NETOP REMOTE CONTROL FOR LINUX AND MAC USER'S GUIDE

NETOP®

RemoteControl

Secure Remote Management and Support

31 January 2017

NETOP

RemoteControl

Please send any comments to:

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

The document is optimized for double-sided printing.

Contents

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**: 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.

1.2 Security

The **Guest Access Security** functions of the Host can protect against unauthorized access and limit the actions available to the Guest:

- 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.

See also

Netop Host Manager, Security section

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.

Communication profiles are stored in the Netop Host configuration file as follows:

- For Hosts running on Linux: `var/opt/netop/host/host.xml.`
- For Hosts running on Mac: `/Library/Application Support/netop/host/host.xml.`

See also

Communication profile on the Host
Communication Profile Edit

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 Internet (TCP)) 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 WebConnect and Netop Portal without Live Update selected).
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.

Start a remote control session from other Guest window tabs

1. On the Phonebook tab or History 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.

Tab	Description
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.

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 `~/.netopguest/phbook/*.dwc`.

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 or right-click on the phonebook entry and select the **Connection Properties** option.

   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 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** > **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** > **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.

2.3 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.

2.3.1 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.

2.4 Transfer files

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

If allowed by the **Guest 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.

   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 File Transfer** button on the toolbar in the **Netop File Manager**.

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

2.5 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.

There are two types of logs: DTL logs and Debug logs. For troubleshooting purposes you need to retrive the logs and send them to the Netop Support team.

See also

Troubleshooting
Event Log

2.6 Multisession Support

Each Linux Host supports up to 8 simultaneous sessions, no matter the communication protocol (TCP, UDP or Web Connect). However, it depends on the session type and the Host hardware:

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

2.7 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	Select this command to send the keystroke combination **CTRL+ESC** to the Host. Alternatively, click the **Send Ctrl+Esc** button on the toolbar.
Send Ctrl+Alt+Delete	Select this command to send the keystroke combination **CTRL+ALT+DEL** to the Host. Alternatively, click the **Send Ctrl+Alt+Del** button on the toolbar. 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. **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.
Send Alt+Tab	Select this command to send the keystroke combination **ALT+TAB** to the Host. This keystroke combination switches the active window clockwise on the Host computer screen.
Send Alt+Shift+Tab	Select this command to send the keystroke combination **ALT+SHIFT +TAB** to the Host. This keystroke combination switches the active window counter-clockwise on the Host computer screen.
Send Print Screen	Select this command to send a **PRINT SCREEN** command to the Host. 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 (in Netop Host Manager, **Configuration > Local Configuration > Guest users > Security > Roles >** <guest user> option **Use keyboard and mouse** is set to **Disabled**).

2.8 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**.

3 Troubleshooting

In case of failures, please contact Netop technical support team which will assist you with the issue. For troubleshooting purposes, include debugging logs along with any error reports.

3.1 DTL Logs

If the component crashes or you do not have access to the graphical user interface, use DTLSpy - automatically installed with the Netop Guest.

If it does not crash, use the following steps to retrieve the logs:

1. Start the Guest and Host.
2. On both Guest and Host go to **Help** > **About** and press **Alt + z**.
3. Close the **About** window.
4. Reproduce the error.
5. Select **Tools** > **Debug Trace**.

A dialog prompts you to view the debug trace. The log is saved as follows:

On Linux

- The log on the Guest is saved to file `/home/$USER/.netopguest/guest_log`.
- The log on the Host is saved to file `/var/log/netop_host*`.

On Mac

- The log on the Guest is saved to file `/Users/$USER/.netopguest/guest_log`.
- The log on the Host is saved to file `/Users/$USER/Library/Logs/netop_host*`.

3.2 Debug Logs

3.2.1 For the Host

1. Go to **Tools** > **Options**.
2. Fill in the required credentials. The **Netop Host Manager** will open.
3. Go to **NetopHost** > **Configuration** > **Local configuration** > **Host computer** > **Debug log** and make sure the values are set as **Enabled** – **Enabled** and **Level** – **Trace**.
4. Go to **Debug Log** > **File** and set the **Level to Debug**.
5. Reproduce the error.
6. Retrieve the log from the location specified under **Debug Log** > **File** (E.g.: `/var/log/netop_host.log`) and send it.

