

Remote Support & Management

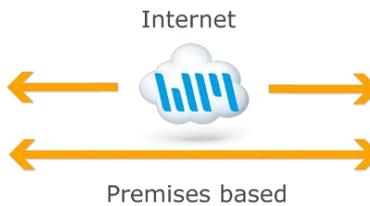
PC – Server – Mac – Tablet – Smartphone – Embedded device

Windows – macOS – Android – iOS – CE

WiseMo Guest module
for example on your Windows PC



WiseMo Host module
on your PC or Server



WiseMo develops software for remote control between computers and devices, for example between PCs, Servers, Mac computers, Smartphones, Tablets, and other handheld or un-attended devices. Using WiseMo software you have a powerful set of remote control and management features available to increase your efficiency – saving you time and money.

Guest & Host modules

The WiseMo Guest module runs on the computer or device from where you want to access and take remote control of other computers and devices.

The WiseMo Host module runs on computers and devices to prepare them for secure remote access by authenticated users with a Guest module.

Cloud & On-premises connectivity:

Connection between the Guest module and the Host module is either established via WiseMo's myCloud connectivity over the Internet or directly using TCP/IP communication on a LAN/WAN network managed by you.

For Cloud connectivity (WiseMo myCloud), your computer or device must be able to use the Internet, for example via fixed line, Wi-Fi or mobile operator network (3G, 4G, 5G). This will allow you to reach a computer or device wherever it may be and from wherever you are – as long as there is Internet connectivity on both the Guest and the Host computer.

By using TCP/IP directly between Guest and Host computer on your own network (e.g. your Wi-Fi, LAN or WAN) you can avoid Internet traffic and possible data charges from your mobile operator.

The WiseMo Host program for PCs and Servers running Windows

This guide provides information on how to install, configure, use, and uninstall the Windows Host program – our Host module for use on Windows PCs and Servers. The Host module prepares the PC or Server for easy, fast, and secure remote control from computers and devices running a WiseMo Guest module.

Notice: You use a WiseMo Guest module to remote control computers / devices running the Host module. For information on how to set up a Guest module, please refer to the tutorials for such module. Available documents can be found here: <http://www.wisemo.com/support/documents/>



1. Installation of the Windows Host program

Install the Windows Host app, to prepare the computer for remote control by authenticated users running a WiseMo Guest module.

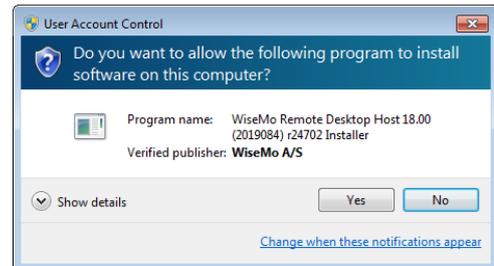
The Windows Host app supports Windows 11, 10, 8.x, 7, Vista and XP and Windows Server 2003 and later versions.

The installation file, an .msi file, may come from a myCloud domain (pre-licensed and pre-configured) or it may come from another source, where initial license and configuration, such as access security, are specified during installation. Please refer to section 1.1 and 1.2 below for details.

Run the installation file and the installation wizard will prompt you to accept the license terms and allow you to change the default installation directory.

Windows will prompt you to accept installation of the program. **You must have administrator rights on the computer to install the program.**

You may be prompted for installation of a WiseMo Smart Card driver and perhaps a Monitor driver (needed for the blank screen feature on some OS versions).



1.1 Installation file from myCloud

Login to the myCloud domain from any browser and select the Windows Host deployment link from the Manage Devices > Deployment page, right column.

Notice, you can also pass the myCloud deployment link to a target PC or Server, for example via email.

When downloading via such default myCloud deployment link, the Host is pre-licensed and pre-configured for both myCloud connectivity (via the Internet) and TCP/IP connectivity (directly on LAN/WAN). The Host will run automatically after installation.

If your myCloud domain has myCloud Device Access Control (mDAC) enabled, which is the default situation when you sign-up for a myCloud trial, the Host deployed is configured to use myCloud Device Access Control (mDAC). The default setup of mDAC permits Guest users authenticated for a specific myCloud domain to access mDAC protected Host on-line in that specific myCloud domain and with full rights. To enable / disable mDAC for your myCloud domain, select Device Access Control > Domain security.

If your domain is not configured for mDAC, the Host deployed is configured to use Windows Security Management where all local and Windows domain users will have full access via their Windows user account.

The default configuration deployed is easily changed via the Host user interface itself, for example by running the Configuration Wizard (see section 1.3 below). You can also upload a customized configuration file to myCloud to alter the default settings before deployment.

Please note that mDAC must be enabled for your myCloud domain if you configure the Host to use mDAC, otherwise you cannot connect to the Host. The Host can use Windows Security Management (or other Access methods) regardless of the myCloud domain security setting.

myCloud licensing and configuration require the computer is Internet enabled during installation and with support for https. If an older computer only supports http, special configuration is needed to sign it into a myCloud domain, see section 4.3.3.

1.2 Installation file from other sources than myCloud

You may install the Host via a download link from the email supplied to you after a purchase of perpetual licenses or after requesting a free trial.

You can also download the program here: (v.20.0)

[DOWNLOAD](#)

After installation, the Configuration Wizard is started; please refer to section 1.3 below. You will need to specify a license key. You can purchase a key or use a trial key delivered when you request a free trial.

1.3 The Configuration wizard

The Configuration wizard takes you through commonly used configuration options. You can later start the wizard from the Host, via the Home tab. Below is a brief description of the wizard pages. Which pages you will be presented for depends on previous choices in the wizard and the overall state of the Host.

a. Select license mode

If the Host is not yet licensed, the wizard will ask you to select the type of license.

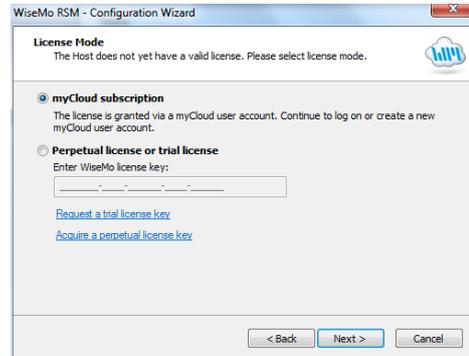
1. License via a myCloud domain

If you have a myCloud domain, you can license the program by logging into this domain. Select myCloud subscription and press "Next".

Then enter your myCloud user account credentials (typically an email address and a password). If the account is 2FA protected, you will be prompted for the verification code.

