the **Wait** dialog box, select **Wait until** in the **Type** field.
Specify a date and time for the copying, and click **OK** to close the dialog box.
The **Wait** command is added to the script and displayed in the tree structure.
9. Select **Wait** in the tree structure, and click the **Add** button. Select **Connect** on the menu.
In the **Connect to Host** dialog box, specify how you want to connect to the Host, for example using a communication profile.
Select communication profile and specify IP address and logon credentials for the Host.
The **Connect** command is added to the script and displayed in the tree structure.

10. Select **Connect** in the tree structure, and click the **Add** button. Select **Copy** on the menu.

The **Copy** dialog box is displayed.

On the **General** tab, in the **Guest** section, specify the file that you want to copy to the Host.

In the Host section, specify the location on the Host that you want to copy the file to, and change any other settings as necessary.

NOTE: You cannot browse, since the Guest is not yet connected to the Host.

Click **OK** to close the dialog box.

11. Click **Save Script**, and click **Run** to enable the script.

12. Click **Close** to close the dialog box.

You have now created a script that will copy the `Test.txt` file to one specific Host on a specific date and time.

If you want to copy the `Test.txt` file to a number of Hosts, the easiest way to specify this in the script is to first edit the script file (`Copy document.dws`, located in `\\Application Data\Netop\NetOp Remote Control\Guest\script\`) in Notepad and then edit it further in the **Script** dialog box.

☐ **Script file contents**

```

;Copy document to Host computer
;*****
Script
SET Copy=G_H
SET Delta=Yes
SET CrashRecovery=Yes
SET OverwriteExisting=Yes
SET OverwriteSystem=No
SET OverwriteReadOnly=No
SET OverwriteHidden=No
SET OnComError=NextHost
SET OnError=NextFile
SET AtEnd=None
SET UnloadGuest=No
SET LogAppend=No
SET Log=SCRIPT.LOG

WAIT Mode=Until 23:55:00 2009-12-24

Connect /Mode=CommProfile /Profile="LAN (TCP)" /Name="10.45.2.33" /
LoginCredentials=Yes
COPY "C:\Documents and Settings\user1\Desktop\Test.txt" "C:\Documents and
Settings\"
ConnectEnd
ScriptEnd

```

1. Copy the **Connect** command (from `Connect /Mode=` through `ConnectEnd`) for as many Hosts as you want to copy the `Test.txt` file to.
2. Save and close the `Copy document.dws` file.
3. Open the `Copy document.dws` file in the Script dialog box again, and for each `Connect` command, edit the IP address and logon credentials in accordance with the individual Hosts that you want to copy the `Test.txt` file to.
4. Save the script.

The script you have created automatically copies the `Test.txt` file to a specified range of Host computers on the specified date and time.

NOTE: The Guest also contains a couple of slightly more advanced example scripts that you can study to see what you can do with Script. See `example1.dws` and `example2.dws` on the **Script** tab. You can open them in Notepad to see the contents.

Once the script has been executed, you can check the script log file (`\\Application Data\Netop\NetOp Remote Control\Guest\`) to see if the script was executed successfully.

See also

[Script](#)
[Global Settings](#)

2.9 Use Intel vPro from Netop Remote Control

The Netop Remote Control Guest provides access to Intel vPro (sometimes also referred to as IAMT - Intel Active Management Technology) functionality which enhances your ability to remote manage enterprise computing facilities.

NOTE: Netop Remote Control Guest supports Intel vPro, up to version 3.0.5. Functionalities that have been introduced after this version are not supported.

The Guest can access vPro even when the computer is turned off, as long as the computer is connected to line power and to a network.

NOTE: Due to a limitation in Intel vPro, it is not possible to establish a connection to Intel vPro on the same computer as the one the Guest is running on.

The Intel Setup and Configuration Service (SCS) provides tools to centrally set up and configure AMT devices. SCS serves as a server for vPro and is also called a provisioning server.

Depending on which permissions the user has, the following SCS realms are relevant when using the vPro Console that the Guest provides access to:

Realm	Comments
General Info	Required
EventLogViewer	If the user has permission to this realm, the Event Management tab will be available, but the Remove all and Filters and Subscriptions buttons will be disabled. So the user will not be able to change anything.
Event Management	If the user has permission to this realm, the Event Management tab will be enabled and all buttons will also be enabled. So the user will be able to make changes.
Remote Control	If the user has permission to this realm, the Remote Control tab will be enabled and the user will be able to execute remote control commands.
Redirection Interface	If user has permission to this realm, the user will be able to execute serial/IDE redirection commands from the Remote Control tab.

If the user has permissions to neither the **Event Management** tab nor the **Remote Control tab**, an "Authentication failed" message box is displayed. This means that either User or Password is wrong or there are no appropriate permissions for the user in question.

NOTE: Even though computers contain Intel vPro technology, the AMT devices will not be

operational until they have been enabled (also called provisioning) in the vPro BIOS.

Intel vPro enables you to

- Remotely access BIOS configuration of the managed computer.
- Remotely boot the managed computer from a floppy or CD-ROM image located on the managing computer.
- Retrieve and view the hardware log file of the managed computer.

2.9.1 Log on to the vPro Console

The **Intel vPro** tab is displayed at the bottom of the **Quick Connect** tab pane following the **Windows Network** tab. When you start the Guest, the **Intel vPro** pane will be empty.

Right-click the **Intel vPro** pane to display a context menu containing the following commands:

Command	Description
Scan IP range for Intel vPro enabled computers	<p>Select this command to scan for Intel vPro enabled computers on your network. You can enter one known IP address to scan for or you can enter an IP range to scan.</p> <p>The computers found during the search will be listed in the Intel vPro pane by IP address. See picture above.</p> <p>NOTE: You can also use the Guest Inventory tab (Summary - Intel vPro State) to find Intel vPro enabled computers on your network.</p>
Retrieve Intel vPro enabled computers from SCS	<p>Select this command or press the Browse button on the Quick Connect tab to retrieve Intel vPro enabled computers from Intel SCS. You must enter the SCS Web Service URL.</p> <p>NOTE: If you do not want to have to enter the SCS Web Service URL every time, go to Tools > Program Options > Intel vPro tab. Select the Connect to SCS check box and enter the SCS Web Service URL in the field below. The address is then saved in the system, so that you will not be prompted to enter the address every time you select the Retrieve Intel vPro Enabled Computers from SCS command.</p>

When you have found one or more vPro enabled computers on your network, the above menu will be extended with the following commands:

Command	Description
Open Intel vPro Console	<p>Right-click a computer in the list in the Intel vPro pane and select this command to open the vPro Console from which you can manage the selected computer.</p> <p>You need a user name and password to log on.</p>
Open Intel vPro Web Interface	<p>Right-click a computer in the list in the Intel vPro pane and select this command to go to the Intel vPro Active Management Technology web page (http) from which you can manage the selected computer.</p> <p>You need to enter a user name and password to log on to the web page.</p>
Open Intel vPro Web Interface (Secure)	<p>As above, but using secured connection (<code>https</code>).</p>

Command	Description
Add to phonebook	Right-click a computer (IP address) in the list in the Intel vPro pane and select this command to add the address to the phonebook. NOTE: You can also add Intel vPro entries to the phonebook by right-clicking the right pane on the Phonebook tab.
Delete	Right-click a computer in the list in the Intel vPro pane and select this command to remove the computer from the list.
Delete All	Right-click the Intel vPro pane and select this command to remove all computers from the list in the Intel vPro pane.

To log on to the vPro Console

1. Right-click a computer on the list in the **Intel vPro** pane and select **Open Intel vPro Console**.
2. On the **Credentials** tab of the displayed **Netop vPro Console Logon** window, select authentication method:
 - **Digest authentication**
 - **Kerberos authentication**

If you select **Digest authentication**, enter user name and password.

Select the **Force using secured connection through TLS** check box, if you prefer. Normally, Transport Layer Security (TLS) is automatically detected and used when available, but if you select this check box, the **vPro Console** will only use secured connection to log on to the AMT device. If the AMT device is not configured to use TLS, you will receive an error message and the connection will not be established.

If you select **Kerberos authentication**, the tab will look slightly different, and either a current Windows user account or a different user account (user, password, domain) can be used to log on to the AMT device.

In addition to the **Force using secured connection through TLS** check box, you will see a **Log on using current Windows account** check box. This check box is selected by default, and as a consequence the **User name**, **Password**, and **Domain** fields are disabled, and the credentials of the current Windows user will be used.

NOTE: When using Kerberos authentication the console should be connected to the Host using FQDN name (fully qualified domain name). For example, it is not possible to do the Kerberos authentication when connecting to an AMT device using its IP address.

3. If you select the **Force using secured connection through TLS** check box, a client certificate is required to establish the TLS connection when the AMT device is configured for mutual TLS authentication.

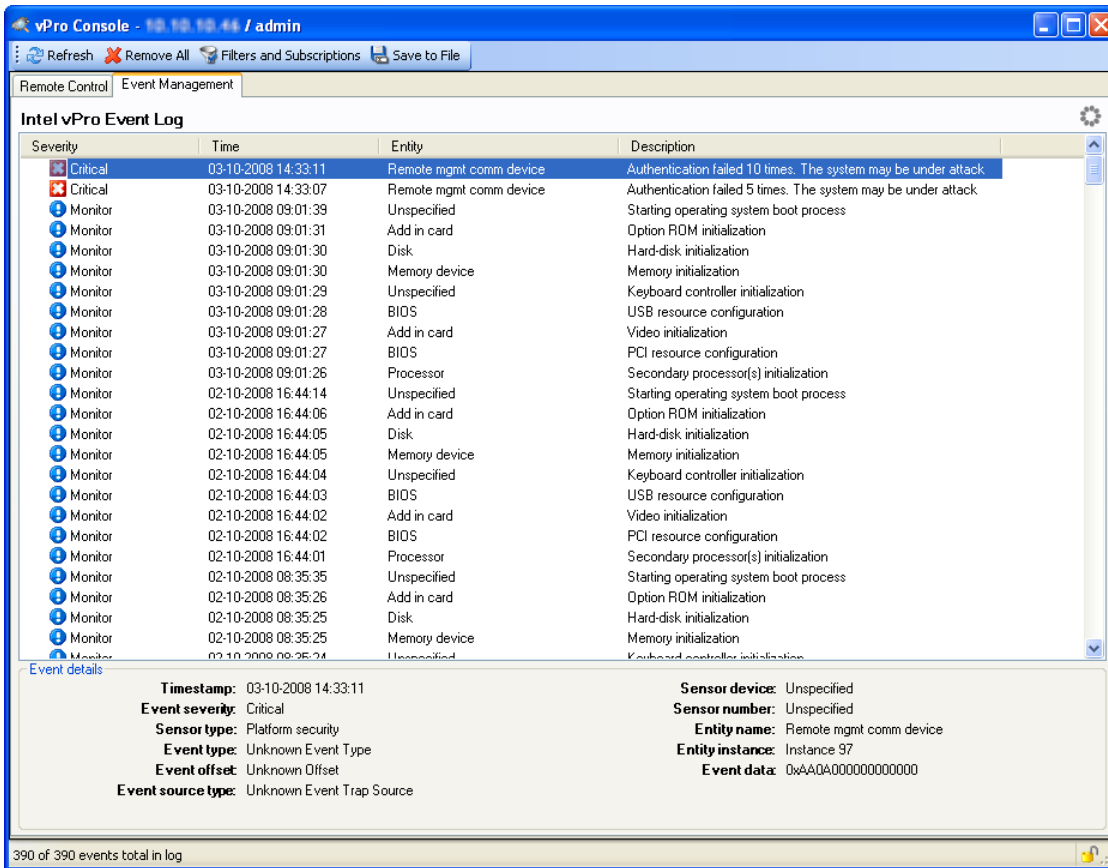
Click the **Certificate** tab and specify the certificate to be used by first selecting either **Personal Certificate Storage** or **File** in the **Location** list and then selecting the certificate in the **Certificate** combo box.

4. Click **Log on** to log on to the **vPro Console**.

When you have logged on, the **vPro Console** window will be displayed.

2.9.2 vPro Console

The **vPro Console** window contains a toolbar at the top and two tabs: the **Event Management** tab, on which you can retrieve and view the **Intel vPro Event Log** for the computer being managed, and the **Remote Control** tab, on which you can access the BIOS of the computer, boot from a floppy or CD-ROM image, and manage the power state of the computer remotely.



Event Management tab

The **Event Management** tab displays the **Intel vPro Event Log** for the computer being managed. The events are displayed in the **Intel vPro Event Log** pane with information about severity, time, and entity together with a description. Selecting an event in the pane will display further details about the event in the area below the pane.

In the bottom right corner of the **vPro Console** window you see a security indicator, a lock icon. A closed lock indicates that a secured connection is being used, while an open lock indicates that an unsecured connection is being used. In the top right corner you see a network activity indicator that looks like a flower. This icon indicates that the vPro Console is waiting for response from the remote AMT device.

At the top of the **vPro Console** window you find a toolbar with tools that you can apply to the log. In addition to the **Refresh** button, the **Remove All** button, and the **Save to File** button (save events to a .txt (tab delimited) file or a .csv (comma delimited) file), a **Filters and Subscriptions** button is available.

Manage filters, alerts, and subscriptions

The **Filters and Subscriptions** button opens a window from which you can manage event filters, alerts and subscriptions.

The **Event Filters, Alerts and Subscriptions** window is divided into two areas, on the left a tree pane listing the alerts and filters set on the AMT device and on the right a dialog panel. The dialog panel changes depending on the node selected in the tree pane.

The toolbar above the tree pane contains buttons that you can apply to the tree nodes. The toolbar changes depending on the node you select in the tree pane.

Root node

If you select the root node, the dialog panel displays system information on two tabs:

- Use the **System Sensors** tab to see a list of sensors and a detailed description of the currently selected sensor.
- Use the **Alert Settings** tab to change the SNMP community strings for alerts.

In addition to the **Refresh** button on the toolbar, you see an **Add Alert** button, which you can use to add a new alert to the tree.

NOTE: The alert ID entry in the tree can be edited. However, depending on your user rights you may or may not be able to change alert ID entries and associated filters and subscriptions. Non-administrator users cannot change subscriptions owned by other users. Administrators can take ownership of other user's subscriptions (AMT 2.5 and later).

Alert id node

If you select an **Alert ID** node, the dialog panel displays a list of subscriptions for the alert. When an alert with the specified ID is triggered on the remote AMT device, the PET (Platform Event Trap) or SOAP (Simple Object Access Protocol) event will be sent to all IP addresses or URLs subscribing to this alert.

NOTE: A platform event is defined as an event that is originated directly from platform firmware (BIOS) or platform hardware independently of the state of the operating system or system management hardware. The Platform Event Trap format is used for sending a platform event in an SNMP Trap.

You can select and remove one or more subscriptions (click the first, hold down SHIFT, and click the next) from the list using the **Remove** button below the list.

You can also add SNMP subscriptions from the **Add SNMP subscription** section at the bottom of the **Alert Subscriptions** dialog panel:

1. Enter the IP address you want to subscribe to the alert in the **IP address** field.
2. Select the **Use custom community string** check box (available on AMT 2.5 and later, disabled for older versions).
3. When you have selected the **Use custom community string** check box, the **Community string** field below will display *public* by default, but you can change it.
4. Then click the **Add** button to add the specified IP address to the list of subscriptions.

In addition to the **Refresh** button on the toolbar, an **Add Filter** button is available. Use this button to create a new filter with default properties under the currently selected alert ID. The filter properties are displayed in the **Event Filter Properties** dialog panel on the right. Click the **Apply** button at the bottom of the dialog panel for the new filter with default properties to be created.

On the toolbar you will also see a **Remove** button. Use this to remove all filters under the selected alert node and cancel all the subscriptions. You will be prompted for confirmation when you select the **Remove** button.

Filter node

If you select a filter node, the dialog panel displays editable properties for the selected filter:

Property section	Description
Filter settings	In the Filter settings section you can enable the filter by selecting the

Property section	Description
	<p>Enable event filter check box. If you do not select the check box, the filter is disabled and no actions are performed.</p>
Filter criteria	<p>In the Filter criteria section you can set various criteria for the filter. When an event matches the specified filter criteria, the action specified in the Filter action section will be performed.</p>
Filter action	<p>In the Filter action section you can set the action to be performed when the event matches the specified filter criteria.</p> <p>Selecting the Log event check box will have the effect that events matching the specified filter criteria will be written to the log on the AMT device.</p> <p>Selecting the Alert event check box will have the effect that events matching the specified filter criteria will trigger the alert.</p>
Alert settings	<p>In the Alert with severity field you can set the Event severity field in a PET alert. When an alert is generated either the event's own severity or a severity for matching filters, whichever has the highest numerical value, will be used for the specified Alert ID.</p> <p>Numerical values for severity levels:</p> <ul style="list-style-type: none"> • 00h - Unspecified • 01h - Monitor • 02h - Information • 04h - OK (return to OK condition) • 08h - Non-critical, a.k.a Warning • 10h - Critical • 20h - Non-recoverable <p>Example:</p> <p>We have an event with the severity Monitor and 3 filters match the event. Alert with severity for one filter is set to Unspecified, for the second filter to Information and for the third filter to Critical. The value Critical will then be used. This is because the severities correspond to numerical values: Unspecified corresponds to the lowest value, Monitor corresponds to a higher value, Information corresponds to an even higher value, and Critical corresponds to the highest value of the four.</p> <p>If all filters have the severity Unspecified, then the event's original Monitor severity will be used because it constitutes the severity with the highest numerical value.</p> <p>In the Alert ID list, select the filter's Alert ID.</p>

You must click the **Apply** button to save any changes that you make to the filter properties. If you click **Close** after having made changes to the properties, you will be asked whether you want to save the changes.

Remote Control tab

The **Remote Control** tab provides access to the terminal window, which you can use for remote BIOS access and floppy/CD-ROM redirection.

The toolbar for the **Remote Control** tab contains the following buttons:

Button	Description
Remote Control	<p>The menu that opens when you click the Remote Control button down arrow on the toolbar contains the following menu commands:</p> <ul style="list-style-type: none"> • Normal Reboot • Reboot to BIOS* (If you click the Remote Control button instead of the down arrow, this menu command will be selected by default) • Boot from Console Floppy • Boot from Console CD <p>When you select menu commands on the Remote Control menu, you will be able to see the screen of the computer being booted on the Remote Control tab of the vPro Console.</p>
Execute Command	<p>The menu that opens when you click the Execute Command button down arrow on the toolbar contains the following menu commands:</p> <ul style="list-style-type: none"> • Normal Reboot* (If you click the Execute Command button instead of the down arrow, this menu command will selected by default) • Boot from Console Floppy • Boot from Console CD <p>When you select menu commands on the Execute Command menu, the boot command will be executed on the remote computer, but you will not see the screen of the computer being booted on the Remote Control tab of the vPro Console.</p>
Power	<p>The menu that opens when you click the Power button on the toolbar contains the following menu commands, which you can use to manage the power state of the remote computer:</p> <ul style="list-style-type: none"> • Power On • Power Off • Cycle Power Off and On* (default)
Custom command	<p>The menu that opens when you click the Custom command button down arrow on the toolbar contains the following menu commands, which you can use to customize the menus and menu items to the left of Custom command:</p> <ul style="list-style-type: none"> • Send command - Select this command to open the Send Custom Command dialog box, which allows you to specify a custom command and send it immediately. The custom command will not be saved for later use. • Customize - Select this command to open the Customize Remote Control Toolbar dialog box, which allows you to add and specify menus, commands and separators, reorder these elements, and send commands. The changes will be saved, but you can reset the toolbar again. <p>On the left side in the Customize Remote Control Toolbar dialog box a</p>

Button	Description
	<p>pane containing the menu structure is displayed. If you select a menu, settings for adjusting the menu are displayed to the right of the pane. You can move the menu up and down in the toolbar, change the appearance of the menu and more.</p> <p>If you select a command in the pane, command options are displayed to the right of the pane.</p> <p>Both dialog boxes contain the same command options, but depending on the command you select, different sets of options will be enabled. You can specify command type and parameters, CD/floppy redirection and boot options for the command you select.</p>
<p>IDE Redirection Settings</p>	<p>Clicking the IDE Redirections Settings button on the toolbar opens the IDE Redirections Settings window where you can select settings for Floppy redirection and CD redirection, i.e. the drives and image files that are to be used for Boot from Console Floppy and Boot from Console CD.</p>
<p>Netop vPro Console Settings</p>	<p>Clicking the Terminal Settings button on the toolbar opens the Netop vPro Console Settings window where you can edit settings for the following:</p> <p>Terminal - Set Font and Emulation.</p> <p>Keyboard - Set Special key mode and Send Esc button code.</p> <p>Warnings - Select the warnings that you want to receive in relation to the Keyboard settings:</p> <ul style="list-style-type: none"> • Warn if the special key mode cannot be detected automatically • Warn when trying to detect keyboard mode without having Hardware Assets Realm permission

2.10 Tunnel

The Tunnel function establishes a secure connection between the Guest and Host and allows application ports to be redirected from the Host to the Guest through the Tunnel.

This means that the Guest can run local applications while interacting with the connected Host without having to control the Host machine remotely.

The Tunnel is ideally suited, but not exclusive to environments where no traditional desktop is available for use with standard remote control (screen, keyboard and mouse control); however support and system administrative tasks still need to be carried out remotely whilst conforming to industry regulatory standards such as PCI-DSS, HIPAA and FIPS.

Such environments can include embedded Linux systems where operating machinery and hardware contains a streamlined version of a Linux operating system, for example, fuel dispensers and retail systems. Enterprises can also take advantage of the Tunnel for managing and supporting their Linux Desktops and Servers using common applications and services such as Shell clients, HTTP and SFTP.

The Guest's ability to use the Tunnel along with the associated ports can be governed by the central Netop Security Server solution. This allows organizations to apply granular access privileges. Even when remote systems have a desktop, it may not be required to give Guest users full remote control access on certain machines but limit their ability to use certain application ports through the Netop Tunnel.

2.10.1 Predefine local ports for the tunnel

When using the Tunnel capabilities, it is sometimes necessary to configure the local port to a fixed port. This way, when actually tunneling into the machine, the same local port will always correspond to the remote port.

To configure local ports for the tunnel

1. Create the `NetopTunnelPorts.ini` file and define the list of local ports and their corresponding remote ones.

The .ini file should have the following structure:

```
[default]
key = value
[section]
key = value
```

Where `section` is the Remote IP, `key` is the remote port and `value` is the local predefined port.

2. Place the `ini` file in the `C:\windows` folder.

It will help identify either the remote port or the remote IP/remote Hostname/remote port pair and assign it a predefined fixed local port that the Guest will open when initiating the tunnel.

NOTES:

- In the `NetopTunnelPorts.ini` file you can define the host by providing either the Host ID or the Host IP Address. When connecting to the Host, the proper definitions are used, otherwise default definition will apply.
- For the TCP/IP communication profile, there might be a cross Host ID - IP Address compatibility. Ini file defined with Host ID works if connection is made with Host IP Address or Host ID. Otherwise, the default definition is used.

.ini file sample

```
[default]
80=80
8080=8080
8090=8090
[192.168.201.82]
80=90
8080=91
8090=92
8181=93
[192.168.201.137]
80=94
8080=95
8090=96
8181=97
```

2.10.2 Open tunnel session

The Guest can initiate the Tunnel session with a Host in the same way as any other session:



The Tunnel is also available from the context menu on the **Quick Connect** tab, **Phonebook** tab or the **History** tab.

Once the Guest has been authenticated, the assigned ports will be assigned by the Netop Security

Server and the Tunnel console will appear confirming which remote ports are available along with the randomly assigned ports that can be used by the Guest.

For details about setting up and using the secure tunnel please refer to separate documentation available on netop.com.

2.11 Run a remote program

While carrying out maintenance work, you might for example want to run programs for cleaning up the system, or you might want to run a program that carries out a system scan, if anti-virus software has been installed on the computers.

If allowed by the **Guest Access Security** settings on the Hosts, the Netop Guest can run a program on one or multiple Host computers using the **Run Program** function.

The **Run Program** function is also useful if you are providing support and want to demonstrate something to a Host user.

To run a program

1. On one of the **Guest** window tabs, select the Host computer that you want to connect to and run a program on.

The Guest can connect and run a program from the **Phonebook** tab, the **Quick Connect** tab, or the **History** tab.

When already connected, the Guest can run a program from the **Phonebook** tab, the **Quick Connect** tab, the **Connections** tab or the **History** tab.

2. Click the  **Run Program** button on the toolbar.

Alternatively, on the **Connection** menu, select the **Run Program**.

3. Click **Browse**.

4. In the **Run** dialog box, click the **Browse** button and select the program that you want to run on the selected Host computer.

When the program file is added in the **Local File name** field, the global file name with the absolute path replaced by environment variables is also added in the **Global File Name** field. This is especially useful if your computers are running **different Windows platforms**.

Select the **Global File name** option, so that you do not have to consider which operating system version or operating system language the Host computer is using.

