NETOP®

RemoteControl

Secure Remote Management and Support

May 27th, 2021

Table of Contents

1 Overview 4
1.1 Remote Control modules 4
1.2 Security 5
1.3 Communication profiles 5
2 Managing Hosts 6
2.1 Grant permissions for the Host (for macOS 10.14 and above) 6
2.2 Start and end a remote control session 8
2.2 Use Netop phonebook to manage connections 9
2.2.1 Edit phonebook records 10
2.2.2 Organize your phonebook 10
2.3 Tunnel 10
2.3.1 Open tunnel session 11
2.4 Transfer files 11
2.5 Log events 13
2.6 Multisession Support 14
2.7 Send special keystrokes 14
2.8 End a remote control session from a Host computer 15
3 Troubleshooting 16
3.1 Debug Logs 16
3.2.1 Log Levels 17
4 Command Line Options 18
4.1 Guest Options 18
4.2 Host Options 19
5 Netop Host Manager 20
5.1 Host Configuration 20
5.1.1 General Configuration 20
5.1.2 Communication 21
5.1.3 Names 24
5.1.4 Security 25
5.1.5 Debug Log 28
5.1.6 Event Log 30
5.1.7 Tunnel Configuration 30
5.1.8 Host Monitor 31
5.2 Guest Users Security 32
5.2.1 Roles 32
5.2.2 Netop Portal access rights 33

5.2.3 Security Server authentication 34
5.2.4 System authentication 34
5.2.5 Netop authentication 35
6 Guest dialog boxes 36
6.1 Communication Profile Edit 36
6.2 Connection Properties 37
6.3 Netop File Manager Options 42

1 Overview

1.1 Remote Control modules

Remote Control has the following modules:

- **Guest**: Enables the computer user to remote control and interact with another computer running a **Host** or extended **Host**.
- **Host**: Enables the computer for remote control and to interact with a computer running a **Guest**.
- **WebConnect**: A secure web-based service consisting of a **Connection Manager** that serves as a meeting hub for the **Netop Guests** and **Hosts**, and at least one **Connection Server** that routes the traffic between the **Guests** and the **Hosts**. The **Connection Server** is an extended **Host**. This is available as an on-premise application.
- **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 the **Guests** and the **Hosts**. The **Connection Server** is an extended **Host**. This is available as an on-premise application. **WebConnect 3.0** has improved security.
- **Portal**: A browser-based interface allowing the users to manage the **Guest** authentication and authorization, view connected devices and do remote sessions using a lightweight support console that does not require any kind of installation.
- **Browser Based Support Console**: A browser-based interface for the **Guest**, allowing the supporters to remote control devices. The browser-based support console doesn't require to be installed.
- **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**.
- **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 sends it using another communication device. This ability enables the **Netop Gateway** to provide communication between the **Netop** modules that use mutually incompatible communication devices, typically to connect the **Netop** modules inside a network or terminal server environment with the **Netop** modules outside a network or terminal server environment.
- **Name Server**: An extended **Host** that can connect **Netop modules** across segmented networks. The **Name Server** resolves the **Netop names** into **IP** addresses, that 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 dictates 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 sessions, including notification, confirm access and illegal connection attempts.

The communication between the **Netop modules** can be encrypted using different methods depending on the environment.

See also
Netop Host Manager, Security section

1.3 Communication profiles

For the **Netop modules** to be able to communicate with each other, make sure that you 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 the default communication profiles. To optimize the communication in your environment, 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 macOS: **`/Library/Application Support/netop/host/host.xml`**.

See also
Communication profile on the Host
Communication Profile Edit

2 Managing Hosts

2.1 Grant permissions for the Host (for macOS 10.14 and above)

To use the **Netop Host** on macOS 10.14 and above, it is necessary that you manually allow the following permissions on the **Host:**

- **Accessibility**

  The **Accessibility** permission allows the **Host** to receive control over the mouse and keyboard of the **Host** computer. You use this permission to have control over the mouse and keyboard on the **Host** computer during a remote control session.

