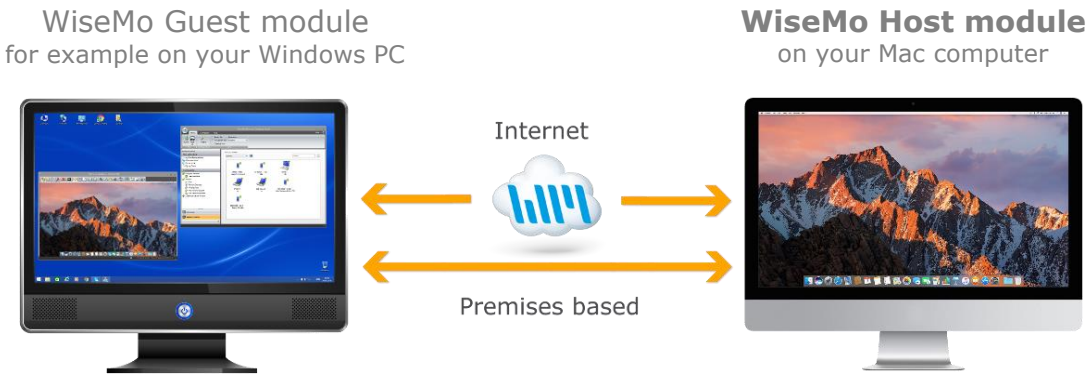
Remote Support & Management
PC – Server – Mac – Tablet – Smartphone – Embedded device
Windows – macOS – Android – iOS – CE



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 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, etc.). 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 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 Host program for computers running macOS

This guide provides information on how to install, configure, use and uninstall the Mac Host program – our Host module for use on computers with macOS 10.9 or later. The Host module prepares the computer 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 setup 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 Mac Host program

The program is installed on your Mac computer, so you can remote control it from computers and devices running a WiseMo Guest module. The Mac Host program runs on macOS 10.9, 10.10, 10.11, 10.12, 10.13, 10.14, 10.15, 11. This guide assumes you install a WiseMo Mac Host v.18 (build 2021.055) or later.

1.1 Download the Host

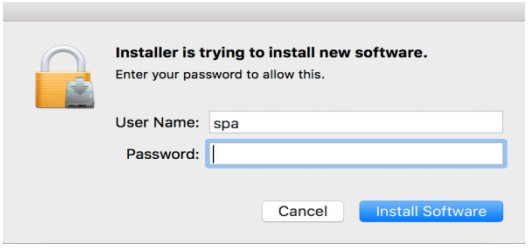
You can get the Host installation file, a .pkg file, from various sources, for example via the Deploy tab in a WiseMo myCloud domain (trial or paid) or via a download link from the email supplied to you after a purchase or after requesting a free trial.

You can also download the program here: (v.18.0)

For download via the Deploy tab in your myCloud domain (log on from a browser), select the Mac Host link, which brings you to the download page. Notice you can also deploy the download link, for example via email, to the target Mac computer. When downloading via myCloud, the Host will come pre-configured for both myCloud connectivity and TCP/IP connectivity.

1.2 Install the Host

Run the installation file and the installation wizard will prompt you to accept the license terms. macOS will prompt you to accept installation of the program.



If the Host was deployed from a myCloud domain without specifying a license key, it will be myCloud licensed. It is by default configured to run automatically after installation. Access security is defined to use System Security authentication where built-in Administrators on the Mac computer are permitted as Guest user. By default such user has full access. You can upload a customized configuration file to myCloud to alter the default settings. myCloud licensing and configuration require the computer is Internet enabled during installation and configuration. The default configuration is easily changed via the Host user interface itself, or for example by running the Configuration Wizard.

(NOTE: IF you deploy a Host with default settings to a 3rd. party computer, a Guest user must have Administrator credentials on that 3rd. party computer to gain access. Configure instead the Host to use one of the other authentication methods prior to deployment, or use the Host's "Share my Mac" feature).

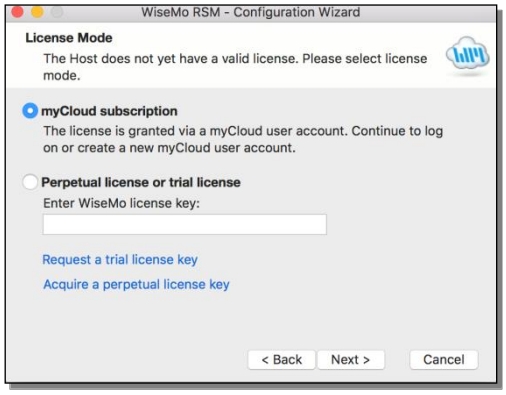
If the Host is not yet licensed when installed, for example if downloaded via the Download button above, it will start the Configuration Wizard.