If the selected program needs to be started using command line switches, use the **Command line switches** field to type those. This could for example be starting Internet Explorer with a specific address.

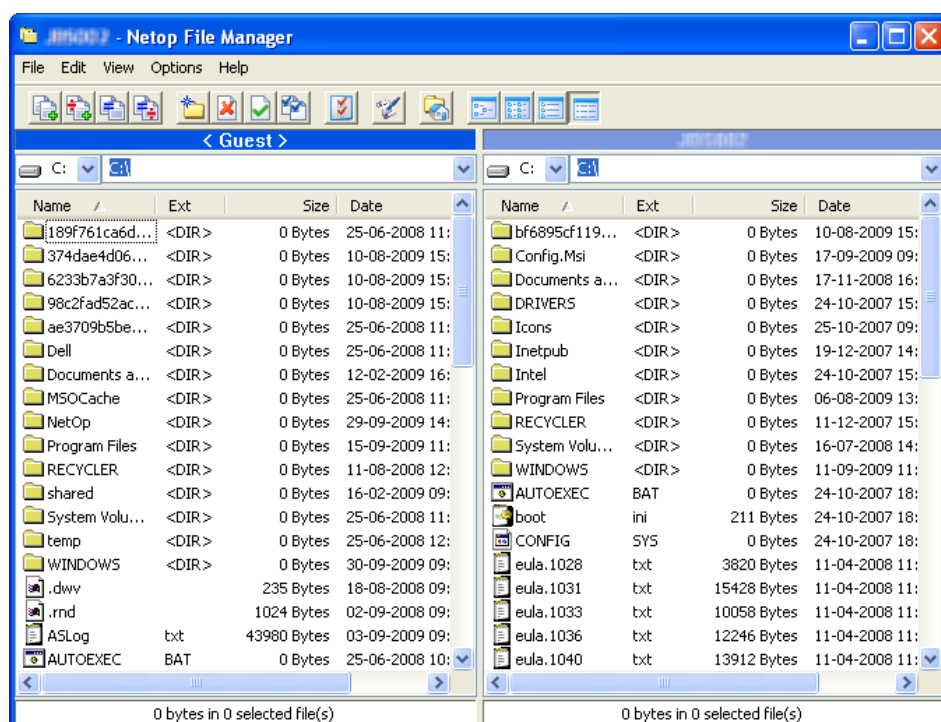
Under **Run**, define how the program should start. Select **Normal**, **Maximized** or **Minimized**.

5. Click **OK** to run the specified program on the selected Host computer.

NOTE: The program file must be available on the Host computer in the location specified in the **Run** dialog box. The program can also be specified on the **Tools > Program Options > Run** tab. If the program is not available on the Host computer in the specified location, you can use the Netop File Manager to transfer the file to the Host before running it. See [Transfer files](#) for further information.

2.12 Transfer files

You can use the **Netop File Manager** to transfer files between a Guest and a Host computer.



If allowed by the **Guest Access Security** settings on the Host, the Guest can start a file transfer session with a Host to transfer files between the Guest and the Host computer. This includes copying, moving, synchronizing, and cloning files.


You can also use the **File Manager** to transfer files locally on the Guest computer.

To start a file transfer session

1. On one of the Guest tabs, select the Host to or from which you want to transfer files.

The Guest can connect to start a file transfer session from the **Phonebook** tab, the **Quick Connect** tab, or the **History** tab, or in response to a help request from a **Help Request** tab.


When already connected, the Guest can start and end a file transfer session from the **Phonebook** tab, the **Quick Connect** tab, the **Connections** tab, or the **History** tab.

2. Click the  **File Transfer** button on the toolbar to open the **File Manager**.

NOTE: If the Host allows multiple simultaneous Guest connections, multiple Guests can run separate file transfer sessions.

Copy files

To copy files from one computer to another

1. Select files and/or folders in one of the two **File Manager** panes and click the  **Copy File(s)** button on the toolbar.

Alternatively, select files in one of the two **File Manager** panes and select **Copy File(s)** on the **File** menu.

2. In the **Copy** dialog box, check the location in the **To** field and change the location if necessary.

Click the **Options** button to view the **Options** dialog box and specify options for the copy


process. See [Netop File Manager Options](#) for further information.

3. Click **OK** to start the copy process.

NOTE: You can also use drag-and-drop to copy files from one **File Manager** pane to the other.

☐ **Move files**

To move files from one computer to another

1. Select files and/or folders in one of the two **File Manager** panes and click the  **Move File(s)** button on the toolbar.

Alternatively, select files in one of the two **File Manager** panes and select **Move File(s)** on the **File** menu.

2. In the **Move** dialog box, check the location in the **To** field and change the location if necessary.

Click the **Options** button to view the **Options** dialog box and specify options for the move process. See [Netop File Manager Options](#) for further information.

3. Click **OK** to start the move process.

☐ **Synchronize files**

To synchronize files between two computers

1. Click the  **Synch File(s)** button on the toolbar.

Alternatively, select **Synch File(s)** on the **File** menu.

2. In the **Synchronize** dialog box, check the location in the **To** field and change the location if necessary.

Click the **Options** button to view the **Options** dialog box and specify options for the synchronize process. See [Netop File Manager Options](#) for further information.

3. Click **OK** to start the synchronize process.

WARNING! Be careful when synchronizing! By default, synchronization will transfer files and folders in both directions, replacing older files and folders with newer files and folders. On the **Transfer** tab of the **Options** dialog, you can change this into **Transfer only if file exists** and **Transfer only one way** for the file transfer process.

☐ **Clone Files**

To clone files from one computer to another

1. Click the  **Clone File(s)** button on the toolbar.

Alternatively, select **Clone File(s)** on the **File** menu.

2. In the **Clone** dialog box, check the location in the **To** field and change the location if necessary.

Click the **Options** button to view the **Options** dialog box and specify options for the clone process. See [Netop File Manager Options](#) for further information.

3. Click **OK** to start the clone process.

WARNING! Be careful when cloning! Cloning will transfer all folders and files in the selected pane to the other pane deleting existing folders and files in it.

TIP: To be more in control of what happens and avoid deleting or overwriting files unintentionally

when you synchronize or clone files, select all options in the **Confirmation** tab of the **Options** dialog box. See [Netop File Manager Options](#) for further information. A dialog box will then be displayed when you are about to delete or overwrite a file, allowing you to choose what you want to do with the individual file.


Transfer files locally on the Guest computer

If you want to transfer files from one location on the Guest computer to another, click the  **Local** button on the toolbar in the **File Manager**.

The folder structure of the Guest computer will then be displayed in both panes.

Run a script from the File Manager

You can open, edit, and run a script while you are in the **File Manager**.

- Click the  **Script Editor** button on the toolbar to open the **Script** dialog box.

For further information about using scripts, see [Create and run a Netop script](#).

2.13 Log events

To support security functions, Netop Remote Control includes an extensive event logging feature that enables you to log session activity and logon attempts to multiple logging destinations.

You can log Netop events

- In a Netop log on the local computer.
- In the database of a central Netop Server.
- In an SNMP enabled management console (by sending SNMP traps to an SNMP enabled central management console, such as HP OpenView).

Enable logging

1. On the **Tools** menu, select **Log Setup**.
2. In the **Log Setup** dialog box, on the **Log Setup**, select where you want to log events.
3. Click the relevant tab to set up the logging, for example the **Netop Local** tab, if you selected **Log Locally** on the **Log Setup** tab.
4. On the **Netop Local** tab, select the events you want to view in the list of events, all or a specific type of events.
5. On the list of events select the individual events that you want to include in the logging.

By default each Netop event is written to the local Netop log file immediately. Clear the **Write to disk for each log entry** check box to write Netop events to the local Netop log file when the Netop module is unloaded. This consumes less processor capacity.

6. Click **OK** to close the dialog box and start logging.

NOTE: The **Log file name** field displays the (path and) name of the log file (default: NETOP.LOG). If no path is specified, the log file is located in the Netop configuration files folder, typically C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\

See also

[Log Setup](#)

2.14 Record sessions

For documentation purposes you can record remote control sessions. You can choose to record sessions for a specific connection, or you can choose to record sessions for all connections.

NOTE: Recording will reduce remote control session transfer speed.

Record sessions for a specific connection

Before connecting to a Host

1. On the **Quick Connect** tab, click **Connection Properties**.
2. In the **Connection Properties** dialog box, click the **Record** tab and select the **Record remote control session** check box.
3. Click **OK**.

When you connect to a Host every remote control session that you run for that specific connection will now be recorded.

Record sessions for all connections

If you want to record sessions for all connections

1. On the **Tools** menu, select **Program Options**.
2. In the **Program Options** dialog box, click the **Recording** tab.
3. Select the **Enforce recording** check box to activate session recording.
Select other settings as preferred.
4. Click **OK**.

From now on sessions will be recorded for all connections, until you change these settings again.

See also

[Connection Properties](#)
[Program Options](#)

2.14.1 Play back session recordings



Session recordings will be listed on the **Recordings** tab in the **Guest** window.



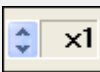
To play back a session recording

1. On the **Recordings** tab, select the session recording that you want to play back.
2. On the **Connection** menu, select **Play back session recording** to start playing back the session recording.

Alternatively, double-click the session recording to start playing back the session recording.

In the **Play back recording** window, you can use the following buttons to control the playback:

Button	Description
	Click the Stop button to close the window.
	Click the Pause button to pause playback. Click this button again to resume playback.

Button	Description
	Click the Play button to start playback or resume playback when paused. When playback has ended, this button is disabled.
	Click the Back button to return to the beginning of the recording showing a black show area.
	Playback Speed: By default, the spin box field will show x1 indicating true speed. Click the up/down arrows to change the playback speed by a factor x1 to x20 as shown in the spin box field.

2.15 Use a skin to see the Host button layout

A Host, typically a CE/Mobile device, can transfer information about its button layout to Netop Guests enabling 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, skins enable you to see the Host device and execute commands on the Host device by clicking buttons on the applied skin. A device 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 Guest.

If the Guest does not have the skin that is needed for a remote control session with a particular Host, it will attempt to collect a suitable skin from the Skin Repository Server. If the necessary skin is not available, the Guest will use a default skin.

The address and port number of the Skin Repository Server that the Guest collects skins from is specified in **Program Options** on the **Skins** tab. If you click the **View Models** button on the **Skins** tab, you can also see the skins available on the Skin Repository Server.

To use skins, you need to enable the function in the Guest **Connection Properties**. Click the **Display** tab and select options for the use of skins in the **Skin** section.

NOTE: You can design additional skins using the Netop Skin Designer and add them to the Skin Repository Server.

See also

[Connection Properties](#) (Display tab)

[Program Options](#) (Skins tab)

2.16 Multisession Support

Each Windows Host supports up to 24 simultaneous sessions, no matter the communication protocol (TCP, UDP or Web Connect). However, it depends on the session type and the Host hardware:

- up to 24 simultaneous sessions for Remote Control.
- up to 12 simultaneous sessions for File Transfer or Tunnel.

Each Windows Guest supports only one session initiated from the same guest instance to the same host.

3 Getting remote support

3.1 Request help

If the **Help Request** function has been enabled on the Host, you can request help from a Guest that offers help services.

To request help


1. Click the  **Request help** button on the toolbar.

Alternatively, on the **Session** menu, select the **Request help** command.

If the Host is minimized you can request help by double-clicking the **Netop Help Request** icon in the notification area.

2. Depending on how the **Help Request** function has been set up, you may now be prompted to enter various information. The Guest user can provide you with the information you need. Enter the necessary information when prompted.

When you have entered the necessary information, your help request is delivered to the help provider, who will typically start a remote control session.

While the help request status is "Pending", you can choose to cancel it by clicking the  **Cancel help** button on the toolbar.

See also

[Set up Help Request on Guest and Host Program Options](#) (Help Request tab)
[Advanced Help Request Options](#)

3.2 Notification

You may be notified of connecting Guests in different ways upon connection, during connection and after connection, depending on the connection notification setup.

Upon connection

You may be notified by a sound being played or a balloon tip or a list of connecting Guests being displayed in the notification area in the lower right corner of the screen.

The connection list may be set to disappear after a specified number of seconds, or you may have to enter a password to close the history list.

During connection

A sound may be played at certain intervals, the Guest name may be displayed in the Host title bar, and the Host icon in the notification area may be animated.

After connection

You may be notified by a balloon tip or a history list of connections in the notification area when a Guest disconnects.

The history list may be set to disappear after a specified number of seconds, or you may have to enter a password to close the history list.

NOTE: You may also be prompted to confirm Guest access, if this has been set in the **Guest Access Security** dialog box on the **Guest Access Privileges** tab.

See also

[Program Options](#) (Connection Notification tab)
[Guest Access Security](#) (Guest Access Privileges tab)


3.3 Communicate with Guest users

Netop Remote Control offers two ways in which you can communicate with Guest users while receiving remote support.

If allowed by the **Guest Access Security** settings on the Host, the Guest can start a chat or an audio-video chat with a Host, and the Host can likewise start a chat or an audio-video chat with the Guest.

Chat

To start a chat with a connected Guest

1. Click the  **Chat** button on the toolbar.
Alternatively, on the **Session** menu, select **Chat**.
2. In the **Chat** dialog box, type your message.
3. Click **Send**.

NOTE: You can save the chat as an `rtf` file for documentation purposes.

Multi chat

If the Netop Host allows multiple simultaneous Guest connections, a Guest that the Guest Access Security settings allow to act as multi Guest session administrator can start a multi chat with the Host and all connected Guests.

Audio-video chat

Audio-video chat requires audio-video equipment to be installed on both sides.

To start an audio-video chat with a connected Guest

Click the  **Audio-Video Chat** button on the toolbar.

Alternatively, on the **Session** menu, select **Audio-Video Chat**.

The **Audio-Video Chat** dialog box will be displayed.

Depending on the hardware available, you can now use your microphone to talk to the Guest user, and if **Video** is enabled by the Guest user, you can also see each other in the dialog box.

Use the slide bars on the right to control sound and video.

Only the Guest can end the audio-video chat session.

NOTE: Each Guest and each Host can run only one audio session including **Transfer Sound** at a time.

See also

[Guest Access Security](#)
[Program Options](#) (Audio-Video Chat tab)

3.4 End a remote control session from a Host computer

If your computer is being remote controlled and you feel that you do not want to continue the session for whatever reason, you can end the session from the Host.

To end a remote control session from the Host

Click the  **Disconnect** button on the toolbar.

Alternatively, on the **Session** menu in the **Host** window, select **Disconnect**.

If the Host is minimized and only visible as an icon  in the notification area in the lower right corner of the screen, you can end the remote control session by right-clicking the icon and selecting **Disconnect**.

4 Providing remote support

4.1 Set up Help Request on Guest and Host

If you offer help services, the **Help Request** function should be set up on both Guest and Host before Host users can request help from your help service.

You also need to specify the communication profile or profiles to be used.

▣ Set up the Help Request function on the Guest

1. On the **Tools** menu, select **Program Options**.
2. Click the **Help Request** tab.
3. Select the **Enable Help Request** check box.
4. On the **Help Service** tab, select the **Enable Help Service** check box.

In one of the **Help Service** fields below, specify the name of your help service. You may have more than one help service.

▣ Setup use of tickets

If you have an extended Guest, you see two more sub-tabs on the **Help Request** tab.

Service Tickets tab

The **Service Tickets** tab enables an extended Guest to service help requests by a service ticket number. Service tickets are used for Netop Remote Control and Netop OnDemand Remote Control (1.74 and earlier versions).

1. Select the **Enable Service Tickets** check box to enable use of service tickets to service help requests by a service ticket number.
2. In the **Service Ticket Format** field enter a service ticket format using any character plus the control characters #, @, and *.

produces a number (0-9), @ produces a letter (A-Z), and * produces a number or a letter (0-9, A-Z), for example @##-****. On the **Help Request** tab in the **Guest** window, this generates service tickets that look like this: JK50-M3SR.

NOTE: The service ticket generated from this can only be used once, after which a new ticket will be generated.

3. In the **Number of auto generated Service Tickets** field specify the number (0-3, 0 = manually) of service tickets to be auto-generated.

WebConnect tab

The **WebConnect** tab enables an extended Guest to service help requests by a WebConnect ticket. WebConnect tickets are used for Netop OnDemand Remote Control 2.0 and later versions.

1. Select the **Enable WebConnect tickets** check box to enable use of WebConnect tickets.
2. In the **WebConnect Ticket** field enter anything that you want to use as a WebConnect ticket for identification purposes during a help request session using WebConnect, for example an email address, a name, or a keyword, for example Security Server.
3. Select a communication profile in the **WebConnect Communication Profile** list.

The WebConnect communication profile contains the credentials and the Connection Manager URL to be used for the WebConnect connection.

The profile itself should be defined in the Setup Wizard or in **Program Options > Communication Profiles** before you can select it here. One or more WebConnect profiles

can be defined in **Communication Profiles**.

4. In the **Update interval** field, specify how often the Netop Guest should communicate with WebConnect and check for new tickets. Specify an interval in seconds.
5. Click **OK** to close the **Program Options** dialog box.

☐ **Set up the Help Request function on the Host**

1. On the **Tools** menu, select **Program Options**.
2. Click the **Help Request** tab.
3. In the **Help provider** field, enter the name of a help service provider.
4. Specify the communication profile that should be used for the connection.

Select one of these options:

Use current Host communication profiles

Select this option to send help requests using communication profiles enabled in **Tools > Communication Profiles**.

If you have enabled more than one communication profile, or if you have enabled only communication profiles using networking communication devices, the **Select Help Request Communication Profile** dialog box will be displayed when requesting help.

Select a communication profile.

You can only use TCP/IP, if Guest and Host are on the same network.

If Guest and Host are not on the same network, select for example LAN (TCP) or Internet (TCP). You must then also specify the Guest IP address.

Use specific Communication Profile

Select this option to use a specific communication profile. Select one of the available Host communication profiles in the drop-down list.

You can only use TCP/IP, if Guest and Host are on the same network.

If Guest and Host are not on the same network, select for example LAN (TCP) or Internet (TCP). You must then also specify the Guest IP address.

You can specify the IP address at this point in the **Advanced Help Request Options**, if you prefer. Otherwise, the Host user will be prompted for the IP address when requesting help. The latter allows the Host user to specify different addresses and thereby contact different supporters when requesting help.

Advanced Help Request Options

1. Click the **Advanced** button.
The **Advanced Help Request Options** dialog box is displayed.
2. In the **Phone number or IP address** field enter the IP address of the Guest.
You can also change the **Help request timeout if not answered** setting, if necessary.
3. If requesting help through a Guest network Netop Gateway,

you can specify the gateway logon credentials in the **Gateway logon** section. Otherwise the Host user will be prompted to enter these when requesting help.

Select the **Use current logon credentials for Windows Security authentication** check box, if the Host user should log on using the name, password and domain that the user used to log on to Windows on the Host computer.

5. Select the **Enable Help Service** check box.

4.2 Respond to a help request

If you are using service tickets (extended Guest for Remote Control OnDemand 1.74 and earlier versions) for help requests, you must first pass on a service ticket to the Host user by phone or e-mail.

You find the service ticket on the Guest **Help Request** tab. The service ticket can only be used once, after which a new ticket will be generated. The Host user then uses the service ticket to send a help request to you.

If you are using WebConnect tickets (extended Guest for Remote Control OnDemand 2.0 and later versions), you do not need to do anything.

The WebConnect ticket can either be predefined in the OnDemand Host or the Host user can enter anything, for example a name or a keyword in the OnDemand Host.

All incoming help requests are displayed on the Guest **Help Request** tab.

Double-click a help request on the list to start a default session, which is typically remote control.

Alternatively, select a help request and click a button on the toolbar to start a remote control session or another type of session.

You will be prompted to log on to the Host.

Once you have logged on to the Host, you can start helping the Host user using the available remote control functions, and you can communicate with the Host user using for example chat.

NOTE: To be able to service help requests you must first set up communication profiles and **Help Request** options on both Guest and Host. See [Set up Help Request on Guest and Host](#).

4.3 Run a multi Guest session

If allowed on the **General** tab of the Host **Program Options**, multiple Guests can connect to the same Host in a multi Guest session.

For example, if you need help from another supporter while providing support to a Host user, other Guests can join your session by connecting to the same Host.

In a multi Guest remote control session, one Guest at a time can have keyboard and mouse control. The Guest that has keyboard and mouse control can execute all actions allowed to it by the **Guest Access Security** settings on the Host.

Guests that do not have keyboard and mouse control can execute only a limited range of actions.

The **Host** window title bar displays the name of the Guest that has keyboard and mouse control. Other connected Guests are indicated by `+<Number of other connected Guests>`.

Example: Connected [User1]+1

Guests that the **Guest Access Security** settings allow to act as multi Guest session administrator can manage a multi Guest session. This means that these Guests can:

- Show a connection list of connected Guests

- Suspend further connections
- Disconnect all other Guests
- Start a multi chat session with all connected Guests and the Host.

Guests that do not have the right to act as multi Guest session administrator cannot carry out these actions.

See also



[Communicate with Host users](#)
[Guest Access Security](#)

4.4 Send special keystrokes

During remote control you can send various keystroke combinations to the Host computer using the **Send Keystrokes** command on the title bar menu of the **Remote Control** window.

You also find the most commonly used commands as toolbar buttons in the **Remote Control** window.

CAUTION! Using these keystroke combinations from the keyboard can have undesired effects.

Keystroke combination	Description
Send Ctrl+Esc	<p>Select this command to send the keystroke combination CTRL+ESC to the Host.</p> <p>Alternatively, click the  Send Ctrl+Esc button on the toolbar.</p> <p>This keystroke combination displays the Start menu on a Windows Host computer or the Window List on an OS/2 Host computer.</p>
Send Ctrl+Alt+Del	<p>Select this command to send the keystroke combination CTRL+ALT+DEL to the Host.</p> <p>Alternatively, click the  Send Ctrl+Alt+Del button on the toolbar.</p> <p>This keystroke combination displays the security dialog box on a Windows 2000/XP/2003/2008/Vista/7 Host computer or restarts an OS/2 Host computer.</p> <p>NOTE: Send Ctrl+Alt+Del is disabled with a Windows ME, 98 or 95 Host computer. Select Restart Host PC to restart the Host computer.</p>
Send Alt+Tab	<p>Select this command to send the keystroke combination ALT+TAB to the Host.</p> <p>This keystroke combination switches the active window clockwise on the Host computer screen.</p>
Send Alt+Shift+Tab	<p>Select this command to send the keystroke combination ALT+SHIFT+TAB to the Host.</p> <p>This keystroke combination switches the active window counter-clockwise on the Host computer screen.</p>
Send Print Screen	<p>Select this command to send a PRINT SCREEN command to the Host.</p>





Keystroke combination	Description
	This copies an image of the entire Host computer screen to the Host computer clipboard.
Send Alt+Print Screen	Select this command to send an ALT+PRINT SCREEN command to the Host. This copies an image of the active window on the Host computer screen to the Host computer clipboard.

NOTE: The **Send Keystrokes** command will be disabled if the **Guest Access Security** settings on the Host do not allow use of keyboard and mouse.

4.5 Use clipboard commands

During remote control you can use the clipboard.

You access the clipboard commands from the **Clipboard** command on the title bar menu of the **Remote Control** window. You also find these commands as toolbar buttons in the **Remote Control** window.

Command	Description
Send to Host	Select this command to send the Guest computer clipboard content to the Host computer clipboard. Alternatively, click the  Send Clipboard button on the toolbar. NOTE: This command is disabled if the Guest Access Security settings on the Host do not allow Transfer clipboard .
Retrieve from Host	Select this command to retrieve the Host computer clipboard content to the Guest computer clipboard. Alternatively, click the  Retrieve from Host button on the toolbar. NOTE: This command is disabled if the Guest Access Security settings on the Host do not allow Transfer clipboard .
Save Screen to Clipboard	Select this command to capture the Host computer screen image to the Guest computer clipboard. Alternatively, click the  Save Screen to Clipboard button on the toolbar.
Save Screen to File	Select this command to capture the Host computer screen image and save it as a bitmap file with the name <code><Host name>-<Date>-<Time>.bmp</code> in the <code>SnapShot</code> folder. You can change the file name and folder before saving. Alternatively, click the  Save Screen to File button on the toolbar.


4.6 Communicate with Host users

Netop Remote Control offers a number of ways in which you can communicate with Host users while providing remote support.

If allowed by the **Guest Access Security** settings on the Host, the Guest can start a chat or an audio-video chat with a Host, or the Guest can send a message to the Host.

Chat

To start a chat, when already connected to a Host

1. In the **Remote Control** window, click the  **Chat** button on the toolbar.
2. In the **Chat** dialog box, type your message.
3. Click **Send**.

To start a chat, if not already connected to a Host

1. In the **Guest** window, select the Host that you want to chat with.
2. Click the **Chat** button on the toolbar.
Alternatively, select **Chat** on the **Connection** menu.
3. In the **Chat** dialog box, type your message.
4. Click **Send**.


The Host user can reply, and the chat session remains open until either you or the Host user close it by clicking **End chat**.

