

Remote Support & Management

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

Windows – macOS – Android – iOS – CE

WiseMo Guest module
for example on your Windows PC



Internet



Premises based

WiseMo Host module
on your Mac computer



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 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 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: <https://www.wisemo.com/support/documents/>



WiseMo develops cloud based and premises based remote control software for use between computers and devices, e.g. between PCs, Servers, Mac, Smartphones, Tablets, and other handheld or un-attended devices. Our cross platform solutions target the commercial and industrial remote support and management (RSM) market. For more information, see www.wisemo.com.

1. Installation of the Mac Host

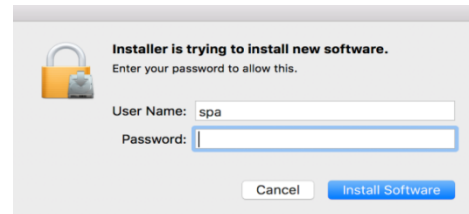
Install the Mac Host app, to prepare the computer for remote control by authenticated users running a WiseMo Guest module.

The Mac Host app runs on macOS from version 10.9 to 15+.

The installation file, a .pkg 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 after installation at first start of the Host app. 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.

macOS will prompt you to accept installation of the program. It may also prompt you to allow the installer to administer your computer, you should allow this for all features to work.



For newer macOS versions the user is upon first run prompted for permissions needed for remote control, please see section 1.4 below for details.

1.1 Installation file from myCloud

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

Notice, you can also pass the myCloud deployment link to a target Mac computer, 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 without further 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 Mac's System Security Management where built-in Administrators and Users on the Mac computer have full access via their Mac user account.

The default configuration is easily changed via the Host user interface itself, or for example by running the Configuration Wizard. 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 Guest users cannot see the mDAC enabled Host and cannot connect to it. The Host can use System 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)



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, by pressing the Wizard button in the toolbar.

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

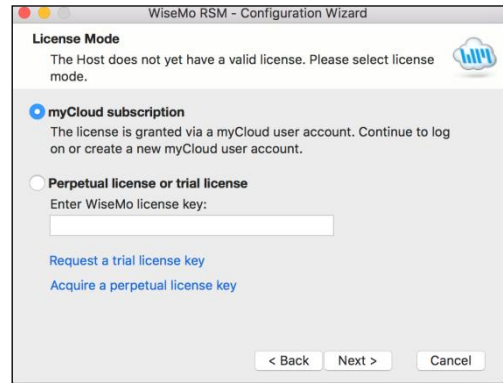
If you have a myCloud domain, you can license the program by logging into this domain. Select myCloud subscription and press "Next".

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 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 "System 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 authenticated 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 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. 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; 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 Required permissions for macOS

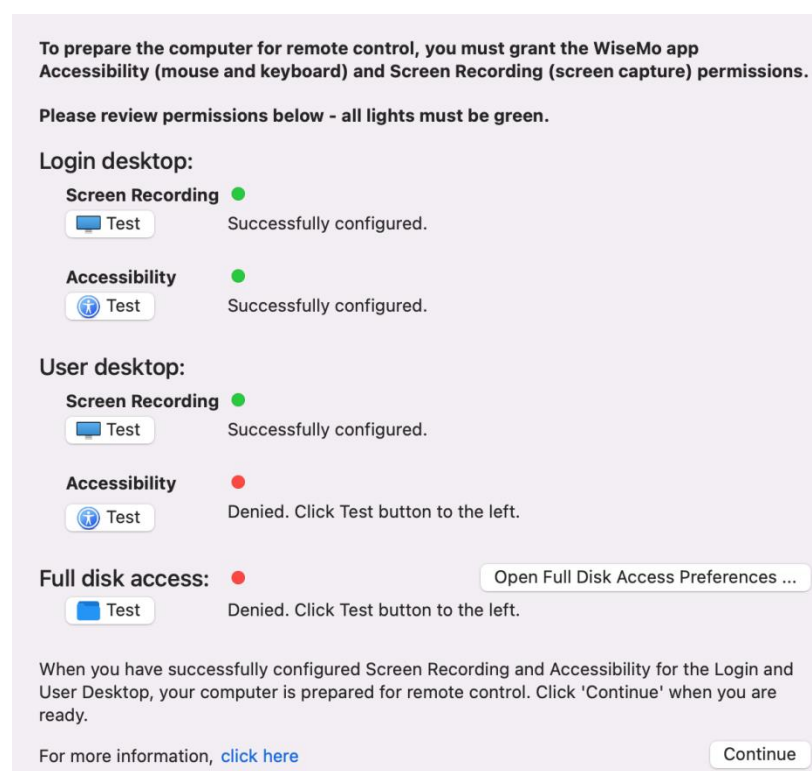
Apple introduced a new security mechanism for macOS 10.14 and later versions.