2. License via a license key

You can license the program by entering a license key (a trial key or a purchased perpetual key). Paste the key into the license key field and press "Next".



Use the license key method to allow the program to work in environments where there is no access to the internet. With the license key method, it is possible also to use myCloud for connectivity – when you have Internet access and subscribe to a myCloud domain.

b. General options

You have the choice to change some default options for the Host. Those can also be changed later from within the program's user interface. See later in this document for a description of options.

c. Guest Access Authentication Method

Define the authentication method. The default method (if not myCloud deployed) is "Shared password" where you define a password. If multiple people should access the Host, you may want to select the "Windows Security Management" option or the "User name and password" option, to avoid sharing a password. Consider myCloud Device Access Control if you prefer centralized management of user credentials and what such users may do on which computers.

d. Two-factor Authentication

You can strengthen the Authentication protection of the end-point with Two-factor authentication, 2FA. This adds an extra layer of protection in addition to the usual credentials, as a second factor, the verification code, is needed before access is possible.

e. Guest Access Role

Security roles define what an authenticated Guest user is permitted to do. There are 4 WiseMo defined roles. You can later change a security role or define completely new security roles. If a WiseMo defined security role has been modified, the Wizard text will provide you with a warning.

f. Defining Guest users

If the authentication method chosen requires the definition of Guest users, the Wizard will present you with the option to do so.

g. Configure for myCloud

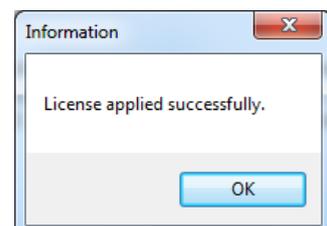
If the license method is perpetual, the wizard will prompt you with the option to configure the Host for myCloud connectivity. You can also do this later, e.g. by running the Wizard again.

h. Communication profiles

The Wizard will allow you to modify communication profiles. This is for advanced usage and usually you will not need to change these settings.

i. Completing the configuration

Press the button Finish to complete configuration and you should see the message screen "License applied successfully", if the program was licensed via the Wizard. The configuration file host.xml and the license file host.lic are stored / updated. See section 5. for info on where those files are located.



IF you exit the Wizard prematurely, the program may not be licensed to run and any changes to the default settings will not take effect. You can run the Wizard again from the Host; select the Home tab and press the Wizard button.

You may also see a warning screen if Power Options are defined to allow the computer to sleep / hibernate even when it is plugged-in. It may not be possible to remote control the computer in those situations where access to the network is prevented.

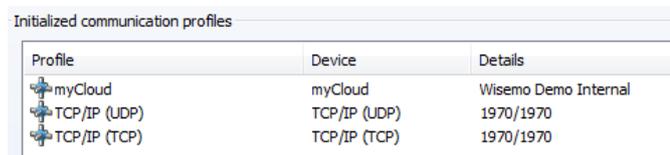
1.4 Ready for remote control

When installed and configured, the Host program is running and ready for a Guest user to connect to it.

To verify this, point the mouse on the Host icon (cloud) and check that the status shows "Running". You may find the Host icon via the Windows tray. Open the Host Manager and select the "Program Status" option found in the left pane. Verify that the "Status" section in the right pane shows Running. Check also that the Title bar says Running.

Verify that a valid IP address is shown in the "Names and addresses" section. This section also shows the Host ID and possibly a Windows user name. These are important ID's, a Guest user may use to address or identify the Host with.

Check the "Initialized communication profiles" section to verify the Host is on-line with your myCloud domain, if it has been setup for communication via myCloud. You should see a profile with myCloud in the Device column, and the name of your domain shown in the Details column. This section also shows if the Host can be reached directly via UDP or TCP including their respective port numbers (displayed as 'Send port' / 'Receive port').



| Profile | Device | Details |
|--------------|--------------|----------------------|
| myCloud | myCloud | Wisemo Demo Internal |
| TCP/IP (UDP) | TCP/IP (UDP) | 1970/1970 |
| TCP/IP (TCP) | TCP/IP (TCP) | 1970/1970 |

You may also want to check the About box to verify the program is properly licensed.

2. Examples of Remote Control

Use a WiseMo Guest module to access and remote control a PC or Server that has the WiseMo Host module installed and running.

You can remote control your Windows PC or Server from a number of different platforms by using the applicable WiseMo Guest module. You can remote control from another Windows PC, from an Android device (Smartphone / Tablet), an iOS device (iPhone / iPad), and from a Mac computer.

If you launch a connection from a browser, you may be prompted to install the appropriate Guest module, and if done, the connection can be executed. The most feature rich Guest module is our Windows Remote Desktop Guest, installed on a Windows PC.

In this chapter we show a few examples of remote control from our Windows Remote Desktop Guest module, via myCloud (internet connection) and remote control directly via TCP/IP on a network managed by you, for example your LAN. We also show an example of remote control over the Internet from an iPad or Android device.

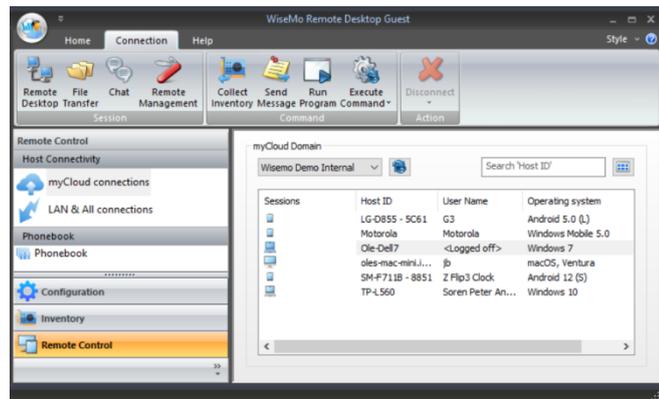
For more detailed info on the use of these Guest types, please find the documentation relevant for each module here: <http://www.wisemo.com/support/documents/>

2.1 Remote control over the Internet (using WiseMo myCloud)

This example assumes that you have a myCloud domain and that you have deployed at least one Windows Host module that is connected to this myCloud domain.

myCloud from WiseMo is a cloud based service for easy remote control connectivity between computers and devices, e.g. PCs, Servers, Mac, Smartphones, Tablets and other handheld or un-attended devices. It also provides deployment options, including download links and SMS deployment links, to help you easily deploy pre-configured and pre-licensed Host and Guest modules. If you do not already have a myCloud domain, you can sign up for a free trial here: www.wisemo.com/mycloud

1. Start the Windows Remote Desktop Guest module on your PC. You can get a Guest module [here](#) or from the Deploy tab in your myCloud domain.
2. Select "myCloud connections" from the menu, found in the left pane, and log on to your myCloud domain to see the list of on-line Host computers.
3. Double click on Host or right click and select the Remote Desktop option.