1.3 The Configuration wizard

The Configuration wizard takes you through commonly used configuration options. You can later start the wizard from the Host, by pressing the Wizard button.
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 type of license.



1. Licensed 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. Licensed via a license key

Alternatively, 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 to use myCloud for connectivity – when you have Internet access and 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 a shared password. If multiple Guest users should access the Host, you may want to select the "System Security Management" option or the "User name and password" option.

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 usual credentials, as a second factor, the verification code, is needed before access is possible.

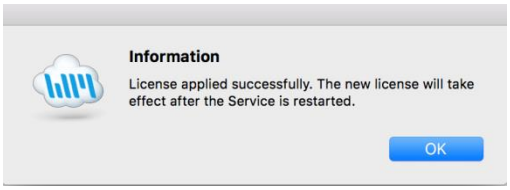
e. Guest Access Role
Security roles define what an authenticated Guest user is permitted to do. There are 3 WiseMo defined roles. You can later change a security role or define completely new security roles. If a WiseMo defined security role has been modified, the Wizard text will provide you with a 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, by running the Wizard again.

h. Communication profiles
The Wizard will allow you to enable / disable communication profiles. 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. 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; 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 is not possible to remote control the computer in those situations.

1.4 Required permissions for macOS

Apple introduced a new security mechanism in macOS 10.14 Mojave and made it stricter in macOS 10.15 Catalina.

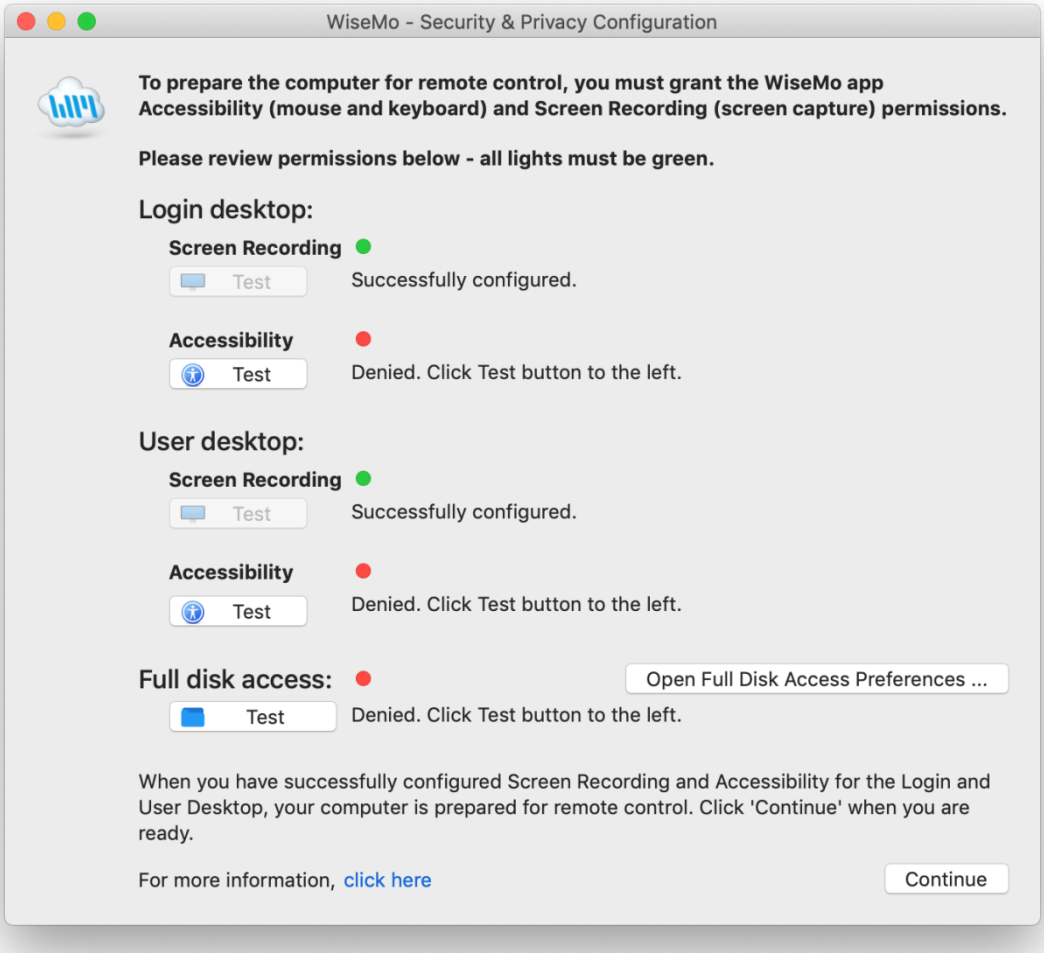
The security mechanism requires that special access is granted to remote control applications, and therefore also to the WiseMo Mac Host module. When those permissions are provided, you will be able to view and remote control both prior to login and after login, and fully use the WiseMo File Manager feature.