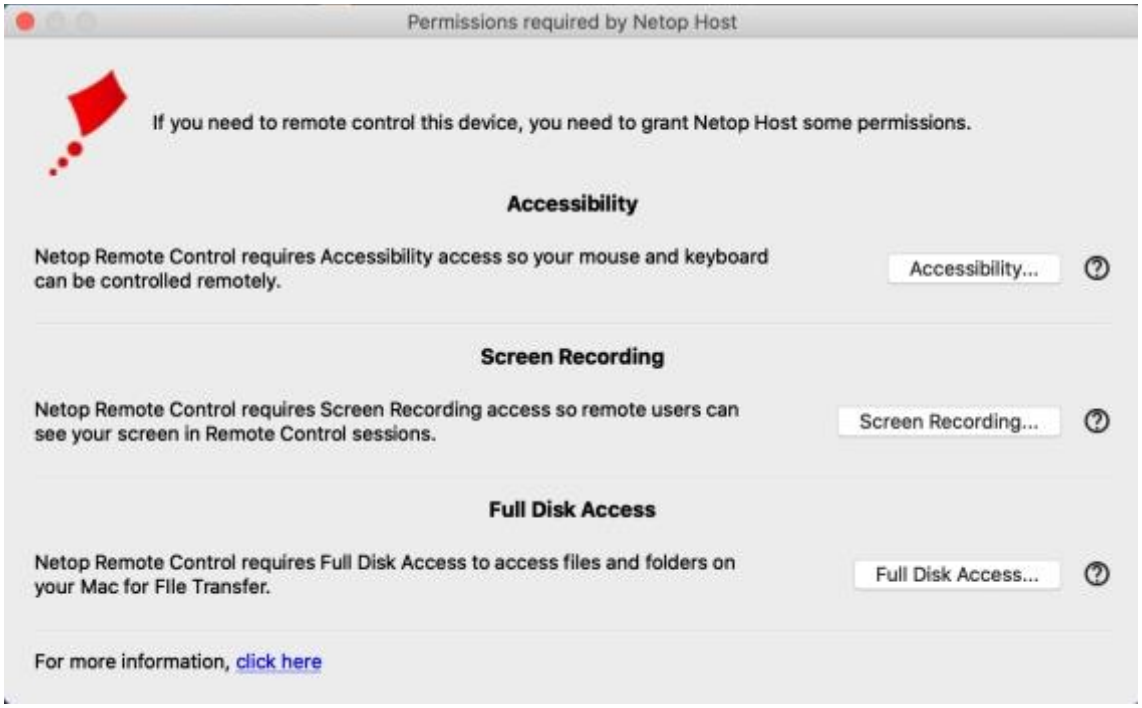
- **Screen recording**

  The **Screen recording** permission allows the **Host** to capture the screen. You use this permission to view the screen of the **Host** computer in a remote control session.

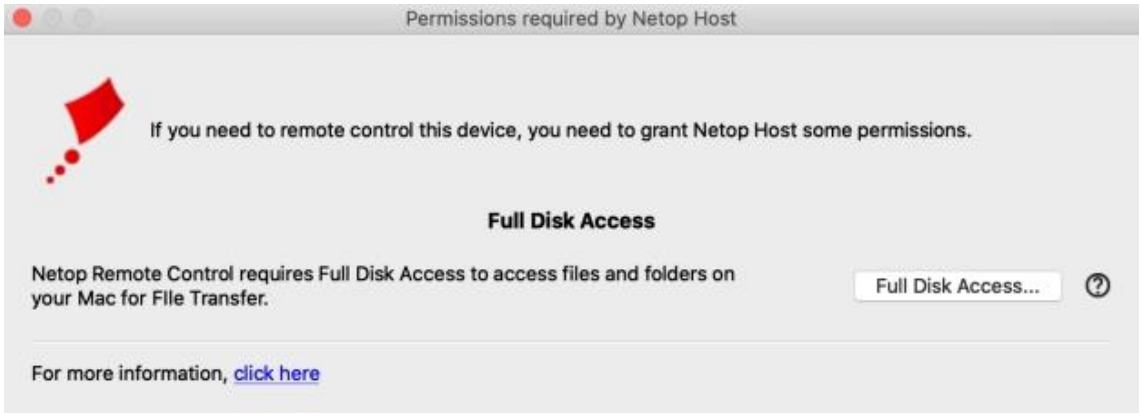
  NOTE: The **Screen recording** permission applies to macOS 10.15.

- **Full Disk Access**

  The **Full Disk Access** permission allows the **Netop Host** access to all the files and folders on your computer.



NOTE: The **Host** only prompts you for the unset permissions. You are prompted to grant these permissions manually after you successfully install the **Host**, start or restart the **Host**.



To grant the **Screen Recording** permission, proceed as follows:

1. From the **Apple** menu, select **System Preferences**.
2. Click on the **Security & Privacy** icon.
3. Click on the **Privacy** tab at the top of the **Security & Privacy** window.
4. From the **Security & Privacy** window, select **Screen Recording**.
5. Click the lock to make changes.
6. To enable the **Screen recording** permission for the `NetopHost`, check the `NetopHost` checkbox.

To grant the **Full Disk Access** permission, proceed as follows:

1. From the **Apple** menu, select **System Preferences**.
2. Click on the **Security & Privacy** icon.
3. Click on the **Privacy** tab at the top of the **Security & Privacy** window.
4. From the **Security & Privacy** window, select **Full Disk Access**.
5. Click the lock to make changes.
6. To add the `NetopHost`, click on the **+** sign.
7. Browse for the `NetopHost`.
8. Click on **Open**.

The grant the **Accessibility** permission, proceed as follows:

1. From the **Apple** menu, select **System Preferences**.
2. Click on the **Security & Privacy** icon.
3. Click on the **Privacy** tab at the top of the **Security & Privacy** window.
4. From the **Security & Privacy** window, select **Accessibility**.
5. Click the lock to make changes.

6. To enable the **Accessibility** permission for the **NetopHost**, check the **netophost** checkbox.

   NOTE: You cannot grant the **Accessibility** permission manually. If you remove the **Accessibility** permission for the "**netophost**", you cannot set it back again until you reinstall the **Netop Host**.

Refer to the knowledge base article for more information on the macOS permissions.