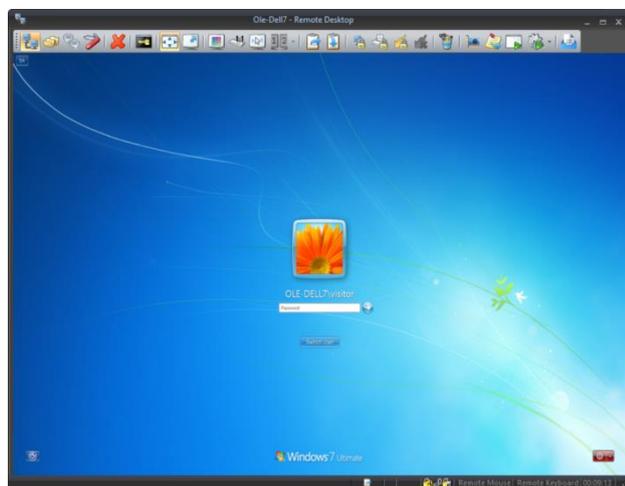


You can also select the Host and use the Remote Desktop button found on the Connection tab in the toolbar.

4. The program will connect to the remote computer and open a separate remote desktop control window, showing the desktop of the remote Host computer or device. Select the window and start remote controlling the remote Host computer – as if you were seated in front of it.



Notice the button available so you easily can execute the Ctrl-Alt-Del command on the remote PC or Server, e.g. to show the sign-in screen.



5. The remote control session can be ended by closing the window, or by pressing the disconnect button.

2.2 Remote control on a LAN / WAN using TCP/IP

A typical and quick method for taking control of a computer or device on your own TCP/IP network is to specify the IP address or Computer name of the remote computer, and then connect.

1. Start the Windows Remote Desktop Guest module on your PC.
2. Select "LAN & All connections" from the menu, found in the left pane.
3. Enter the IP address or computer name in the Host ID field.
4. Press the Connect button



(or click the Remote Desktop button on the Connection tab)

5. The program will connect to the remote Host computer. On your Windows Guest computer it opens a separate remote desktop control window, showing the desktop of the remote Host computer or device. Select the window and start remote controlling the remote computer. Your mouse and keyboard input are executed on the remote computer or device.



By pressing this button, you can easily view the complete remote desktop inside the sizeable window.

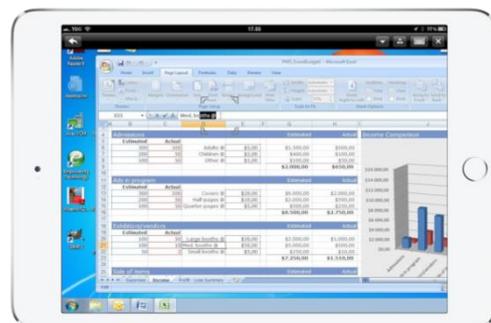
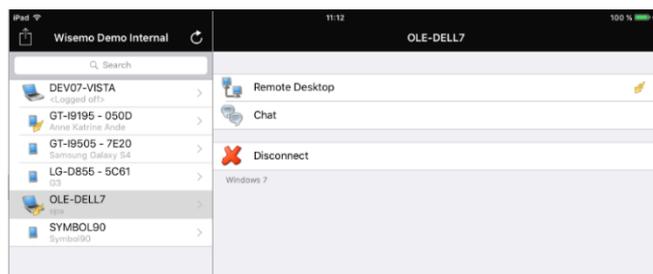


2.3 Remote control from iOS or Android over the Internet

Using a Tablet or Smartphone, you can reach your PCs and Servers from anywhere. Whether you are connected via Wi-Fi or the mobile data network, WiseMo provides fast and stable remote control connectivity to your Windows PCs and Servers.

This example assumes that you have a myCloud domain and that you have deployed at least one Windows Host module that is connected to your myCloud domain.

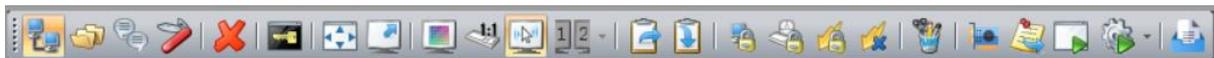
1. Download the iOS Guest module or the Android Guest module to your device.
2. Sign-in to your myCloud domain to view the list of online computers and devices.
3. Select a Host computer from the list, click Remote Desktop and you will see the Windows PC desktop on your device. Start to remote control it from your device.
4. For info on how to operate from the iOS Guest module or the Android Guest module, please see the guides here: <http://www.wisemo.com/support/documents/>



3. Host features

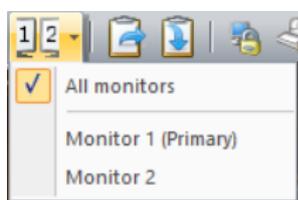
The Host module prepares a Windows PC or Server so it can be remote controlled by users running the WiseMo Guest module. The WiseMo Host module provides a number of features and functions that greatly enhances your benefit and value. This irrespective of whether your purpose is to support the un-attended situation or the situation where a user is present at the computer. You can remotely work on the computer as if you were in front of it, or provide remote support and assistance to a user in need of help. You can remotely perform system management tasks on the computer, like ending or starting services and processes. Perhaps you need to transfer files and directories back and forth and that without interrupting a user working on the computer's desktop. Or perhaps you connect from anywhere to log off or shut-down the computer.

Subject to support by the Guest module used, and permitted by the security settings applied, the Host provides for Remote Desktop Control (view and control), Remote clipboard transfer, Host screen blanking for privacy, back-ground File Transfer, File box, Hardware / Software inventory collection, Chat, Remote execution of programs, Receipt of messages from Guests, and more. It also allows for multiple Guests connecting simultaneously to the same host.



The Windows Host supports many features, here is an example of buttons available to the Windows Guest user when connected to a Windows Host computer.

One feature available when already connected is the Desktop Marker utility, which a Guest user can launch on the Host desktop. It includes the ability to draw freehand, transparent marker, arrow, text, ellipse, rectangle, "sticky notes" and it provides a screen magnifier and spotlight that follows the mouse. Use the Desktop Marker to mark areas on the desktop, when you are helping a troubled user, or to leave a note on the Desktop.