Depending on macOS version, some permission may automatically have been granted; other needs the user to grant such permission.

Permissions may be needed for remote control of the User Desktop and for remote control of the Login screen. (Screen recording permission to be able to remotely view the screen and Accessibility permission to be able to remotely use the keyboard and mouse).

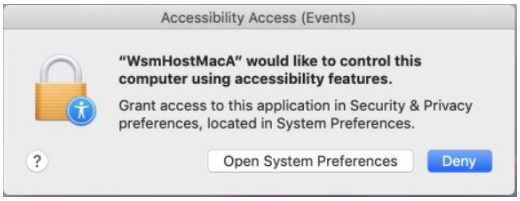
Permission may also be needed to be able to access otherwise restricted areas of the disk when using the WiseMo File Transfer feature.

Upon first run the Mac Host module prompts you for the needed permissions; and you will see a WiseMo guidance dialog.

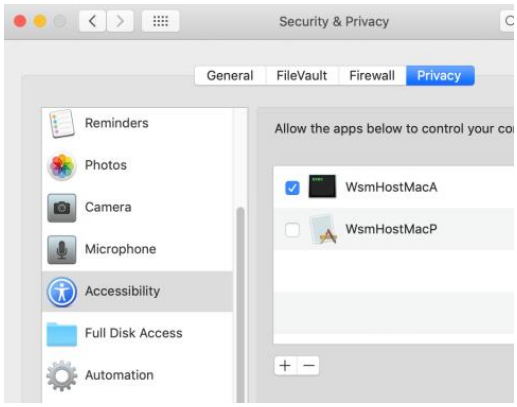


Click any active Test button to obtain a green light for each – for complete configuration.

When you click a Test button for an item with a red light, you will be prompted to Deny.



Here you must instead **select "Open System Preferences"**, which takes you to the Security & Privacy screen of the Mac computer:



Now you can enable the permission for the WiseMo apps needed via a checkmark for each appropriate app.

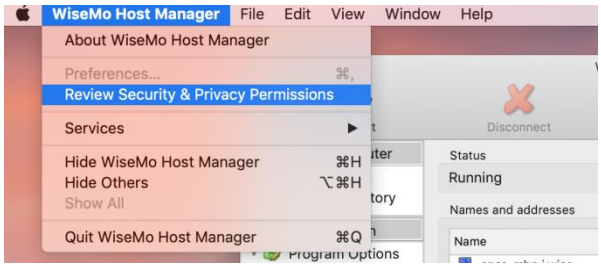
You may need to permit access for the WsmHostMacA and the WsmHostMacP apps under Accessibility (for remote input of keyboard and mouse).

You may need to permit access for the WiseMo Host Manager and the WsmHostMacP apps under Screen recording (for remote screen viewing).

You may need to permit access for the WiseMo Host Manager app under Full Disk Access to allow the WiseMo File Manager feature to access areas of the disk that are otherwise not accessible.

IF the needed WiseMo files are not listed in the dialogs shown, after you have activated the Test buttons, please click here for further information.

To later review the Security & Privacy Permissions, select the WiseMo Host Manager:



1.5 Ready for remote control

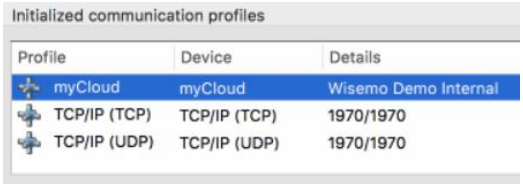
When installed and configured, the Host is running and ready for a Guest user to connect to it.

To verify it is ready, open the Host Manager program, e.g. via the status bar. Click the Host icon and select Show.

Select the "Program Status" option found in the left pane. Verify that the "Status" section in the right pane shows 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 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 as Device, and the name of your domain shown in the Details column.

This section also shows if the Host can be reached via UDP or TCP including their respective port numbers (displayed as 'Send port'/'Receive port').

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 Mac computer that has the WiseMo Host module installed and running.

You can remote control your Mac from a number of different platforms by using the applicable WiseMo Guest module. You can remote control from an Android device (Smartphone / Tablet), an iOS device (iPhone / iPad), from a Chrome browser on Mac, Linux or Windows, from an IE browser or Windows browsers supporting NPAPI components. 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 communication) 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.