A Host can also request a chat with the Guest.

NOTE: You can save the chat as an `rtf` file for documentation purposes.

Multi chat

If the Netop Host allows multiple simultaneous Guest connections, a Guest that the Guest Access Security settings allow to act as multi Guest session administrator can start a multi chat with the Host and all connected Guests. See [Run a multi Guest Session](#).


A  **Start Multi Chat** button will be displayed on the toolbar in the **Remote Control** window of the Guest that is multi Guest session administrator. Click this button to start a chat with the Host and all other connected Guests at the same time.

Audio-video chat

The Guest can start an audio-video chat session with a Host, provided that audio-video equipment has been installed on both sides.

Also the Host can request an audio-video chat session with the Guest, if they are already connected.

To start an audio-video chat, when already connected to a Host

In the **Remote Control** window, click the  **Audio-Video Chat** button on the toolbar.
The **Audio-Video Chat** dialog box will be displayed.

To start an audio-video chat, if *not* already connected to a Host

1. In the **Guest** window, select the Host that you want to chat with.


2. Click the **Audio-Video Chat** button on the toolbar.

Alternatively, select **Audio-Video Chat** on the **Connection** menu.

The **Audio-Video Chat** dialog box will be displayed.

Depending on the hardware available, you can now use your microphone to talk to the Host user, and if **Video** has been enabled, you can also see each other in the dialog box.



Use the toolbar buttons at the top and the slide bars on the right to control sound and video.

Only the Guest can end the audio-video chat session--by clicking the  **Stop Audio-Video Chat** button on the toolbar.

NOTE: Each Guest and each Host can run only one audio session including **Transfer Sound** at a time.

Message

To send a message to a Host, when already connected

1. In the **Remote Control** window, click the  **Send Message** button on the toolbar.
2. Type the text you want to send and click the  **Send Message** button on the toolbar.

To send a message to a Host, if *not* already connected

1. Select the Host that you want to send a message to.
2. Click the **Send Message** button on the toolbar.
Alternatively, select **Send Message** on the **Connection** menu.
3. Type the text you want to send and click the **Send Message** button on the toolbar.

The message is displayed on the Host computer. The Host user cannot reply or send new a message. If you want the Host user to reply, use one of the chat options.

[Guest Access Security Program Options](#) (Audio-Video Chat tab)

4.7 Send or receive print jobs

You can send a Guest computer print job to a Host computer printer (remote printer). Host users can likewise send a print job to a Guest computer printer.

A Netop printer and the correct remote printing device driver must be installed on the computer sending the print job.

To add a Netop printer on the Guest computer

1. On the **Tools** menu, select **Options**.
2. Click the **Remote Printing** tab.
3. Click the **Add printer** button.
The **Add printer guidelines** window is displayed.
4. Read the guidelines and click **Ready** to start adding a Netop printer using the **Add Printer Wizard**.

The **Add printer guidelines** window remains on the screen while you go through the wizard.

Send a print job to a remote printer

Once you have added a Netop printer on the Guest computer, you can send a print job to the remote printer in question.

Example: If you want to print a Word document on the remote printer, activate the print job as you normally would in Word. Make sure that you choose the Netop printer that you added.

4.7.1 Redirect a print job

You can redirect a print job sent from the Host computer to the Guest computer to any printer specified on the Guest computer.

To redirect a print job

1. On the **Tools** menu, select **Options**.
2. Click the **Remote Printing** tab.
3. In the **Redirect print to** section, select one of these options:


Option	Description
Default printer	Redirect the print job to the default Guest computer printer.
Prompt with a list of available printers	Select this option and click Browse to display the Select Print Redirection Printer dialog box. The dialog box contains the names of Guest computer printers. Select a name and click OK to specify the printer name in the field. Incoming Netop print jobs will then be redirected to this printer.

4.8 Share your screen

When providing support you might want to demonstrate a procedure to a Host user.

If allowed by the **Guest Access Security** settings on the Host, you can start a demonstrate session with a Host. This enables you to display the Guest computer screen image on the Host computer while you are carrying out a particular procedure.

To start a demonstrate session

- When already connected, in the **Remote Control** window, click the  **Demonstrate** button on the toolbar.
- If you are not already connected, you can connect and run a demonstrate session from the **Phonebook** tab, the **Quick Connect** tab, or the **History** tab.
 1. On one of the these tabs, select the Host computer that you want to connect to and and run a demonstrate session with.
 2. Then click the **Demonstrate** button on the toolbar in the **Guest** window.

When you start the demonstrate session, and before anything is displayed on the Host computer, the **Mask Windows** dialog box is displayed. This dialog box enables you to mask Guest computer screen elements that you do not want the Host user to see. These elements will be displayed as black rectangles in the Host computer screen.

To mask/unmask a screen element

1. Select the element in the pane.
2. Click the **+** (plus) or **-** (minus) button at the bottom of the dialog box to mask or unmask the

element.

Select the **New screen window warning** check box to have the **New window** dialog box displayed if a new screen element that does not belong to a masked application element opens on the Guest computer screen.

Select what you want to mask.

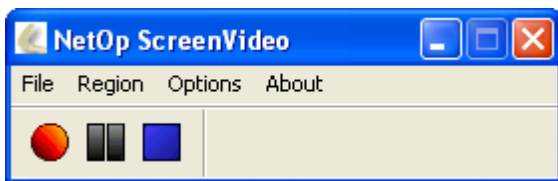
3. Click **OK**.

The **Netop Demonstration** window is displayed on the selected Host computer screen.

During a demonstrate session, a small toolbox is displayed on the Guest computer screen. It allows you to stop the demonstration or display the **Mask windows** dialog box, if you want to make changes to the masking.

4.9 Netop Screen Video

Netop Screen Video is a tool for recording the actions you take and the commands you click.



To start Netop Screen Video

On the Windows **Start** menu, point to **All Programs**, **Netop Remote Control**, **Tools** and then click **Screen Video**.

Use the tool to create a video within an area of the screen or of the entire screen.

To capture a screen video

1. Set up the tool according to your preferences.

On the **Region** menu, select the area you want to capture.

TIP: Typically **Full Screen** is selected.

On the **Options** menu, select recording options and define settings.

TIP: It is often a good idea to hide the program when recording starts, and to define keyboard shortcut keys to start and stop the recording.

These settings are saved and can be used the next time you want to capture a screen video.

2. Click **Record** to start recording.

Click the appropriate commands to demonstrate the task you want to record.

3. Stop recording by pressing the shortcut key you defined.

Alternatively, you can right-click the **Netop Screen Video** icon in the notification area and click **Stop** on the shortcut menu.

☐ Overview of the Options menu

Option	Description
Video Options	Change the encoder to be used for the video recording. For the configurable

	<p>encoders, click Configure to set for example compression.</p> <p>Move the Quality slider to the right to increase quality. Note that a higher quality video file will be larger.</p> <p>You can let Netop Screen Video automatically adjust frame rates: Leave the Auto Adjust check box selected.</p> <p>Or you can clear the Auto Adjust check box and set the options yourself:</p> <p>Max frame rate left end represents recording 200 frames/second and Max frame rate right end represents recording 1 frame/minute. When you move the slider, the Set Key Frames Every, Capture Frames Every and Playback Rate fields are automatically adjusted:</p> <table border="1"> <thead> <tr> <th>Recording frame rate</th> <th>Set Key Frames Every</th> <th>Capture Frame Every</th> <th>Playback Rate</th> </tr> </thead> <tbody> <tr> <td>200 - 1 frames/second</td> <td>Second</td> <td>0.005 - 1 second</td> <td>Recording frame rate</td> </tr> <tr> <td>60 - 1 frames/minute</td> <td>20 frames</td> <td>1 - 60 seconds</td> <td>20 frames/second</td> </tr> </tbody> </table> <p>NOTE: Playback will synchronize at each key frame. A large number of frames will make a large file.</p>	Recording frame rate	Set Key Frames Every	Capture Frame Every	Playback Rate	200 - 1 frames/second	Second	0.005 - 1 second	Recording frame rate	60 - 1 frames/minute	20 frames	1 - 60 seconds	20 frames/second
Recording frame rate	Set Key Frames Every	Capture Frame Every	Playback Rate										
200 - 1 frames/second	Second	0.005 - 1 second	Recording frame rate										
60 - 1 frames/minute	20 frames	1 - 60 seconds	20 frames/second										
Cursor Options	Define whether the mouse pointer should be included in the recording, and define the pointer appearance.												
Audio Options	Define options for recording sound as well as video.												
Autopan Speed	<p>Setting autopan speed is relevant when Enable Autopan has been selected (command above in the same menu). Automatic panning means that the recording region center is automatically moved towards the mouse pointer position while recording. When Enable Autopan is not selected, the recording region center does not move.</p> <p>Autopan Speed defines how fast the recording region center is moved.</p>												
Recording Thread Priority	<p>Recording Thread Priority means that a priority is set for use of computer resources for Netop Screen Video as compared to other program running at the same time.</p> <p>General guideline: If the video recording does not play smoothly, computer resources may be too scarce and it might help to raise the Recording Thread Priority.</p>												
Keyboard Shortcuts	Define keyboard keys to control the recording.												

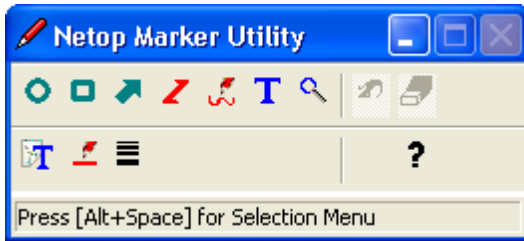
4.10 Netop Marker Utility

Use the Netop Marker Utility to draw and write or magnify something on the Host computer screen during a remote control session.


The tool can be used by both the Guest computer and the Host computer. Note, though, that the Host user cannot initiate this feature. It only opens if the Host is remote controlled and the Guest user decides to start the Marker Utility.

The texts and lines created using the Netop Marker Utility 'float' over the desktop. If other applications are opened, texts and lines remain on top.

The Netop Marker Utility includes tools for drawing shapes like circles and rectangles and for writing text or magnifying a part of the screen.



To start the Netop Marker Utility from the Netop Guest

1. Connect to the Host.
2. In the **Remote Control** window, click the  **Marker Mode** button on the toolbar.

The Netop Marker Utility opens and you can start using the tools. Place the mouse pointer on a toolbar button for a description of the tool.

To close the Netop Marker Utility from the Guest

In the **Remote Control** window, click the **Marker Mode** button on the toolbar.

Alternatively, on the title bar menu of the **Remote Control** window, select the **Marker Mode** command.

5 Dialog box help

5.1 Guest dialog boxes

5.1.1 Advanced audio settings

Use the **Advanced audio settings** dialog box to specify preferred audio playback and recording devices to be used in connection with audio-video chat.

Playback

The **Preferred device** drop-down list contains the names of audio playback devices found by Windows. Select your preferred audio playback device in the list.

Record

The **Preferred device** drop-down list contains the names of audio recording devices found by Windows. Select your preferred audio recording device in the list.

NOTE: If multimedia devices are connected to the computer, the <Use any available device> selection may select a connected device instead of the computer sound system. In that case, select the computer sound system.

Audio Compression

The **Try audio compression codecs in the following order** pane contains a Windows prioritized list of mono audio compression codecs available on the Guest computer.

Use the **Up/Down** buttons to move a codec up or down in the prioritized list. You can restore the default codec priority by clicking the **Use defaults** button.

The highest prioritized Guest computer codec that is also available on the Host computer will be used.

See also

[Program Options](#) (Audio-Video Chat tab)

5.1.2 Advanced Help Service

Use the **Advanced Help Service** dialog box to specify actions to be executed when a help request arrives.

Option	Description
Action	<p>Select an action in the list.</p> <p>The list contains the following options:</p> <ul style="list-style-type: none"> • None: No action. • Send message: Run a local program if specified and send a message to the Host. The fields below are enabled. • Run local program: Run a local program if specified. The fields below, except Send message, are enabled.
Command line	<p>Specify the command line of a Guest computer program, typically a helpdesk program to register the help request. Click [...] to select a program file.</p> <p>You can add the following arguments to the command:</p>

Option	Description
	<ul style="list-style-type: none"> • %H: Help request Host name. • %T: Help request time. • %P: Help request problem description.
Timeout	Specify a number of seconds (default: 5, range 0-9999, 0 = no timeout). The command specified above times out (cancels if unsuccessful) after the specified number of seconds.
Send message	Specify the path and name of an .rtf file to send a message with the .rtf file content to the Host requesting help. See also Communicate with Host users (Message). Click [...] to open an .rtf file.
Clear help request	Select this check box to delete the help request record in the Help Request tab when the actions specified above have been executed successfully. NOTE: Deleting the Help Request tab record will not cancel the help request.
Display a notification message when new help request arrives	Select this check box to be notified when a help request arrives. The notification message contains the help request Host name, time and, if specified, problem description.

See also

[Set up Help Request on Guest and Host](#)
[Respond to a help request](#)
[Program Options](#) (Help Request tab)

5.1.3 Advanced inventory option

Use the **Advanced inventory option** dialog box to specify inventory processing and custom inventory items.

Run program after inventory scan

You can specify an inventory processing program to automatically process each newly retrieved Host computer inventory. Select one of these options:

Option	Description
Disable	Disable running the program specified below.
Run for each Host	Run the program specified below when a Host computer inventory has been retrieved.
Run after all scans have completed	Run the program file specified below when a batch of Host computer inventories has been retrieved.
File name	Specify an inventory processing program file path and name including required command line switches. Click the Browse button to open an inventory processing program file.

Option	Description
	The path and name of the file will be displayed in the field.

Custom inventory items

Click the **Add** button to add custom inventory items. The **Custom Inventory Items** dialog box is displayed. See [Custom Inventory Items](#).

Click the **Edit** button if you want to edit a custom inventory item after adding it.

When you generate Host inventories, the inventories will contain the custom inventory item that you defined.

See also

[Program Options](#) (Inventory tab)

5.1.4 Advanced TCP/IP Configuration

Use the **Advanced TCP/IP Configuration** dialog box to set advanced options for the TCP/IP communication profile.

Bindings

Option	Description
Use all available IP addresses	Select this check box to use all available IP addresses. If the computer has multiple IP addresses and only one of them is to be used for Netop communication, clear the check box to enable the IP address field or interface list.
IP address	Specify the IP address that is to be used for Netop communication.
Use an interface	Specify which network interface is to be used for Netop communication.

Specify Port Numbers

Option	Description
Use default port numbers	Select this check box to use the default Netop port number 6502 for Receive port and Send port . Port number 1970 is officially registered to Netop Remote Control. However, port number 6502 is the preferred default port number for compatibility with older Netop versions.
Receive port	If the Use default port numbers check box is selected, the port number 6502 is displayed. If the Use default port numbers check box is not selected, the number is editable. You can specify a number in the range 1025-65535.
Send port	If the Use default port numbers check box is selected, the number 6502 is displayed.

Option	Description
	<p>If the Use default port numbers check box is not selected, the number is editable. You can specify a number in the range 1025-65535.</p> <p>The Send port number of the source module should correspond to the Receive port number of the destination module.</p>

Options

Select the **Use TCP for session if possible** check box to connect by TCP/IP, but if available on Guest and Host, switch to TCP/IP (TCP) when connected for high speed session communication.

Netop Name Server

Option	Description
Use Netop Name Server	<p>Select this check box to use Netop Name Server to resolve Netop names into IP addresses.</p> <p>Using Netop Name Server will facilitate connecting across segmented IP networks including the Internet.</p>
Primary	Use 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.
Secondary	Use 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.
Ignore port information from Name Server	<p>Select this check box to replace the destination module Receive port number received from Netop Name Server by the port number specified below.</p> <p>NOTE: Some types of firewalls replace sent Receive port numbers by invalid port numbers to protect network computers against connection attempts. In that case, Netop Name Server will receive, store and return invalid Receive port numbers, which must be replaced by valid Receive port numbers.</p>
Use Port	<p>Specify the port number that should replace the Receive port number received from the Netop Name Server.</p> <p>NOTE: To use Netop Name Server, specify the applicable Name Space ID under Tools > Program Options > Host Name > Netop Name Server.</p>

See also

[Communication Profile Edit](#)

5.1.5 Advanced Video

Use the **Advanced Video** dialog box to set advanced video options.

Select the driver to use for video in the drop-down list. If a video camera is installed, the field will contain its driver name, and the image frame will display the image captured by the camera.

Click the **Format** button to display the Windows **Video Format** dialog box and format the video

capture image.

Click the **Properties** button to display the Windows **Video Source** dialog box and change video source properties.

To disable video data compression, select the **Disable compression** check box.

5.1.6 Communication Profile Edit

Use the **Communication Profile Edit** dialog box to create or edit a communication profile.

Communication information

Option	Description
Description of communication profile	<p>Enter a communication profile name. The name should be unique.</p> <p>If the field already contains a communication profile name, you can edit the field contents.</p> <p>NOTE: You can create multiple differently named communication profiles that use the same communication device.</p>
Communication device	<p>Specify the name of the communication device to be used by the communication profile.</p> <p>Select a communication device on the drop-down list.</p>
Use dial-up networking	<p>This check box will be enabled only if a TCP/IP family communication device is selected in the Communication device field.</p> <p>Select the check box to expand the Communication Profile Edit dialog box with a Dial-up network connection section.</p>

Dial-Up Network Connection

Option	Description
Dial-up network profile	On the list of available dial-up network profiles, select a profile to use to connect to a network.
Dialing from Calling card	The dialing properties of the selected dial-up network profile will be displayed here.
Configure	Click this button to display the Dial-up Connection dialog box and configure the dial-up connection.
Dialing properties	Click this button to display the Phone and Modem Options dialog box and edit the dialing properties of the selected dial-up network profile.
Add profile	Click this button to display the Network Connection Wizard , which helps you add a dial-up network profile.

[Communication profile name]

The lower dialog box section is named according to the communication device displayed in the **Communication device** field.

In this section, you can specify the configuration of the communication device that should apply to the communication profile. The options vary depending on the communication device.

For further information about the most commonly used communication devices see the list below.

☐ TCP/IP

Max packet size (MTU)	Specify the maximum packet size (range 512- 5146, default: 2600). A high MTU will increase communication speed and a low MTU may contribute to solving communication problems.
Optimize for Internet communication	Select this check box to apply settings (MTU, data compression, etc.) optimized for communicating across the Internet.
Advanced	Click this button to display the Advanced TCP/IP Configuration dialog box. See Advanced TCP/IP Configuration .
IP Broadcast list	Click this button to display the IP Broadcast List dialog box. See IP Broadcast List .

General information about Netop TCP/IP

Netop TCP/IP is a *UDP* based communication device that connects by UDP and optionally communicate by TCP/IP (TCP) during a session.

Each communication profile that uses TCP/IP can support multiple Netop connections.

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 port number must match the destination module port number, see [Advanced TCP/IP Configuration](#).

If you connect from outside a network protected by a network address translation (NAT) firewall or proxy server to a Netop module on a network computer, specify the firewall or proxy server public IP address with the port number assigned to the network computer, for example 192.168.20.51:1234.

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. The following name response options are available:

- If a Guest connects or browses using the Host name qualifier H:;, the Host can respond by its enabled Netop Name type name.
- If a Guest connects or browses using the Host name qualifier U:;, the Host can respond by its enabled LAN User type name.
- If a Host requests help, the Guest can respond by its enabled Help service names.

NOTE: A broadcast will reach only computers on the local network segment and computers whose IP address or DNS name is specified in the communication profile **IP Broadcast List**.

Name resolution

Name resolution will resolve a specified name into its corresponding IP address. These name resolution options are available:

- In the **Advanced TCP/IP Configuration** dialog box, select the **Use Netop Name Server** check box and specify the Netop Name Servers to be used.

Under **Program Options > Host Name > Netop Name Server**, specify the **Name Space 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.

Netop Name Server will resolve the name into the corresponding IP address and connect by it across segmented IP networks including the Internet. You can also browse for Hosts using Netop Name Server.

- If a Guest connects by a name using the Host name qualifier DNS::, a domain name server will interpret the name as a DNS name and attempt to resolve it into a corresponding IP address, so the Guest can connect by it across segmented IP networks, including the Internet.

NOTE: In most cases, if the Host name qualifier H:: is used, a domain name server will interpret the name as a DNS name and attempt to resolve it into a corresponding IP address.

- If a Guest connects by a name using the Host name qualifier LDAP::, the Guest will search directory services specified on the **Directory Services** tab in the **Program Options** dialog box for a user with this name and connect by the corresponding address attribute, which is typically an IP address.

You can also browse for Hosts using directory services.

See also

[Program Options](#) (Host Name tab)

Connect problems

In case of connect problems, you should first verify that an IP connection is available by from a command prompt by typing:

```
PING <Netop module IP address>
```

The PING utility will send four data packets requesting a reply. If you receive replies, an IP connection is available.

If an IP connection is available and connectivity problems persist, consult your network/system administrator or submit a support request to Netop Support.

☐ TCP/IP (TCP)

Option	Description
Optimize for Internet communication	Select this check box to apply settings (MTU, data compression, etc.) optimized for communicating across the Internet.
Encapsulate in HTTP	Select this check box to wrap data packets as HTTP packets to ease firewall passage. This is also known as HTTP-tunneling.
Use Proxy Settings	If you select Encapsulate in HTTP , the Use Proxy Settings check box will become available for selection.

Option	Description
	If you select this check box, proxy authentication is activated in the used communication profile. The application will use the proxy settings defined in Windows.
Advanced	Click this button to display the Advanced TCP/IP Configuration dialog box. See Advanced TCP/IP Configuration .

Netop TCP/IP (TCP) is a TCP based communication device.

Each communication profile that uses TCP/IP (TCP) can support one Netop connection. To support multiple Netop connections, you can create multiple communication profiles that use TCP/IP (TCP).

To connect, specify a computer IP address.

If you connect from outside a network protected by a network address translation (NAT) firewall or proxy server to a Netop module on a network computer, specify the firewall or proxy server public IP address with the port number assigned to the network computer, for example 192.168.20.51:1234.

Ask the firewall or proxy server administrator which port number is assigned to a specific network computer.

- If a Guest connects directly to a Host, specify the Host computer IP address.
- If a Guest connects through a remote network Netop Gateway to a Host, specify the IP address of the gateway computer and optionally the Host name.
- If a Host requests help, a Guest connected to directly or on a remote Netop Gateway network can respond by its enabled Help service names.

TCP/IP (TCP IPv6)

Option	Description
Optimize for Internet communication	Check this box to apply settings (MTU, data compression, etc.) optimized for communicating across the Internet.
Advanced	Click this button to display the Advanced TCP/IP Configuration dialog box. See Advanced TCP/IP Configuration .

Netop TCP/IP (TCP IPv6) is a TCP IPv6 based communication device.

Each communication profile that uses TCP/IP (TCP IPv6) can support one Netop connection. To support multiple Netop connections, you can create multiple communication profiles that use TCP/IP (TCP IPv6).

You can use TCP/IP (TCP IPv6) only between computers connected to an IPv6 network.

To connect, specify a computer IPv6 address.

- If a Guest connects directly to a Host, specify the Host computer IPv6 address.
- If a Guest connects through a remote network Netop Gateway to a Host, specify the Gateway computer IPv6 address and optionally the Host name.
- If a Host requests help, a Guest connected to directly or on a remote Netop Gateway network can respond by its enabled Help service names.

WebConnect

Option	Description
Address	Specify the URL of the WebConnect / WebConnect 3 service, i.e. the Connection Manager, that facilitates the WebConnect / WebConnect 3 connection.
Account	Specify a WebConnect / WebConnect 3 service recognized account.
Password	Specify the password corresponding to the WebConnect / WebConnect 3 service recognized account
Domain	Specify the domain corresponding to the WebConnect /WebConnect 3 service recognized account.
Optimize for Internet communication	Select this check box to apply settings (MTU, data compression, etc.) optimized for communicating across the Internet.
Advanced	Click this button to display the Advanced TCP/IP Configuration dialog box. See Advanced TCP/IP Configuration .
Test	Click the Test button to verify the WebConnect Service URL.

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.

NOTE: WebConnect 3 service has improved security; therefore, we strongly recommend you to use it.

Netop Portal

Option	Description
Address	Specify the address of the Netop Portal: portal.netop.com .
Username	Specify the Netop Portal username.
Password	Specify the Netop Portal password.
Live Update	Select this check box to see the available hosts in real-time.
Test	Click the Test button to verify the Netop Portal address and credentials.

Netop Portal is a service which that provides connectivity across the internet. It does not require direct visibility between end points.