2.2 Start and end a remote control session

You can connect and start a remote control session in several ways. Before you start a remote control session, specify a communication profile corresponding to a communication profile - the default communication profile is **Internet (TCP)** - enabled on the **Host** in the **Communication Profile** section of the **Quick Connect** tab.

To start a remote control session from the **Quick Connect** tab, in the **Guest** window, proceed as follows:
In the **Quick Connect** tab, the **Host** section, specify a **Host** name or address as required by the selected communication profile.

1. Click on the **Connect** button to connect and start a remote control session. Alternatively, click on a toolbar button or select a command from the **Connection** menu to connect and start a session. Usually, a **Netop** login window is displayed that prompts you to log on to the **Host**.
2. Type your credentials to log on. When you have logged on to the **Host**, the session starts.

Connections are displayed in the **Connections** tab. To change the session type or execute action commands, right-click on a **Host** from the **Connections** tab.

Other ways to connect from the Quick Connect tab

1. Click on the **Browse** button (Applies only when using profiles that use **WebConnect** and **Portal** without **Live Update** selected).
2. Select one or multiple **Hosts** in the **Browse** list (**Netop Network** tab).
3. Click on the **Connect** button. Alternatively, click on a toolbar button or select a command from the **Connection** menu to connect and start a session. A login 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.

To start a remote control session from other **Guest** window tabs, proceed as follows:
1. In the **Phonebook** tab or **History** tab, select one or multiple **Hosts**.

2. Click on a toolbar button or select a command on the **Connection** menu to connect and start a session.
   A **Netop** login 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 the **Host** records that you 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 on the **Disconnect** button from the toolbar. Alternatively, click on the **Remote Control** button on the toolbar.

OR

In the **Guest** window, select the connection from the **Connections** tab. Click on the **Disconnect** button on the toolbar. Alternatively, select **Disconnect** from 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 like a personal quick-dial telephone directory with the communication profile necessary to connect and the passwords. Passwords are encrypted by a secure algorithm.
Phonebook records are saved as files with the **.dwc** extension in **`~/.netopguest/phbook/*.dwc`**.

Create phonebook records from the Phonebook tab

To create a phonebook record from scratch, proceed as follows:
1. Click on the **Phonebook Entry** button from 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.
3. Click on **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 the information such as the specified communication profile or the **Host** credentials, you can do that in **Connection Properties**.

To edit a phonebook record, proceed as follows:

1. Select the phonebook record in the right pane of the **Phonebook** tab.
2. Click on 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 on **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, proceed as follows:

1. In the **Edit** menu, select **New** > **New Folder**.
2. Enter a name for the folder.
3. Click on **OK**. Alternatively, right-click and create a folder using the shortcut menu.

To create a new subfolder, proceed as follows:

1. In the left pane, select the folder in which you want to create a subfolder.
2. In the **Edit** menu, select **New** > **New Folder**.
3. Enter a name for the folder.
4. Click on **OK**. Alternatively, right-click on 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). Support and system administrative tasks are still necessary to be executed remotely whilst conforming to industry regulatory standards such as **PCI-DSS**, **HIPAA,** and **FIPS**.

Such environments can include embedded Linux systems where the operating machinery and hardware contain 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 necessary to give the **Guest** users full remote control access on certain machines, only to 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** is authenticated, the tunneled ports are assigned by the **Netop Security Server**. The **Tunnel** console appears to confirm 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 **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** the files.

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

To start a file transfer session, proceed as follows:

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

NOTE: The **Guest** can connect to start a file transfer session from the **Phonebook** tab, the **Quick Connect** tab, or the **History** tab. When 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 on 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, proceed as follows:

1. Select files and/or folders in one of the two **File Manager** panes. Alternatively, select the files in one of the two **File Manager** panes and select **Copy File(s)** from the **File** menu.
2. Click on the **Copy File(s)** button on the toolbar.
3. In the **Copy** dialog box, check the location in the **To** field. Change the location if necessary.
4. Click on the **Options** button to view the **Options** dialog box. Specify the options for the copy process. Refer to the Netop File Manager Options for more information.
5. To start the copy process, click on **OK.**

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, proceed as follows:

1. Select the files and/or folders in one of the two **File Manager** panes. Alternatively, select the files in one of the two **File Manager** panes and select **Move File(s)** from the **File** menu.
2. Click on the **Move File(s)** button from the toolbar
3. In the **Move** dialog box, check the location in the **To** field. Change the location if necessary.
4. Click on the **Options** button to view the **Options** dialog box. Specify the options for the move process. Refer to the Netop File Manager Options for further information.
5. To start the move process, click on **OK.**

Synchronize files

To synchronize files between two computers, proceed as follows:

1. Click on the **Synch File(s)** button on the toolbar. Alternatively, select **Synch File(s)** from the **File** menu.
2. In the **Synchronize** dialog box, verify the location in the **To** field. Change the location if necessary.
3. Click on the **Options** button to view the **Options** dialog box. Specify the options for the synchronization process. Refer to the Netop File Manager Options for more information.
4. Click on **OK** to start the synchronization process.