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

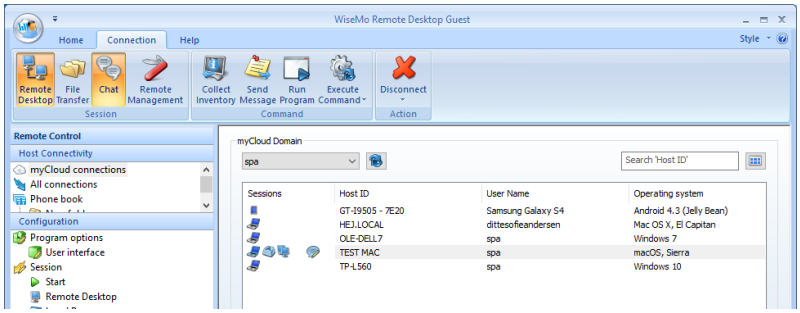
2.1 Remote control over the Internet (using WiseMo myCloud)

This example assumes that you have a myCloud domain and that you have deployed at least one Mac 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, 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 a 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.



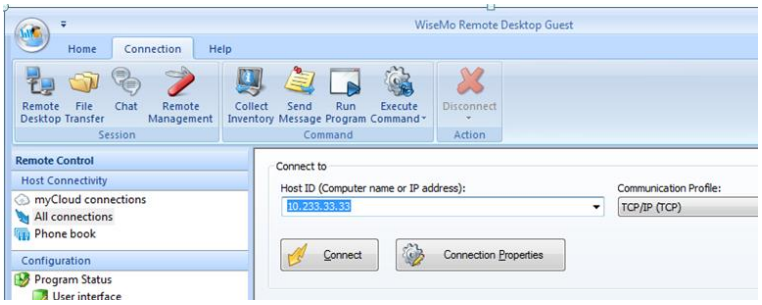
4. The program will connect to the remote computer and open a separate remote desktop control window, showing the desktop of the remote Host computer or device. Select the window and start remote controlling the remote Host computer – as if you were seated in front of it.

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

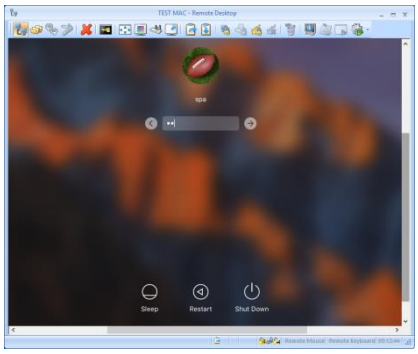
1. Start the Windows Remote Desktop Guest module on your PC.
2. Select "All connections" from the menu, found in the left pane.
3. Enter the IP address or computer name in the Host ID field.
4. Press the Connect button



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

5. The program will connect to the 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 Host. Your mouse and keyboard input is executed on the remote Host computer or device.

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

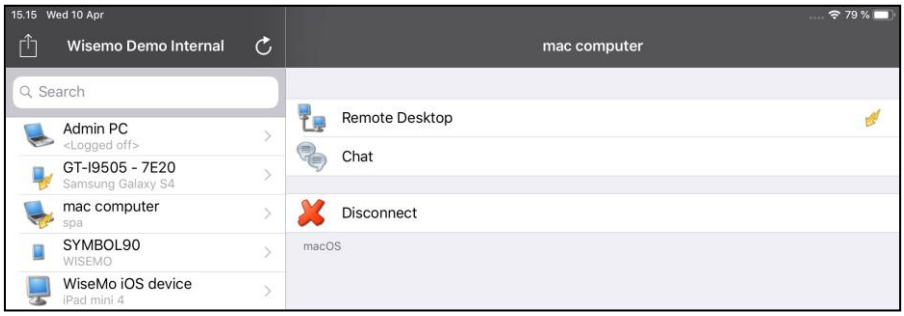


2.3 Remote control from iOS or Android over the Internet

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

This example assumes that you have a myCloud domain and that you have deployed at least one Mac Host module that is connected to this 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 and start to remote control it from your device.

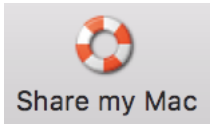
3. Host features

The Host module prepares a Mac computer to be remotely reached by WiseMo Guest users, and 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 troubled users. Perhaps you need to transfer files and directories back and forth or just connect from anywhere to log out or shut-down the computer.

Subject to being supported by the Guest module used, and permitted by the security settings on the Host, the Host provides for Remote Desktop Control (view and control), Remote clipboard transfer, Host screen blanking for privacy, File Transfer, Hardware / Software inventory collection, Chat and more. It also allows for multiple Guests connecting simultaneously to the same host.