The security mechanism requires that special access is granted to remote control applications, and therefore also to the WiseMo Mac Host app. 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.

Permissions may be needed for both 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.

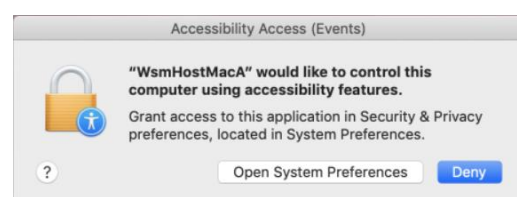
Upon first run the Mac Host module prompts you for the necessary permissions; and you will see a WiseMo guidance dialog.

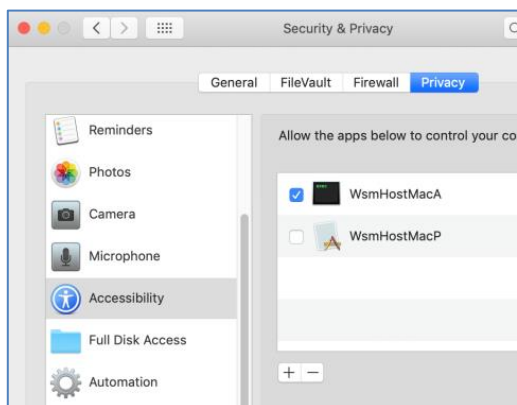


Click any active Test button to obtain a green light for each – for complete configuration.

When you click the Test button for an item with a red light, you will be prompted to "Deny" or "Open System Preferences". You must **select "Open System Preferences"**.

This 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 or switch for each appropriate app.

There are up to 4 WiseMo apps that need permission: WiseMo Host Manager, WsmHostMacA, WsmHostMacP and WsmHostMacD.

Provide permission to all of those app's if shown in:

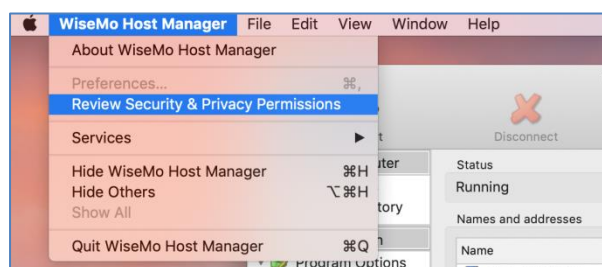
Security & Privacy >:

- Accessibility (input of keyboard and mouse).
- Screen Recording (remote screen viewing).
- Full Disk Access (WiseMo File Manager access)

IF you are not taken to the Security & Privacy items after having clicked each Test button, you can open System Preferences, go to Security & Privacy and select the appropriate item. Then click the lock to be able to make changes and checkmark / switch on the WiseMo files seen.

IF you still do not see a green light after clicking each Test button, [click here](#) for further information.

To later review the Security & Privacy Permissions, open the WiseMo Host Manager and select "Review Security & Privacy Permissions" in the Host menu:



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 (a cloud) and select Show from the popup menu.



Select the "Program Status" option found in the left pane of the Host Manager window. 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.

Initialized communication profiles		
Profile	Device	Details
myCloud	myCloud	Wisemo Demo Internal
TCP/IP (TCP)	TCP/IP (TCP)	1970/1970
TCP/IP (UDP)	TCP/IP (UDP)	1970/1970

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 another Mac computer, from an Android device (Smartphone / Tablet), an iOS device (iPhone / iPad) and from a Windows PC.