To remote control a Host using the Netop Portal authentication and authorization you need to:

1. Make sure that you have a Netop Portal account. Get credentials from your account administrator.
2. On the Host create a Netop Portal communication profile using the credentials you received from the account administrator.
3. On the Guest select the Netop Portal communication profile, select the Host and click the

Connect button. You will be prompted to enter the Host credentials

Gateway

Option	Description
Access Gateway via communication profile	<p>In the drop-down list, select the communication profile that should be used to access the local network Netop Gateway.</p> <p>Select <Any initialized communication> to connect to or browse for Gateway device groups using any enabled communication profile that uses a networking communication device.</p> <p>Select another communication profile to connect or browse using only that communication profile, which does not need to be enabled.</p> <p>Select Terminal Server only if your Netop module is located on a terminal server client.</p>
Gateway device group	<p>Gateway device groups are administrator specified names of available outgoing communication on local network Netop Gateways.</p> <p>Select one of these options:</p> <p>Use device group: Select this option to specify a Gateway device group name in the field.</p> <p>Browse for device groups: Select this option to display the Gateway Device Group List dialog box when connecting.</p>

Gateway is a Netop proprietary communication device that enables a network Netop module to connect through a local network Netop Gateway.

Each communication profile that uses Gateway can support only one Netop connection.

To connect, specify a modem telephone number or computer IP address according to the selected device group type. The device group type is selected in the **Gateway Device Group List** dialog box.

- If a Guest connects through a local network Netop Gateway directly to a Host, specify the modem telephone number or computer IP address of the Host computer.
- If a Guest connects through a local network Netop Gateway through a remote network Netop Gateway to a Host, specify the Gateway computer modem telephone number or computer IP address and optionally the Host name.
- If a Host requests help through a local network Netop Gateway, a Guest connected to directly or on a remote Netop Gateway network can respond by its enabled Help service names.

Resources

To use Gateway, one or multiple outgoing Netop Gateways must run on the local network.

Terminal Server

Terminal Server is a Netop proprietary communication device that enables Netop modules running in a terminal server environment to communicate.

Each communication profile that uses Terminal Server can support multiple Netop connections.

To connect, specify a name by which the destination Netop module can respond:

- If a Guest connects or browses using the Host name qualifier **H:**, the Host can respond by its enabled Netop Name type name.

- If a Guest connects or browses using the Host name qualifier `U: :`, the Host can respond by its enabled LAN User type name.
- If a Host requests help, a Guest can respond by its enabled Help service names.

If Netop Gateway runs on the terminal server console, terminal server Netop modules and Netop modules outside the terminal server environment can connect through it. See the Administrator's Guide.

5.1.7 Communication Profile Setup

For Netop modules to be able to communicate with each other, you need to define a communication profile. A communication profile is a specific configuration of a communication device.

A communication device is a Netop adaptation of a generally available communication protocol or a Netop proprietary communication protocol.

A newly installed Netop module includes default communication profiles. You typically need to modify the default communication profiles or create communication profiles to optimize communication in your environment.

Use the **Communication Profile Setup** dialog box to enable/disable, create, edit and delete communication profiles.

Select check boxes in the **Communication Profile List** to enable communication profiles at Netop module loading.

Click the **New** button to create a communication profile. The **Communication Profile Edit** dialog box is displayed.

If you want to edit a communication profile, select the communication profile and click the **Edit** button. The **Communication Profile Edit** dialog box is displayed.

NOTE: To apply changes to enabled communication profiles, you must reload the Guest.

See also

[Communication Profile Edit](#)

5.1.8 Connect to Host

Use the **Connect to Host** dialog box to add or edit a **Connect** command.

Select how you want to connect in the **Connect using** list:

Option	Description
Phonebook file	Connect to a Host using its Netop phonebook file.
Communication profile	Connect to a Host using a communication profile and a Host name and/or a Host computer telephone number or IP address.
Local	Connect locally to the Guest computer.

The dialog box changes depending on what you select in the **Connect using** list.

- If you select **Phonebook file**, you can specify a phonebook file by browsing for it or entering the path and name of a file in the **Phonebook file** field.
- If you select **Communication profile**, specify the following:

Option	Description
Communication profile	Select a communication profile in the drop-down list which contains available Guest communication profiles.
<Host connect information>	Specify Host connect information in one or two fields according to the communication profile selection above. In a field in which you can specify an IP address, you can also specify an IP address range, e.g. 192.168.1.1-192.168.1.5, to connect to multiple Host computers from one script. In this case the logon information below must be the same for all Hosts that you specify.
Logon name	Specify any logon name required by the Host.
Logon password	Specify the corresponding password.
Logon domain	Specify the corresponding domain or directory server.
Use current logon credentials for Windows Security authentication	Select this check box to log on to the Host by the Windows logon user credentials of the Guest computer user.

- If you select **Local**, no further specification is required.

Click **OK** to add the **Connect** command in the upper pane of the **Script** dialog box.

See also

[Script](#)
[Create and run a script](#)

5.1.8.1 Connection Properties

Use the **Connection Properties** dialog box to set a number of properties to optimize Host connections according to user preferences. The properties are applied individually to Host connections.

Connect tab

Host PC Information

Option	Description
Description	Identifies the Host record. The field may be empty. You can leave it empty to automatically specify the applicable Host name or phone number/IP address in it when creating the Host record. You can edit the field contents.
Phone number/IP address	This field will be included if the communication profile selected in the Communication section uses a point-to-point, gateway, or network point-to-point communication device. Specify the Host telephone number or IP address if connecting directly to the Host, otherwise the telephone number or IP address of the network connecting Netop Gateway for the Host.

Option	Description
Name	<p>If the field label does not include "(optional with Gateway)", specify the name by which the Host should respond.</p> <p>If the field label includes "(optional with Gateway)", you can either leave the field empty to browse for Hosts or specify the name by which the Host should respond.</p>
Comments	Specify a comment to be displayed in the Comment column of the right pane of the Phonebook tab or the History tab.

Communication

Option	Description
Communication profile	Specifies the selected communication profile name. You can change the communication profile name by selecting another communication profile in the drop-down list.
Wake on LAN MAC address	If Wake on LAN has been enabled, you can specify the MAC address of the Host computer network card to be able to start the Host computer by connecting to the Host.

NOTE: The **Connect** tab is only included if you open the **Connection Properties** dialog box from the **Phonebook** tab or the **History** tab.

Logon tab

Use the **Logon** tab to specify Host and Host network connecting Gateway logon credentials in order to connect without being prompted for logon credentials.

Depending on the Guest access method defined on the Host, the credentials need to be defined as follows:

Guest access method	Logon name	Logon password	Logon domain
Default access privileges	Empty	Password	Empty
Netop authentication	Guest ID	Password	Empty
Windows security management*	Domain\Username	Password	Empty
Directory services	Username	Password	Directory Service Name
Netop Portal**	N/a	N/a	N/a
NSS - Windows username & password	Domain\Username	Password	Empty
NSS - Netop Guest ID &	Guest ID	Password	Empty

Guest access method	Logon name	Logon password	Logon domain
Password			
NSS - RSA	N/a	N/a	N/a
NSS - Directory services	Username	Password	Directory Service Name

*When authenticating to a Host configured to use Windows authentication, the domain is now integrated in the username field and is only needed if authenticating to a domain.

The domain field is inferred from the username when a “\” character is provided, otherwise the local computer is assumed. Examples of accepted entries in a username field are:

Username field	Host in a domain	Host NOT in a domain
Domain\username	Login OK	Login Error
Computer\username	Login OK	Login OK
.\username	Login OK	Login OK
\username	Login OK	Login OK
username	Login Error	Login OK

** : If the Guest and Host are version 12.60 or higher and the communication profile used is based on the Netop Portal, the logon credentials will not work.

Select the **Use current logon credentials for Windows Security authentication** check box to log on using the Windows logon user name, password and domain of the Guest computer user.

NOTE: The **Logon** tab is not included if you open the **Connection Properties** dialog box from the Remote Control window.

☐ **Protect Item tab**

Use the **Protect Item** tab to protect a Host record and file with a password.

Password characters will be displayed as asterisks or dots. Leave fields empty to disable password protection.

Select the **Connect without password** checkbox if you want the Guest user to be able to use a phonebook record without knowing the password. The password protection will then only apply to the contents of the connection properties, so that these are protected against being changed unintentionally.

NOTE: The **Protect Item** tab is only included if you open the **Connection Properties** dialog box from the **Phonebook** tab or the **History** tab.

☐ **Startup tab**

Use the **Startup** tab to set startup properties for remote control sessions.

Host window startup size

Option	Description
Windowed	Display the Host screen image in a Remote Control window. If Fit window to Host screen is selected on the Display tab, the window can be resized to its maximized size.
Full screen	Display the Host screen image in full screen to cover the entire Guest computer screen.
Maximized	Display the Host screen image in a maximized Remote Control window covering the entire Guest computer screen except the Windows taskbar.
Minimized	Display the Remote Control window as a button on the Windows taskbar.

Monitors

This section allows you to select which monitors will be displayed before connecting to the Host.

Option	Description
All monitors	Displays all Host monitors. This is the default setting; if you do not select which Host monitor to display, when remote controlling the Host, all Host monitors will be displayed on the screen.
Primary monitor	Displays the Host monitor which is set as the primary monitor.
Monitor: <monitor number>	Displays the selected Host monitor. If the <monitor number> is higher than the number of monitors available on the Host, when remote controlling the Host All monitors will be displayed on the screen.

Remote control window startup size

Option	Description
Enable	Select this check box to enable the elements below and apply their values at startup. Leave unchecked to apply the last displayed Remote Control window position and size.
x	Specify the horizontal offset in pixels of the upper left corner of the Remote Control window from the upper left corner of the Guest computer screen at startup.
y	Specify the vertical offset in pixels of the upper left corner of the Remote Control window from the upper left corner of the Guest computer screen at startup.
Width	Specify the width in pixels of the Remote Control window at startup.

Option	Description
Height	Specify the height in pixels of the Remote Control window at startup.

Actions

Option	Description
Lock Host keyboard and mouse	Select this check box to disable the Host computer keyboard and mouse at startup.
Blank Host display	Select this check box to display a black screen image to the Host user at startup.
Transfer sound	Select this check box to transfer Host computer application sound at startup.
Suspend other Guests from connecting to Host	Select this check box to deny further Guests access to the Host at startup.

NOTE: The **Startup** tab is not included if you open the **Connection Properties** dialog box from the **Remote Control** window.

▣ **Display tab**

Use the **Display** tab to set display properties for the Host screen image.

Host window fit

Option	Description
Fit window to Host screen	<p>Resize the Remote Control window to fit the 1:1 scale Host screen image.</p> <p>If the Host screen image has more pixels than the display area of the maximized Remote Control window, the Remote Control window will have scrollbars.</p>
Fit Host screen to window	Scale the Host screen image to fit within the Remote Control window.
Do not fit	<p>Display the part of the 1:1 scale Host screen image that will fit within the Remote Control window.</p> <p>If the Host screen image has fewer pixels than the display area, black borders will surround it.</p> <p>If the Host screen image has more pixels than the display area, the Remote Control window will have scrollbars.</p>

Limit number of colors in bitmap mode

Option	Description
No, use actual number of colors	Display true colors. Consumes the most transmission bandwidth.
Max 256 colors	Displays reduced palette colors. Consumes less transmission bandwidth.
Max 16 colors	Displays crude colors. Consumes little transmission bandwidth.
Max 2 colors	Displays black and white colors. Consumes a of minimum transmission bandwidth.

DOS Box Font

During remote control, if you start a command prompt window on the Host computer, the command prompt window characters are by default displayed on the Guest computer using the default font of the Guest computer system. You can change the font used.

Clear the **System default** check box to allow selection of another font.

Click the **Select Font** button to select the command prompt window font. The font change is only seen when displaying the command prompt window in full screen.

Skin

On the **Display** tab of the Guest **Connections Properties** you can define how you want the Guest to use skins on connection.

Option	Description
Automatic	Select this option to enable automatic use of skin. The Host device, typically a CE/Mobile device, sends a string ID to the Guest, and the Guest contacts the Skin Repository Server to get the corresponding skin. If the Guest does not find the corresponding skin on the Skin Repository Server a default skin is used.
Do not use skin	Select this option not to use skins for remote control sessions.
Use specific skin model	Select this option, if you want to overrule the Automatic option and use a specific skin model. If you select this option, the Select Model button is activated. Click the Select Model button to open the Skin Models window and select the skin that you want to use. In the List of Models , select the skin and then click OK .
Show as transparent window	The skin will be displayed as a transparent window without frame or background, showing only the device itself (default).

Option	Description
	If you clear the check box, you will see a normal window with frame and a white background behind the device.

See also

[Use a skin to see the Host button](#)
[Program Options](#) (Skins tab)

Keyboard/Mouse tab

Use the **Keyboard/Mouse** tab to set keyboard and mouse control properties for remote control sessions.

Keyboard

Option	Description
Remote keyboard (Send all keystrokes to Host)	Send all Guest computer keystrokes to the Host computer.
Local keyboard (Don't send special keystrokes)	Send Guest computer keystrokes except Send Keystrokes keystroke combinations to the Host computer. Send Send Keystrokes keystroke combinations to the Guest computer.
No keyboard control	Send all Guest computer keystrokes to the Guest computer.
Use Guest keyboard layout	If Guest and Host computer keyboard layouts are different, some Guest computer keystrokes may come out wrong on the Host computer. To avoid this, select the Use Guest keyboard layout check box.
Don't transfer Host Num Lock, Scroll Lock, Insert and Caps Lock	With some display adapters, enabling these Host computer keyboard options may cause the Guest computer keyboard lights to flash. To avoid this, select the Don't transfer Host Num Lock, Scroll Lock, Insert and Caps Lock check box.

Mouse

Option	Description
Remote mouse (send all mouse events)	Send all Guest computer mouse events (clicks, drags and moves) to the Host computer.
Local mouse (Only send clicks and drags)	Send only Guest computer mouse clicks and drags to the Host computer to save transmission bandwidth.
No mouse control	Send no Guest computer mouse events to the Host.
Display Host mouse movements	Move the Guest computer mouse pointer in accordance with Host computer mouse pointer movements.

NOTE: To suppress Guest computer mouse pointer movements induced by the Host computer, press and hold CTRL.

☐ **Compression/Encryption tab**

Use the **Compression/Encryption** tab to set data transmission properties.

Compression level

Netop Remote Control can compress transmitted data to speed up transmission across slow communication links. However, data compression takes time.

Option	Description
Automatic	Selects compression based on the properties of the applied communication profile. In most cases this will provide the fastest transmission.
No compression	Typical selection for fast communication links.
Low	Typical selection for medium fast communication links.
High	Typical selection for slow communication links.

Host screen transfer

Option	Description
Transfer Host screen as commands	Typically faster, but with some Host computer display adapters some Host screen image details may be lost or corrupted.
Transfer Host screen as bitmap	Typically slower, but transfers Host screen image details correctly. When this option is selected the slider below becomes available. The slider has three options that range from better accuracy (Quality) to better performance (Speed). The middle option is a combination of the two. The default option will be set to best quality. Here is how you use the slider: Quality: More accuracy using an enhanced compression algorithm. Center: Less accuracy but better performance using a TurboJPEG high compression ratio of 80. Speed: Much less accuracy but much better performance using a TurboJPEG high compression ratio of 50.

NOTE: This section is disabled if you open the **Connection Properties** dialog box from the **Remote Control** window.

Cache

Command mode Host screen transfer stores the screen image in cache memory and transfers only image changes. This saves transmission bandwidth and optimizes update speed.

The **Cache size** field displays the selected cache memory size. You can select **Automatic** and values from **None** to **10240 kb** on the drop-down list.

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

NOTE: This section is disabled if you open the **Connection Properties** dialog box from the **Remote Control** window.

Total Netop cache memory sharing and size is specified on the **Cache** tab in the **Program Options** window.

Preferred Encryption Type

The field displays the encryption type preferred by the Guest. You can select another encryption type on the drop-down list.

If the preferred encryption type is enabled on both Guest and Host, it will be applied.

If **Netop 6.x/5.x Compatible** is the preferred encryption type and not enabled on both Guest and Host, select a higher encryption level.

If another encryption type is preferred and this encryption type is not enabled on the Host, an encryption type that is enabled on both Guest and Host will be applied.

If no common encryption type is enabled on Guest and Host, enable additional encryption types on the **Encryption** tab in the **Program Options** dialog box to achieve a match.

NOTE: The icon of the encryption type used in a remote control session will be displayed on the status bar.

Desktop tab

Use the **Desktop** tab to specify transfer properties for Host computer desktop features.

Optimize screen transfer

Advanced Host computer desktop features will slow down Host screen transfer in command mode and are typically unimportant to the Guest user. Therefore, Netop Remote Control by default transfers the Host screen image without advanced desktop features.

However, you can change this and select which advanced desktop features to transfer.

Option	Description
Always	Always transfer without advanced desktop features.
Only when high compression	Transfer without advanced desktop features only with high compression, see Compression/Encryption tab.
Never	Never transfer without advanced desktop features.

Optimization parameters

Option	Description
Full optimization	Transfer without the desktop features listed below.
Custom optimization	Select to enable the Custom options section below. You can then clear the selection of specific custom options to enable transfer of these advanced desktop features. Custom options:

Option	Description
	<ul style="list-style-type: none"> • Disable wallpaper • Disable screen saver • Disable animation gimmicks • Disable full window drag • Disable Active Desktop <p>By default, all check boxes are selected.</p>

Record tab

Use the **Record** tab to enable remote control session recording.

Select the **Record remote control session** check box to record a remote control session.

Recording a remote control session will create a record on the **Recordings** tab. You can play back the recording from the **Recordings** tab.

If you select the **Enforce recording** check box on the **Program Options** window **Recording** tab, remote control sessions are recorded regardless of the selection on the **Record** tab.

NOTE: The **Record** section is disabled if you open the **Connection Properties** dialog box from the **Remote Control** window. Recording will reduce remote control session transfer speed.

Custom tab

Use the **Custom** tab to specify the properties of a custom application command.

Option	Description
Description	Specify a custom application name that will be added as a command to the Host record context menu.
Command line	<p>Specify the custom application command line (program file path, name and switches.)</p> <p>Click Browse to open a program file and specify its path and name in the field.</p>

NOTE: The **Custom** tab is only included if you open the **Connection Properties** dialog box from the **Phonebook** tab or the **History** tab.

5.1.9 Inventory

When you add an **Inventory** command to a script, the **Inventory** dialog box is displayed allowing you to specify what should happen to the inventory that is generated.

Option	Description
Inventory step	<p>Select an Inventory step option in the drop-down list:</p> <ul style="list-style-type: none"> • One Step: Generate, retrieve, copy and complete a Host computer inventory. • Generate: Generate inventory on the Host computer.

Option	Description
	<ul style="list-style-type: none"> Retrieve: Save the generated inventory to the %TEMP%\si_out.xml file on the Host computer. NOTE: To make the retrieved inventory available for completion on the Guest computer, it must be copied by a file transfer Copy command from the Host computer to the Guest computer, typically to the %TEMP% directory. Complete: Move a Host computer inventory file copied to the Guest computer to the inventory directory to enable displaying it on the Inventory tab. <p>The inventory directory is located in the Netop configuration files directory, typically C:\Documents and Settings\<user name="">\Application Data\Netop\Netop Remote Control\Guest\inventor.</user></p>
Inventory file path	This field is enabled only if Complete is displayed in the Inventory step field. Specify the Guest computer path and name of the inventory file to be completed.

See also

- [Script](#)
- [Create and run a script](#)
- [Generate a Host inventory](#)

5.1.10 Name Not Found

The **Name Not Found** dialog box advises you on how to overcome connect problems.

Here is some additional advice:

- Verify that communication can physically reach the Host computer:
 If communicating across an IP network, execute this command in a Windows command prompt window:

```
PING <Host computer IP address>
```

 This command sends four data packets to the specified IP address requesting replies. If positive replies are received, communication can physically reach the Host computer. If negative replies are received, check your network setup or consult your network/system administrator.
 If communicating across a modem connection using Windows Modem, the setup of your modem in Windows may not satisfy Netop requirements. Try setting up your modem using Serial instead.
- In the **Host** window, on the **Names** tab, verify that the Host will respond to the specified name or address with the selected communication profile. See [Communication Profile Edit](#) for further information about the characteristics of the communication device used by the selected communication profile.
- Try connecting to other Hosts starting with Hosts close to you. Try using other communication profiles and other Host names or addresses.
- Consult your network/system administrator.
- As a last resort, submit a support request to [Netop Customer & Product Support](#).

5.1.11 Custom Inventory Items

Use the **Custom Inventory Items** dialog box to define additional inventory items that should be retrieved during an inventory scan.

Option	Description
Name	Enter a name for the custom inventory item.
Item type	Select an item type, for example Registry key , and fill in all fields for the selected item type as necessary.

The custom inventory item you created is displayed in the **Custom Inventory Items** pane in the **Advanced inventory option** dialog box.

NOTE: The pane contents are stored in the Netop configuration file `InvCuItm.xml`, which is typically located here: `C:\Documents and Settings\\Application Data\Netop\Netop Remote Control\Guest`.

When you generate Host inventories, the inventories will contain the custom inventory item that you defined.

See also

[Advanced inventory option](#)

[Program Options \(Inventory tab\)](#)

[Process Host computer inventory information](#)

5.1.12 Global Settings

Use the **Global Settings** dialog box to specify the script global settings that should apply as default settings for the subsequent script commands. The dialog box is displayed when you create a script.

To edit the global settings of a script, in the **Script** dialog box upper pane, select the **Global Settings** element and click **Edit**.

General tab

Use the **General** tab to specify the global file transfer direction.

Option	Description
From	Select Guest or Host in the drop-down list. Displays the global source Netop module name.
To	Displays the receiving Netop module, i.e. the Netop module name that has not been selected in the From drop-down list. The field cannot be edited.

Transfer tab

Use the **Transfer** tab to specify global file transfer settings.

Option	Description
Use delta file transfer	Select this check box to compare source files with destination files and

Option	Description
	transfer only the difference between source files and destination files. This saves transmission bandwidth.
Enable crash recovery	Select this check box to transfer files in a way so that they can be recovered after a computer or network crash during transfer.

Overwrite/Delete tab

Use the **Overwrite/Delete** tab to specify global overwrite and delete settings.

Option	Description
Allow overwriting/ deleting existing files/ folders	Select this check box to allow overwriting and deleting files and folders on the destination computer.
Allow overwriting/ deleting system files	Select this check box to allow overwriting and deleting system files on the destination computer.
Allow overwriting/ deleting read-only files	Select this check box to allow overwriting and deleting read-only files on the destination computer.
Allow overwriting/ deleting hidden files	Select this check box to allow overwriting and deleting hidden files on the destination computer.

Advanced tab

Use the **Advanced** tab to specify global error handling and log file settings.

Error Handling

Option	Description
On communication error	<p>Specifies the action in case of a communication error.</p> <p>Select an option in the drop-down list:</p> <ul style="list-style-type: none"> Exit: End the script. Next Host: Proceed to the next Host specified in the script. Retry 1 time: Retry the failed command once. Retry 2 times: Retry the failed command twice. etc.
On transfer error	<p>Specifies the action in case of a file transfer error.</p> <p>Select an option in the drop-down list:</p> <ul style="list-style-type: none"> Exit: End the script. Next Host: Proceed to the next Host specified in the script. Next File: Proceed to the next file specified in the script.

Option	Description
	<ul style="list-style-type: none"> • Retry 1 time: Retry the failed command once. • Retry 2 times: Retry the failed command twice. • etc.

Log File

Option	Description
Generate log file	Select this check box to generate a log file when running the script.
Append if log exists	<p>Select this check box to append the log to an existing log file with the specified name. Clear the selection to overwrite.</p> <p>The field below the check box specifies the log file path and name (default: <code>SCRIPT.LOG</code>).</p> <p>Click the Browse button to open a different log file. If no path is specified, the log file is located in the Netop configuration files folder, typically <code>C:\Documents and Settings\<user name="">\Application Data\Netop\Netop Remote Control\Guest\</user></code>.</p>

Option	Description
Restart script when finished	Select this check box to restart the script at script end.
Close Guest when finished	Select this check box to unload the Guest at script end.

See also

[Script
Create and run a script](#)

5.1.13 IP Broadcast List

For TCP/IP broadcast communication to reach computers on remote network segments when Netop Name Management is not used, IP addresses or DNS names must be listed in the **IP Broadcast List**. For further information about Netop Name Management, see the Administrator's Guide.

Click the **Add** button to open a dialog box allowing you to add a DNS name or IP addresses.

Specify an IP address, for example `192.168.102.57`, an IP address range, for example `192.168.102.20-192.168.102.30`, or a DNS name, for example `MAIL_SVR`, to add it to the **IP Broadcast List**, and click **OK**.

NOTE: Specifying an IP address range will make each broadcast send a number of data packets corresponding to the number of IP addresses in the range. To avoid excessive network traffic, do not specify larger IP address ranges than justified.

Select the **Disable local subnet broadcast** check box to disable broadcast communication to local network segment computers.

See also

[Communication Profile Edit](#)

5.1.14 Log Setup

Log Setup tab

Use the **Log Setup** tab to specify where to log.