WARNING! By default, the synchronization process transfers the files and folders in both directions, replacing the older files and folders with newer files and folders. In 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, proceed as follows:

1. Click on the **Clone File(s)** button on the toolbar. Alternatively, select **Clone File(s)** from the **File** menu.
2. In the **Clone** dialog box, verify the location in the **To** field. Change the location if necessary.
3. Click on the **Options** button to view the **Options** dialog box and specify the options for the cloning process. Refer to the Netop File Manager Options for more information.
4. Click on **OK** to start the cloning process.

WARNING! The cloning process transfers all the folders and files in the selected pane to the other pane deleting the existing folders and files in it.

TIP: To be in control of what happens and to avoid deleting or overwriting files unintentionally when you synchronize or clone files, select all the options in the **Confirmation** tab of the **Options** dialog box. Refer to the Netop File Manager Options for more information. A dialog box is then displayed when you are about to delete or overwrite a file. This allows 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 on the **Local File Transfer** button from the toolbar in the **Netop File Manager**. The folder structure of the **Guest** computer is 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 the session activity and logon attempts to multiple logging destinations. You can log the **Netop** events in a **Netop** log on the local computer.

There are two types of logs:

- **DTL logs**
- **Debug logs**

For troubleshooting purposes, make sure that you retrieve 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, regardless of the communication protocol (**TCP**, **UDP** or **WebConnect**). 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 **CTRL+ESC** keystroke combination to the **Host**. Alternatively, click on the **Send CTRL+ESC** button on the toolbar.
Send CTRL+ALT+DELETE	Select this command to send the **CTRL+ALT+DEL** keystroke combination to the **Host**. Alternatively, click on the **Send CTRL+ALT+DEL** button from 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**: The **Send CTRL+ALT+DEL** button is disabled with a Windows ME/98/95 **Host** computer. Select the **Restart Host PC** command to restart the **Host** computer.
Send ALT+TAB	Select this command to send the **ALT+TAB** keystroke combination 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 **ALT+SHIFT+TAB** keystroke combination to the **Host**. This keystroke combination switches the active window counterclockwise on the **Host** computer screen
Send Print Screen	Select this command to send the **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 the **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 is disabled if the **Guest access security** settings on the **Host** do not allow the use of keyboard and mouse (in the **Netop Host Manager**, **Configuration > Local Configuration > Guest users > Security > Roles >** <**guest user**> the **Use keyboard and mouse** option is set to **Disabled**).

2.8 End a remote control session from a Host computer

If your computer is being remote controlled and you consider that you do not want to continue the session, you can end the session from the **Host**.

To end a remote control session from the **Host**, click on the **Disconnect** button on the toolbar. Alternatively, in the **Session** menu, in the **Host** window, select **Disconnect**.

3 Troubleshooting

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

3.1 Debug Logs

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

To retrieve the logs, proceed as follows:

For the Host

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

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 the **Netop** support.

A dialog prompts you to view the debug trace. The log is saved by default 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 macOS**

  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*`**.

3.2.1 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 that is necessary to be addressed and can result in an unstable state.
Warning	Gives a warning about an unexpected event to the user.
Info	Gives the progress and chosen state information. This level is generally useful for the end-user. This level is one level higher than the **Debug** one.
Debug	It helps the developer to debug the application. The level of the message is focused on providing support to an 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 the command line options. The full list of parameters is 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 the **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 the 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 the log file. The file is rotated at this size.
`--logfile-max-size arg`	Specifies the maximum size in **MB** of all log files.
`--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 **Host** command line options, open a terminal and enter the following command:

netophost -h.

Option	Description
-h [--help]	Lists the **Host** options.
-v [--version]	Shows the **Netop Host** version details.
--enable-logging [=arg(=1)] (=1)	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 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 (=host.xml modules)	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/)	Specifies the name of the log file.
--logfile-old-logs-folder arg (=/var/log/netop_host_old)	Specifies the folder path where you store the old log files.
--logfile-rotation-size arg (=10)	Specifies the maximum size in **MB** of the log file. The file is rotated at this size.
--logfile-max-size arg (=40)	Specifies the maximum size in **MB** of all the log files.
--logfile-min-free-space arg (=10)	Specifies the minimum free space necessary to create the 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, **Host Options** is disabled.

Use one of the following commands in the terminal in order to start the daemon:

- `sudo service netophostd start`
- `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 the account for changing the **Host** configuration and click on **OK**.

The **Netop Host Manager configuration** window is 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 display messages from the **Netop Host Manager**.

NOTE: To help ensure that the changes apply, restart the **Netop Host** after setup changes.

It contains a branch structure of **Netop Host** setup elements. The attributes of a selected setup element are displayed in the attributes pane.

The **Local** configuration branch expands into these branches:

- **Host Computer**
- **Address lists**
- **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. The default value is **Disabled**.