If you launch a connection from a browser, you may be prompted to install the appropriate Guest module, and if installed, the connection can be launched. 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 or Android device.

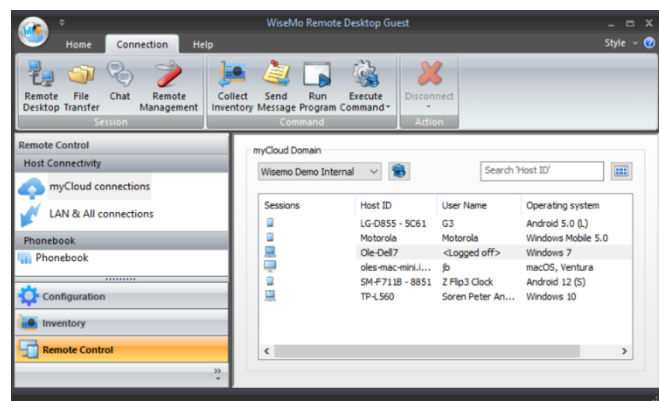
For more detailed info on the use of these Guest types, please find the documentation relevant for each module here: <https://www.wisemo.com/support/documents/>

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: <https://mycloud.wisemo.com/rsm/Domain/Create>

1. Start the Windows Remote Desktop Guest module on your PC. You can get a Guest module [here](#) or from the Manage Devices > Deployment 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.

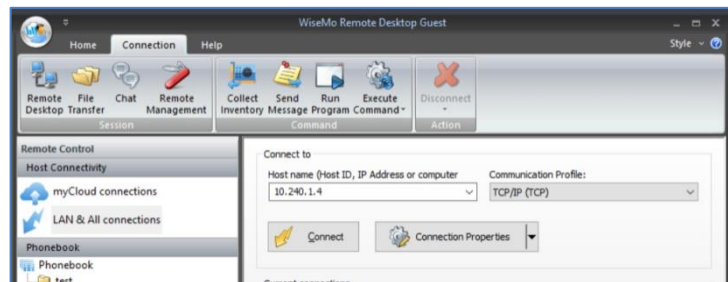
4. The program will connect to the remote computer and open a separate remote desktop control window, showing the desktop of the remote Host computer or device. Select the window and start remote controlling the remote Host computer – as if you were seated in front of it.
5. The remote control session 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 the DNS name for 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 DNS name in the Host name field.
4. Press the Connect button

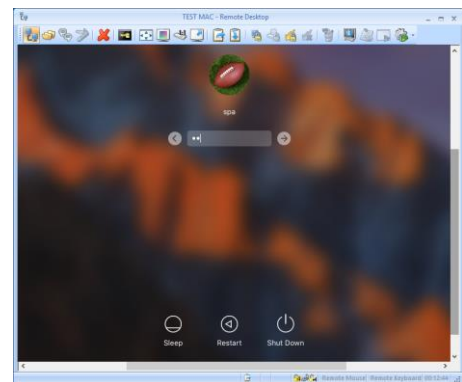


(or click the Remote Desktop button on the Connection tab)

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.

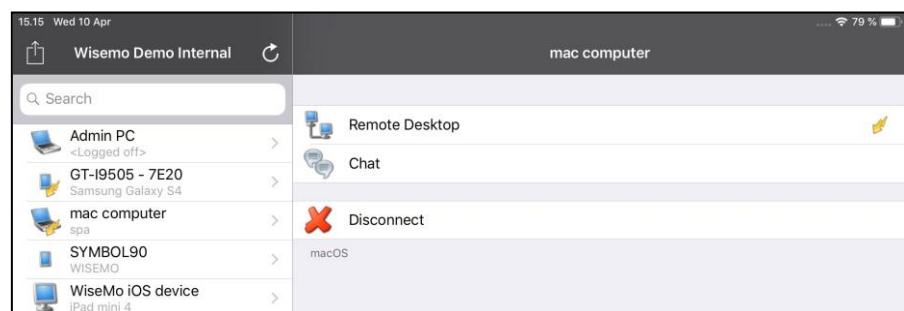


2.3 Remote control from iOS or Android over the Internet

Using a Tablet or Smartphone, you can reach your 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. Install 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 Mac desktop on your device.
4. For info on how to operate from the iOS Guest module or the Android Guest module, please see the guides here:

<https://www.wisemo.com/support/documents/>



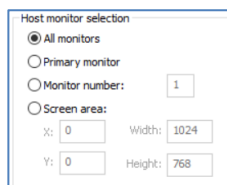
3. Host features

The Wisemo Host module prepares a Mac computer so it can be remote controlled by users running the WiseMo Guest module. The 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. 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.