3.2.2 For the Guest

On the Guest side, debug logs can be retrieved only from the command line:

1. Launch the Guest using the logging parameters (global logging level, file logging level and location of the actual log file)

```
netopguest --global-log-level trace --logfile-name ~/netop_guest.log --file-log-level=trace
```

2. Replicate the error.
3. Retrieve the log file from where you decided to save and send it over to Netop support.

3.2.3 Log Levels

The following table describes the Netop log levels:

Option	Description
no_log	Turns off the logging.
critical	Gives information about a critical issue that has occurred.
error	Gives information about a serious error which needs to be addressed and may result in unstable state.
warning	Gives a warning about an unexpected event to the user.
info	Gives the progress and chosen state information. This level will be generally useful for end user. This level is one level higher than DEBUG.
debug	Helps developer to debug application. Level of message logged will be focused on providing support to a application developer.
trace	Gives more detailed information than the DEBUG level and sits on top of the hierarchy.

4 Command Line Options

As an alternative to using the Netop Guest and Host graphical user interfaces, you can use the command line window (terminal window) to connect from a Guest to a Host by using command line options.

The full lists of parameters are given below.

4.1 Guest Options

To view the Guest command line options, open a terminal and enter the following command: `netopguest -h`.

Option	Description
`-v [ --version ]`	Shows Netop Guest version details.
`-H [ --Host ] arg`	Connects to the specified Host in full screen remote control.
`-U [ --username ] arg`	Username
`-P [ --password ] arg`	Password
`--no_xinit arg (=0)`	No call to XInitThreads is made. If application fails to start, try this option.
`--serialno arg`	Validates and sets the serial number (serialno), then exits.
`--no_splash [=arg(=1)] (=0)`	Do not show the splash screen at start-up.
`-k [ --kiosk ] [=arg(=1)] (=0)`	Enters the Kiosk Mode.
`--phonebook arg`	Automatically loads the phonebook file.
`--global-log-level [=arg(=trace)] (=trace)`	It specifies which level is used across all loggers. If a logger has a higher level, then that level is used.
`--console-log-level [=arg(=trace)] (=no_log)`	Specifies the level for console logging.
`--file-log-level [=arg(=trace)] (=no_log)`	Specifies the level for logging to file.
`--syslog-log-level [=arg(=trace)] (=no_log)`	Specifies the level for system logging.
`--modules-log-level arg`	Specifies the modules log levels; `arg: module[=log_level]`
`--logfile-name arg (=log)`	Specifies the name of the log file.
`--logfile-folder arg (=./)`	Specifies the folder where old log files are stored.
`--logfile-rotation-size arg`	Specifies the maximum size of log file. The file is rotated at this size.
`--logfile-max-size arg`	Specifies the maximum size in MB of all log files.

Option	Description
`--logfile-min-free-space arg`	Specifies the minimum free space in MB needed to create the log file.
`--help`	Lists the program options.

See also

Log Levels

4.2 Host Options

To view the Guest command line options, open a terminal and enter the following command: `netophost -h`.

Option	Description
`-h [ --help ]`	Lists the Host options.
`-v [ --version ]`	Shows Netop Host version details.
`--testlic [=arg(=1)] (=0)`	Tests the product license.
`--license.dat arg`	Plain-text input license file.
`--enable-logging arg (=0)`	Enables logging.
`--global-log-level [=arg(=trace)] (=trace)`	Specifies which level is used across all loggers. If a logger has a higher level, then that level is used.
`--console-log-level [=arg(=trace)] (=no_log)`	Specifies the level for console logging
`--file-log-level [=arg(=trace)] (=info)`	Specifies the level for logging to file
`--syslog-log-level [=arg(=trace)] (=no_log)`	Specifies the level for system logging
`--modules-log-level arg`	Specifies the modules log levels; `arg: module[=log_level]`
`--logfile-name arg (=/var/log/ netop_host.log)`	Specifies the name of the log file
`--logfile-folder arg (=/var/log/ netop_host_old)`	Specifies the name of the log file
`--logfile-rotation-size arg (=10)`	Specifies the maximum size in MB of log file. The file is rotated at this size
`--logfile-max-size arg (=40)`	Specifies the maximum size in MB of all log files
`--logfile-min-free-space arg (=10)`	Specifies the minimum free space needed to create log file

See also

Log Levels

5 Netop Host Manager

Netop Host Manager is used to manage the configuration settings for the Netop Host

Note: Make sure that the Netop Host Daemon is started, otherwise the **Host Options** is disabled. Use one of the following commands in the terminal in order to start the daemon: `sudo service netophostd start or sudo /etc/init.d/netophostd start`.