Log events

Option	Description
Log locally	Select this check box to log Netop events in a log file on the computer.
Log on Netop server	Select this check box to log Netop events in the database log of a central Netop Security Server.
Log to Windows event log	Select this check box to log Netop events in the Windows event log of the computer and/or of another Windows NT/2000/XP/2003/2008/Vista/7 computer.
Log using SNMP traps	Select this check box to log Netop events by sending SNMP messages to a management information system.
Custom Host Name for all log events	<p>Select this check box to identify logged events by a customized Host name.</p> <p>The left field specifies the customized Host name composed from components and keyboard characters on the drop-down list to the right. Select a component on the drop-down list to add it in the left field.</p> <p>The following components are available:</p> <ul style="list-style-type: none"> • %A: IP/MAC address • %I: Host ID • %C: Computer name • %L: Windows logon user name
Custom Guest name for Connection and Session log events	<p>Select this check box to identify Guests engaged in Connection and Session log events by a customized name.</p> <p>The left field specifies the customized Guest name composed from components and keyboard characters on the drop-down list to the right. Select a component on the drop-down list to add it in the left field.</p> <p>The following components are available:</p> <ul style="list-style-type: none"> • %A: IP/MAC address • %U: Authenticated user name • %I: Guest ID • %C: Computer name

Option	Description
	<ul style="list-style-type: none"> • %L: Windows logon user name <p>Example of a custom Host and Guest name local Netop log</p> <pre> 20080903,14:10,Host1+User1,0,00000,00000,HCON +, 20080903,14:10,Host1+User1,1,00000,00000,HSES +,User2@192.168.1.2 20080903,14:10,Host1+User1,2,00000,00000,HSESRC +,User2@192.168.1.2 20080903,14:10,Host1+User1,3,00000,00000,HSESFXFER +,User2@192.168.1.2 20080903,14:10,Host1+User1,4,00000,00000,HSESCHAT +,User2@192.168.1.2 20080903,14:10,Host1+User1,5,00000,00000,HSESAUDIO +,User2@192.168.1.2 20080903,14:10,Host1+User1,6,00000,00000,HSESAUDIO- ,User2@192.168.1.2 20080903,14:10,Host1+User1,7,00000,00000,HSESCHAT - ,User2@192.168.1.2 20080903,14:11,Host1+User1,8,00000,00000,HSESFXFER- ,User2@192.168.1.2 20080903,14:11,Host1+User1,9,00000,00000,HSESRC - ,User2@192.168.1.2 20080903,14:11,Host1+User1,10,00000,00000,HSES - ,User2@192.168.1.2 </pre> <p>The Host name was customized as %C+%L. The Guest name was customized as %U@%A.</p> <p>The Host was started and the Guest started a remote control session, a file transfer session, a chat session and an audio-video chat session and ended sessions in reverse order.</p>

Netop Security Server has an additional check box:

Act as log server: Select this check box to enable logging other Netop modules' Netop events in the security database Netop Log.

Netop Local tab

Use the **Netop Local** tab to specify which Netop events should be logged and the local Netop log file.

Select Events to view in list

Option	Description
View all Events	Display all available events in the Events to log list.
View Selected	Select event types to display in the Events to log list: <ul style="list-style-type: none"> • Connection • Session • Action • Security

Option	Description
	<ul style="list-style-type: none"> Configuration

Events to log

In the **Events to log** list, select the events you wish to log.

See [Available Netop log event codes and arguments - Guest](#).

Log File

This section is only enabled if the **Log locally** check box has been selected on the **Log Setup** tab.

Option	Description
Log file name	<p>Displays the (path and) name of the log file (default: <code>NETOP.LOG</code>).</p> <p>If no path is specified, the log file is located in the Netop configuration files folder, typically <code>C:\Documents and Settings\<user name="">\Application Data\Netop\Netop Remote Control\<module name=""></module></user></code>.</p>
Write to disk for each log entry	<p>Select this check box to write each Netop event to the local Netop log file immediately.</p> <p>Clear the check box to write Netop events to the local Netop log file when the Netop module is unloaded, which consumes less processor capacity.</p> <p>NOTE: A new local Netop log file that is created when the Netop module is loaded overwrites an old local Netop log file with the same path and file name.</p>

Netop Server tab

Use the **Netop Server** tab to specify which Netop events should be logged and the Host ID of the logging server.

Select Events to view in list

Option	Description
View all Events	Display all available events in the Events to log list.
View Selected	<p>Select event types to display in the Events to log list:</p> <ul style="list-style-type: none"> Connection Session Action Security Configuration

Events to log

In the **Events to log** list, select the events you wish to log.

See [Available Netop log event codes and arguments - Guest](#).

Host ID for Log Server

This section is only enabled if the **Log on Netop server** check box has been selected on the **Log Setup** tab.

Specify the Host ID of the Netop server on which Netop events should be logged. Click the **Browse** button to browse the network for available logging Netop servers.

NOTE: If the **Use Netop Security Server** option (in **Guest Access Security**) is selected on a Host or extended Host, leave the **Host ID for Log Server** field empty to log in the database log of the specified security server.

☐ **Windows Event Log tab**

Use the **Windows Event Log** tab to specify which Netop events should be logged and Windows event logs.

Select Events to view in list

Option	Description
View all Events	Display all available events in the Events to log list.
View Selected	Select event types to display in the Events to log list: <ul style="list-style-type: none"> • Connection • Session • Action • Security • Configuration

Events to log

In the **Events to log** list, select the events you wish to log.

See [Available Netop log event codes and arguments - Guest](#).

Use Windows event log

This section is only enabled if the **Log to Windows event log** check box is selected on the **Log Setup** tab.

Option	Description
Local	Select this check box to log Netop events in the Windows event log of the computer.
Remote	Select this check box to log Netop events in the Windows event log of a remote Windows NT/2000/XP/2003/2008/Vista/7 computer. Specify the Windows name of the remote computer.

SNMP Traps tab

Use the **SNMP Traps** tab to specify which Netop events to log in a management information system.

Select Events to view in list

Option	Description
View all Events	Display all available events in the Events to log list.
View Selected	Select event types to display in the Events to log list: <ul style="list-style-type: none"> • Connection • Session • Action • Security • Configuration

Events to log

In the **Events to log** list, select the events you wish to log.

See [Available Netop log event codes and arguments - Guest](#).

If the **Log using SNMP Traps** box is selected on the **Log Setup** tab, a Simple Network Management Protocol (SNMP) message will be sent when a selected Netop event occurs.

NOTE: Netop SNMP events are defined in the `danware.mib` file located in the folder where the Netop module is installed.

5.1.14.1 Available Netop log event codes and arguments - Guest

The Guest can log the following Netop log events:

Connection

Event Name	Event Code	Arguments
Con: Call Host	GCONCALL	Host name
Con: Disconnect Host	GCONHNGUP	Host name
Con: Connection lost	*CONLOST	Host name
Con: User authenticated	GCONUSER	(none)

Session

Event Name	Event Code	Arguments
Ses: Remote control started	GSESRC +	Host name

Event Name	Event Code	Arguments
Ses: Remote control stopped	GSESRC -	Host name
Ses: File transfer started	GSESFXFER+	(none)
Ses: File transfer stopped	GSESFXFER-	(none)
Ses: Chat started	GSESCHAT +	(none)
Ses: Chat stopped	GSESCHAT -	(none)
Ses: Audio started	GSESAUDIO+	(none)
Ses: Audio stopped	GSESAUDIO-	(none)
Ses: Remote Management started	GSESRM +	Host name
Ses: Remote Management stopped	GSESRM -	Host name

Action

Event Name	Event Code	Arguments
Act: Help service start	GACTHLPSV+	(none)
Act: Help service stop	GACTHLPSV-	(none)
Act: Help request received	GACTHLPRQ+	Host name
Act: Help request canceled	GACTHLPRQ-	Host name
Act: File received	*ACTFILE +	File path and name
Act: File Sent	*ACTFILE -	File path and name
Act: Host Rebooted	*ACTBOOT	Host name
Act: Session recording started	GACTREC +	Recording file path and name
Act: Session recording stopped	GACTREC -	Recording file path and name
Act: Windows event logging failed	*ACTWIN !	(none)
Act: SNMP trapping failed	*ACTSNMP !	(none)
Act: Received Clipboard	*ACTCLPB +	(none)
Act: Sent Clipboard	*ACTCLPB -	(none)
Act: Received Print Job	*ACTPRINT+	(none)

Event Name	Event Code	Arguments
Act: Sent Print Job	*ACTPRINT-	(none)
Act: Communication Profile Started	GACTCOMPR+	Communication profile name
Act: Communication Profile Stopped	GACTCOMPR-	[Communication profile name]
Act: Inventory received	GACTINV	Host name
Act: Message sent	GACTMSG	Host name

Security

Event Name	Event Code	Arguments
Sec: Password rejected	*SECPW !	Host name
Sec: Confirm access granted	*SECCA (10 characters, 4 blank spaces at the end)	Host name
Sec: Confirm access denied	*SECCA !	Host name
Sec: Security Server logon	GSECACSRV+	Logon name
Sec: Security Server logoff	GSECACSRV-	(none)

Configuration

Event Name	Event Code	Arguments
Cfg: Help service name defined	GCFGHLPSV+	Help service name
Cfg: Help service name deleted	GCFGHLPSV-	Help service name
Cfg: Local logging turned on	*CFGLLOC +	Log file name
Cfg: Local logging turned off	*CFGLLOC -	Log file name
Cfg: Local logging filename changed	*CFGLFILE*	New log file name
Cfg: Server logging turned on	*CFGLSRV +	Log server name
Cfg: Server logging turned off	*CFGLSRV -	Log server name
Cfg: Windows event logging turned on	*CFGLWIN +	If remote: computer name
Cfg: Windows event logging turned off	*CFGLWIN -	If remote: computer name

Event Name	Event Code	Arguments
Cfg: Sending SNMP traps turned on	*CFGLSNMP+	(none)
Cfg: Sending SNMP traps turned off	*CFGLSNMP-	(none)
Cfg: Security Server password changed	GCFGACPW *	Netop Guest ID
Cfg: Web update check	*CFGWUCHK	Old build, new build, [timeout error]
Cfg: Web update download	*CFGWUDL	File name, [timeout error]
Cfg: Web update install	*CFGWUINST	(none)
Cfg: Web update success	*CFGWU *	Old build, new build
Cfg: Web update failed	*CFGWU !	Old build, error message

5.1.14.2 Available Netop log event codes and arguments - Host

The Host or extended Host can log the following Netop log events:

Connection

Event Name	Event Code	Arguments
Con: Host started	HCON +	(none)
Con: Host stopped	HCON -	(none)
Con: Callback	HCONCALLB	Callback number
Con: Connection lost	*CONLOST	(none)
Con: Name Server started	HCONNNS +	(none)
Con: Name Server stopped	HCONNNS -	(none)
Con: Security Server started	HCONNSS +	(none)
Con: Security Server stopped	HCONNSS -	(none)
Con: Gateway started	HCONGW +	(none)
Con: Gateway stopped	HCONGW -	(none)

Session

Event Name	Event Code	Arguments
Ses: Session started	HSES +	Guest name

Event Name	Event Code	Arguments
Ses: Session stopped	HSESES -	Guest name
Ses: Remote control started	HSESRC +	Guest name
Ses: Remote control stopped	HSESRC -	Guest name
Ses: File transfer started	HSESFXFER+	Guest name
Ses: File transfer stopped	HSESFXFER-	Guest name
Ses: Chat started	HSESCHAT +	Guest name
Ses: Chat stopped	HSESCHAT -	Guest name
Ses: Audio started	HSESAUDIO+	Guest name
Ses: Audio stopped	HSESAUDIO-	Guest name
Ses: Remote Management started	HSESRM +	Guest name
Ses: Remote Management stopped	HSESRM -	Guest name
Ses: Maintenance password for confirm access wrong. Guest access denied	SESACCTR!	Guest name
Ses: Maintenance password for confirm access ok. Guest allowed access	SESACCTR	Guest name

Action

Event Name	Event Code	Arguments
Act: Help request sent	HACTHLPRQ+	Help service name, problem description
Act: Help request canceled	HACTHLPRQ-	(none)
Act: File received	*ACTFILE +	File path and name
Act: File sent	*ACTFILE -	File path and name
Act: Host reboot	*ACTBOOT	(none)
Act: Run Program	HACTRUN	Program name
Act: Execute Command	HACTEXE	Command name
Act: Windows event logging failed	*ACTWIN !	(none)

Event Name	Event Code	Arguments
Act: SNMP trapping failed	*ACTSNMP !	(none)
Act: Received clipboard	*ACTCLPB +	(none)
Act: Sent clipboard	*ACTCLPB -	(none)
Act: Received print job	*ACTPRINT +	(none)
Act: Sent print job	*ACTPRINT -	(none)
Act: Keyboard and mouse assigned	HACTKBDMS+	Guest name
Act: Keyboard and mouse revoked	HACTKBDMS-	Guest name
Act: Keyboard locked	HACTKBD -	(none)
Act: Keyboard unlocked	HACTKBD +	(none)
Act: Screen blanked	HACTSCR -	(none)
Act: Screen unblanked	HACTSCR +	(none)
Act: Host user logged off	HACTLOFF	(none)
Act: Gateway logon	HACTGW +	Connecting module name
Act: Inventory sent	HACTINV	Guest name
Act: Message received	HACTMSG	Guest name

Security

Event Name	Event Code	Arguments
Sec: Individual security enabled or changed	HSECINDIV+	Guest access method
Sec: Individual security disabled	HSECINDIV-	Guest access method
Sec: Security role added	HSECROLE +	Security role name
Sec: Security role deleted	HSECROLE -	Security role name
Sec: Security role changed	HSECROLE *	Security role name
Sec: Guest added to role	HSECGUEST+	Guest name
Sec: Guest deleted from role	HSECGUEST-	Guest name
Sec: Guest changed in role	HSECGUEST*	Guest name

Event Name	Event Code	Arguments
Sec: Password enabled	HSECPW +	If individual: Guest name
Sec: Password disabled	HSECPW -	If individual: Guest name
Sec: Password changed	HSECPW *	If individual: Guest name
Sec: Callback enabled (default only)	HSECCALLB+	(none)
Sec: Callback disabled (default only)	HSECCALLB-	(none)
Sec: Callback changed (default only)	HSECCALLB*	(none)
Sec: Confirm access enabled	HSECCA +	If individual: security role name
Sec: Confirm access disabled	HSECCA -	If individual: security role name
Sec: Password rejected	*SECPW !	Guest name
Sec: Confirm access granted	*SECCA (10 characters, 4 blank spaces at the end)	(none)
Sec: Confirm access denied	*SECCA !	(none)
Sec: Illegal password limit reached	HSECPWLIM!	(none)
Sec: Timeout limit exceeded	HSECTMOUT	AC (inactivity), AU (authentication) or CA (confirm access)

Configuration

Event Name	Event Code	Arguments
Cfg: Local logging started	*CFGLLOC +	Log file name
Cfg: Local logging stopped	*CFGLLOC -	Log file name
Cfg: Local logging filename changed	*CFGLFILE*	New log file name
Cfg: Server logging started	*CFGLSRV +	Log server name
Cfg: Server logging stopped	*CFGLSRV -	Log server name
Cfg: Windows event logging started	*CFGLWIN +	If remote: computer name
Cfg: Windows event logging stopped	*CFGLWIN -	If remote: computer name

Event Name	Event Code	Arguments
Cfg: Sending SNMP traps started	*CFGLSNMP+	(none)
Cfg: Sending SNMP traps stopped	*CFGLSNMP-	(none)
Cfg: Option change: Start at load	HCFGOWAIT*	ON/OFF
Cfg: Option change: Load with OS	HCFGOLOAD*	ON/OFF
Cfg: Option change: Minimize at startup	HCFGOMIST*	ON/OFF
Cfg: Option change: Stealth mode	HCFGOSTLT*	ON/OFF
Cfg: Option change: Minimize on connection	HCFGOMICO*	ON/OFF
Cfg: Option change: On top	HCFGOTOP *	ON/OFF
Cfg: Option change: Show file transfer	HCFGOSFX *	ON/OFF
Cfg: Option change: Send keep alive	HCFGOLIV*	ON/OFF
Cfg: Option selected: Boot after disconnect	HCFGOBOOT+	(none)
Cfg: Option selected: Logoff after disconnect	HCFGOLOGO+	(none)
Cfg: Option selected: Lock after disconnect	HCFGOLOCK+	(none)
Cfg: Option selected: Nothing after disconnect	HCFGONOTH+	(none)
Cfg: Option change: Naming method	HCFGONAME*	(none)
Cfg: Option change: Public Host name	HCFGOPUBN*	ON/OFF
Cfg: Option change: Enable user name	HCFGOUSRN*	ON/OFF
Cfg: Option change: Connection notification	HCFGONOTI*	(none)
Cfg: Option change: Help Request description	HCFGOHRD *	(none)

Event Name	Event Code	Arguments
Cfg: Option change: Help Request provider	HCFGGOHRP *	(none)
Cfg: Option change: Help Request communication	HCFGGOHRC *	(none)
Cfg: Option change: Help Request phone/IP	HCFGGOHRPI *	(none)
Cfg: Option change: Help Request show icon	HCFGGOHRSI *	ON/OFF
Cfg: Option change: Audio full duplex	HCFGGOAUFD*	ON/OFF
Cfg: Option change: Audio silence level	HCFGGOAUSL*	(none)
Cfg: Option change: Audio line hold	HCFGGOAULH*	(none)
Cfg: Option change: Name space ID	HCFGGONSID*	(none)
Cfg: Maintenance requiry changed for Guest	HCFGMRQG*	(none)
Cfg: Maintenance requiry changed for Gateway	HCFGMRQGW*	(none)
Cfg: Maintenance requiry changed for other	HCFGMRQO *	(none)
Cfg: Maintenance requiry changed for exit/stop	HCFGMRQEX*	(none)
Cfg: Protect files changed	HCFGPROTS*	(none)
Cfg: Maintenance password changed	HCFGMTPW *	(none)
Cfg: Guest access allow to changed (default only)	HCFGGALLW*	(none)
Cfg: MAC/IP address list changed	HCFGMACIP*	(none)
Cfg: File transfer disable changed	HCFGFX *	(none)
Cfg: Security Server group ID changed	HCFGSSG *	(none)
Cfg: Web update check	*CFGWUCHK	Old build, new build, [timeout error]

Event Name	Event Code	Arguments
Cfg: Web update download	*CFGWUDDL	File name, [timeout error]
Cfg: Web update install	*CFGWUINST	(none)
Cfg: Web update success	*CFGWU *	Old build, new build
Cfg: Web update failed	*CFGWU !	Old build, error message
Cfg: Maintenance password for confirm access enabled	HCFGACCTR+	(none)
Cfg: Maintenance password for confirm access disabled	HCFGACCTR-	(none)

Netop Gateway can log these Netop log special Gateway events:

Event Name	Event Code	Arguments
GW: Gateway access allowed	HGW ACCES+	(none)
GW: Gateway callback	HGW CALLB	Callback number
GW: Gateway callback changed (default only)	HGW CALLB*	(none)
GW: Gateway callback disabled (default only)	HGW CALLB-	(none)
GW: Gateway callback enabled (default only)	HGW CALLB+	(none)
GW: Gateway group defined	HGW GROUP+	Security role name
GW: Gateway group deleted	HGW GROUP-	Security role name
GW: Gateway Guest added	HGW GUEST+	Guest name
GW: Gateway Guest changed	HGW GUEST*	Guest name
GW: Gateway Guest deleted	HGW GUEST-	Guest name
GW: Gateway individual security disabled	HGW INSEC-	(none)
GW: Gateway individual security enabled (or changed)	HGW INSEC+	(none)
GW: Gateway NSS GID changed	HGW SSGID*	(none)
GW: Gateway password changed (default only)	HGW PW *	(none)
GW: Gateway password	HGW PW -	(none)

Event Name	Event Code	Arguments
disabled (default only)		
GW: Gateway password enabled (default only)	HGW PW +	(none)
GW: Gateway password rejected	*SECGWPW !	Connecting module name

5.1.15 Netop File Manager Options

Use the **Options** dialog box to set up how file transfer should work.

You can set up synchronization options, general transfer options, options for display of confirmation dialog boxes in relation to deleting/overwriting files during file transfer, **File Manager** layout options, and options for logging during file transfer.

Transfer tab

Synchronize

Option	Description
Transfer only if file exists	Select this check box to synchronize files only if they exist in the unselected pane.
Transfer only one way	Select this check box to synchronize files only from the selected pane to the unselected pane.

General Transfer

Option	Description
Include subfolders	Select this check box to transfer also the contents of subfolders of selected folders.
Use delta file transfer	Select this check box to compare source files with corresponding destination files and transfer only differences between source and destination files. This saves transmission bandwidth.
Enable crash recovery	Select this check box to transfer files so that they can be recovered after a computer or network crash during file transfer.
Close dialog when finished	Select this check box to close the Transfer Status window when a file transfer is finished.
End session when finished	Select this check box to end the file transfer session when a file transfer is finished.

Confirmation tab

Confirm when...

Option	Description
Delete non-empty folders	<p>Select this check box to display a confirmation dialog box if you are about to delete a folder containing folders or files.</p> <p>The confirmation dialog box allows you the following choices with regard to the deletion:</p> <ul style="list-style-type: none"> • Skip: Click this button to skip deleting the specified folder. • Delete: Click this button to delete the specified folder. • Advanced: Click this button to change your delete confirmation selections for this file transfer only. • Cancel: Click this button to cancel the file transfer at this point. You cannot undo executed file transfer actions.
Overwriting/deleting files	<p>Select this check box to display a confirmation dialog box if you are about to overwrite or delete files.</p> <p>The confirmation dialog box allows you the following choices with regard to the overwriting/deletion:</p> <ul style="list-style-type: none"> • Skip: Click this button to skip overwriting the specified file. • Overwrite: Click this button to overwrite the specified file. • Advanced: Click this button to change your overwriting confirmation selections for this file transfer only.
Overwriting/deleting read-only files	Select this check box to display a confirmation dialog box if you are about to overwrite/delete read-only files.
Overwriting/deleting hidden files	Select this check box to display a confirmation dialog box if you are about to overwrite/delete hidden files.
Overwriting/deleting system files	Select this check box to display a confirmation dialog box if you are about to overwrite/delete system files.
Drag and drop (copying files with the mouse)	Select this check box to display a confirmation dialog box before executing a drag and drop file transfer.

☰ **Layout tab**

Screen

Option	Description
Show toolbar	Select this check box to display the toolbar of the Netop File Manager window.
Show status bar	Select this check box to display a status bar at the bottom of the two panes in the Netop File Manager window.
Save session path at exit	<p>Select this check box to display the same pane contents when starting a file transfer session with the same Host the next time.</p> <p>Uncheck to always display the system drive contents when starting a</p>

Option	Description
	file transfer session.

Keyboard

Option	Description
Use system hotkey layout	Select this option to use the operating system hotkey layout, see the table below.
Use Netop hotkey layout	Select this option to use the Netop hotkey layout, see the table below.

Function	Windows hotkey	Netop hotkey
Copy Files		F3
Move Files		F6
New Folder		F7
Delete	DELETE	F8
Rename	F2	
Close	ALT+F4	F10
Properties	ALT+ENTER	SHIFT+F1
Select All	CTRL+A	
Select by		+
Deselect by		-
Invert selection		*
Arrange Icons By Name		CTRL+F3
Arrange Icons By Type		CTRL+F4
Arrange Icons By Size		CTRL+F6
Arrange Icons By Date		CTRL+F5
Refresh	F5	CTRL+R
Select the left record panel		ALT+F1
Select the right record panel		ALT+F2
Help	F1	F1

Icons

Option	Description
Local associated and Host 'exe' icons	Display file icons in the Netop File Manager window panes according to Guest file associations, but display Host exe file icons according to Host file associations.
Local associated icons	Display file icons in the Netop File Manager window panes according to Guest file associations. This saves transmission bandwidth.
Default icons	Display the same default icon for all files in the Netop File Manager window panes. This saves transmission bandwidth and processor capacity.

Logging tab

Option	Description
Generate log file	Select this check box to generate a file transfer log file when ending a file transfer session.
Append if log file exists	Select this check box to append new log entries to an existing log file. If you do not select it, any existing log file will be overwritten.
Filename	This field specifies the log file (path and) name. The default name is <code>NFM.LOG</code> . The file is located in the Netop configuration files folder, typically <code>C:\Documents and Settings\<user name="">\Application Data\Netop\Netop Remote Control\Guest</user></code> . Click the Browse button to specify another log file path and name.

See also

[Transfer files](#)

5.1.16 Modem

Use the **Modem** dialog box to manage the modem database.

NOTE: The modem database is stored in the Netop configuration file `modems.ndb`, which is typically located in the directory `C:\Documents and Settings\\Application Data\Netop\Netop Remote Control\.`

In the **Modem List** the first `_Modem Database YYYYDDD` record specifies the modem database update year and day number. You can download and install the newest available update from the Netop KnowledgeBase, see the Download Updates subsection.

NOTE: Downloading and installing `modems.ndb` will overwrite your current `modems.ndb`.

Other records represent modem configurations created by Netop Support or added by a user.

You can create, edit and delete modem configurations using the buttons at the bottom of the dialog box.