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

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



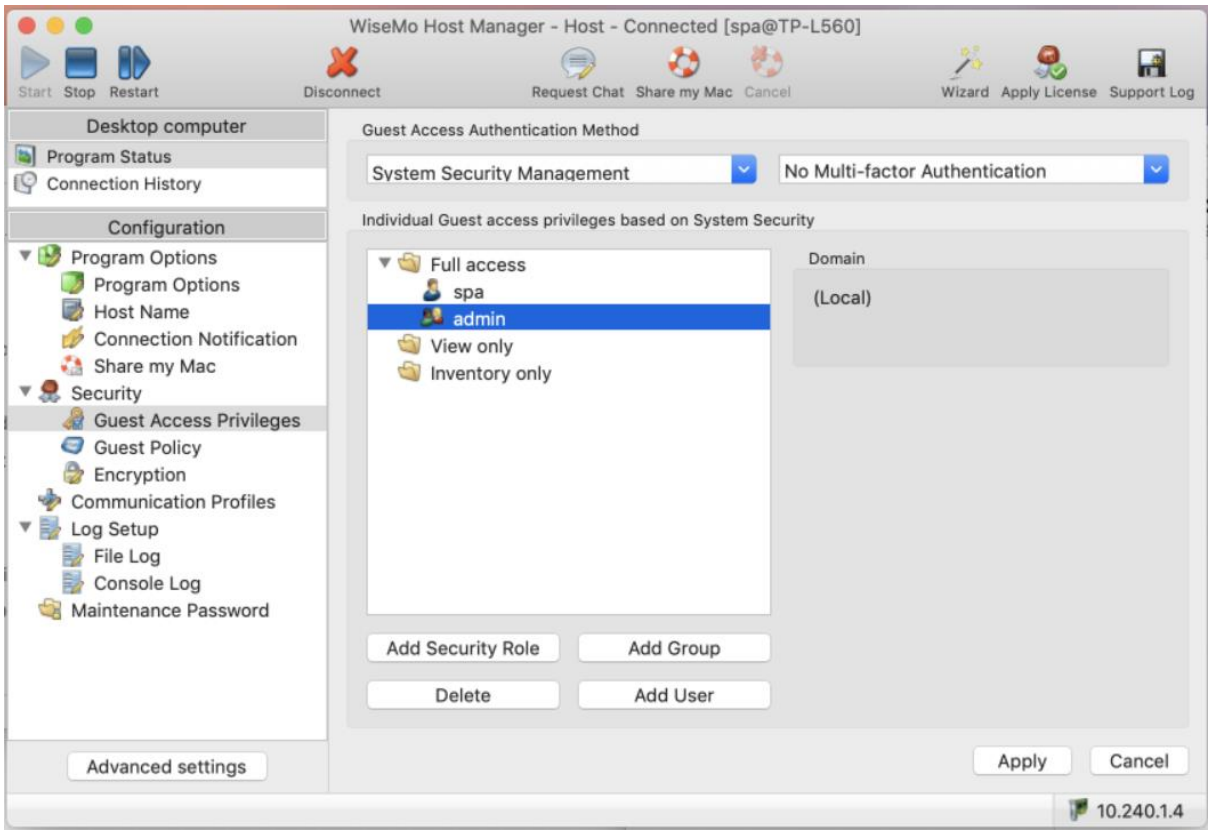
Notice the "Share my Mac" feature that a user on a Host computer can use to invite someone to temporarily access the computer, maybe to provide quick help, or to demonstrate a point. The "Share my Mac" feature creates a link the Host user can pass on to anyone with a WiseMo Guest module or a supported browser (Chrome, IE, ...).

The Mac Host program is localized to various languages, and will automatically use the language chosen for the Mac computer, if available. Otherwise it defaults to English.

4. Host structure

The Host module consists of a Host Daemon and a Host Manager program that provides the user interface. The Host Daemon 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.

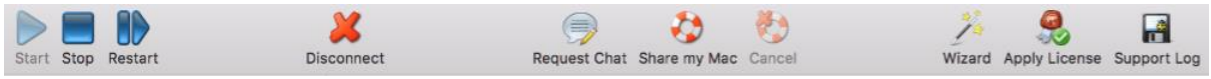
The Host Manager's user interface is organized with a Toolbar with buttons at the top and a Navigation bar in the left pane, where the details of each menu item are shown in the right pane.



Advanced settings

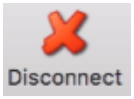
The button "Advanced settings" can also edit the host.xml file that contain the configuration settings. Configuration of the Mac Host should be done via the Wizard and the configuration settings available in the Host Manager. You should normally NOT try to modify settings via the "Advanced settings" button.

4.1 The tool bar



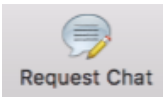
There are tool-tips available explaining each button shown on the toolbar - just position the cursor over the button in question. Right click on the toolbar to customize it.

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 a call from a Guest user. Please notice: Default settings in Program Options cause auto start of the communication after computer restart or log on. This to ensure the computer always is ready for remote control. If you do not want this behavior, modify Program Options in the Host.