Another feature is remote control of computers with multi monitors. From the Guest side it is possible prior to connection to select which specific monitor to view, or to view all. From the Windows based Guest module, it is also possible to switch between the different monitors while connected. As default it shows the extended desktop. Remote control of only a specific part of the screen is also supported.

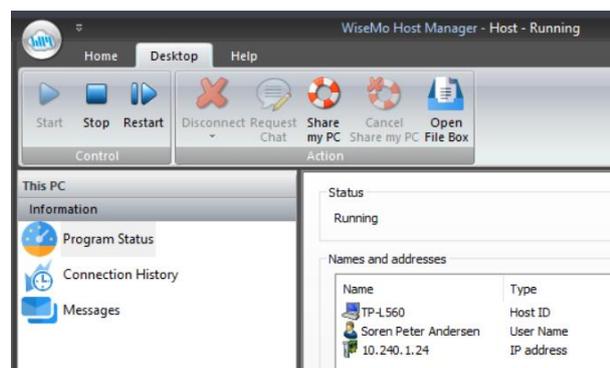


There is the File box feature, where the Guest / Host user can drag files to the File box, and those are then sent to the File box at the other end. This is an easy-to-use method for quickly exchanging files between the Guest / Host user.

The Host module also supports re-direction of Smart-card readers. This feature enables you to use a Guest side smart reader as if it was physically attached to the Host computer. Consider the situation where Windows on the Host side prompts you to insert your smart card to authenticate yourself. That would normally be physically impossible but with WiseMo remote control you can simply insert the smart card in a smart card reader on the Guest side. If prompted to choose a smart card reader on the Host, select the "WiseMo A/S Virtual Smart Card Reader".



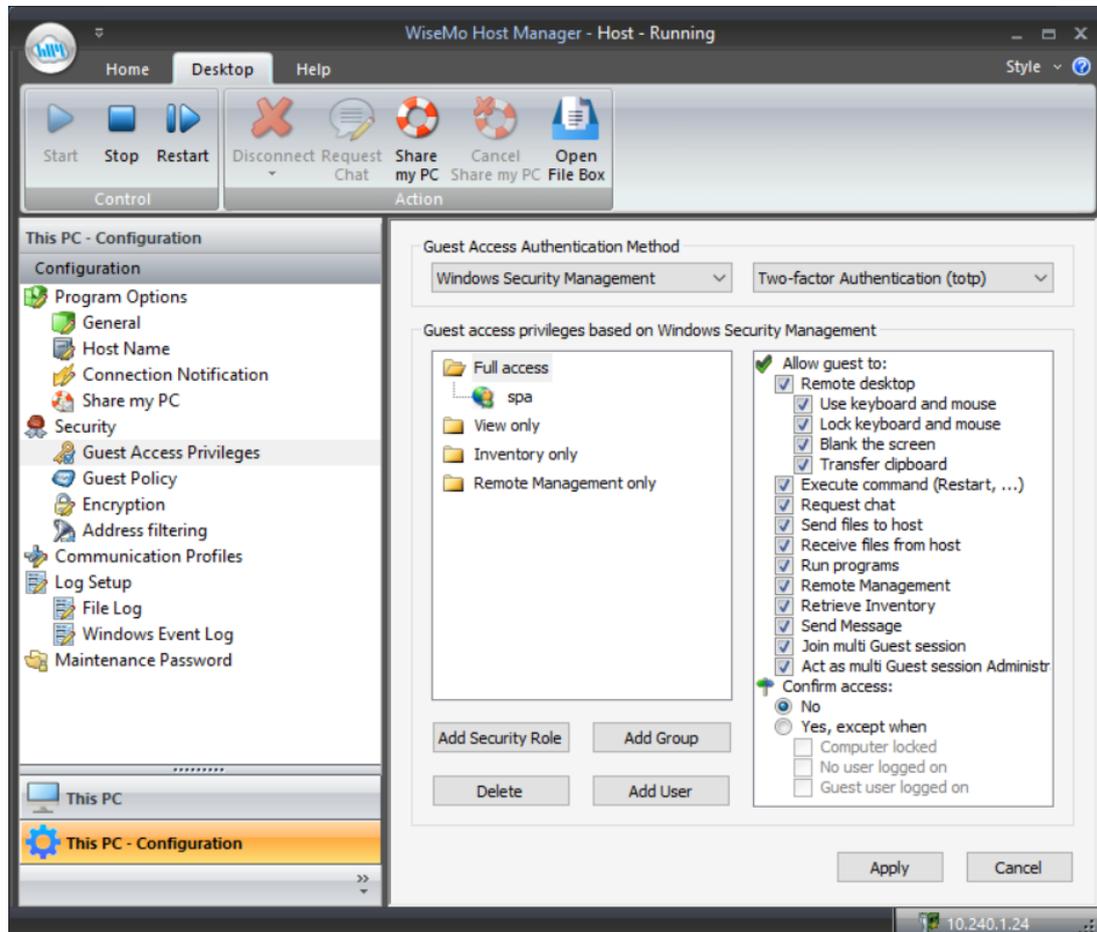
Another feature available to the user at the Host computer is the "Share my PC" feature. If enabled, this feature can be used to invite someone to temporarily access the computer, maybe to provide quick help, or to demonstrate a point. The "Share my PC" feature creates a link you can pass on to anyone with a WiseMo Guest module.



4. Host structure

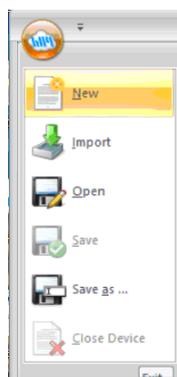
The Host module consists of a Windows service that handles for example communication and a Host Manager program that provides the user interface. The Host service may run without the Host Manager running, however with some features unavailable, for example Chat, or the Confirm Access screen, as they require user interface. As a system administrator you can enable / disable the Host service, like any other Windows service.

The Host Manager's user interface is organized with a Ribbon toolbar with buttons at the top and a Navigation bar in the left pane, where the details of each menu item are shown in the right pane.



The menu shown in the Navigation bar depends on your choice of menu category. The menu category is chosen at the bottom of the Navigation bar. Normally you have two categories available, This PC and This PC – Configuration.