To base a new modem configuration on an available modem configuration, select the modem configuration in the pane before clicking the **New** button.

See also

[Modem Configuration](#)

5.1.17 Modem Configuration

Use the **Modem Configuration** dialog box to create or edit a modem configuration in the modem database.

With some modem configurations, some or all fields will be disabled to protect the original modem configuration. If you select a modem configuration in the **Modem** dialog box and click **New**, the properties of the selected modem configuration are displayed in the **Modem Configuration** dialog box with all fields enabled.

The **Name** field contains the modem configuration name, which must be unique within the modem database. You can edit the field contents.

Modem command strings

These fields specify the modem AT command strings. Consult with your modem manual or the modem manufacturer website to find the AT command strings required by your modem.

Max data rate

In the **Max data rate** drop-down list, select a data rate applicable to your modem and the modem you want to connect to.

Settings

Option	Description
RTS/CTS Flow control	Select this check box to use Return To Send/Clear To Send flow control.
Ignore carrier signal	Normally, no carrier signal indicates an error. However, in some situations there may not be any carrier signal, without this being an error. Select this check box to not wait for a carrier signal.

See also

[Modem](#)

5.1.18 Novell Network Numbers

Unless a network list is created, IPX communication will reach only Netop modules on the local network, but you can extend communication to remote networks.

In the **Novell Network Numbers** dialog box you can add, edit, and delete network numbers using the buttons on the right side of the network list.

The pane displays the 8-digit hexadecimal network numbers of selected remote networks.

See also

[Communication Profile Edit](#)

5.1.19 Program Options

☐ **Layout tab**

Use the **Layout** tab to specify layout options for the **Guest** window.

Enable

Option	Description
Tool bar	Clear the selection of this check box to remove the toolbar.
Status line	Clear the selection of this check box to remove the status bar.
Menu hints	Clear the selection of this check box to disable the display of menu command and toolbar button hints in the status bar.
Add Guest icon to tray	Clear the selection of this check box to display no Netop Guest icon in the notification area in the lower right screen corner when the Guest is loaded.
Hide Guest from taskbar when minimized	This option is only available if the check box Add Guest icon to tray is selected. Clear the selection of this check box to display the minimized Guest as an icon in the taskbar at the bottom of the screen. If selected, the minimized Guest is displayed only as a Netop Guest icon in the notification area in the lower right corner of the screen.
Save Guest minimize state on exit	Select this check box to load the Guest minimized if minimized when the Guest last unloaded.
Stealth mode (hide Guest when started)	Select this check box to load the Guest hidden to the computer user. To unhide the Guest when loaded in stealth mode, execute showgst.exe, which is located in the directory in which the Guest was installed.

Use the **Menu and Toolbar Theme** list to select color theme for the menu and toolbar.

Tab layout

Use the **Tab layout** option to enable/disable tab panel tabs and rearrange the order of the tabs.

The pane contains a list of available tab panel tab names.

Remove the selection of a check box to remove the tab in question from the tab panel.

The order of the tab names in the pane from top to bottom controls the order of the tab panel from left to right. Select a tab name and click one of the **Up/Down** buttons to move it.

NOTE: You need to restart the Guest for the changes to take effect.

☐ **General tab**

Use the **General** tab to specify general connect options.

Host session default mode

Select a session to start when connecting to a Host. Remote control is the default session.

Inactivity

In the **Inactivity timeout** field, specify a number of minutes after which to disconnect if there has been no Guest user keyboard or mouse activity within the specified number of minutes (default: 0, range 0-999).

Keep Alive

Select the **Send keep alive message** check box to send a data packet at intervals while connected to alert the Guest if the connection is lost.

NOTE: To maintain an ISDN (CAPI) connection during short periods of inactivity, do not select this check box. Instead select the Short-hold mode check box in the **Edit** dialog box for the ISDN (CAPI) communication profile.

Confirm when

Select the **Exiting Guest while connected** check box to display a warning if you attempt to unload the Guest while being connected to a Host. You will be prompted to confirm if you want to unload the Guest anyway.

Connection

Option	Description
Connection attempts	Specify a number of connection attempts in the range 1-999 that the Guest should automatically make to connect to a Host.
Auto reconnect	In the list, select the reconnect option that should apply if a connection is lost: <ul style="list-style-type: none"> • Never: Never reconnect. • Abnormal disconnect only: Reconnect only if the connection was lost by an abnormal event. • Host disconnect only: Reconnect only if the Host disconnected. • Always: Always reconnect.

Cache tab

Use the **Cache** tab to specify disk cache options for the remote control screen image.

When the Guest remote controls a Host in command mode, the Guest will store the Host screen image in disk cache memory to transfer only image changes. This speeds up Host screen image update and saves transmission bandwidth.

Host screen command transfer disk cache

Option	Description
Use separate cache file for each Host	Select this option to reserve a disk cache section for each connected and disconnected Host. If you connect to many different Hosts, a large total disk cache size will be required to achieve high update and reconnect speed.
Use shared cache file for all Hosts	Select this option to share the available disk cache among connected and disconnected Hosts.

Option	Description
	Total disk cache size demand will typically be lower.
Don't save cache between sessions	Select this option to share the available disk cache only among connected Hosts. Total disk cache demand will be lowest, but reconnects will be slower.
Limit total disk cache size to	In this field, specify a disk cache size in the range 200-64000 (default: 10000). The number should typically be larger than default if you regularly run command mode remote control sessions with many different Hosts.

Logon tab

Use the **Logon** tab to specify Guest logon and name options.

Guest ID

The contents of the **Guest ID** field specify the name by which the Guest will identify itself when communicating (default: computer name).

You can edit the field content.

If the field is empty, the Guest will identify itself by its computer address, typically IP address or network card MAC address.

NOTE: If the Guest runs on a network computer, we recommend naming it by its computer name. If the Guest runs on a terminal server client, we recommend naming it by its user logon name. See the Administrator's Guide, Advanced Tools, Netop Naming in a TSE.

Authentication

Select the **Cache logon passwords** check box to store the most recently used logon credentials in cache memory and apply them when connecting.

Cached logon credentials will be lost when the Guest is unloaded.

Access Server 6.x/5.x

Option	Description
Use Access Server on Guest side	Select this check box to enable Guest side authentication with Hosts that are Guest side authentication enabled on an older version of Netop Access Server. NOTE: Netop Security Server (version 7+ only) does not support Guest side authentication.
Ignore if access to Host cannot be authenticated	Select this check box to ignore Guest side authentication with Hosts that are not Guest side authentication enabled on a Netop Access Server.

Host Name tab

Use the **Host Name** tab to specify Host name and Netop Name Server name space ID options.

Default Host name qualifier

Netop interprets a name specified in the **Quick Connect** tab, in the **Host** section **Name** field as a certain type of name according to this default Host name qualifier or a prefixed Host name qualifier (shown in parentheses below).

Option	Description
Host ID (H: :)	Interprets a Host name without a prefix as a Host ID.
User name (U: :)	Interprets a Host name without a prefix as a user name.
DNS name (DNS: :)	Interprets a Host name without a prefix as a Domain Name Server name.
LDAP name (LDAP: :)	Interprets a Host name without a prefix as a directory services user attribute value. See Directory Services tab.

Duplicate names

If connecting by a networking communication device, multiple Hosts may respond by the same name, for instance if the same user is logged on to multiple computers. By default, the Guest will connect to the first responding Host.

Select the **Check for duplicate names before connecting** check box to wait a few seconds for Host responses and display a **Multiple Host Names found** window if multiple Hosts respond. The window prompts you to select a Host.

Netop Name Server

To connect by name resolution using Netop Name Server, use a communication profile that uses the TCP/IP communication device. In the **Advanced TCP/IP Configuration** dialog box, select the **Use Netop Name Server** check box and specify the resolving Netop Name Server addresses. You must also specify the same Name Space ID as the Netop modules that you want to connect to.

In the **Name Space ID** field specify the Name Space ID specified by the Netop modules that you want to connect to using Netop Name Server (default: `PUBLIC`).

See also

[Communication Profile Edit](#)

Administrator's Guide, Netop Name Management.

☐ Directory Services tab

Use the **Directory Services** tab to specify directory services to enable the Guest to connect to and browse for Hosts using the `LDAP: :` Host name qualifier.

General

Option	Description
Directory Server	Specify the directory server IP address or DNS name.
Port	Specify the port through which to connect to the directory server (default: <code>389</code> , the Lightweight Directory Access Protocol (<code>LDAP</code>) port).

Option	Description
	Select the Use secure connection check box to connect to the directory server by a secure connection. The <code>LDAP</code> secure connection port number is <code>636</code> .
Base DN	Specify the directory services distinguished name from which a search should start.

Credentials tab

Specify the credentials by which the Guest should log on to the directory server. The credentials determine the user rights by which directory services information will be available.

Option	Description
Anonymous bind	Select this check box to search the directory service with anonymous user rights. Clear the selection to enable the fields below.
User DN	Specify a directory service user distinguished name to search the directory service with the rights of this user. You must also specify the corresponding password.

Settings tab

Specify the settings for searching directory services for user attribute values to return corresponding name and address attribute values.

For guidance on filling in the **User search filter** and **User attribute** fields, click the **Default** button to display the **Display Directory Service** dialog box. Select a directory service name in the list of available directory services and click **OK**.

Selecting a directory service, for example Active Directory, populates the **User search filter** and **User attribute fields** with default values for the selected directory service. You can edit the values if you have customized your directory service and require different values.

Attributes:

Option	Description
Name attribute	Specify or edit the name attribute.
Address attribute	Specify or edit the address attribute designation.
Search name prefix	Specify or edit any prefix (e.g. <code>cn=</code>) that should be added before search values.

☐ Remote Control tab

Use the **Remote Control** tab to specify general remote control session options.

NOTE: You can specify individual remote control session options for each Host connection in the **Connection Properties** dialog box, which you can access either by clicking the **Connection Properties** dialog box on the **Quick Connect** tab, or in a running remote control session, by

clicking **Connection Properties** on the toolbar.

Enable

Option	Description
Toolbar	Select this check box to display the Remote Control window toolbar.
Toolbox in full screen	Select this check box to display the Remote Control full screen display toolbox.
Full screen toolbox roll-up	Select this check box to reduce the Remote Control full screen display toolbox to the corresponding title bar when not in use.
Status line	Select this check box to display the Remote Control window status bar.

Hot keys assignment

You can assign hotkeys (keystroke combinations) to specified actions. By default, CTRL+Z is assigned to Zoom in and out (switch between **Remote Control** window and full screen). Assign desired hotkeys by selecting check boxes and specifying a character in the last field.

Remote control window

Option	Description
Host window auto scroll	Select this check box to enable automatic Host screen image scroll when the mouse pointer approaches Remote Control window borders.
Show full screen as topmost window	Select this check box to display the Remote Control full screen display in front of any other window.
Show full screen on all monitors	Select this check box to display the Remote Control full screen display on all available monitors.
Auto take control	Select this check box to enable acquiring multi Guest session keyboard and mouse control by a keystroke or mouse click.
Switch to window mode password	Specify a password that should be requested to switch from full screen to window. The field displays password characters as dots or asterisks.
Disconnect password	Specify a password that should be requested to disconnect. The field will display password characters as dots or asterisks.

☰ **Clipboard tab**

Use the **Clipboard** tab to specify remote control clipboard transfer options.

Automatic clipboard transfer

Option	Description
Automatically transfer clipboards below	Select this check box to enable contents placed on the Guest computer or Host computer clipboard during a remote control session to automatically become the clipboard contents of both computers if smaller than the number of kilobytes specified in the field.
Show progress dialog during transfer	Select this check box to display a small window with a progress bar while clipboard contents are being transferred from one computer to the other.

Monitor tab

Use the **Monitor** tab to specify monitor options.

Option	Description
Monitor interval	Specify a number of seconds in the range 1-999 after which to switch to the next Host after monitoring a Host (default: 15).
Start Monitor in full screen	Select this check box to initially display monitored Host screen images in full screen mode. If unchecked, Host screen images will initially be shown in window mode.

Audio-Video Chat tab

Use the **Audio-Video Chat** tab to specify audio and video chat options.

Audio-video chat settings

Option	Description
Start audio chat when conference is started	Select this check box to enable sound transfer at session start.
Start video when conference is started	Select this check box to enable image transfer at session start.

Audio Chat

Select the **Enable full-duplex audio** check box to enable sound transfer in both directions at the same time.

NOTE: Some computer sound systems do not support full-duplex audio.

Microphone sensitivity

Option	Description
Silence level	Drag the slider bar to specify the microphone sound input level below

Option	Description
	which no sound data should be transferred.
Line hold	<p>Drag the slider bar to specify the time period in which sound data should continue to be transferred after the microphone sound input level has dropped below the silence level.</p> <p>TIP: Try out different Silence level and Line hold settings to optimize sound transfer.</p>
Check sound system	Click this button to check the computer sound system. A result message will be displayed.
Advanced	Click this button to display the Advanced audio settings dialog box. See Advanced audio settings .

Video

Option	Description
Capture size	Select a video capture frame size on the list. The size is displayed in pixels (default: 160 x 120).
Advanced	Click this button to display the Advanced Video dialog box. See Advanced Video .

Remote Printing tab

Use the **Remote Printing** tab to specify remote Netop printers and incoming print job redirection.

Remote Netop printers

You can add a Netop printer on the Guest computer to enable sending a Guest computer print job to a Host computer printing device (remote printer).

Click the **Add printer** button and following the instructions in the displayed **Add printer guidelines** window. Click the **Ready** button to start adding a Netop printer.

The **Remote Netop printers** pane will display the names of Netop printers in the Windows **Printers** folder on the Guest computer.

NOTE: You can also add a Netop printer on a Host computer to enable sending a Host computer print job to a Guest computer printing device. You can remove a Netop printer by selecting the printer in the pane and clicking the **Remove printer** button.

If you are connected to multiple Hosts while sending a print job to a Netop printer, a dialog box prompting you to select the Host to which you want to send the print job is displayed.

NOTE: Special instructions for remote printing from DOS applications are available in the [Netop KnowledgeBase](#).

Redirect print to

You can redirect a print job sent from the Host computer to the Guest computer to any printer specified on the Guest computer.

Option	Description
Default printer	Select this option to redirect the print job to the default Guest computer printer.
Prompt with a list of available printers	Select this option and click Browse to display the Select Print Redirection Printer dialog box allowing you to select a printer from a list of available printers.

See also

[Send a print job to a remote printer](#)

Recording tab

Use the **Recording** tab to specify remote control session recording options.

Options

Option	Description
Use compatible mode	Remote control session recording was improved in Netop Remote Control version 8. Older Guest versions cannot play back version 8+ recordings. Select this check box to make older version compatible recordings.
Enforce recording	Select this check box to record all remote control sessions even if the Record remote control session check box is not selected (Connection Properties > Record tab).
Disconnect if recording fails	Select this check box to disconnect if recording a remote control session fails.

Recording

A **Recordings** tab record and recording file name will identify the remote control session Guest. Select one of these identity options:

Option	Description
Guest ID	Identify by the Guest ID. See Logon tab for further information.
Guest user	Identify by the Guest computer Windows or network logon user name.

See also

[Record sessions](#)

Sounds tab

Use the **Sounds** tab to specify sounds played upon selected events.

Select an event check box to play a sound upon the event. Clear the selection to suppress playing a sound upon the event.

Select an event and click **Select Sound** to open a sound file with the extension `.wav` to replace

the current sound. The event will be marked with an asterisk (*). Select an event marked (*) and click **Default Sound** to reassign the default sound to the event and remove the (*) mark.

If you want to listen to the sound while editing the sound settings, select an event and click **Play** to play the sound assigned to the event.

☐ **Help Request tab**

Use the **Help Request** tab to set up use of help request.

Select the **Enable help request** check box to enable the Guest to receive help requests.

Click the **Advanced** button to display the **Advanced Help Service** dialog box allowing you to specify actions that are to be executed when a help request arrives. See [Advanced Help Service](#).

Help Service tab

The Guest can receive Host help requests only if the **Enable help request** and **Enable help services** check boxes are selected, at least one Help service name is specified and communication profiles are enabled at Guest loading.

The Host uses the term help provider for a help service name.

Option	Description
Enable help services	Select this check box to enable the help services specified below.
Help service 1-3	In these fields, specify the names of the help services that this Guest is to offer.

Service Ticket tab

The extended Guest also has a **Service Tickets** tab that enables it to service help requests by service ticket numbers. Service tickets are used for both Netop Remote Control and Netop OnDemand Remote Control (1.74 and earlier versions).

Option	Description
Enable service tickets	Select this check box to enable use of service tickets to service help requests by a service ticket number.
Service ticket format	Enter a service ticket format using any character plus the control characters #, @, and * (# produces a number (0-9), @ produces a letter (A-Z) and * produces a number or a letter (0-9, A-Z)), for example @##-****. The service ticket generated from this can only be used once, after which a new ticket will be generated.
Number of auto generated service tickets	Enter the number (0-3, 0 = manually) of service tickets to be auto-generated.

WebConnect tab

The extended Guest also has a WebConnect tab that enables it to service help requests by WebConnect tickets. WebConnect tickets are used for Netop OnDemand Remote Control 2.0 and later versions.

Option	Description
Enable WebConnect tickets	Select this check box to enable use of WebConnect tickets.
WebConnect ticket	Enter anything that you want to use as a WebConnect ticket for identification purposes during a Netop OnDemand remote control session using WebConnect, for example an email address, a name, or a keyword, for example Security Server.
WebConnect profile	Select a WebConnect profile in the list. The WebConnect profile contains the credentials and the Connection Manager URL to be used for the WebConnect connection. The profile itself should be defined in the Setup Wizard before you can select it here. You can also set up the profile in Communication Profiles . One or more WebConnect profiles can be defined in Communication Profiles . See Communication Profile Edit for further information.
Update interval	Enter an interval in seconds to specify how often the Guest should communicate with WebConnect and check for new tickets.

See also

[Set up Help Request on Guest and Host](#)

Run tab

Use the **Run** tab to specify programs to include in the **Run Program** drop-down menu on the **Guest** window and **Remote Control** window toolbars.

The pane displays specified programs as records in a table with a description and the program file path and name.

NOTE: Table contents are stored in the `runprog.ndb` Netop configuration file, which is typically located here: `C:\Documents and Settings\\Application Data\Netop\Netop Remote Control\Guest`.

Click the **Add** button to add a program to the pane. The **Run** dialog box in which you can specify a program to run is displayed. See [Run](#).

To see the properties of a record in the pane, select the record and click the **Properties** button. The **Run** dialog box is displayed, and you can edit the properties specified.

To delete a record again, select it in the pane and click the **Delete** button.

See also

[Run a program on one or multiple Hosts](#)

Encryption tab

Use the **Encryption** tab to enable encryption types.

The communication between Netop modules is protected by encrypting transmitted data.

A range of encryption types is available on Netop Remote Control modules.

Communicating Netop modules will automatically negotiate to encrypt communication by an encryption type that is enabled on both modules. See [Connection Properties \(Compression/Encryption tab\)](#). Netop modules on which no common encryption type is enabled cannot communicate.

Select the check boxes next to the various encryption types to enable them.

To see encryption details about the individual encryption types, select an encryption type and click the [Show Details](#) button.

Inventory tab

Use the [Inventory](#) tab to specify what inventories should contain and how the contents should be displayed in the [Guest](#) window [Inventory](#) tab.

Summary view

The pane contains a list of available inventory details. Select check boxes to specify the inventory details of the [Guest](#) window [Inventory](#) tab summary, which is displayed in the details pane on the right when a folder is selected in the contents pane on the left.

The pane top-to-bottom order of selected inventory details will determine the left-to-right order of details pane columns.

Use the [Up/Down](#), [Select All](#), [Deselect All](#) buttons to arrange the contents of the pane.

Click the [Advanced](#) button to specify inventory processing and custom inventory items. The [Advanced inventory option](#) dialog box is displayed. See [Advanced inventory option](#).

See also

[Generate a Host inventory](#)

Smart Card tab

Use the [Smart Card](#) tab to specify the Smart Card reader whose reading will be applied to Smart Card authentication.

Smart Card Reader

Option	Description
Select Smart Card reader	In the drop-down list, select the Smart Card reader that you want to use. The list contains Default and the names of connected Smart Card readers found by Windows.
Support Remote Smart Card Logon	Select this check box to enable remote Smart Card logon. This means that using a local Smart Card reader you can log directly into remote enterprise and application systems using a Smart Card for authentication and authorization.

Intel vPro tab

Use the [Intel vPro](#) tab to specify the address of the SCS Web Service.

Select the [Connect to SCS](#) check box and enter the SCS Web Service URL in the field below.

The address is then saved in the system, so that every time you select the **Retrieve Intel vPro Enabled Computers from SCS** command on the context menu for the **Intel vPro** tab pane on the **Quick Connect** tab, you won't be prompted to enter the address.

See also

[Use Intel vPro from Netop Remote Control](#)

☐ Skins tab

If you run a remote control session, skins enable you to see the Host device and execute commands on the Host device by clicking buttons on the applied skin. A device 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 Guest.

If the Guest does not have the skin that is needed for a remote control session with a particular Host, it will attempt to collect a suitable skin from the Netop Skin Repository Server. If the necessary skin is not available, the Guest will use a default skin.

On the **Skins** tab, the address and port number of the Netop Skin Repository Server are displayed.

Click the **View Models** button if you want to see the available skin models.

☐ Web Update tab

Use the **Web Update** tab to specify web update options to automatically update the Guest installation.

Option	Description
Update server	Specify the web address of the server from which to download Guest update files (default: update.netop.com, the Netop manufacturer web update server). NOTE: To update many Netop installations in an organization, we recommend publishing new updates to an internal web update server (select Publish New Updates on the Tools menu).
HTTP Proxy	Specifying a HTTP proxy is typically not required. Before specifying a HTTP proxy, click Update now to test the web update connection. If you receive a message indicating connection to the update server, specify no HTTP proxy. If Update now yields no connection, click the Detect button to make Netop attempt to detect the HTTP proxy server and display its name and port number in the HTTP Proxy field. Click Update now to test the connection. If unsuccessful, consult your network/system administrator about what to specify in the HTTP Proxy field (format: <Server name>:<Port number>).
Update now	Click this button to connect to the update server specified in the Update server field. A web update message will notify you if connection to the update server fails, if no updates are available or if updates are available, and in the latter case ask you if you want to download and install updates.
Schedule	Click this button to display the Web Update Schedule dialog box and specify a schedule of checks for updates including download and

Option	Description
	installation of available update files.

5.1.20 Run

Use the **Run** dialog box to specify a program file to run using the **Run Program** function and how the program should start.

File

Type a descriptive text in the **Description** field. This text will appear on the menu.

File name

Make sure that the **Local file name** option has been selected and then click the **Browse** button to locate the program .exe file.

When the program file is added to the **Local file name** field, the global file name is automatically added to the **Global file name** field. The absolute path has been replaced with environment variables. This is especially helpful if your computers are running different Windows platforms.

Example of a local file name and the corresponding global file name:

```
C:\Program Files\Adobe\Acrobat 6.0\Reader\AcroRd32.exe
%ProgramFiles%\Adobe\Acrobat 6.0\Reader\AcroRd32.exe
```

TIP: Once you have added a program to the **Local file name** field and the global file name has been added automatically to the **Global file name** field, select the **Global file name** option, so that you do not have to consider which operating system version or operating system language Host computers are using.

If the selected program needs to be started using command line switches, use the **Command line switches** field to type those. This could for example be starting Internet Explorer with a specific address or for Adobe Acrobat Reader, the name of the document to read.

Run

Under **Run**, select **Normal**, **Maximized** or **Minimized** to define how the program should start when opened from the **Run Program** button on the toolbar or from the **Run Program** command on the **Connection** menu.

5.1.21 Script

A script is a user specified command structure that can execute a task, typically an unattended scheduled file transfer.

Use the **Script** dialog box to create and edit scripts in a graphical tree structure.

Option	Description
Filename	Specify a script file name. If you do not specify a file extension and a path, the script file gets the extension .dws and will be located in the Netop configuration files folder, typically C:\Documents and Settings\ <user name="">\Application Data\Netop\Netop Remote Control\Guest\script\.</user>

Option	Description
	If you create a new script, you will be prompted for confirmation. Click Yes . The Global Settings dialog box is then displayed.
Open Script	Click this button to open a script file.
Comment	Enter a comment about the script. The comment will be displayed in the Comments column on the Script tab (Optional).
Save Script	Click the Save Script button to save a new or edited script.
Add	Click the Add button to add a script command in the upper pane under the selected script command. See Commands list below.
Edit	Select a script command in the upper pane and click the Edit button to display the corresponding editing window.
Run Script	Click this button to run the script.
Delete	Select a script command in the upper pane and click the Delete button to delete it, including the command sub tree under it.

☐ **Commands list**

To specify the first command of a script, in the upper pane of the **Script** dialog box, select the **Global Settings** element and click **Add** to display a drop-down menu.