Netop Host Manager allows you to configure the Netop Host. In order to open the Netop Host Manager select **Tools** > **Options**. Enter account for changing the Host configuration and click **OK**.

The **Netop Host Manager configuration** window will be displayed. The **Netop Host Manager** window has three panes:

- An upper left selection pane where you can select the element to set up.
- An upper right attributes pane where you can edit the attributes of the element in the selection pane.
- A lower message pane that can show messages from Netop Host Manager.

Note: To ensure that changes have been applied, restart Netop Host after setup changes.

It contains a branch structure of Netop Host setup elements. The attributes of a selected setup element will be shown in the attributes pane.

The Local configuration branch expands into these branches:

- HostComputer
- Addresslists
- Guest users

5.1 Host Configuration

5.1.1 General Configuration

Use the **General** branch to specify the Host display and the startup options.

Option	Description
Exit when idle after seconds	Exits the Host when idle after the specified time.
Hide menu item 'Exit'	Connects to the specified Host in full screen remote control. Default value is **Disabled**.
In tray	If the attribute is set to **Enabled**, the Host icon displays in tray. Default value is **Disabled**.
Load at boot	If the attribute is set to **Enabled**, communication will start when Netop Host Program loads to enable the Netop Guest to connect. If set to **Disabled**, communication will not start when the Netop Host Program loads.
Start at load	If the attribute is set to **Enabled**, when the Host is started and loaded, it enables communication. Default value is **Enabled**.
Wake up every day	If set to **Enabled**, you schedule to bring the Host computer out of standby daily. Default value is **Disabled**.

Option	Description
Wake up hour	If the **Wake up every day** is set to **Enabled**, specify the scheduler details, that is in this case, the specific hour when the Host computer exists the standby. Default value is **20**.
Wake up minute	If the **Wake up every day** is set to **Enabled**, specify the scheduler details, that is in this case, the specific minute when the Host computer exists the standby. Default value is **0**.

Set DISPLAY for Hosts running on Linux

A Host running on Linux a display can have multiple screens.

To set which screen to display to Guest connecting to the Host, click on **General**, double-click the **Display** attribute and enter the screen value in teh following format: ":<screen value>".

5.1.2 Communication

Use the **Communication** branch to specify communication profiles.

WebConnect / WebConnect 3

Option	Description
Enable	If set to **Enabled** the WebConnect communication profile will be active. By default, the attribute value is **Enabled**.
Name	The name of the WebConnect communication profile.
WebConnect Service Domain	Specify the domain of a WebConnect / WebConnect 3 service recognized account.
WebConnect Service Password	Specify the password corresponding to the WebConnect / WebConnect 3 service recognized account username you entered.
WebConnect Service URL	Specify the URL of the WebConnect / WebConnect 3 service, i.e. the Connection Manager, that facilitates the WebConnect connection.
WebConnect Service Username	Specify a WebConnect / WebConnect 3 service recognized account username.

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 has improved security; therefore, we strongly recommend you to use it.

Netop Portal

Attribute	Description
Enable	If set to Enabled the Netop Portal communication profile will be active. By default, the attribute value is **Enabled**.

Attribute	Description
Name	The name of the Netop Portal communication profile.
Netop Portal Service Address	<String of characters> The address of the Netop Portal service: portal.netop.com.
Netop Portal Service Password	<String of characters> The field will show dots or asterisks. The Netop Portal password.
Netop Portal Service Username	<String of characters> The Netop Portal username.

TCP

A TCP setup element will be identified by the Name attribute value. Initially, a "TCP – TCP" setup element with default other attribute values will be available.

You can create multiple TCP setup elements.

Each TCP setup element will make a communication profile that uses the TCP/IP (TCP) communication device available to Netop Host. If the **Enable** attribute value is **Enabled**, the communication profile will be enabled if Netop Host communication is enabled.

The Use HTTP attribute will encapsulate data packets in HTTP making it easier to traverse firewalls.