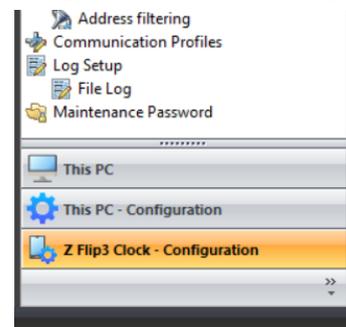
However, the Host Manager can also function as Host Configuration Manager for devices running WiseMo's Android Host or Windows Mobile/CE Host, making it easier to modify the xml-based configuration file for those devices.



System menu

You can from the system menu open an existing host.xml file or you can create a completely new default configuration file. Each appears as a menu category at the bottom of the Navigation pane. Select one to modify, for example to protect access with User name / password credentials instead of a just a password. Modified configuration files can be stored, and you can close "the device" category to remove it from the Category menu.

If you connect Android or Windows Mobile / CE devices to your PC via a USB cable, each device will appear as a menu category, if your PC can detect and open the host.xml file on the device.



Navigation bar

4.1 The Ribbon tool bar

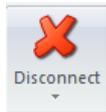
The Ribbon tool bar consists of 3 tabs, Home, Desktop and Help. Usually when working with the Host user interface, it is the Desktop tab you will be using. There are tool-tips available explaining each button shown in the Ribbon toolbar - just position the cursor over the button in question.

4.1.1 The Desktop tab

The Desktop tab provides you with various buttons for control and for executing tasks:

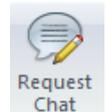


The Restart button allows you to stop and start the Host communication with a single click, especially beneficial after remotely having made configuration changes that require a re-start to take effect. The button Stop will pause the ability of the Host to communicate. Use the Start button to start Host communication if not already running. Start will initialize the host communication, so the Host is ready to receive calls from a Guest user. Please note: Default settings in Configuration > Program Options cause auto start of the communication after computer re-start. This is to ensure the computer always is ready for remote control. If you do not want this behavior, modify the Program Options.



Disconnect the session with the Guest.

If multiple Guests are connected to the Host computer simultaneously, all will be disconnected. Select the drop-down arrow to only end a session with a specific Guest user.



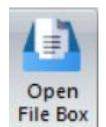
When connected to a Guest user, it is possible from the Host Manager to initiate a chat session with the Guest user.



The "Share my PC" button provides the Windows Host user with the possibility to create an invitation link, to allow a third-party temporary access to the computer. This feature requires that the Host is logged into a myCloud domain, and that the feature is enabled. Clicking the button brings up the "Share my PC" window, from where it is possible to define the duration of the invitation link, security settings and create the actual link. When created, pass the link onto a third party, e.g. by emailing it. The third party can execute the link from any installed WiseMo Guest (for example Android, iOS, Mac, and Windows). **TIP:** From the Hosts configuration menu, you can enable / disable the feature or configure the number of connections allowed and actions to happen after the link has expired.



An active link can be cancelled by using the button Cancel Share my PC, or via the button Show Share invitation, which brings up the "Share my PC" window used when creating the link. This screen also shows the time left of the invitation.



Press this button to open the File box. File box is used to exchange files between the Guest user and the Host user, by dragging a file into the box. The file is then sent, and it appears in the File box at the other end.

4.1.2 The Home tab

The Home tab provides program wide configuration options.

Import, Open, and Save

The Host configuration is stored in an XML file.

You can import one to replace the currently active, or open it for modifications. You can save the configuration, as a back-up or if you want to attach a customized configuration file to a Host deployment link in your myCloud domain. The host.xml file for the Windows Host is located in the folder:

%ProgramData%\WiseMo\WiseMo RSM\Remote Desktop Host

Wizard

Use the Configuration wizard if you want to change your Host from one myCloud domain to another. It also guides you through various Host configuration settings, such as Security choices. See also section 1.3 above. If the program is not licensed, you can also do so via the Wizard.



Language

Select among available languages. Use automatic, to have the program use your PC's language definition – if available, otherwise it will use English.

4.1.3 The Help tab

The Help tab provides buttons to access support and other resources online. You also have buttons that work on the Host program itself.



Support

This button will access the WiseMo support page from where you can file an observation or report a bug.

Knowledge Base

Connects you with a WiseMo collection of frequently asked questions regarding the usage of our product modules.

Registration

Connects you to WiseMo's system for registering on-line that you are a user of our product.

Apply License

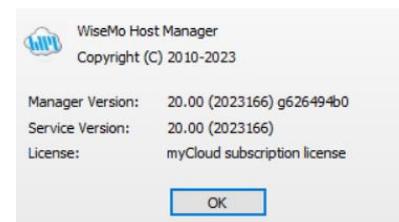
Allows you to define the license to use, either myCloud or via a WiseMo license key.

Support Log

Saves the WsmHostWin.log file with low-level communication between Guest and Host – used for trouble shooting purposes. If you need to report a problem, WiseMo support may request that you create this Support log and send it to us.

About

The About screen provides information about the program including version, licensing and copyright notices. If it is not possible to connect to the Windows computer from a WiseMo Guest, you can verify here if the Windows Host module is validly licensed. Perhaps a trial license has expired.



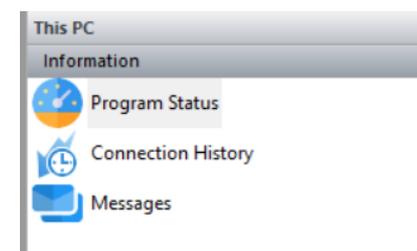
4.2 Host Information

In the navigation bar (left pane, bottom), you can select This PC, which will show Information with 3 menu items.

Select an item and its details are shown in the right pane.

4.2.1 Program Status

Select Program Status and view the information displayed in the right pane. The status of the Host service is shown in the Status section. The Names and addresses section shows the Host ID, User name (if any) and the IP address(es). The Initialized communication profiles section shows the Communication Profiles that are initialized. For the myCloud profile, the Details column shows the name of the domain the Host is logged into.



To be ready to receive a connection from a Guest user, the Host must be licensed (check the About box), have the status of Running, and at least one communication profile must be initialized. A Guest user connects to the Host using one of the initialized communication profiles.

The section "Active guest connections" shows which Guest(s) is connected to the Host, the type of session (indicated by small images), the Guest User's name, and which encryption level is used.

4.2.2 Connection History

A list of Guests connected / disconnected, with date and time stamp, since the Host was started. For more advanced logging, please use the extensive logging features available (see later).

4.2.3 Messages

Select Messages to see a list of messages received from Guest users.