This menu contains script commands that can execute on the Guest:

- Connect Select the **Connect** command to add a **Connect** command, which will connect to a Host.
- Wait Select the **Wait** command to add a **Wait** command, which will delay script execution.
- Run Select the **Run** command to add a **Run** command.

A **Connect** command will branch the script into commands that execute with or on the connected Host computer or in case of a local **Connect** command on the Guest computer.

In the upper pane, click the **+** (plus) next to a **Connect** command to expand it and select the expanded **Connect** command or a command below it.

Click **Add** to display the following menu, which contains script commands that can execute with a connected Host or a Guest connected locally to itself:

- Copy Select one of these commands to display a <File transfer> dialog box and add a **File Transfer** command.
- Move
- Synch
- Clone
- Delete
- Wait Select this command to display the **Wait** dialog box and add a **Wait** command to delay script execution.
- Run Select this command to display the **Run Program** dialog box and add a

Run command to run a program on the connected to computer. You can schedule scripts to be run from the Guest on the Host by using elevated privileges; select **Use a different account** and enter the credentials of a user who has elevated privileges on the Host machine.

- Logoff
- Restart
- Poweroff
- Lock
- Inventory
- Send Message

Select one of these commands to add an **Action** command to execute an action on the connected to computer.

See also

- [Create and run a script](#)
- [Global Settings](#)
- [Netop File Manager Options](#)

5.1.22 Send Message

When you add a **Send Message** command to a script, the **Send Message** dialog box is displayed allowing you to specify how the message should be sent.

Option	Description
Send Message step	<p>Select a Send Message step option in the drop-down list:</p> <ul style="list-style-type: none"> • One Step: Select this option to copy a message file on the Guest computer to the Messages directory on the Host computer and display it in a Send Message window on the Host computer screen. <p>NOTE: Create and save the message file in the Message window.</p> <ul style="list-style-type: none"> • Display Message: Select this option to display a message file located on the Host computer in the Messages directory in a Message window on the Host computer screen.
Message path	<p>Specify the Guest computer (One Step) or Host computer (Display Message) path and name of the message file to (copy and) display.</p> <p>Click Browse to open a message file on the Guest computer and display its path and name in the field.</p> <p>NOTE: The Host computer Messages directory, which is located in the Netop configuration files directory, typically <code>C:\Documents and Settings\All Users\Application Data\Netop\Netop Remote Control\Host\Messages</code>, is identified by the environment variable <code>%RootConfig%Messages</code>. To display in the Message window on the Host computer screen, the message file name must use the syntax <code><Date>T<Time>;<Sender>.rtf</code> with the date format <code>YYYY-MM-DD</code> and the time format <code>HHMM-SS</code>.</p>

See also

- [Script](#)
- [Create and run a script](#)
- [Communicate with Host users](#)

5.2 Host dialog boxes

5.2.1 Advanced Help Request Options

Communication

Option	Description
Phone number or IP address	<p>If requesting help by a communication profile that uses a point-to-point or network point-to-point communication device other than Infrared (IrDA), a telephone number or IP address should be specified.</p> <p>If not specified in this field, the Connect to Help Provider dialog box will be displayed when requesting help, and you can specify the telephone number or IP address there.</p>
Help request timeout if not answered	Specify a number in the range to cancel the help request if not responded to by a help provider within the specified number of minutes (default: 0, i.e. the help request will not be canceled).

Gateway logon

If requesting help by a communication profile that uses a point-to-point or network point-to-point communication device through a Guest network Netop Gateway, it may request logon.

Specify Gateway logon name, password and domain in this section.

If valid Gateway logon credentials are not specified here, a Gateway logon dialog box may be displayed when requesting help, and you can specify the credentials there.

Select the **Use current logon credentials for Windows Security authentication** check box to log on by the name, password and domain of the user logged on to Windows on the Host computer.

See also

[Program Options](#) (Help Request tab)
[Request help](#)

5.2.2 Allowed ISDN Numbers

If Guest ISDN number check is enabled in the **Communication Profile Edit** dialog box for ISDN, a Host and a connecting Gateway can allow connections by ISDN (CAPI) communication only from telephone numbers in the **Allowed ISDN Numbers** list.

The **Allowed Network Numbers** dialog box displays allowed ISDN telephone numbers. You can add, edit and delete ISDN telephone numbers in the dialog box.

NOTE: Allowed ISDN numbers are stored in the Netop configuration file anumlist.ndb, which is typically located in the directory C:\Documents and Settings\All Users\Application Data\Netop\Netop Remote Control\

See also

[Communication Profile Edit](#)

5.2.3 Directory Service

Use the **Directory Service** dialog box to specify a directory service.

General

Option	Description
Name	Specify the name that should identify the directory service in Directory Services tab pane.
Directory server	Specify the directory server IP address or DNS name.
Port	Specify the port through which the Host should connect to this directory server (default: 389, the Lightweight Directory Access Protocol (LDAP) port). Select the Use secure connection check box to connect to the directory server by a secure connection. The LDAP secure connection port number is 636.
Base DN	Specify the directory service distinguished name from which a search should start.

Credentials tab

Use the **Credentials** tab to specify the credentials by which the Host should log on to the directory server. The credentials determine what directory service information is available to the Host.

Option	Description
Anonymous bind	Select this check box to search the specified directory service with anonymous user rights, which are typically very limited.
User DN	Specify a directory service user distinguished name to search the directory service with the rights of this user.
Password/Confirm password	Specify the corresponding password and confirm it.

Settings tab

Use the **Settings** tab to specify the search criteria that should be applied to retrieve the properties of a connecting Guest user. Initially, the fields are empty.

Click the **Default** button to display the **Select Directory Service** dialog box.

The drop-down list contains names of commonly used directory services such as Microsoft Active Directory. Select a directory service type in the drop-down list. If the directory service type of the directory server specified in the **Directory Server** field of the **Directory Service** dialog box is available in the list, select this in the list.

Click the **OK** button to close the dialog box and specify the default settings of the selected directory service type in the **Settings** tab fields.

NOTE: If the **Settings** tab fields are filled in when you select a directory service type in the **Select Directory Service** dialog box, you will typically not need to edit their contents.

Option	Description
User search filter	Optionally (recommended), specify a search filter to limit the search for user attributes to a certain object class.
User attribute	Specify the type designation of the searched for user attribute.
User browse filter	Optionally (recommended), specify a user browse filter to limit the browse for user attributes to certain object classes.
Group search filter	Optionally (recommended), specify a search filter to limit the search for group attributes to a certain object class.
Group attribute	Specify the type designation of the searched for group attribute.
Group browse filter	Optionally (recommended), specify a group browse filter to limit the browse for group attributes to certain object classes.
OU search filter	Optionally (recommended), specify a search filter to limit the search for organizational unit attributes to a certain object class.

See also

[Program Options](#) (Directory Services tab)

5.2.4 Guest Access Security

☐ Guest Access Privileges tab

Use the **Guest Access Privileges** tab to select the Guest access method to apply to connecting Guests.

Select a method in the **Guest Access Method** list:

Grant all Guests default access privileges

This selection means that all Guests share the same privileges and use the same password to log on to the Host.

When a Guest connects, the Host requests a password. If the Guest returns the password set up for the default user, the Host grants the Guest the privileges set up for the default security role.

☐ Setup

In the left pane, select **Default Security Role** to display the access privileges of this security role, i.e. what Guests should be allowed to do when connecting to the Host, in the right pane.

The **Confirm access** section in the right pane specifies whether and when access to the Host computer needs confirmation.

NOTE: For practical reasons, the **Netop message** and **Get inventory** functions have been exempted from **Confirm access** security, as these are often used when there is no user present on the Host side.

Select **Default User** in the left pane to set password and call back options. In the right pane, specify a password of max. 64 characters to enable shared password authentication.

To disable shared password authentication and request no password from a connecting Guest, clear both password fields. This, however,

leaves the Host without Guest access authentication, and any Guest can then connect to the Host. Unless suppressed, a security warning is displayed when the Host starts communicating.

The **Call back** section below the **Password** section specifies whether or not to use call back.

Option	Description
No call back	Do not apply call back.
Call back to	Specify a telephone number or an IP address to make the Host disconnect and reconnect to the specified telephone number or IP address, if a Guest connects by a communication profile that uses a point-to-point or network point-to-point communication device. Call back to a specified telephone number or IP address will enable connections only from a Guest on a computer with this telephone number or IP address.
Roving call back	Select this option to request a call back telephone number or IP address from a Guest that connects by a communication profile that uses a point-to-point or network point-to-point communication device. When the Host receives this information, it will disconnect and reconnect to the specified telephone number or IP address. Roving call back is typically used to make connection costs payable by the Host organization, e.g. when a traveling employee connects to the home computer.

Grant each Guest individual access privileges using Netop authentication

This selection means that each Guest has its own privileges and password to log on to the Host.

When a Guest connects, the Host requests the Netop credentials, i.e. ID and password, defined for that specific Guest. When the Guest returns the required information, the Host grants the Guest the privileges set up for the specific Guest.

Setup

Each security role specifies what is allowed to the Guest and the selected confirm access option. Each Guest profile specifies Guest logon credentials and the selected call back option.

Initially, the left pane contains the security role folders **Full access**, **View only**, **Inventory only** and **Remote Management** only. You can add a security role by clicking the **Add security role** button and defining the new security role by clearing check boxes in the right pane. Select an option in the **Confirm access** section to specify whether and when access to the Host computer needs confirmation.

You can add Guests to a security role by selecting it and clicking the **Add Guest** button. In the displayed **Guest Profile** dialog box, specify

Guest name, password and call back option. See [Guest Profile](#).

Select a Guest profile element in the left pane to display its **Password** section and **Call back** section to the right.

Grant each Guest individual access privileges using Windows Security Management

This selection means that each Guest has its own privileges and logs on to the Host by its Windows logon user credentials.

When a Guest connects, the Host requests the Windows user name, password and domain. If a match is found in Windows Security Management, the Host grants the Guest the privileges of the security role assigned to the Windows account object.

A Guest user who is assigned different security roles individually and as a member of groups is allowed what is allowed by any of the applicable security roles, i.e. the sum of privileges of the applicable security roles.

Setup

Each security role specifies what is allowed to the Guest and the selected confirm access option.

Initially, the left pane contains the security role folders **Full access**, **View only**, **Inventory only** and **Remote Management** only. Select a security role folder to display the privileges in the right pane. You can add a security role by clicking the **Add security role** button and defining the new security role by clearing check boxes in the right pane. Select an option in the **Confirm access** section to specify whether and when access to the Host computer needs confirmation.

You can add a user or group to a security role by selecting it and clicking the **Add User** or **Add Group** button. In the displayed **Select Users** or **Select Groups** dialog box, specify the users or groups you want to add.

Select a Windows user or group element to display its **Domain** section, **RAS** section and **Call back** section to the right.

The **Domain** section displays the domain of the selected Windows user or group.

The **RAS** section is only included if the Host computer runs on a Windows NT, 2000, XP, 2003, 2008, Vista or 7 operating system. Select the **Get call back information from Windows NT Remote Access Service (RAS)** check box to use call back information stored in Windows NT Remote Access Service.

The **Call back** section is only displayed if the check box in the **RAS** section is not selected.

Specify whether or not to use call back.

Option	Description
No call back	Do not apply call back.
Call back to	Specify a telephone number or an IP address to make the Host disconnect and reconnect to the specified telephone number or IP address, if a Guest connects by a communication profile that uses a point-to-point or network point-to-point communication device.

Option	Description
	Call back to a specified telephone number or IP address will enable connections only from a Guest on a computer with this telephone number or IP address.
Roving call back	<p>Select this option to request a call back telephone number or IP address from a Guest that connects by a communication profile that uses a point-to-point or network point-to-point communication device.</p> <p>When the Host receives this information, it will disconnect and reconnect to the specified telephone number or IP address.</p> <p>Roving call back is typically used to make connection costs payable by the Host organization, e.g. when a traveling employee connects to the home computer.</p>

The **Windows User Manager** button is included only if the Host computer runs on a Windows NT, 2000, XP, 2003, 2008, Vista or 7 operating system. Click this button to display the Windows user manager window according to the administrator rights of the user logged on to Windows on the Host computer to manage users and groups.

Grant each Guest individual access privileges using Directory services

This selection means that each Guest has its own privileges and logs on to the Host by directory services user credentials.

When a Guest connects, the Host requests the directory service user name, password and directory server for that specific Guest. If a match is found on the directory server, the Host grants the Guest the privileges of the security role assigned to the directory services account element.

A Guest user who is assigned different security roles individually and as a member of groups is allowed what is allowed by any of the applicable security roles, i.e. the sum of privileges of the applicable security roles.

Setup

Each security role specifies what is allowed to the Guest and the selected confirm access option.

Initially, the left pane contains the security role folders **Full access**, **View only**, **Inventory only** and **Remote Management** only. Select a security role folder to display the privileges in the right pane. You can add a security role by clicking the **Add security role** button and defining the new security role by clearing check boxes in the right pane. Select an option in the **Confirm access** section to specify whether and when access to the Host computer needs confirmation.

You can add a user or group to a security role by selecting it and clicking the **Add User** or **Add Group** button. In the displayed **Select Directory Services Users** or **Select Directory Services Groups** dialog box, specify the users or groups you want to add.

Select a directory services user or group element to display its **Directory service** section and **Call back** section to the right.

The **Directory Service** section displays the directory service name and the selected directory services user or group element distinguished name (dn).

Specify whether or not to use call back:

Option	Description
No call back	Do not apply call back.
Call back to	Specify a telephone number or an IP address to make the Host disconnect and reconnect to the specified telephone number or IP address, if a Guest connects by a communication profile that uses a point-to-point or network point-to-point communication device. Call back to a specified telephone number or IP address will enable connections only from a Guest on a computer with this telephone number or IP address.
Roving call back	Select this option to request a call back telephone number or IP address from a Guest that connects by a communication profile that uses a point-to-point or network point-to-point communication device. When the Host receives this information, it will disconnect and reconnect to the specified telephone number or IP address. Roving call back is typically used to make connection costs payable by the Host organization, e.g. when a traveling employee connects to the home computer.

Use Netop Security Server

This selection means that the Host will use Netop Security Server to authenticate each connecting Guest and assign a security role to it.

When a Guest connects, the Host requests logon credentials according to Netop Security Management preferences. For further information about Netop Security Management, see the Administrator's Guide.

The Host forwards returned credentials to Netop Security Server for validation and compilation of the security role that is to be assigned to the Guest according to the security data stored in the security database. The Host applies the resulting security role to the Guest.

Setup

The **Public Key** field is used to secure a trusted connection between your Hosts and Security Servers.

NOTE: In production environments, we recommend that you replace the default Public Key with a newly generated Public Key using the Security Manager.

The Public Key should be copied to the Hosts exactly as it is shown in the Security Manager. It is recommended that you change the Public Key before deploying your Hosts.

For more information about generating a Public Key from the Security Manager, see the Netop Security Management section in the Administrator's Guide.

Use Netop Portal access rights

This selection means that the Host will use Netop Portal to authenticate each connecting Guest and assign permissions to it.

When a Guest connects, the Host requests logon credentials according to the Netop Portal account. For further information about Netop Portal, see the Netop Remote Control Portal User's Guide.

The Host forwards returned credentials to Netop Portal for validation and compilation of the security permissions that are to be assigned to the Guest. The Host applies the resulting security permissions to the Guest.

Guest Policy tab

Use the **Guest Policy** tab to specify Guest access security policies. The policy functions determine how the Host behaves before, during and after the remote control session.

Password

Option	Description
Maximum invalid password attempts	Specify a number in the range 0 - 9 for the number of logon attempts that should be allowed to a Guest before the action selected in the drop-down list below will be executed.
Action if maximum attempts are exceeded	In the drop-down list, select what should happen if maximum password attempts are exceeded: <ul style="list-style-type: none"> • Disconnect: Disconnect the Guest. • Disable Host: Make the Host reject any connection attempt. • Restart Windows: Restart Windows on the Host computer, which - depending on the Host setup - may load and start the Host and make it available for connection.

Disconnect

Option	Description
Action after disconnect	In the drop-down list, select what should happen after disconnect: <ul style="list-style-type: none"> • None: No action. • Lock computer: Lock the Host computer. The Windows Computer Locked window is displayed. The Host will remain running and available for connection. • Log off Windows: Log off the Host computer user from Windows. The Welcome to Windows window is displayed. The Host will remain running and available for connection. • Restart Windows: Restart Windows on the Host computer, which - depending on the Host setup - may load and start the Host and make it available for connection.
System-wide	Select any of the first four check boxes and optionally specify a

Option	Description
disconnect hotkey	character in the last check box to compose a keystroke combination that will disconnect all connected Guests whether the Host window is active or not.

File Transfer

Select the **Disable file transfer before local logon** check box to disable file transfer if no user is logged on to the Host computer.

Record Sessions

Option	Description
Enable	Select this check box to enable Host recording of remote control sessions. If you enable the Record Sessions function, you will be able to document any unauthorized procedures that a Guest might carry out on the Host.
Folder	Specify the path of the directory in which session recording files should be saved. Click the Browse button to select a folder, the path of which will be specified in the field.
Disconnect if recording fails	Select this check box to disconnect if session recording fails. NOTE: Session recording files will be named <Time stamp>- <Guest ID>- <Host ID>.dwr. You only can play back session recording files on a Guest.

Timeout

Option	Description
Confirm Access	Specify a number in the range 1 - 9999 to disconnect if the Host user has not confirmed Guest access within the specified number of seconds.
Authentication	Specify a number in the range 1 - 9999 to disconnect if Guest authentication has not completed within the specified number of seconds.
Inactivity	Specify a number in the range 1 - 9999 to disconnect if there has been no Guest keyboard or mouse activity within the specified number of seconds.

MAC/IP Address List Setup tab

MAC/IP Address List

Select the **Enable MAC/IP address check** check box to limit the network addresses from which a Guest can connect to the addresses specified in the pane.

Click the **Add** button to specify MAC/IP addresses.

MAC addresses will apply if communicating by NetBIOS or IPX. IP addresses will apply if communicating by TCP/IP or TCP/IP (TCP).

Encryption tab

The communication between Netop modules is protected by encrypting transmitted data.

A range of encryption types is available on Netop Remote Control modules.

Communicating Netop modules will automatically negotiate to encrypt communication by an encryption type that is enabled on both modules. Netop modules on which no common encryption type is enabled cannot communicate.

Select the check boxes next to the various encryption types to enable them.

To see encryption details about the individual encryption types, select an encryption type and click the **Show Details** button.

Smart Card

Use the **Smart Card** tab to specify Smart Card logon options to use Smart Card for authentication with Windows Security Management or Directory Services.

Windows Security Management

If you have selected the Guest access method **Grant each Guest individual access privileges using Windows Security Management** on the **Guest Access Privileges** tab, select an option in this section.

Option	Description
Never log on with Smart Card	Enable only credentials logon.
Always log on with Smart Card	Enable only Smart Card logon.
Allow both logon with Smart Card and credentials (name, password and domain)	Enable both credentials and Smart Card logon.

Directory Services

If you have selected the Guest access method **Grant each Guest individual access privileges using Directory services** on the **Guest Access Privileges** tab, select an option in this section.

Option	Description
Never log on with Smart Card	Enable only credentials logon.
Always log on with Smart Card	Enable only Smart Card logon.
Allow both logon with Smart Card and	Enable both credentials and Smart Card logon.

Option	Description
credentials (name, password and server)	
Subject Field	Retrieve the user identification from the Subject field of the Smart Card certificate.
Subject Alternative Name Field (must be a User Principal Name (UPN))	Retrieve the user identification from the Subject Alternative Name field of the Smart Card certificate.
The Certificate Field matches this Directory Services Attribute	<p>Specify the directory services attribute compatible with the Smart Card certificate field contents. This is necessary only if different from a user object distinguished name.</p> <p>For Directory Services Smart Card logon to succeed, the Host must be able to resolve the Smart Card certificate user identification into a Directory Services user identification. If the Smart Card certificate user identification and Directory Services user identifications are incompatible, Smart Card logon will fail.</p> <p>To find available Smart Card certificate user identifications, insert the Smart Card and in Internet Explorer click the Internet Options command on the Tools menu to display the Internet Options dialog box.</p> <p>On the Content tab, click Certificates to display the Certificates dialog box.</p> <p>On the Personal tab, double-click the appropriate certificate record to display the Certificate dialog box. The Details tab displays the contents of available certificate fields including Subject and Subject Alternative Name.</p>

See also

[Program Options](#) (Smart Card tab)

5.2.5 Guest Profile

Use this dialog box to create a Guest profile element in the security role folder that you selected on the **Guest Access Privileges** tab.

Guest name

In the **Guest ID** field, specify the name that a Guest using this Guest profile should specify to log on to the Host. This will be the name that identifies the Guest profile.

NOTE: A Guest is not limited to logging on by the name that identifies the Guest. Guest logon does not verify Guest identity but validates Guest credentials.

Password

In the **Password** section, specify a password of max. 64 characters to enable password authentication.

Call back

In the **Call back** section specify whether or not to use callback.

Option	Description
No call back	Do not apply call back.
Call back to	Specify a telephone number or an IP address to make the Host disconnect and reconnect to the specified telephone number or IP address, if a Guest connects by a communication profile that uses a point-to-point or network point-to-point communication device. Call back to a specified telephone number or IP address will enable connections only from a Guest on a computer with this telephone number or IP address.
Roving call back	Select this option to request a call back telephone number or IP address from a Guest that connects by a communication profile that uses a point-to-point or network point-to-point communication device. When the Host receives this information, it will disconnect and reconnect to the specified telephone number or IP address. Roving call back is typically used to make connection costs payable by the Host organization, e.g. when a traveling employee connects to the home computer.

See also

[Guest Access Security](#) (Guest Access Privileges tab)

5.2.6 Help Providers

In connection with a help request, if help providers are found, but no problem description and/or no Help provider was specified in the **Program Options** dialog box on the **Help Request** tab, the **Help Providers** dialog box is displayed.

Specify a problem description and a help provider:

Option	Description
Problem description	This field will display any problem description specified in the Program Options dialog box on the Help Request tab. You can leave the field empty or specify or edit a problem description.
Help providers	Names of help providers found (on Netop Guest named help services) are displayed in the Help providers pane. Select one and click Select to deliver the help request to the selected help provider.

5.2.7 Help Request

Select one of these options:

Option	Description
Use help service to search for help	Select this option to request help from a help service.

Option	Description
providers	
Use service ticket to connect to a specific help provider	<p>Select this option to request help by a received service ticket number.</p> <p>Selecting this option enables the following fields:</p> <ul style="list-style-type: none"> • Service ticket: In this field, specify the service ticket number. • Problem description: In this field, you can describe your problem.

NOTE: This dialog box will display only the service ticket fields if **Enable Service Tickets** has been selected in the **Program Options** dialog box on the **Help Request** tab. A Netop OnDemand enabled Guest can issue service ticket numbers and forward a service ticket number to you to enable you to return a help request.

See also

[Set up Help Request on Guest and Host Program Options](#) (Help Request tab)

5.2.8 Maintenance Password

You can protect the Host setup with a maintenance password, so that no unauthorized people can make changes to the Host setup.

Use the **Maintenance Password** dialog box to specify a maintenance password, what it protects, and Host configuration files (.ndb) protection.

Click the **Change Maintenance Password** button to display the **Change Maintenance Password** dialog box, where you can specify the maintenance password (max. 64 characters), change it, or disable it by deleting it.

Specify what the maintenance password should apply to and when:

Maintenance password required for

Option	Description
Guest access security	Select this check box to apply maintenance password protection to the Guest Access Security command on the Tools menu and the Guest Access Security button on the toolbar.
All other configuration	Select this check box to apply maintenance password protection to all other setup commands on the Tools menu and other tool buttons on the toolbar.
Unload and Stop	<p>Select this check box to apply maintenance password protection to unloading the Host and stopping the Host.</p> <p>Apply Unload and Stop maintenance password protection to prevent Host stop or unload that will make it unavailable for connection and/or to protect security configuration files.</p>
Confirm access	<p>Select this check box to require the user to enter the maintenance password before the remote session can begin.</p> <p>Using Confirm access, the local user on the Host machine has the ability</p>

Option	Description
	to allow or deny the remote session. In some situations, such as large industrial environments or senior executives within a large organization, the maintenance password is often known by the local Host user. As an extra level of security and to help prevent unauthorized users from allowing the remote support session, the local user on the Host machine can now enter the maintenance password in the Confirm Access Password dialog box before the remote session can begin.

Protect security configuration files

Option	Description
Protect by maintenance password only (if applies)	Protect Host setup only by any applied maintenance password protection. This does not protect Host configuration files (default selection).
Protect files when connected	Protect Host configuration files and disable setup commands on the Tools menu when the Host status is "Connected" to prevent a connected Guest from changing Host setup.
Protect files when connected and running	Protect Host configuration files and disable setup commands on the Tools menu when the Host status is "Connected", "Help requested" or "Running" to prevent a Host computer user from changing the Host setup. Combined with the Unload and Stop option, the maintenance password protection also prevents the Host user from stopping and unloading the Host and then changing the Host security configuration files.