In tray	If the option is set to **Enabled**, the **Host** icon displays in the tray. The default value is **Disabled**.
Load at boot	If the attribute is set to **Enabled**, communication starts when the **Netop Host Program** loads to enable the **Netop Guest** to connect. If the option is set to **Disabled**, communication starts when the **Netop Host Program** loads.
Standby on idle at exit	
Start at load	If the option is set to **Enabled** when the **Host** starts and loads, it enables communication. The default value is **Enabled**.
Wake up every day	If the option is set to **Enabled**, your schedule to bring the **Host** computer out of standby daily. The default value is **Disabled**.
Wake up hour	If the **Wake up every day** option is set to **Enabled**, specify the scheduler details, that is in this case, the specific hour when the **Host** computer exists standby. The default value is **20**.
Wake up minute	If the **Wake up every day** option is set to **Enabled**, specify the scheduler details, that is in this case, the specific minute when the **Host** computer exists standby. The default value is **0**.
Display	A **Host** running on Linux a display can have multiple screens. To set which screen to display to the **Guest** connecting to the **Host**, click on **General**, double-click on the **Display** attribute and enter the screen value in the following format: ":<**screen value**>".

5.1.2 Communication

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

WebConnect / WebConnect 3

Attribute	Description
Enable	If the attribute is set to **Enabled** the **WebConnect** communication profile is active. The default value for the attribute 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 the incoming traffic. All the traffic is outgoing.

NOTE: We recommend using **WebConnect 3** since it has improved security.

Netop Portal

Attribute	Description
Enable	If the attribute is set to **Enabled**, the **Netop Portal** communication profile is active. The attribute value is set to **Enabled** by default.
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 displays dots or asterisks.
Netop Portal Service Username	**<String of characters>** The **Netop Portal** username.

TCP

A **TCP** setup element is identified by the **Name** attribute value. Initially, a "**TCP – TCP**" setup element with default other attribute values is available. You can create multiple **TCP** setup elements.
Each **TCP** setup element makes the communication profile that uses the **TCP/IP (TCP)** communication device available to **Netop Host**. If the **Enable** attribute value is **Enabled**, the communication profile is enabled if the **Netop Host** communication is enabled.
The **Use HTTP** attribute encapsulates 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 set to **Enabled** by default.
Name	The name of the **TCP/IP** communication profile. The default name is **TCP 1**.
Receive port	The port on which the **Netop Host** listens. The default port number is **6502**. You can specify a number in the range of **1025** – **65535**.
Send port	The port that the **Netop Host** uses to communicate with the connected **Guests**. The default port number is **6502**. You can specify a number in the range of **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 the firewall passage. This is also known as **HTTP-tunneling**. The attribute is **Disabled** by default.

UDP

A **UDP** setup element is identified by the **Name** attribute value. Initially, a "**TCP – TCP/IP**" setup element with default other attribute values is available. You can create multiple **UDP** setup elements.

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

Attribute	Description
Broadcast to subnet	Broadcast communication to the local network segment computers is set to **Enabled** by default. For **TCP/IP** broadcast communication to reach computers on remote network segments when the **Netop Name Management** is unused. Make sure that the **IP** addresses or **DNS** names are listed in the **IP Broadcast List**. Refer to the Netop Remote Control Administrator's Guide for more information about the **Netop Name Management**.
Enable	Enables the **UDP** communication profile.
Ignore port info from Name Server	Set the attribute to **Enabled** in order to replace the destination module **Receive port number** received from the **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**).
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 secondary **Netop Name Server** on your corporate network.
Receive port	The **Receive port number** received from the **Netop Name Server**.
Secondary name server	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.
Use Netop Name Server	Set the attribute to **Enabled** in order to use the **Netop Name Server** to resolve **Netop names** into **IP** addresses. Using the **Netop Name Server** facilitates the connection 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 on a **UDP** setup element, point to **New** and click on the **Broadcast list** attribute to create in a new branch below the **UDP** setup element.

A **Broadcast list** setup element is identified by the **Broadcast list** name attribute value. Initially, a "**Broadcast list – #1**" setup element is available. You can create multiple **Broadcast list** setup elements. Each **Broadcast list** setup element makes 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 are deleted automatically.

5.1.3 Names

Use the **Names** branch to specify the name by which the **Host** identifies itself when communicating.

To communicate by a communication profile that uses a networking communication device, make sure that each **Host** uses a unique name. A **Host** that uses a name that is already used by another communicating **Host** is denied communication.

Public

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

Host Naming

The computer name identifies the **Netop Host** by its computer name (generally recommended). Enter or leave blank identifies the **Netop Host** by the **Host Name** attribute value.

Attribute	Description
Hostname	Specify 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. Make sure that the Netop modules specify the same **Name Space ID** attribute value to connect with the **Netop Name Management**.

Attribute	Description
Namespace ID	The **Namespace ID** specified on the **Guests** with which the **Host** can communicate by using the **Netop Name Server**. The default **Namespace ID** is **Public**.

5.1.4 Security

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

Netop Portal certificate settings

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

Attribute	Description
Connection allowed when using an invalid certificate	If the attribute is set to **Enabled**, a **Guest** can connect to a **Host** that communicates through the **Netop Portal** with an invalid certificate.
Display invalid certificate warning	If the attribute is set to **Enabled**, a warning notifies 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 the available encryption options, click on the **Allowed encryptions** button.

The communicating **Netop modules** negotiate automatically to encrypt communication by an encryption type that is enabled on both modules. The **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: 256-bit SHA HMAC Screen and other data:160 bit SHA HMAC Logon and password: 256-bit SHA HMAC
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. 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 and mouse: 256-bit SHA HMAC Screen and other data: 160-bit SHA HMAC Logon and password: 256-bit SHA HMAC
Key exchange	Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256-bit SHA.