Attribute	Description
Enable	Indicates whether the TCP/IP communication profile is active. The attribute value is **Enabled** by default.
Name	The name of the TCP/IP communication profile. Default name is **TCP 1**.
Receiveport	The port on which the Netop Host listens. Default port number is **6502**. You can specify a number in the range 1025-65535.
Sendport	The port Netop Host uses to communicate with the connected Guests. Default port number is **6502**. You can specify a number in the range 1025-65535. The Send port number of the source module should correspond to the Receive port number of the destination module.
Use HTTP	Enable this attribute in order to wrap data packets as HTTP packets to ease firewall passage. This is also known as HTTP-tunneling. The attribute is **Disabled** by default.

UDP

A UDP setup element will be identified by the Name attribute value. Initially, a "TCP – TCP/IP" setup element with default other attribute values will be available.

You can create multiple UDP setup elements.

Each UDP setup element will make a communication profile that uses the TCP/IP (TCP) communication device available to Netop Host. If the **Enable** attribute value is **Enabled**, the communication profile will be enabled if Netop Host communication is enabled

Attribute	Description
Broadcast to subnet	Broadcast communication to local network segment computers is by default Enabled. 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 Netop Remote Control Administrator's Guide.
Enable	Enables the UDP communication profile.
Ignore port info from Name Server	Set the attribute to **Enabled** in order to replace the destination module Receiveport number received from Netop Name Server by the port number specified in the **Override port attribute**.
Maximum transmission unit (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.
Name	The name of the UDP communication profile.
Override port	Specify the port number that should replace the Receive port number received from the Netop Name Server.
Primary nameserver	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.
Receiveport	The Receive port number received from the Netop Name Server.
Secondary nameserver	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.
Sendport	The Send port number received from the Netop Name Server.
Use Netop Name Server	Set the attribute to **Enabled** in order to use Netop Name Server to resolve Netop names into IP addresses. Using Netop Name Server will facilitate connecting across segmented IP networks including the Internet.
Use TCP for sessions	Set the attribute to Enabled in order to connect by TCP/IP for high speed session communication.

Create a broadcast list:

Right-click a **UDP** setup element, point to **New** and click **Broadcastlist** to create in a new branch below the UDP setup element:

A Broadcastlist setup element will be identified by the **Broadcastlist** name attribute value. Initially, a "Broadcastlist – #1" setup element will be available.

You can create multiple Broadcastlist setup elements.

Each Broadcastlist setup element will make an IP broadcast list available to the UDP setup element.

You can delete the UDP setup element or only the Broadcast list. If you delete the UDP setup element, any Broadcast list setup elements below will be deleted automatically.

5.1.3 Names

Use the Names branch to specify the name by which the Host will identify itself when communicating.

To communicate by a communication profile that uses a networking communication device, 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.

Public

Attribute	Description
Public hostname	Enable this attribute in order to respond to Guests that browse for Hosts by the Host name.
Public username	Enable this attribute in order to enable the name of a user logged on to the Host computer to enable connections by the user name.

Host Naming

Computer name will identify Netop Host by its computer name (generally recommended). Enter or leave blank will identify Netop Host by the Host Name attribute value.

Attribute	Description
Hostname	Allows you to enter a Host name.
Naming mode	Specify a name in the field or leave the field blank to name the Host by the specified Hostname or leave it without a name.

Name servers

The **Name Space ID** attribute value identified a private section of a Netop Name Server name database. Netop modules must specify the same **Name Space ID** attribute value to connect by Netop Name Management

Attribute	Description
Namespace ID	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

5.1.4 Security

This section describes all the attributes you can set to ensure the Host security.

Netop Portal certificate settings

When a Guest connects to a Host via the Netop Portal, based on the Netop Portal certificate settings configured on the Host, connection will be allowed or not.

Attribute	Description
Connection allowed when using an invalid certificate	If attribute is set to **Enabled**, a Guest can connect to a Host which communicates though Netop Portal with an invalid certificate.
Display invalid certificate warning	If attribute is set to **Enabled**, a warning will notify the user that the Netop Portal certificate is invalid.

Encryption

The communication between Netop modules is protected by encrypting transmitted data.

A range of encryption types is available on Netop Remote Control modules. To view available encryption options, click **Allowed encryptions**.

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.

Data Integrity

Item	Description
Description	Data is protected from being changed in transit.
Scope	Use for communication in environments where encryption is prohibited except for authentication.
Encryption	**Keyboard and mouse**: None **Screen and other data**: None **Logon and password**: None
Integrity check	**Keyboard, mouse**: 256bit SHA HMACs **Screen and other data**: 160 bit SHA HMACs **Logon and password**: 256 bit SHA HMACs
Key exchange	Combination of 1024 bits Diffie-Hellman and 256 bit SHA hashes.