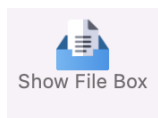
Subject to support by the Guest module used, and permitted by the security settings applied, the Host provides for Remote Desktop Control (view and control), Remote clipboard transfer, Host screen blanking for privacy, back-ground File Transfer, File box, Hardware / Software inventory collection, Chat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



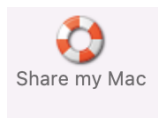
The Mac Host supports many features, here an example of features available to the Windows Guest user when connected to a Mac Host computer.



Remote control of computers with multi monitors is also supported. From the Windows and iOS Guest it is possible, prior to connection, to define via Connection Properties > Display settings, which specific monitor to view. As default, all types of Guests show the primary monitor. Remote control of 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 and Host users.



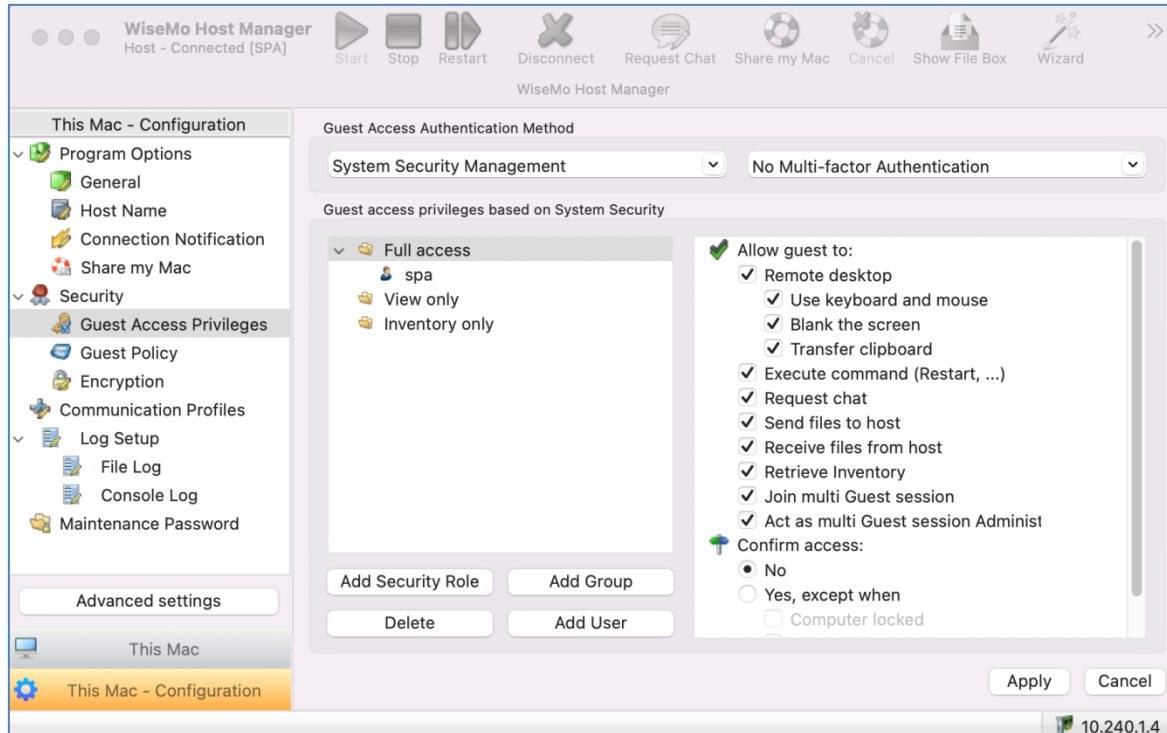
Another feature available to the user at the Host computer is the "Share my Mac" feature. If enabled, this feature can be used to invite someone to temporarily access the computer, maybe to provide quick help, or to demonstrate a point. The "Share my Mac" feature creates a link you can pass on to anyone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

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.