High

Item	Description
Description	All the 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: 256-bit SHA HMAC Screen and other data: 160-bit SHA HMAC Logon and password: 256-bit SHA HMAC
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. Make sure that the keystrokes and password details are encrypted.
Encryption	Keyboard and mouse: 256 bit AES Screen and other data: None Logon and password: 256 bit AES
Integrity check	Keyboard, mouse: 256-bit SHA HMAC Screen and other data: None Logon and password: 256-bit SHA HMAC
Key exchange	Combination of 1024 bits Diffie-Helman, 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 backward 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.
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 HMAC Screen and other data: 256-bit SHA HMAC Logon and password: 256-bit SHA HMAC
Key exchange	Combination of 1024 bit Diffie-Hellman, 256 bit AES and 256-bit SHA.

Maintenance

If the **Password** attribute has a value, maintenance password protection is enabled. If enabled, the **Netop Host** or **Netop Host Manager** requests 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** to apply the maintenance password protection to all the 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** to apply the maintenance password protection to the **Guest Access Security** command.
Password	Set the maintenance password.
Program exit and Stop Host	Set this attribute to **Enabled** to apply the maintenance password protection to unload the **Host** and stop the **Host**.

5.1.5 Debug Log

The **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. The **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 the **Debug Log** button 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** contains messages with severity levels higher than **Warning**: **Warning**, **Error** and **Critical**.
- The **Console log** contains messages severity levels higher than **Error**: **Error** and **Critical**.
- The **File log** contains messages severity levels higher than **Warning**: **Warning**, **Error** and **Critical**.

Syslog

The logs are saved using the **syslog daemon**. To set the severity of the messages which are logged to the **Syslog**, click on the **Syslog** button, on the left pane double-click on the **Level** attribute and select the log level, then click on **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 are logged in the console, click on the **Console** button on the left pane double-click on the **`Level`** attribute and select the log level, then click on **OK**.

File

All actions are saved to a specified log file. The 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 saves the log file in the folder **`/var/log/netop_host_old`** and continues to log to the **`/var/log/netop_host.log`** file path.

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

Attribute	Description
Filename	The name of the log file where the logs are saved. By default, all the logs are saved in `/var/log/netop_host.log`.
Level	Log level for the messages which are logged to the log file specified within the **File** section.
Maximum size (MB)	The maximum size of the log file in **MB**. The 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 logs are saved. By default, all the logs are saved to `/var/log/netop_host.log`
Rotation size	This 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 provide are 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 are logged. The 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 the traffic that can 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 listens for connections.

To predefine local ports for the tunnel, proceed as follows:

1. Right-click on the **Allowed Tunnels** button.
2. Select **New** and **Endpoint**. A generated endpoint entry is added to the list of **Allowed Ports**.
3. On the right pane, double-click on the newly added endpoint. An edit attribute window is displayed.
4. Enter the **IP address** of the **Host** and click on **OK**. The endpoint is displayed in the **Allowed Tunnels** list.
5. Right-click on the endpoint, select **New** and **Port**. A generated port entry is added to the selected endpoint.
6. On the right pane, double-click on the new range entry. An edit attribute window is displayed.
7. Enter the range of ports where incoming connections are 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, it is necessary that you block the tunneling on specific ports on the **Host**, add them here.
The procedure for defining **Blocked Tunnels** is like 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 that enable logging to the **Netop Host Daemon (netophostd)**. **netophostd** is a service that runs as a background process that waits 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*`**

5.2 Guest Users Security

Use the **Security** branch to define the authentication method and individual permissions for accessing the **Host**.

Guest security mode

This section allows you to define the authentication method used by the **Host**. The following options are available:

Value	Description
Netop authentication	You can define a global password for accessing the **Host**, and the role that the **Guest** receives after successful authentication.
Security Server authentication	A **Security Server** can be used to centrally manage which users have access to specific **Hosts**, and the type of access they are granted after successful authentication. The **Security Server** is located with the help of a public key, which you can configure in the **Security Server** authentication section.
System	You can use the existing system accounts to grant access to the **Host**. By default, all the system users have the **Default Role** permissions. Alternatively, you can add individual users and assign a specific role to each user. This can be configured under **System authentication**.
Netop Portal access rights	The **Portal** can be used to centrally manage authentication and authorization. For this authentication method, make sure that a **Netop Portal** profile is configured and enabled in the **Communication** section.

5.2.1 Roles

This section allows you to create custom security roles. Each security role contains a list of permissions to be allowed or denied during a **Guest** session.

To create a new role, right-click on **Roles** > **New** > **Role**.