Data integrity and keyboard

Item	Description
Description	Data is protected from being changed in transit and only keystrokes, logon and password details are encrypted.
Scope	Use for communication in environments where speed is important, but you require data integrity check and keystrokes / password details must be encrypted.
Encryption	**Keyboard and mouse**: 256 bit AES **Screen and other data**: None

	Logon and password: 256 bit AES
Integrity check	**Keyboard, mouse**: 256bit SHA HMACs **Screen and other data**: 160 bit SHA HMACs **Logon and password**: 256 bit SHA HMACs
Key exchange	Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256 bit SHA.

High

Item	Description
Description	All transmitted data is encrypted with 128 bit keys. Keystrokes, mouse clicks and password details are encrypted with 256 bit keys.
Scope	Use for communication in environments where security is important, but speed cannot be ignored.
Encryption	**Keyboard and mouse**: 256 bit AES **Screen and other data**: 256 bit AES **Logon and password**: 256 bit AES
Integrity check	**Keyboard, mouse**: 256bit SHA HMACs **Screen and other data**: 160 bit SHA HMACs **Logon and password**: 256 bit SHA HMACs
Key exchange	Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256 bit SHA.

Keyboard

Item	Description
Description	Only keystrokes, logon and password are encrypted.
Scope	Use for communication in environments where speed is important, but keystrokes and password details must be encrypted.
Encryption	**Keyboard and mouse**: 256 bit AES **Screen and other data**: none **Logon and password**: 256 bit AES
Integrity check	**Keyboard, mouse**: 256bit SHA HMACs **Screen and other data**: none **Logon and password**: 256 bit SHA HMACs
Key exchange	Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256 bit SHA.

Netop 6.5 compatible

Item	Description
Description	Compatibility mode for communication with Netop version 6.x, 5.x and 4.x.
Scope	Use for communication in environments where speed and backwards compatibility are important.
Encryption	**Keyboard and mouse**: proprietary algorithm **Screen and other data**: none **Logon and password**: proprietary algorithm
Integrity check	**Keyboard, mouse**: none **Screen and other data**: none **Logon and password**: none
Key exchange	Proprietary algorithm

No encryption

Item	Description
Description	No encryption at all
Scope	Use for communication in environments where maximum transfer speed is important and security is no issue.
Encryption	**Keyboard and mouse**: none **Screen and other data**: none **Logon and password**: none
Integrity check	**Keyboard, mouse**: none **Screen and other data**: none **Logon and password**: none
Key exchange	160 bit SHA for session uniqueness

Very high

Item	Description
Description	Everything is encrypted with 256 bit keys
Scope	Use for communication in environments where security is important and speed is not a major issue.
Encryption	**Keyboard and mouse**: 256 bit AES

	Screen and other data: 256 bit AES **Logon and password**: 256 bit AES
Integrity check	**Keyboard, mouse**: 256 bit SHA HMACs **Screen and other data**: 256 bit SHA HMACs **Logon and password**: 256 bit SHA HMACs
Key exchange	Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256 bit SHA.

Maintenance

If the **Password** attribute has a value, maintenance password protection will be enabled. If enabled, Netop Host or Netop Host Manager will request the **Password** attribute value to execute a maintenance password protected action including changing the **Password** attribute value.

To change the maintenance password, specify the current maintenance password as the **Old Password** attribute value and the new maintenance password as the **Password** attribute value.

Attribute	Description
All other configuration	Set this attribute to **Enabled** if you want to apply maintenance password protection to all other Host configurations.
Backup of old password	To change the maintenance password, specify the current maintenance password as the **Old Password** attribute value and the new maintenance password as the **Password** attribute value.
Guest access security	Set this attribute to **Enabled** if you want to apply maintenance password protection to the **Guest Access Security** command.
Password	Set the maintenance password.
Program exit and 'Stop Host'	Set this attribute to **Enabled** if you want to apply maintenance password protection to unloading the Host and stopping the Host.

5.1.5 Debug Log

The Netop Host running on Linux allows you to direct the messages to various destinations based on the software type of the application that generated the message and severity:

Debug Log is the global severity level. The other ones are filters for various log destinations.