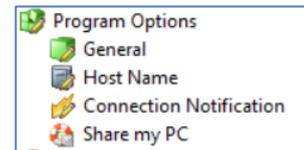
4.3 Host Configuration

In the navigation bar (left pane, bottom), you can select This PC – Configuration which will show a number of menu items.

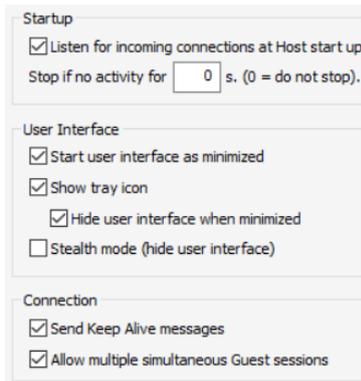
Select an item and the details are shown in the right pane. When changes are made, remember to press the Apply button. Some changes require the Host to be re-started to take effect.

4.3.1 Program Options

This section contains configuration options for the Host program and consists of the 4 items covered below.



General



The screenshot shows the General configuration pane with three sections: Startup, User Interface, and Connection. In the Startup section, 'Listen for incoming connections at Host start up' is checked, and 'Stop if no activity for' is set to 0 seconds. In the User Interface section, 'Start user interface as minimized', 'Show tray icon', and 'Hide user interface when minimized' are checked, while 'Stealth mode (hide user interface)' is unchecked. In the Connection section, 'Send Keep Alive messages' and 'Allow multiple simultaneous Guest sessions' are checked.

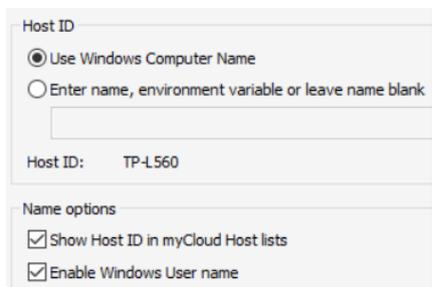
Startup: Check this setting to have the Host service initialize communication when the service is loaded. Otherwise, you will manually have to press the Start button in the Host Manager. You can define that the Host should automatically stop after a specified time of inactivity (no Guest user connected).

User Interface: Settings that define whether the Host Manager is visible or not, and if visible, how and where it is shown.

Connection: Controls various connection settings. The "Send Keep Alive messages" ensures that the Host will detect if the Guest module suddenly is no longer available. The Host can be accessed by multiple Guests simultaneously, unless the setting "Allow multiple simultaneous Guest sessions" is unchecked.

Host Name

Settings to help you customize which IDs are available for Guest users, when they need to address or select the Host.



The screenshot shows the Host Name configuration pane. Under 'Host ID', 'Use Windows Computer Name' is selected. There is an option to 'Enter name, environment variable or leave name blank' with an empty text field. The 'Host ID' field displays 'TP-L560'. Under 'Name options', both 'Show Host ID in myCloud Host lists' and 'Enable Windows User name' are checked.

Normally you will use the Windows Computer name as Host ID.

Alternatively, you can enter your own Host ID or use an environment variable.

You can also via the Enter name field tell the Host to read the Host ID from a file. Specify how the name should be retrieved from the file according to the following syntax:

```
%CSV:[DELIMITER]:[LOOKUP KEY]:[VALUE COLUMN]:[FILE NAME]%
```

If you check the Enable Windows User name, the name of the logged in Windows User will be shown in the myCloud list of Hosts, if the Host is on-line with a myCloud domain.

If Show Host ID in myCloud Host lists is not checked, the Host will not be shown in the myCloud list of Hosts. This list is shown to Guest users logged into a myCloud domain where the Host is also logged into. If un-checked, a Guest user will have to enter the Host ID to be able to connect to the Host via myCloud. Hint for third-party integration: The Host reports its Host ID to the WiseMo.ini file found in the Windows folder.

Connection Notification

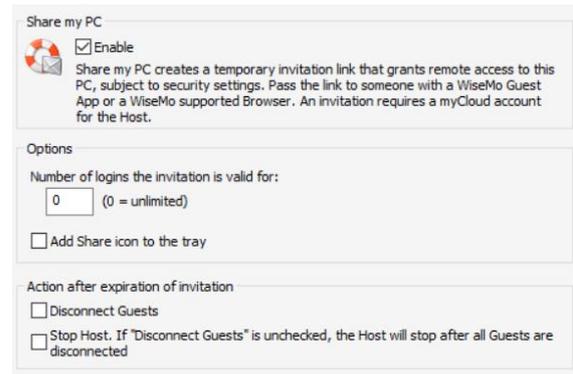
A number of options are available to tailor how a user is notified upon connection, during connection and after connection. This includes sound and visual displays. As default, the Guest name (if available) is shown in the title bar, and the Host icon is animated (flashing to indicate a Guest is connected).

Share my PC

Configuration options for the behavior of invitation links created by the Share my PC feature. Disabling the feature will disable the Share my PC button.

Options include how many connections are allowed from a link and whether a Share icon should be added to the tray for easier access. The Action after expiration of an invitation allows you to ensure that Guests will be disconnected when the link expires.

It is also possible to automatically stop the Host (so it does not listen for incoming connections) upon expiration of the link, meaning connection is no longer possible from any Guest, until the Host communication is started again. (Notice: This does not override the Startup setting to automatically listen for incoming connections, when the Host service is started, for example after re-boot of the computer).



4.3.2 Security



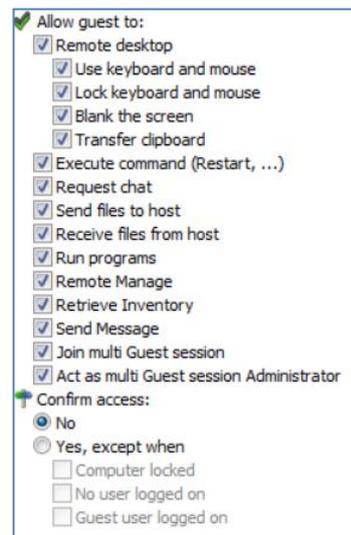
This section controls the security settings for the Host, and consists of 4 items, each is described below.

Guest Access Privileges

Controls the Authentication method and what an authenticated Guest user is permitted to do. To further protect access to the end-point, Two-factor authentication can be applied.

Permissions

Permissions define what an authenticated Guest user is allowed to do. Permissions are assigned via the Security role a Guest user assigned to. A Guest user can directly or indirectly be assigned to multiple Security roles.



There are many different actions an authenticated Guest user may or may not be allowed to do. As default, WiseMo has created 4 different Security roles. You can define your own security roles, or modify the roles defined by WiseMo.