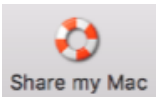


Disconnect the connection with a Guest.

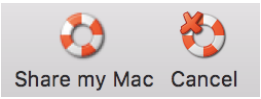
If multiple Guests are connected simultaneously, all will be disconnected.



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



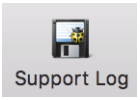
The "Share my Mac" button provides the Mac Host user with the possibility to create an invitation link, to allow a third party temporary access to the computer. This feature requires that the Host is logged into a myCloud domain, and that the feature is enabled. Clicking the button brings up the "Share my Mac" window, from where it is possible to define the duration of the invitation link, security settings and execute the actual creation of the link. When created, pass the link to a third party, e.g. by emailing it. The third party can execute the link from a supported browser or from an installed WiseMo Guest (for example on Android, iOS and Windows). **TIP:** From the Hosts configuration menu, disable / enable the feature and 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" or via the button Share my Mac, which brings up the "Share my Mac" window used when creating the link. This screen also shows the time left of the invitation.

Press the Wizard button to run the Configuration wizard. Use it for example to change which mycloud domain the Host should connect to. It also guides you through various Host configuration settings, such as Security choices. See also section 1.3 above.

The Apply License button allows you to enter a WiseMo license key – without having to run the Wizard.



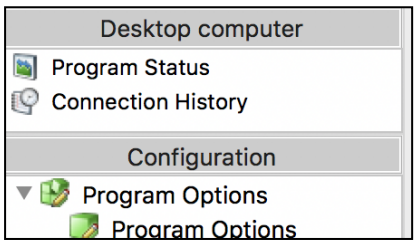
Saves the WsmHostMac.log file with lower level communication between Guest and Host – used for trouble shooting purposes. If you need to report a problem, WiseMo support may request that you create this Support log and send it to us.

The About screen is reached via the WiseMo Host icon shown in the status bar at the top of the Mac computer. It provides information about the program including version, licensing and copyright notices.

If it is not possible to connect to the Mac computer from a WiseMo Guest, you can verify here if the Mac Host module is validly licensed. Perhaps a trial license has expired.

4.2 Host Information and Configuration

The navigation bar is divided into two groups, Desktop computer and Configuration. Each group contains a number of menu items, which are covered below.



Select an item in the navigation bar (left pane), and the 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 daemon 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 call from a Guest user, the Host must be licensed (check About box), have the status of Running, at least one communication profile must be initialized and it must

show a valid IP address. A Guest user must connect to the Host using one of the initialized communication profiles.

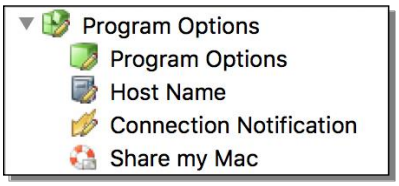
The section "Active guest connections" shows which Guest(s) is connected to the Host, the type of session (indicated by small images), the Guest User's name, and which encryption level is used.

4.2.2 Connection History

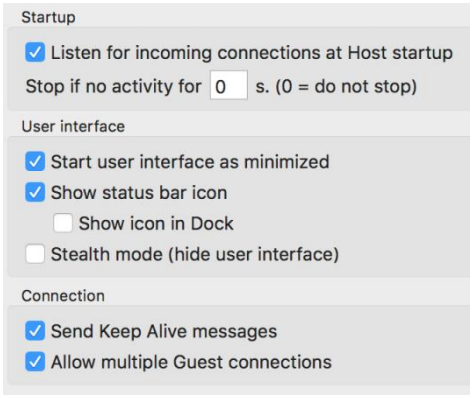
A list of Guests connected / disconnected, with date and time stamp, since the Host was started. For more advanced logging, please use the extensive logging features available (see later).

4.2.3 Program Options

This section contains configuration options for the Host program and consists of 4 items covered below. When changes are made to configurations, remember to press the Apply button. Some changes require the Host to be re-started to take effect.



Program options

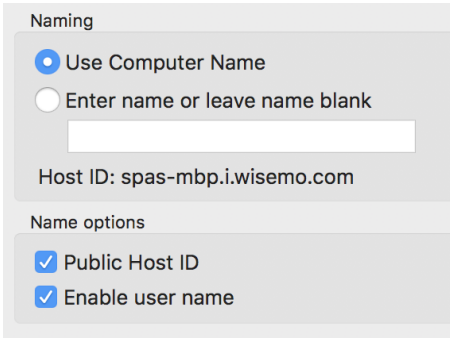


Startup: Check this setting to have the Host daemon initialize communication when it is loaded. Otherwise you will manually have to press the Start button in the Host Manager. You can define that the Host should automatically stop after a specified time of inactivity (no Guest user connected).