Attribute	Description
Audio chat	If the attribute is set to **Enabled**, the audio chat feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Blank screen	If the attribute is set to **Enabled**, the blank screen feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Confirm access	Controls whether a prompt is displayed on the **Host** screen when a **Guest** is trying to connect, asking if the connection is allowed. • **Never** means that the prompt to confirm access is never displayed. • **Always** means that the prompt to confirm access is always displayed. • **Only when logged in** means that the prompt to confirm access is only displayed if a user is logged in on the **Host** machine.
Execute command	If the attribute is set to **Enabled**, the execute command feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Lock keyboard and mouse	If the attribute is set to **Enabled**, the lock keyboard and mouse feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Name	The name of the security role.
Receive files from Host	If the attribute is set to **Enabled**, the **Guest** can receive files from the **Host** during a file transfer session.
Redirect print	If the attribute is set to **Enabled**, the redirect print feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Remote control (view)	If the attribute is set to **Enabled**, the **Guest** can view the **Host** screen during a session.
Remote manager	If the attribute is set to **Enabled**, the remote manager feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Request chat	If the attribute is set to **Enabled**, the request chat feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Retrieve inventory	If the attribute is set to **Enabled**, the retrieve inventory feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Run programs	If the attribute is set to **Enabled**, the run programs feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Send files to Host	If the attribute is set to **Enabled**, the **Guest** can send files to the **Host** during a file transfer session.
The Guest can record demo files	If the attribute is set to **Enabled**, the **Guest** can record demo files during a **Guest** session, if supported by the **Guest** and **Host** version.
Transfer clipboard	If the attribute is set to **Enabled**, the transfer clipboard feature is available during a **Guest** session, if supported by the **Guest** and **Host** version.
Use keyboard and mouse	If the attribute is set to **Enabled**, the **Guest** is able to use the keyboard and mouse during a remote control session.

5.2.2 Netop Portal access rights

This selection means that the **Host** uses the **Netop Portal** to authenticate each connecting **Guest** and assign permissions to it.

Access rights are defined in the **Portal**. The connection is achieved using the **Netop Portal** profile configured under Communication > Network listen.

When a **Guest** connects, the **Host** requests the logon credentials according to the **Portal** account.

Refer to the Netop Remote Control Portal User's Guide, for more information about the **Portal**.

The **Host** forwards the returned credentials to the **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**.

5.2.3 Security Server authentication

This selection means that the **Host** uses the **Netop Security Server** to authenticate each connecting **Guest** and assign a security role to it.

When a **Guest** connects, the **Host** requests the logon credentials according to the **Netop Security Management** preferences. Refer to the Administrator's Guide for more information about **Netop Security Management**.

The **Host** forwards the returned credentials to the **Netop Security Server** for validation and compilation of the security role that is assigned to the **Guest** according to the security data stored in the security database. The **Host** applies the resulting security role to the **Guest**.

Attribute	Description
NSS public key	The public key of the **Security Server**. The **Public key** is used to secure a trusted connection between the **Hosts** and the **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 displayed in the **Security Manager**. It is recommended that you change the **Public Key** before deploying your **Hosts**.

Refer to the Netop Security Management section in the Administrator's Guide for more information about generating a **Public Key** from the **Security Manager**.

NOTE: For the **Host** to communicate with the **Security Server**, make sure that the Communication > **Network listen** > **UDP 1** profile is enabled. If the **NSS** is on the same network segment as the **Host**, make sure that the **Broadcast to subnet** option is enabled on the **UDP** profile. Alternatively, you can add the **NSS** IP or name to the broadcast list used by the **UDP** profile.

5.2.4 System authentication

This selection means that existing system accounts are used for granting access to **Guests**. When a **Guest** connects, the **Host** requests the system username and password. If the account credentials are validated,

the **Host** grants the **Guest** the privileges of the security role assigned to the system user, if any definition is found, or the **Default Role**, if no custom role was specified.

Assign specific roles to different users

If all the system users should have the same access rights, modify the **Default Role** to reflect the necessary access.

NOTE: The **Default Role** is assigned to all system accounts unless otherwise specified.

However, you can assign different roles to different users. To do this, right-click on **System authentication** > **New** > **User**. A new entry is created.

Attribute	Description
Name	Specify the system account username.
Role	Select the security role that contains the permissions the **Guest** receives after successful authentication with this user's credentials. You manage the defined roles in the **Roles** section.

If the machine is part of a domain, you can also assign specific roles to domain users in the same way as for local system users.

5.2.5 Netop authentication

This selection means that all the **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** correctly enters the password set up for authentication, the **Host** grants the **Guest** the privileges set up for the selected security role.
This section allows you to define the default password and the assigned role.

Attribute	Description
Netop password	Set the password necessary for the **Guests** to enter to access the **Host**. The maximum length allowed is **64**.
Role	Select the desired security role, containing the permissions the **Guest** receives after successful authentication. The defined roles can be managed from the **Roles** section.

6 Guest dialog boxes

6.1 Communication Profile Edit

To edit the communication profile, proceed as follows:

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

NOTE:

- To apply changes to enabled communication profiles, make sure that you reload the **Guest**.
- You can only modify the **WebConnect** and **Netop Portal** communication profiles.

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 recognized account username.
Password	Specify the password corresponding to the **WebConnect / WebConnect3** service recognized the account username you entered.
Confirm password	Confirm the previously entered password.
Domain	Specify the domain of a **WebConnect / WebConnect3** service recognized account.
Test	To verify the **WebConnect / WebConnect3** service address and credentials, click on the **Test** button.