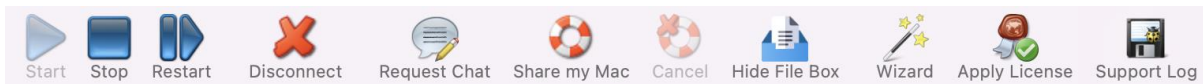


The menu shown in the Navigation bar depends on your choice of menu category. The menu category is chosen at the bottom of the Navigation bar. Normally you have two categories available, "This Mac" and "This Mac - Configuration".

Advanced settings

Configuration of the Mac Host should normally be done via the Wizard and the configuration settings available via "This Mac - Configuration". The button "Advanced settings" can be used for direct editing of the host.xml file that contains the configuration settings. You should normally NOT try to modify settings via the "Advanced settings" button.

4.1 The tool bar



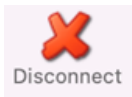
There are tool-tips available explaining each button shown on the toolbar - just position the cursor over the button in question. Right click on the toolbar to customize it.



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.

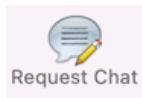
The button Stop will pause the ability of the Host to communicate. Use the Start button to start Host communication if not already running. Start will initialize the host communication, so the Host is ready to receive calls from a Guest user.

Please notice: Default settings in **This Mac - Configuration > Program Options > General** cause auto start of the communication after a computer restart or log off. This to ensure the computer always is ready for remote control. If you do not want this behavior, modify Program Options in the Host.

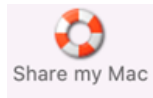


Disconnect the connection with a Guest.

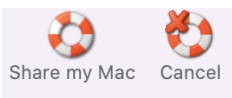
If multiple Guests are connected simultaneously, all will be disconnected.



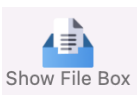
When connected to a Guest user, it is possible from the Host Manager to initiate a chat session with the Guest user.



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 create the actual link. When created, pass the link to 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, disable / enable the feature and configure the number of connections allowed and actions to happen after the link has expired.



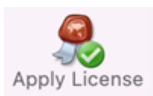
An active Share link can be cancelled by using the button "Cancel" or via the button Share my Mac, which brings up the "Share my Mac" window used when creating the link. This screen also shows the time left of the invitation.



Press 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.



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.



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

The Host About box is found via the WiseMo Host icon shown in the Status bar at the top of the Mac computer.



The About box provides information about the Host 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.

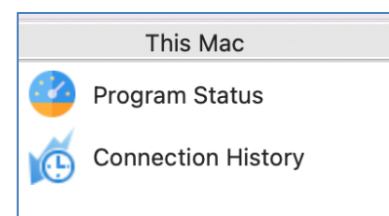
4.2 Host Information

In the navigation bar (left pane, bottom), you can select "This Mac", which will show 2 menu items, Program Status and Connection History.

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 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 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.



Status

Connected




Names and addresses

Name	Type
 spa's MacBook Pro	Host ID
 spa	User Name
 10.240.1.4	IP address

Initialized communication profiles

Profile	Device	Details
 TCP/IP (UDP)	TCP/IP (UDP)	1970/1970
 TCP/IP (TCP)	TCP/IP (TCP)	1970/1970

Active guest connections

Sessions	Login Name	Encryption Mode
  	SPA	Very High

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).

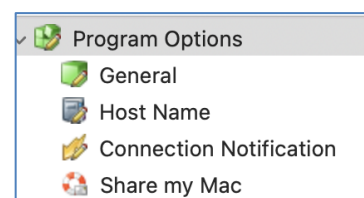
4.3 Host Configuration

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

Select a menu 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 menu items covered below.