NOTE: Host configuration files (.ndb) are located in the Netop configuration files folder, typically C:\Documents and Settings\All Users\Application Data\Netop\Netop Remote Control\Host.

If maintenance password protection is enabled, a dialog box prompting you to enter the maintenance password is displayed when you select a protected command or click a protected button.

There is no limit to the number of maintenance password attempts.

5.2.9 Program Options

☐ General Tab

Use the **General** tab to specify startup and connection options.

Startup

Option	Description
Start Host when loaded	Select this check box to start the Host and enable communication when loaded.
Load Host at Windows startup (run as service)	Select this check box to load the Host when Windows starts on the computer.

Option	Description
	NOTE: Loading the Host at Windows startup and starting the Host when loaded will make the Host ready for connection when the Host computer is started, even if no user is logged on to Windows.
Minimize Host when loaded	Select this check box to minimize the Host to a Netop Host icon when loaded.
Stealth mode (hide Host when started)	Select this check box to load the Host hidden to the Host computer user. If hidden, nothing on the screen will indicate that the Host is loaded. NOTE: To display a hidden Host, run <code>SHOWHOST.EXE</code> which is typically located in the folder where the Host is installed.

Connection

Option	Description
Minimize Host on connection with Guest	Select this check box to minimize the Host window to a Netop Host icon when a Guest connects.
Host top most window on connection with Guest	Select this check box to display the Host window in front of any other window when a Guest connects.
Show file transfer status	Select this check box to display the File Transfer Status window when a Guest starts a file transfer session.
Send keep alive message	Select this check box to send a data packet at intervals while connected to alert the Host user if the connection is lost. NOTE: To maintain an ISDN (CAPI) connection during short periods of inactivity, do not select this check box. Instead select the Short-hold mode check box in the Edit dialog box for the ISDN (CAPI) communication profile.
Allow Multiple Simultaneous Guest Sessions	Select this check box to allow multiple Guest connections to the Host at the same time.

Host Name tab

Use the **Host Name** tab to specify Host naming, name options and the Netop Name Server name space ID.

Naming

This section specifies the name by which the Host will identify itself when communicating.

To communicate by a communication profile that uses a networking communication device (NetBIOS, IPX, TCP/IP, Terminal Server), each Host must use a unique name. A Host that uses a name that is already used by another communicating Host will be denied communicating.

Select one of these options:

Option	Description
Enter name or leave name field blank	Select this option to display a field below. Specify a name in the field or leave the field blank to name the Host by the specified name or leave it without a name.
Use environment variable	<p>Select this option to display a field below. Specify an environment variable name in the field to name the Host by the value of the specified environment variable.</p> <p>NOTE: Do not name a network computer Host by the environment variable <code>USERNAME</code> if it is set up to load at Windows startup. If you do that, the Host will load before a user logs on to Windows to get the name <code>%USERNAME%</code> and retain this name until reloaded while a user is logged on to get the name <code><Windows logon user name></code>. Of multiple Hosts named <code>%USERNAME%</code>, only one can communicate.</p> <p>Name a terminal server session Host typically by the environment variable <code>USERNAME</code>. See the Administrator's Guide, Netop Naming (TSE). To display available Windows environment variables, in a command prompt window type <code>set</code> and press ENTER.</p>
Use Windows computer name	<p>Name the Host by the Host computer Windows name.</p> <p>NOTE: Name a network computer Host typically by the Windows computer name. Do not name a terminal server session Host by the Windows computer name. Terminal server session Hosts share the Windows computer name of the terminal server computer. Of multiple Hosts named by the terminal server computer name, only one can communicate.</p> <p>Select the Prefix with computer workgroup name check box to add a prefix to the Host computer name to ensure Host name uniqueness across multiple domains and workgroups. The prefix can be its domain or workgroup name.</p> <p>Use the Separate with field to specify the separator character. The default character is a back slash (<code>\</code>), but you can replace it by any other character.</p>
Name	The Host name according to the selection above.

Name options

Option	Description
Public Host name	<p>Select this check box to respond to Guests that browse for Hosts by the Host name.</p> <p>NOTE: If the Host computer is connected directly to a public network like the Internet, you may want to clear the selection of this check box to not invite hacking attempts.</p>
Enable user name	<p>Select this check box to enable the name of a user logged on to the Host computer to enable connections by the user name.</p> <p>NOTE: If this check box is selected, the user name will appear on the</p>

Option	Description
	Names tab of the Host window. You may want to clear the selection of this check box on a server Host to disable connecting by the name of a temporarily logged on user or the user as which the Host runs to acquire the computer rights of the user.

Netop Name Server

In the **Name Space ID** field specify the name space ID specified on Guests with which the Host should be able to communicate by using Netop Name Server. The default name space ID is PUBLIC.

The name space ID will apply only if the Host communicates by a communication profile that uses the TCP/IP communication device and for which the **Use Netop Name Server** check box in the **Advanced TCP/IP Configuration** window is selected and Netop Name Servers are specified.

NOTE: For changes to naming or name space ID to take effect, you must restart the Host.

☐ Connection Notification tab

Use the **Connection Notification** tab to specify options for connection notification upon, during and after connection.

Upon connection

Option	Description
Play sound	Select this check box to play a sound when a Guest connects. The sound file <code>StartHRC.wav</code> is located in the Media folder of the folder in which the Host is installed.
Display Connection List	Select this check box to display the Connection List window when a Guest connects. Specify in the field to the right the number of seconds that this window should be displayed. Default is 6. The value 0 makes the Connection List window remain on the screen.
Password to close Connection List	Select this check box and specify a password in the field below to make the Connection List window remain on the screen until closed manually. Characters will display as dots or asterisks. To close the Connection List window, you will then be prompted to enter the specified password.
Display balloon tip	Select this check box to display a balloon tip from the Netop Host icon when a Guest connects.

During connection

Option	Description
Play sound	Select this check box to play a sound during Guest connection at this

Option	Description
	<p>interval.</p> <p>In the Interval field specify a number in the range for the interval between sounds in seconds.</p> <p>The sound file ContHRC.wav is located in the Media folder of the folder in which the Host is installed.</p>
Display Guest name (if available) in the title bar	Select this check box to display the connected keyboard and mouse control Guest name in the title bar, the Windows taskbar Netop Host icon and the Netop Host icon tool tip.
Animate icon	Select this check box to animate the Netop Host icon double corner lines during Guest connection.

After connection

Option	Description
Display History List	<p>Select this check box to display the History List window when a Guest disconnects.</p> <p>Specify in the field to right the number of seconds this window should be shown. Default is 0. The value 0 makes the History List window remain on the screen.</p>
Password to close History List	<p>Select this check box and specify a password in the field below to make the History List window remain on the screen until closed manually.</p> <p>Characters will display as dots or asterisks.</p> <p>To close the History List window, you will then be prompted to enter the specified password.</p>
Display balloon tip	Select this check box to display a balloon tip from the Netop Host icon when a Guest disconnects.

Audio-Video Chat tab

Use the **Audio-Video Chat** tab to specify audio and video settings.

Audio Chat

General

Select the **Enable full-duplex audio** check box to enable sending audio data between Guest and Host in both directions at the same time.

NOTE: Some computer audio systems do not support full-duplex audio.

Microphone sensitivity

Option	Description
Silence level	Drag the slider bar to specify the microphone sound input level below

Option	Description
	which no sound data should be transferred.
Line hold	<p>Drag the slider bar to specify the time period in which sound data should continue to be transferred after the microphone sound input level has dropped below the silence level.</p> <p>TIP: Try out different Silence level and Line hold settings to optimize sound transfer.</p>

Click the **Check sound system** button to test the computer sound system.

Click the **Advanced** button to display the **Advanced audio settings** dialog box. See [Advanced audio settings](#).

Video Chat

Click the **Advanced** button to display the **Advanced Video** dialog box. See [Advanced Video](#).

Remote Printing tab

Use the **Remote Printing** tab to specify remote Netop printers.

Click the **Add Printer** button to add a remote printer. Follow the guidelines in the displayed **Add printer guidelines** dialog box, and click **Ready** to start adding a remote Netop printer.

The remote printers that you add, will be displayed in the **Remote Netop printers** pane.

You can remove a Netop printer by selecting it in the pane and clicking the **Remove Printer** button.

To send a Host computer print job to a Guest printing device while the Guest is connected, print to a Host computer remote Netop printer that specifies the Guest printing device.

NOTE: Special instructions for remote printing from DOS applications are available in the [Netop KnowledgeBase](#).

See also

[Send a print job to a remote printer](#)

Help Request tab

Use the **Help Request** tab to specify general help request options. If unspecified, the Host user can specify individual options with each help request.

Optional help information

Option	Description
Problem description	<p>To always specify the same problem description, specify it in this field.</p> <p>If the field is left empty, the Help Providers window will be displayed when requesting help, allowing you to specify a problem description for the individual help request.</p>
Help provider	<p>To always request help from the same help provider (help service), specify its name in this field.</p> <p>If the field is left empty, the Help Providers window will be shown</p>

Option	Description
	when requesting help, allowing you to specify a help provider for the individual help request.

Communication

Communication profile

Option	Description
Use current Host communication profiles	Select this option to send help requests by enabled communication profiles. Unless only one communication profile or only communication profiles that use networking communication devices are enabled, the Select Help Request Communication Profile dialog box will be displayed when requesting help.
Use specific Communication Profile	Select this option and select one of the available Host communication profiles in the drop-down list to use a specific communication profile.

Click the **Advanced** button to display the **Advanced Help Request Options** dialog box. See [Advanced Help Request Options](#).

Options

Option	Description
Add Help Request icon to the tray	Select this check box to add a help request icon (a life belt) to the notification area in the lower right corner of the screen. If this icon is added, the Host computer user can request help even if the Host is hidden. To request help, double-click the icon or right-click the icon and select Request Help .
Enable Help Service	Select this check box to enable help request by a help service.
Enable Service Tickets	Select this check box to enable help request by a service ticket.

See also

[Request help](#)
[Set up Help Request on Guest and Host](#)

☐ Run As tab

Use the **Run As** tab to enable running the Host with the rights of a Windows user account if no user is logged on to the Host computer, the Host will run with extensive Host computer rights but no network computer rights. See the Administrator's Guide, Netop Remote Control Processes and Windows Security. If a user is logged on to the Host computer, the Host will run with the rights of the logged on user.

Run Host as specific user

Option	Description
Enable	Select this check box to always run the Host as a specific Windows user account.
User name	Specify the Windows user account name.
Password	Specify the corresponding password.
Domain	Specify the corresponding domain. CAUTION! Consider carefully in each case the benefits and drawbacks including security risks of always running the Host as a specific Windows user account. In some cases, you should run the Host as a Windows user account created exclusively for this purpose.
Automatically change to random password every week	Select this check box to change the password of the credentials specified above immediately and every week into a random password to automatically satisfy a password change policy. CAUTION! Do not select this check box if the credentials specified above belong to a user person, as the user person cannot know the random password.

Directory Services tab

Use the **Directory Services** tab to specify directory services to enable authenticating connecting Guests.

Click the **Add** button to add a directory service. The **Directory Service** dialog box in which you can specify the directory service that you want to use is displayed. See [Directory Service](#).

The name of the directory service and the directory server IP address or DNS name is displayed in the pane on the **Directory Services** tab.

To edit the properties of the directory service record, select the record in the pane and click the **Edit** button.

To remove the directory service, select the record in the pane and click the **Delete** button.

See also

[Guest Access Security](#)(Grant Each Guest Individual Access Privileges Using Directory Services tab).

Multi-Factor Services tab

Use the **Multi-Factor Services** tab to enable multi-factor authentication when connecting Guests.

Click the **Add** button to add the corresponding Multi-Factor service. The **Multi-Factor Service** dialog box in which you can specify the multi-factor service that you want to use is displayed.

Multi-Factor Service Settings

Option	Description
Name	Specify a name for the multi-factor service to be defined.
Multi-Factor Service Type	The list of services which help safeguard access to data and applications. Netop Remote Control currently provides integration to Windows Azure Multi-Factor Authentication.
Client Certificate	Click the Choose certificate... button and browse for the Windows Azure certificate to be used for the Windows Azure Multi-Factor Authentication.
LDAP Phone No Attribute	The LDAP attribute identifying the user's telephone number. It will be used to send user the token to be used for multi-factor authentication.
Apply to all roles	Select this check box to apply the current multi-factor authentication service to all roles defined in the Directory Services. Note: Multi-factor authentication applies to all roles only if the Guest Access Method selected from Tools > Guest Access Security is either Grant each Guest individual access privileges using Windows Security Management or Grant each Guest individual access privileges using Directory services .

To edit the properties of the Multi-Factor service record, select the record in the pane and click the **Edit** button.

To remove the multi-factor service, select the record in the pane and click the **Delete** button.

In case there are multiple roles which can apply for a specific authenticating user, each potentially with a different multi-factor authentication services, the multi-factor authentication service to be chosen is the one with the highest priority from the list. Order in the list dictates the priority, top items having the highest priority.

See also

[Guest Access Security](#) (Grant Each Guest Individual Access Privileges Using Directory Services tab).

Web Update tab

Use the **Web Update** tab to specify web update options to automatically update the Host installation.

Web Update Settings

Option	Description
Update server	Specify the web address of the server from which to download Host update files (default: update.netop.com, the Netop manufacturer web update server). NOTE: To update many Netop installations in an organization, we recommend publishing new updates to an internal web update server

Option	Description
	(select Publish New Updates on the Tools menu).
HTTP Proxy	<p>Specifying a HTTP proxy is typically not required.</p> <p>Before specifying a HTTP proxy, click Update now to test the web update connection. If you receive a message indicating connection to the update server, specify no HTTP proxy.</p> <p>If Update now yields no connection, click the Detect button to make Netop attempt to detect the HTTP proxy server and display its name and port number in the HTTP Proxy field.</p> <p>Click Update now to test the connection. If unsuccessful, consult your network/system administrator about what to specify in the HTTP Proxy field (format: <Server name>:<Port number>).</p>
Update now	<p>Click this button to connect to the update server specified in the Update server field.</p> <p>A web update message will notify you if connection to the update server fails, if no updates are available or if updates are available, and in the latter case ask you if you want to download and install updates.</p>
Schedule	<p>Click this button to display the Web Update Schedule dialog box and specify a schedule of checks for updates including download and installation of available update files.</p>

5.2.10 Select Directory Services Users or Groups

The **Select Directory Services Users** dialog box and the **Select Directory Services Groups** dialog box are similar.

The directory services users or groups that you add here are added to the security role selected in the **Guest Access Security** dialog box on the **Guest Access Privileges** tab.

The upper pane displays directory services specified in the **Program Options** dialog box on the **Directory Services** tab.

Users or groups are displayed below the individual directory services in the pane.

Select a user or group in the upper pane and click the **Add** button. The user or group is added to the lower pane. They are displayed by their distinguished name, i.e. directory path and common name of the user/group, and the directory service name as specified in the **Program Options** dialog box on the **Directory Services** tab.

See also

[Guest Access Security](#) (Guest Access Privileges tab)
[Directory Service](#)

A

- Active Management Technology (AMT) 26, 27, 29
- Add to Phonebook 7
- adding a remote printer 50
- adding phonebook references 11
- adding sections 22
- Advanced audio settings dialog box 55
- Advanced Help Request Options dialog box 115
- Advanced Help Service dialog box 55
- Advanced inventory option dialog box 56
- Advanced TCP/IP Configuration dialog box 57
- Advanced Video dialog box
 - compression 58
 - driver 58
- alerts 29
- Allowed Network Numbers dialog box 115
- AMT (Active Management Technology) 26, 27, 29
- AMT, vPro 26, 27, 29
- audio 55
- audio-video chat 42, 49, 128
- authentication
 - Digest 27
 - Kerberos 27

B

- bindings 57
- BIOS 26, 29
- Blank Display 11
- booting 26, 29
- browsing for Hosts 6

C

- cache 66
- call back 117, 125
- capturing video 52
- certificate 27
- chat 42, 49, 128
- clickable bitmap 40
- clipboard 48
- cloning files 36, 94
- Command Console 20
- command prompt 20
- communicating with Guest user 42

- communicating with Host user 49
- communication 66
- communication devices 59, 65
- Communication Profile Edit dialog box 59
- Communication Profile Setup dialog box 65
- communication profiles 5, 44, 59, 65
- Compression/Encryption 66
- Connect 66
- connect problems 76
- Connect to Host dialog box 65
- Connect using
 - communication profile 65
 - local 65
 - phonebook file 65
- connecting 6, 41
- connection 128
- Connection Properties dialog box
 - Compression/Encryption tab 66
 - Connect tab 66
 - Custom tab 66
 - Desktop tab 66
 - Display tab 66
 - Keyboard/Mouse tab 66
 - Logon tab 66
 - Protect Item tab 66
 - Record tab 66
 - Startup tab 66
- copying 24
- copying files 36
- credentials 27, 125
- Custom 66
- custom inventory items 12, 56
- Custom Inventory Items dialog box 77
- customizing commands 29
- cycling power off and on 29

D

- demonstrating 51
- Desktop 66
- Directory Service dialog box 116
- directory services 117, 128, 137
- Disconnect, Host 43
- disconnecting 41

Contents

Disk Drives	16
Display	66
E	
editing communication profiles	59
editing phonebook records	8
Encryption	99, 117
ending a remote control session	6
ending a session, Host	43
error handling	77
Event Management tab	29
Event Properties	16
Event Viewer	16
Execute Command	14
executing system control commands	14
exporting phonebook data	10
F	
File Manager	36
File Manager Options dialog box	94
file transfer	24, 36, 94
confirming deletion/overwriting	94
filters	29
G	
Gateway	4, 59
generating inventory	12
Get Inventory	12
Global Settings dialog box	77
groups	117
Guest	4
Guest Access Privileges	117
Guest Access Security	4, 125
Guest Access Security dialog box	117
Guest ID	125
Guest Policy	117
Guest Profile dialog box	125
H	
help provider	41, 44, 115, 126
Help Providers dialog box	126
help request	41, 46, 126, 128
executing actions	55
Gateway logon credentials	115
IP address	115
notification	55
phone number	115
Remote Control	99
Remote Control OnDemand	99
running a local program	55
sending a message	55
setting up	44
Help Request dialog box	126
Help Request setup	
Guest	44
Host	44
Help Request tab	46
help service	41, 44, 99, 126, 128
Host	4
Host inventory	12
Host name	128
Host name qualifier	59
Host PC information	66
I	
IDE redirection	29
importing phonebook data	10
incoming help requests	46
integrating applications	22
Intel Active Management Technology	26
Intel Setup and Configuration Service	26
Intel vPro	26, 99
Intel vPro Event Log	29
Intel vPro tab	27
interface	57
inventory	12, 20, 77, 99
Inventory dialog box	75
Inventory tab	12
IP address	57
IP broadcast list	
DNS name	79
IP address	79
IP Broadcast List dialog box	79
IPX communication	98
ISDN communication	115

K

- keyboard and mouse control 11
- Keyboard/Mouse 66
- keystrokes, sending 47

L

- Local Users and Groups 20
- Lock Keyboard and Mouse 11
- Lock Workstation 14
- log file 77
- Log Off 14
- Log Properties 16
- Log Setup dialog box (Host) 80
- logging
 - file transfer 94
- logging events
 - Log Locally 38
 - Log on Netop Server 38
 - Log to Windows Event Log 38
 - Log using SNMP Traps 38
- logging events (Host)
 - locally 80
 - on Netop server 80
 - to Windows event log 80
 - using SNMP traps 80
- Logon 66

M

- MAC/IP Address List Setup 117
- magnifying on Host screen 53
- maintenance password 4
- Maintenance Password dialog box 127
- managing
 - alerts 29
 - filters 29
 - subscriptions 29
- Marker Mode 53
- marking objects on Host screen 53
- masking windows 51
- message 49
- Microsoft Management Console (MMC) 15
- MMC (Microsoft Management Console) 15
- Modem Configuration dialog box 98

- Modem dialog box 97
- monitoring Hosts 13
- moving files 36
- multi chat session 49
- multi Guest session 46
- multimedia devices 55

N

- Name Not Found dialog box 76
- Name Server 4
- name space ID 128
- naming 128
- Netop authentication 117
- Netop log
 - event codes and arguments (Guest) 84
 - event codes and arguments (Host) 87
- Netop Marker Utility 53
- Netop Name Server 57, 128
- Netop OnDemand
 - Help Request 126
- Netop Screen Video 52
- Netop Security Server 117
- Netop Skin Designer 40
- Netop Tunnel 33
- notification 128
 - animated Host icon 41
 - balloon tip 41
 - connection list 41
 - history list 41
 - Host title bar 41
- Novell Network Numbers dialog box 98

O

- Options
 - File Manager 94
- organizing 9
- overwrite/delete 77

P

- password 125
- phonebook 8, 11
 - creating records in 7
 - exporting data 10
 - folders 9

Contents

phonebook	8, 11	Host Name tab	128
History tab	7	Multi-Factor Services tab	128
importing data	10	Remote Printing tab	128
Quick Connect tab	7	Run As tab	128
Remote Desktop access	11	Web Update tab	128
save connection information to	7	Protect Item	66
phonebook records		protecting phonebook record files	9
password protection	9	protecting setup with a password	127
Phonebook tab	7, 11	provider	126
playback device	55	provisioning	26
playing back session recordings	39	public key	117
port numbers	57		
powering off, on	29	R	
processing inventory information	12	RDP	11
Program Options dialog box, Guest		rebooting	29
Audio-Video Chat tab	99	Record	66
Cache tab	99	Record Session	39
Clipboard tab	99	recording device	55
Directory Services tab	99	redirecting a print job	50
Encryption tab	99	redirecting print jobs	51
General tab	99	redirection	26
Help Request tab	99	Registry	
Host Name tab	99	Keys pane	17
Intel vPro tab	99	Values pane	17
Inventory tab	99	Remote Control modules	4
Layout tab	99	Remote Control OnDemand	44
Logon tab	99	Remote Desktop access	11
Monitor tab	99	phonebook	11
Recording tab	99	Remote Desktop Entry	11
Remote Control tab	99	Remote Management	15
Remote Printing tab	99	Disk Drives	16
Run tab	99	Event Viewer	16
Skins tab	99	Registry	17
Smart Card tab	99	Services	17
Sounds tab	99	Task Manager	17
Web Update tab	99	Windows Event Log	16
Program Options dialog box, Host		Remote Management pane	15
Audio-Video Chat tab	128	remote printing	50, 51
Connection Notification tab	128	requesting help	41
Directory Services tab	128	responding to a help request	46
General tab	128	Restart	14
Help Request tab	128	Retrieve from Host	48
		Run dialog box	112

- Run Program 35
- running a program 99
- running a program after inventory scan 56
- running a program on a Host 35
- running a remote program 112
- running a script
 - File Manager 36
- running Host as specific user 128

S

- Save Screen to Clipboard 48
- Save Screen to File 48
- script 77
 - commands 112
 - creating 24
 - global settings 112
- Script command
 - Inventory 75
 - Send Message 114
- script commands 24
- Script dialog box 112
- SCS 26
- Secure Tunnel 33
- security 4
- security roles 117
- Security Server 4
- Select Directory Services Users or Groups dialog box 137
- Send Alt+Print Screen 47
- Send Alt+Shift+Tab 47
- Send Alt+Tab 47
- Send Clipboard 48
- Send Ctrl+Alt+Del 47
- Send Ctrl+Esc 47
- Send Message dialog box 114
- Send Print Screen 47
- sending a print job to a remote printer 50
- sending keystrokes 47
- sensors 29
- service tickets 44, 46, 126, 128
- Services 17
- session
 - ending 6
 - starting 6

- session recordings 39
- Sessions 23
- Shared Folders
 - Shares tab 19
 - special shares 19
- Shares tab 19
- sharing your screen 51
- Shut Down 14
- Skin Repository Server 40
- skins 40, 66, 99
- Smart Card 99, 117
- special shares 19
- starting a remote control session
 - Help Request tab 6
 - History tab 6
 - Netop Network tab 6
 - Phonebook tab 6
 - Windows Network tab 6
- startup 66, 128
- subscriptions 29
- support 126
- synchronizing 94
- synchronizing files 36
- System Control
 - actions to perform 20
 - current host state 20
 - displaying a message on the Host computer 20
 - options 20

T

- Task Manager 17
- TCP/IP
 - UDP 59
- TCP/IP (TCP IPv6) 59
- TCP/IP (TCP) 59
- TCP/IP, advanced options 57
- Terminal Server 59
- tickets 44, 46, 99
- TLS (Transport Layer Security) 27
- transfer 77
- transfer clipboard 48
- transferring files 36
- Transport Layer Security (TLS) 27

Contents

Tunnel 33

U

user name 128

users 117

using skins 40

V

video 52

vPro

add to phonebook 27

vPro Console 26, 29

logging on 27

vPro, AMT 26, 27, 29

W

Wake on LAN 14

web update 99, 128

WebConnect 59

WebConnect tickets 44, 46, 99

Windows computer name 128

Windows event log 16

Windows Security Management 117

writing on Host screen 53