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" ensure 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 Guest connections" 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. Normally you will use the Mac computer name as Host ID. Alternatively, you can enter your own Host ID.

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:

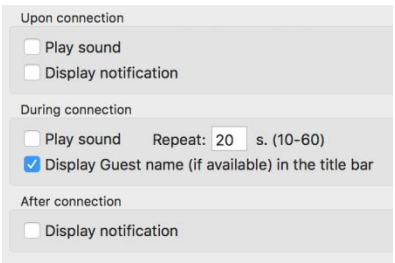
%CSV:[DELIMITER]:[LOOKUP KEY]:[VALUE COLUMN]:[FILE NAME]%

If you check the Enable User name, the name of the logged in Mac User will be shown in the myCloud list of Hosts as well.

If Public Host ID is not checked, the Host will not be shown in the myCloud list of Hosts. This list is shown to Guest users logged into your myCloud domain. A Guest user will then have to enter the Host ID to be able to connect to the Host via myCloud.

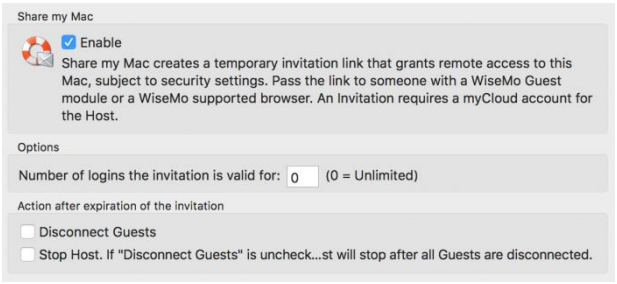
Connection Notification

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.



Share my Mac

Configuration options for the behavior of Invitation links created by the Share my Mac feature. Disabling the feature will disable the Share my Mac button in the toolbar.



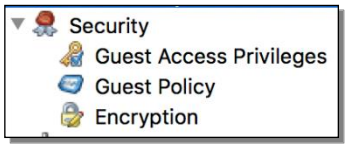
Options include how many connections are allowed from a link and what to do after expiration of the invitation link.

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 daemon is started, for example after re-boot of the computer).

4.2.4 Security

This section controls the security settings for the Host, and consists of 3 items, each is described below.

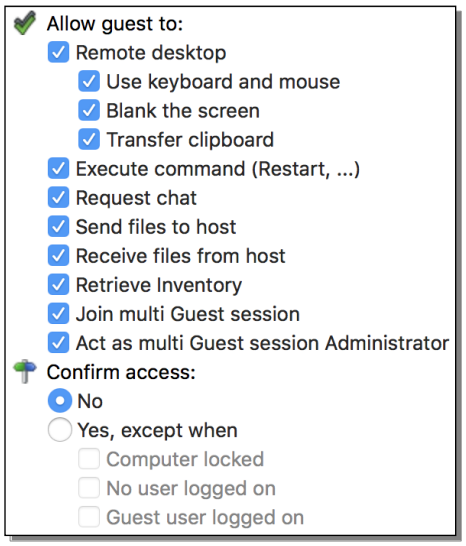


Guest Access Privileges

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

What an authenticated Guest user is permitted to do is controlled via Security roles assigned to a Guest user. There are many different actions an authenticated Guest user may or may not be allowed to do. As default, WiseMo has created 3 different Security roles. You can define your own security roles, or modify the roles defined by WiseMo.

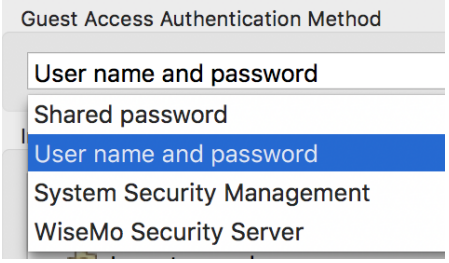


You can for example define whether Sending or Receiving files are permitted, or perhaps restrict the Guest user to only view the screen, but not allow control of keyboard and mouse. The illustration shows the available settings.

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

Authentication methods

There are 4 different authentication methods available:

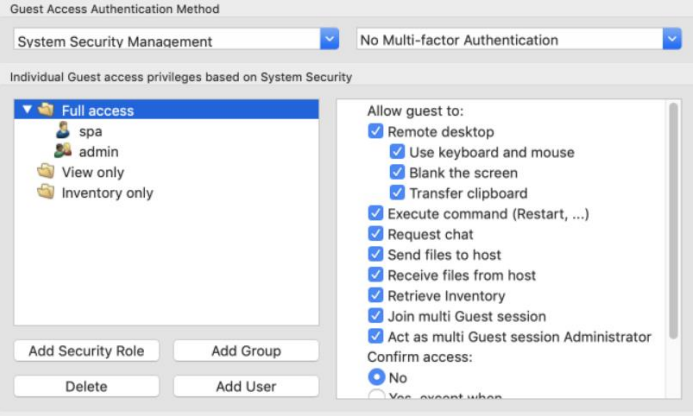


a. Shared password: Access is protected by a single password and the default security role is used for defining permissions.