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	Click on the **Configure** button to select the **Netop Portal** certificate settings: 

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

6.2 Connection Properties

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

Connect tab

Host PC Information

Option	Description
Description	Identifies the **Host** record. The field can be empty. You can leave it empty to automatically specify the applicable **Host** name or phone number / **IP** address in it when you create the **Host** record. You can edit the field contents.
TCP/IP Address	This field is 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 that is 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 the **Host** and the **Host** network connecting **Gateway** login credentials to connect without being prompted for the 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 are displayed as asterisks or dots. Leave the 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 displayed in 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 checkbox to disable the **Host** computer keyboard and mouse at startup.
Blank Host display	Select this checkbox 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.
Do not fit	Display the part of the **1:1** scale **Host** screen image that fits within the Remote Control window. • If the **Host** screen image has fewer pixels than the display area, black borders surround it. • If the **Host** screen image has more pixels than the display area, the Remote Control window has 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	Display a reduced palette of colors. Consumes reduced palette colors.
Max 16 colors	Display crude colors. Consumes little transmission bandwidth.

Keyboard/Mouse tab

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

Keyboard

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

Mouse

Option	Description
Remote keyboard (send all the mouse events)	Send all the **Guest** computers the 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 the transmission bandwidth.
No mouse control	Send no **Guest** computer no mouse to the **Host**.
Display Host mouse movements	Move the **Guest** computer mouse pointer in accordance with the **Host** computer mouse pointer movements.

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

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.

NOTE: Data compression takes time.

Option	Description
Automatic	Selects compression based on the properties of the applied communication profile.
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 can be lost or corrupted.
Transfer Host screen as bitmap	Typically slower but transfers the **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 is 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 a 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 the cache memory and transfers only the image changes. This saves transmission bandwidth and optimizes the 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 selects the cache memory size based on the properties of the used communication profile. In most cases, this provides 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 from the drop-down list.

- If the preferred encryption type is enabled on both **Guest** and **Host**, then it applies.
- If you prefer the **Netop 6.x/5.x Compatible** encryption type and is not enabled on both the **Guest** and **Host**, select a higher encryption level.
- If you prefer another encryption type and the encryption type is not enabled on the **Host**, the encryption type enabled on both the **Guest** and **Host** is applied.

NOTE: The icon of the encryption type used in a remote control session is displayed in 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 slow down the **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 this option to enable the **Custom options** section below. You can clear the selection of custom options to enable the transfer of these advanced desktop features. Custom options: • Disable wallpaper • Disable screen saver • Disable animation • Disable window drag • Disable Active Desktop All checkboxes are selected by default.

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 the display of confirmation dialog boxes in relation to deleting/overwriting files during the 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 checkbox to synchronize files only if they exist in the unselected pane.
Transfer only one way	Select this checkbox to synchronize files only from the selected pane to the unselected pane.

General Transfer

Option	Description
Include subfolders	Select this checkbox to transfer also the contents of subfolders of selected folders.
Use delta file transfer	Select this checkbox to compare source files with the corresponding destination files and transfer only the differences between the source and destination files. This saves transmission bandwidth.
Enable crash recovery	Select this checkbox to transfer files so that they can be recovered after a computer or network crash during file transfer.
Close dialog when finished	Select this checkbox to close the **Transfer Status** window when a file transfer finishes.
End session when finished	Select this checkbox to end the file transfer sessions when a file transfer finishes.

Confirmation tab

Confirm when…

Option	Description
Delete non-empty folders	Select this checkbox to display a confirmation dialog box if you are about to delete a folder containing files and folders. The confirmation dialog box allows you the following choices regarding the deletion: • **Skip**: Click on this button to skip deleting the specified folder. • **Delete**: Click on this button to delete the specified folder. • **Advanced**: Click on this button to change your delete confirmation selections for this file transfer only. • **Cancel**: Click on this button to cancel the file transfer at this point. You cannot undo executed file transfer actions.
Overwriting/deleting files	Select this checkbox to display a confirmation dialog box if you are about to overwrite or delete files. • **Skip**: Click on this button to skip overwriting the specified file. • **Overwrite**: Click on this button to overwrite the specified file. • **Advanced**: Click on this button to change your overwriting confirmation selections for this file transfer only.
Overwriting/deleting read-only files	Select this checkbox to display a confirmation dialog box if you are about to overwrite/delete read-only files.
Overwriting/deleting hidden files	Select this checkbox to display a confirmation dialog box if you are about to overwrite/delete hidden files.
Overwriting/deleting system files	Select this checkbox 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 checkbox to display a confirmation dialog box before executing a drag and drop file transfer.

Layout tab

Screen

Option	Description
Show toolbar	Select this checkbox to display the toolbar of the **Netop File Manager** window.
Show status bar	Select this checkbox 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 checkbox to display the same pane contents when you start a file transfer session with the same **Host** the next time. Deselect this option 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	**SHITF+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	**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 checkbox to generate a file transfer log file when ending a file transfer session.
Append if log file exists	Select this checkbox to append new log entries to an existing log file. If you do not select it, any existing log file is overwritten.
Filename	This field specifies the log file (path and) name. The default name is **`nfm.log`**. The file is in the **Netop** configuration files folder, typically **`~/.netopguest/nfm.log`**. Click on the **Browse** button to specify another log file path and name.

See also
Transfer files