You can for example define whether Sending or Receiving files are permitted, or perhaps restrict the Guest user to only view the screen, but not allow control of keyboard and mouse. The illustration shows the available settings.

Use the Confirm Access feature to ensure an otherwise authenticated user does not get access until a person at the Host computer also has provided permission (use only this feature for situations with attended Host computers).

Please note that permissions are defined on the Host for 3 of the 4 authentication methods. For the authentication method myCloud Device Access Control (mDAC), the users who may access, and their permissions, are defined centrally and not on the Host.

Authentication methods

There are 4 different authentication methods available:

a. Shared password: Access is protected by a single password and the default security role is used for defining permissions.

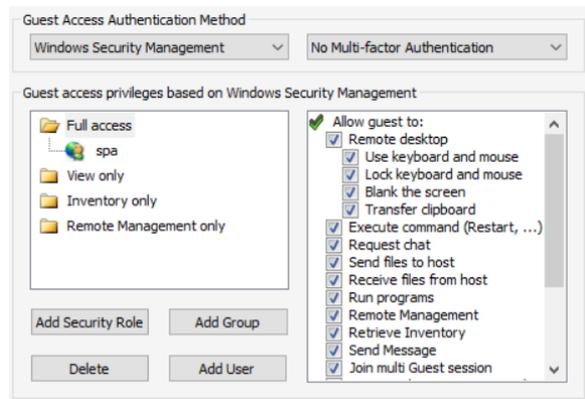


b. User name and password: Guest users have their individual user name and password. Each Guest user is assigned to a security role that governs this person's permission.

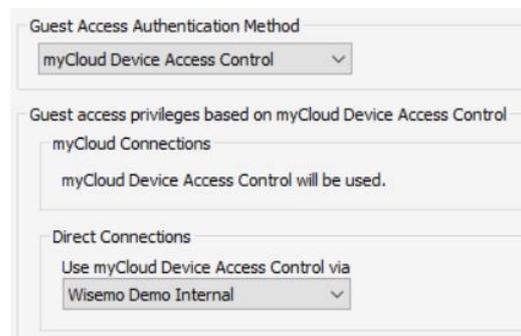
c. Windows Security Management: Uses Windows security (locally and Active Directory) to authenticate the Guest users.

You can add Windows Users and Groups for the local computer and for Windows domains. Each Guest user or group is assigned to a security role that governs permissions.

Please note that a Guest user can be indirectly assigned to more than one security role via their group memberships (e.g. all Windows users are a member of the group Users). The resulting rights are the added rights of all roles the user specifically is added to and indirectly added to via membership of a Windows group. However, Confirm Access is not enabled if a user is directly or indirectly assigned to a role without Confirm Access.



d. myCloud Device Access Control: Authentication of Guest users and their individual access privileges are centrally managed by the myCloud domain establishing the connection. In case of direct TCP/IP connections, authentication is handled via the myCloud domain specified.



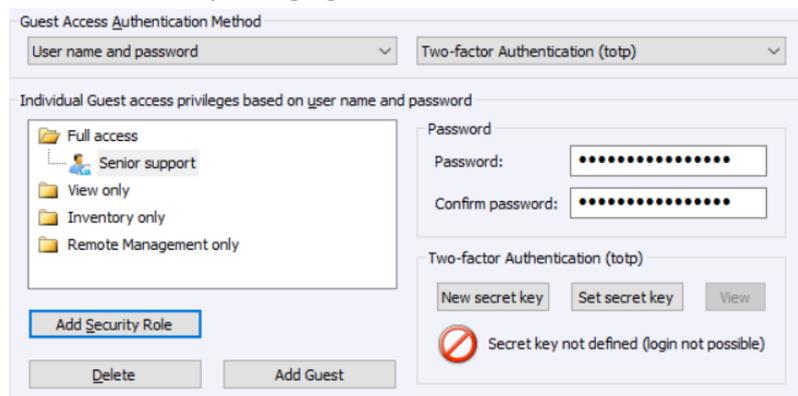
Two-factor Authentication (2FA)

Protecting access to the end-point with 2FA is a very strong security setting. It is typically used to protect access to highly sensitive computers, such as ATMs or your home computer, that only one or a few persons should be able to access.

End-point protection is available for the Authentication methods Shared Password, User name and password, and Windows Security Management. For the authentication method myCloud Device Access Control, 2FA protection is assigned and handled by myCloud.

2FA protection is defined at the Authentication method level, and when defined, Guest users trying to get access must be able to provide the constantly changing verification code – or access will not be possible. The verification code is typically generated on a Smartphone (the second factor) for example via the Google or Microsoft Authenticator App.

For the Authentication modes with defined Guest users, it is possible / advisable to set a separate secret key for each Guest user (very secure!). For more details on configuring 2FA, including configuration of the second factor, please see this [document](#).



Guest Policy

This section controls what should happen after a Guest disconnects, for example do an automatic Windows log off. It offers a hot-key definition to disconnect Guests. It also controls how many password attempts are allowed and what should happen if the maximum is reached.

Encryption

The Host offers a number of encryption levels and integrity features to ensure that the data stream has not been tampered with.

Options include from "None" to "Very high" but only High and Very High are enabled as default.

The Host settings ultimately dictate which encryption settings can be used. A Guest user may request its preference, and if permitted by the Host settings, this preference will be used. Otherwise, an encryption level permitted by the Host will be used. The Classic level is only relevant for compatibility with older special modules.

Name: Very high

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 or less important

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 2048 bits Diffie-Hellman, 256 bit AES and 512 bit SHA

Each type of encryption is explained by selecting it and pressing the Show details button. The picture to the left shows the explanation for the setting Very high.

Using strong encryption may come at the expense of CPU usage. If you are connecting via networks not controlled by you, e.g. the Internet, you should always use some form of encryption. If you are running on a network managed by you, it may make sense to select less secure encryption. WiseMo Guest modules (from v.17) will as default attempt to use VERY HIGH encryption.

Address filtering

You can limit the IP addresses from which a Guest User can connect to the Host. This can also be defined in the form of ranges. It is a good measure to use, if permitted Guest users run from static IP addresses or ranges of IP addresses. Guest users from IP addresses not listed will be denied access early on in the connection process. This feature should be used carefully in connection with myCloud connectivity as you must add all myCloud Connection Servers (routing points).