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

c. System Security Management: Uses macOS system security to authenticate the Guest users. You can add Users and Groups for the local computer. Each Guest user or group is assigned to security roles that govern their permissions.

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

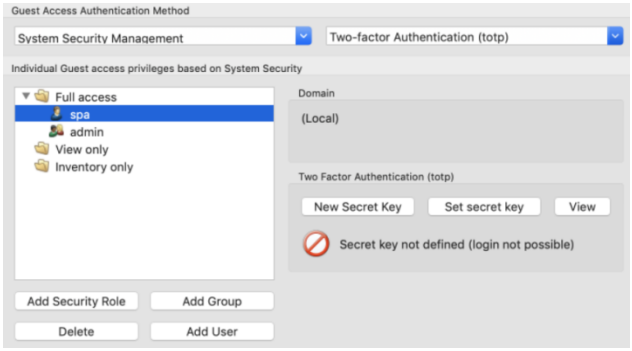


d. WiseMo Security Server: Individual Guest access privileges based on a WiseMo Security Server, which is an extra cost module for centralized management of security between Guests and Hosts.

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.

2FA protection is defined at Authentication method level, and all 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 secrete 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 computer log out. It also controls how many password attempts are allowed and what should happen if the maximum is reached.

Encryption

Encryption Details

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

The Host offers a number of encryption levels and integrity features to ensure that the data stream has not been tampered with. Options includes from "None" to "Very high" encryption.

The Host settings ultimately dictates 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. As default, the Host permits all levels except Classic. The classic level is only relevant for compatibility with some special modules.

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 not be used in connection with myCloud connectivity, and should only be used by experienced users. Use the "Advanced Settings" button, to configure Address filtering.

4.2.5 Communication Profiles

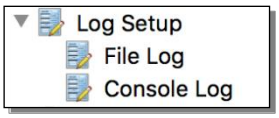
Allows advanced configuration of the communication profiles used by the program. The program supports communication via TCP, UDP and via myCloud connectivity.

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

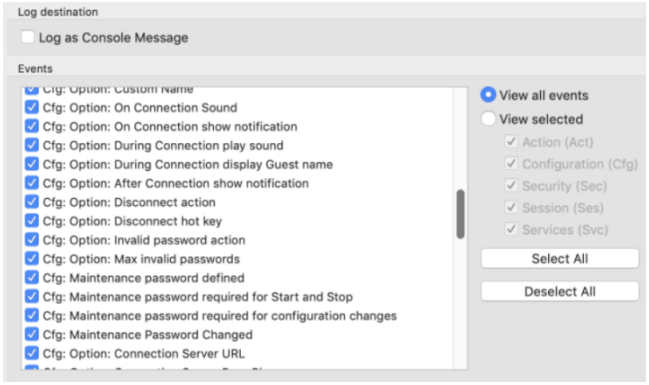
For myCloud profiles, the Connection Account can be defined manually, for example if the Host computer or firewall doesn't allow HTTPS calls. In general, it is recommended to use the Wizard for configuration of myCloud connectivity, as it uses myCloud User account credentials (email + password).

Use the Advanced Settings button, to edit Communication Profiles.

4.2.6 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 console log, either locally or to another computer/server.

4.2.7 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 Mac 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 configuration settings, which are found in the Host.xml file located in the "/etc/WsmHost" folder.

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.

Removal of the WiseMo Host application from a Mac computer is done by running the WiseMo Host Uninstall.pkg file found in folder "/Applications/WiseMo RSM". Uninstalling the Host program does not remove certain temporary files and configuration files, for example the configuration and license files found in the "/etc/Wsmhost" folder.

6. License information for the Host program

The Host program, version 18, can be licensed in various ways.

myCloud license (subscription)
Requires that the Host module is logged on to a myCloud domain, so the computer / device must be able to communicate via the Internet. A Guest user can use myCloud connectivity, as well as direct TCP/IP connectivity to reach the Host.

Use myCloud licensing to reach the Host via the Internet, or if you prefer a subscription based payment model for direct TCP/IP connectivity between internet enabled Guest and Host modules.

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 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 for myCloud connectivity. Doing so will consume a myCloud license.

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 the Deploy tab in your myCloud trial domain. If you already have a Host installed, you can from the Host user interface / the Host Manager 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 un-attended device that runs an operating system supported by the Guest or Host module.

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. A tool used for configuring a WiseMo Host application. It is installed on the computer and communicates with the Host daemon.

Skin – the graphical user interface 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 click 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.