Use the **Debug Log** branch to specify the debugging log levels.

Global Log Level

In order to activate the global log level, click on **Debug Log** and make the following settings by double-clicking on each attribute:

- Set the **Enabled** attribute to **Enabled**.
- Select the desired global log **Level**. For the complete list of log levels, click here.

Example of debug log setup and output:

Debug Log Setup:

- The **Debug Log** severity level is **Warning**.
- The **Syslog** severity level is **Info**.
- The **Console** severity level is **Error**.
- The **File** severity level is **Trace**.

Logs output files:

- The **Syslog** will contain messages with severity levels higher than Warning: Warning, Error and Critical.
- The **Console log** will contain messages severity levels higher than Error: Error and Critical.
- The **File log** will contain messages severity levels higher than Warning: Warning, Error and Critical.

Syslog

The logs are saved using **syslog daemon**.

In order to set the severity of the messages which will be logged to syslog, click on **Syslog**, on the left pane double-click the **Level** attribute and select the log level, then click **OK**.

Console

Logging events to the console is recommended for debugging using the **Command Line**.

In order to set the severity of the messages which will be logged to the console, click on **Console**, on the left pane double-click the **Level** attribute and select the log level, then click **OK**.

File

All actions are saved to a specified log file. Default file location is `/var/log/netop_host.log`. If the log file size exceeds the Maximum size (MB) or the Minimum free space drops below the value set on the Host, it will save the log file in the folder `/var/log/netop_host_old` and will continue logging to `/var/log/netop_host.log`.

To change the attribute values double-click the desired attribute, make the changes and click **OK**.

Attribute	Description
File name	The name of the log file where the log are saved. By default all logs are saved to */var/log/netop_host.log.*
Level	Log level for the messages which will be logged to the log file specified within the File section.
Maximum size (MB)	The maximum size of the log file in MB. Default value is 40 MB.
Minimum free space (MB)	Specifies the amount of free space on the log file.
Old Logs Folder	The name of the log file where the log are saved. By default all logs are saved to */var/log/netop_host.log.*
Rotation size (MB)	The size of the log file to trigger rotation.

Modules

This category is used in special situations. Netop Technical Support might require you to do special settings here in case the logs you provided were insufficient.

See also

Log Levels

5.1.6 Event Log

Use the Host Event Log to specify where and what actions to log.

Log Locally

This section allows you to enable logging Netop events in a log file on the computer.

Attribute	Description
Enable logging	Set this attribute to **Enabled** if you want to log the events (events enabled in the **Log Locally** > **Eventlist**) locally on the Host computer.
Filename	The location on the Host computer where the events will be logged. Default location is `/var/log/netophost.nlg`.

5.1.7 Tunnel Configuration

Use the **Host Tunnel Configuration** to enable scanning the tunneled ports and predefine local ports for the tunnel.

To scan traffic that is allowed to tunnel over specific ports, set the **Scan Tunneled Ports** attribute to **Enabled**.

Allowed Tunnels

You can define a range of ports where the Host machine will listen for connections.

Predefine local ports for the tunnel:

1. Right-click on **Allowed Tunnels**, select **New** and **Endpoint**. A generated endpoint entry is added to the list of **Allowed Ports**.
2. On the right pane, double-click on the newly added endpoint. An edit attribute window will be displayed.
3. Enter the **IP address** of the Host and click **OK**. The endpoint will be displayed in the **Allowed Tunnels** list.
4. Right-click on the endpoint, select **New** and **Port**. A generated port entry is added to the selected endpoint.
5. On the right pane, double-click on the newly range entry. An edit attribute window will be displayed.
6. Enter the range of ports where incoming connections will be forwarded in the following format: **port1-portN**.

   To predefine only one port forwarding, in the **Range** attribute enter the local port for the tunnel.

Blocked Ports

If for security reasons, you need to block tunneling on specific ports on the Host, add them here. The procedure for defining **Blocked Tunnels** is similar to the one described for **Allowed Tunnels**.

5.1.8 Host Monitor

Logging is important for debugging and besides the Event Log and Debug Log, Netop Remote Control allows you to set specific logging parameters which will enable logging to the **Netop Host Daemon (netophostd)**. **netophostd** is a service which runs as a background process waiting to be activated by the occurrence of a specific Host event or condition; it does not involve the direct control of a user.