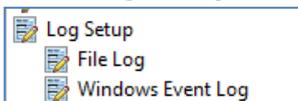
4.3.3 Communication Profiles

Allows advanced configuration of the communication profiles used by the program. The program supports communication via TCP, UDP, HTTP and via myCloud connectivity.

For TCP/IP profiles (TCP, UDP and HTTP), you can for example change the send/receive port numbers the Host uses as default (1970/1970).

For myCloud profiles, the Connection Account can be defined manually, for example if the Host computer or firewall doesn't allow for HTTPS calls. In general, it is recommended to use the Wizard for configuration of myCloud connectivity, as it uses myCloud User account credentials (email + password).

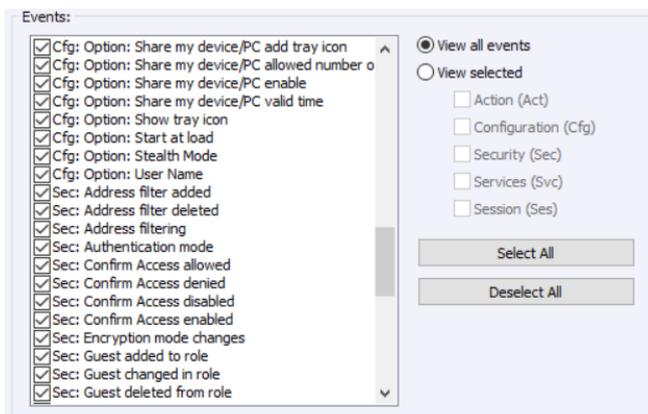
4.3.4 Log setup



The Host provides for extensive logging of event activity related to the Host. This includes changes to configuration settings, specific actions, security related events, and

session events.

Logging can be made to a file and to the Windows event log, either locally or to another computer/server.



4.3.5 Maintenance Password

To protect against changes to the configuration or the use of the Host's control buttons Start, Stop and Re-start, you can add a maintenance password.

5. Updating or removing the Windows Host module

A newer version or service release of the Host application can be installed on top of the previous one.

Updating an existing installation will as default preserve the configuration settings, which are stored in the Host.xml file typically found here:

C:\Program Data\WiseMo\RSM\Remote Desktop Host.

On XP computers the WiseMo folder is typically found here (folders may be hidden):

C:\Documents and Settings\All Users\Application Data\

You can delete the Host.xml file prior to installation, if you want to start with default configuration settings. **Exception:** If you install via a myCloud deployment link, for example sent via email or other methods, the Host will always be enabled for this specific domain. Furthermore, if a customized configuration file has been added to the deployment link, this configuration file is always used, replacing any existing configuration file on the computer. This allows for deployment of configuration settings via the use of myCloud deployment links.

The license file Host.lic is stored in the WiseMo folder under Program Files / Program Files (x86). If removed, the program will not run and may prompt for license info.

Removal of the WiseMo Host application from a Windows PC or Server is done like you would remove any other Windows program. For example, it can be done via the Control panel / Programs and features option (exact terminology depends on the Windows version).

Uninstalling the Host program does not remove certain temporary files, the license file and the configuration file.

The Host Manager is shared with the mobile Host modules. Hence uninstalling the Host might not remove the Host Manager part if there are Mobile Host installation files on the computer. The Host Manager will be uninstalled when the last module using the Host Manager is uninstalled.

6. License information for the Host program

The Host program, version 20, can be licensed in various ways.

myCloud license (subscription)

Use this license mode when you want the Host module licensed via sign-in to a myCloud domain, where it then consumes a subscription based myCloud license. With this mode, you can reach the Host via the Internet, or directly via TCP/IP connectivity. You can also use mDAC for central access security, for myCloud connections as well as direct connections via TCP/IP. The computer / device must be able to communication with myCloud over the Internet.

If you apply a perpetual license key to a myCloud licensed Host, its licensing is switched over to perpetual licensing (see below).

Perpetual license (one-time fee)

Requires that a perpetual license key is applied to the Host. A Guest user can use TCP/IP connectivity to reach the Host. Use perpetual licensing if you only need to reach the Host directly via TCP/IP and you do not want to use or depend on the availability of the Internet.

A perpetual licensed Host can also be signed-in to a myCloud domain if you also wish to use myCloud connectivity, to reach the computer or to protect access via myCloud Device Access Control. Signing a perpetual licensed Host into a myCloud domain will consume a myCloud license.

Closed user group is an option for larger installations to further protect access to the Host. Using a Closed User Group license key prevents Guest users from access, unless they also are licensed via a matching Closed User Group license key.

Trial license

If you provide the Host with a trial license key, the Host behaves as if it is perpetually licensed, but only for a limited period (you can request a trial license key [here](#)).

To test the Host with myCloud licensing, you can download and install the Host installation file from Manage Devices > Deployment page in your myCloud trial domain. If you already have a Host installed, you can from the Help tab > Apply License configure the Host to use myCloud licensing. If you locate and delete the file host.lic prior to installation, you will be prompted for licensing.

7. Glossary

Computer – Any Server, Workstation, Desktop, Laptop that runs an operating system supported by the Guest or Host module.

Device – Any Smartphone, Tablet, Set-top box, Scanner, or other handheld or unattended device that runs an operating system supported by the Guest or Host module. Depending on context, the term Device can also include Computer.

Guest – the module installed on a computer or device, e.g. PC, on an iPad, iPhone, Android device or running from a supported Browser. From the Guest module, a user is able to remote control another device or computer where the Host module is running.

Host – the module installed on the target computer or device that should be remotely controlled from the Guest module. It can for example be a PC, Mac, Smartphone, Tablet, Set-top box, or any other type of device that runs a supported operating system.

Host Configuration Manager – also termed Host Manager or Mobile Host Manager. A tool used for configuring a WiseMo Host application. It is installed on a Windows desktop computer and communicates with the Host service or your device when the device is USB connected to your PC.

Skin – the graphical user interface used by the Guest module on Windows, for remote control of devices. Usually, it is almost an exact graphical copy of the real device which is being remote controlled. Skin buttons are “alive” and imitate the keystroke of the real button: if you click on one of them then the same action will be performed on the device as if you clicked the real button.

Communication profile – protocol configuration for the communication between a Guest module and a Host module. There are two main communication methods: TCP/IP and myCloud. Before connecting from a Guest to a Host you should specify on the Guest which communication profile should be used.

myCloud – one of the communication profiles. myCloud communication is an internet-based protocol that allows connection through firewalls, proxies and NAT'ed networks. It comes as part of WiseMo's myCloud subscription based service for easy remote control connectivity between computers and devices.