The Host logs are stored as follows:

- For the Host running on Linux, the logs are stored in: `/var/log/netop_host_daemonXXXXX.log` and `/var/log/netop_host_daemon_old/`.
- For the Host running on Mac, the logs are stored in `/Users/$USER/Library/Logs/netop_host*`.

6 Guest dialog boxes

6.1 Communication Profile Edit

Note: You can only modify the WebConnect and Netop Portal communication profiles.

To edit the communication profile:

1. Click the **Quick Connect** tab.
2. From the **Communication Profile** drop-down list select the desired communication profile and click the **Edit** button.
3. In the **Edit Profile** dialog box make the desired changes then click **OK**.
4. Use the **Edit Profile** dialog box to create or edit a communication profile.

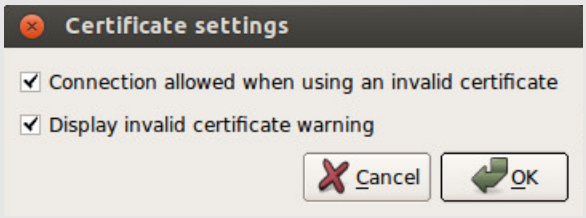
Note: To apply changes to enabled communication profiles, you must reload the Guest.

WebConnect / WebConnect3 Information

Option	Description
WebConnect Service URL	Specify the URL of the WebConnect / WebConnect3 service, i.e. the Connection Manager, that facilitates the WebConnect / WebConnect 3 connection.
Account	Specify a WebConnect / WebConnect3 service service recognized account username.
Password	Specify the password corresponding to the WebConnect / WebConnect3 service service recognized account username you entered.
Confirm Password	Confirm the password previously entered.
Domain	Specify the domain of a WebConnect / WebConnect3 service service recognized account.
test	Click the **Test** button to verify the WebConnect / WebConnect3 service address and credentials.

Netop Portal Information

Option	Description
Address	Specify the address of the Netop Portal service: portal.netop.com.
Username	Specify the Netop Portal username.
Password	Specify the Netop Portal password.
Certificate Settings	Clicking the **Configure** button you can select Netop Portal certificate settings:

Option	Description
	
Test	Click the **Test** button to verify the Netop Portal address and credentials. Click **OK** to exit the window.
Live Update	Select this check box to see the available hosts in real-time.

6.2 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.
TCP/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.
Name	If the field label does not include "(optional with Gateway)", specify the name by which the Host should respond. 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.
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.

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

Login tab

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

NOTE: The **Login** 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.

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.
Full screen kiosk	Display the Host screen image in full screen to cover the entire Guest computer screen while in kiosk mode.

Actions

Option	Description
Lock Host keyboard and mouse	Select this check box to disable the Host computer keyboard and mouse at startup.

Option	Description
Blank Host display	Select this check box to display a black screen image to the Host user 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	Resize the **Remote Control** window to fit the 1:1 scale Host screen image. 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.
Do not fit	Display the part of the 1:1 scale Host screen image that will fit within the **Remote Control** window. If the Host screen image has fewer pixels than the display area, black borders will surround it. If the Host screen image has more pixels than the display area, the **Remote Control** window will have scrollbars.

Limit number of display 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.

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

Option	Description
	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.

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.

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.
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**: • Disable wallpaper • Disable screen saver • Disable animation gimmicks • Disable full window drag • Disable Active Desktop By default, all check boxes are selected.

6.3 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	Select this check box to display a confirmation dialog box if you are about to delete a folder containing folders or files. The confirmation dialog box allows you the following choices with regard to the deletion: • **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	Select this check box to display a confirmation dialog box if you are about to overwrite or delete files.

Option	Description
	The confirmation dialog box allows you the following choices with regard to the overwriting/deletion: • **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	Select this check box to display the same pane contents when starting a file transfer session with the same Host the next time. Uncheck to always display the system drive contents when starting a 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	Netop hotkey
Copy Files	F3
Move Files	F6
New Folder	F7
Delete	F8
Rename	
Close	F10
Properties	SHIFT+F1
Select All	
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	CTRL+R
Select the left record panel	ALT+F1
Select the right record panel	ALT+F2
Help	F1

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 **nfm.log**. The file is located in the Netop configuration files folder, typically `~/.netopguest/nfm.log`.

Option	Description
	Click the **Browse** button to specify another log file path and name.

See also

Transfer files

Index

O

P

R

S

T

W