General

Startup	
<input checked="" type="checkbox"/>	Listen for incoming connections at Host startup
Stop if no activity for	0 s. (0 = do not stop)
User interface	
<input checked="" type="checkbox"/>	Start user interface as minimized
<input checked="" type="checkbox"/>	Show status bar icon
<input checked="" type="checkbox"/>	Show icon in Dock
<input type="checkbox"/>	Stealth mode (hide user interface)
Connection	
<input checked="" type="checkbox"/>	Send Keep Alive messages
<input checked="" type="checkbox"/>	Allow multiple Guest connections

Startup:

Check this setting to have the Host daemon initialize communication when it is loaded (usually when the computer is switched on¹). 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.

¹ Please note that due to security settings in macOS (the disk needs to be unencrypted), a user might have to log on once before the WiseMo daemon is started and hence remote control is available. Users can subsequently remotely log out and in without problems.

Host Name

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

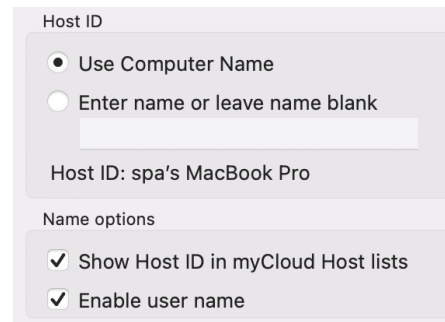
Normally you will use the Mac computer name as Host ID. Alternatively, you can enter your own choice of Host ID.

You can also via the Enter name field tell the Host to read the Host ID from a CSV formatted 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 "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.

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.



Host ID

☒ Use Computer Name

☐ Enter name or leave name blank

Host ID: spa's MacBook Pro

Name options

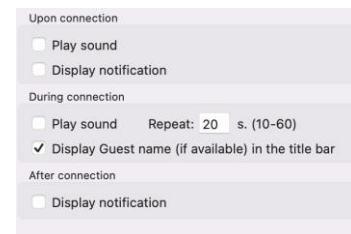
☒ Show Host ID in myCloud Host lists

☒ Enable user name

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.



Upon connection

☐ Play sound

☐ Display notification

During connection

☐ Play sound Repeat: 20 s. (10-60)

☒ Display Guest name (if available) in the title bar

After connection

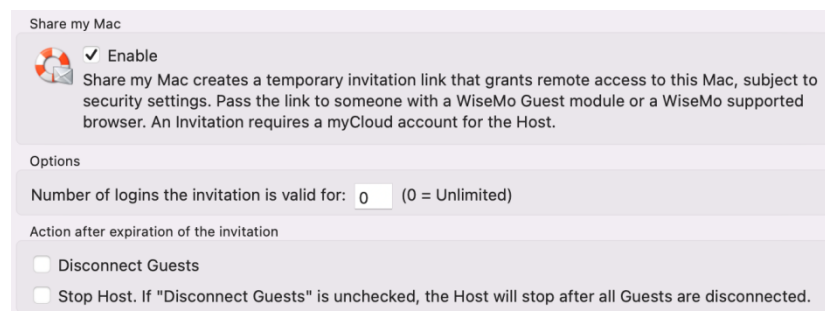
☐ Display notification

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 the invitation" can ensure Guests will disconnect when the link expires.



Share my Mac

☒ Enable

Share my Mac creates a temporary invitation link that grants remote access to this Mac, subject to security settings. Pass the link to someone with a WiseMo Guest module or a WiseMo supported browser. An Invitation requires a myCloud account for the Host.

Options

Number of logins the invitation is valid for: 0 (0 = Unlimited)

Action after expiration of the invitation

☐ Disconnect Guests

☐ Stop Host. If "Disconnect Guests" is unchecked, the Host will stop after all Guests are disconnected.

It is also possible upon expiration of the link to automatically "Stop the Host" (so it does not listen for incoming connections). Then 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).

4.3.2 Security

This section controls the security settings for the Host, and consists of 3 items defined via the menu. There is also one item defined via Advanced configuration.

Each item is described below.



Security

- Guest Access Privileges
- Guest Policy
- Encryption

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 a Security role a Guest user is assigned to.

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 also has allowed access (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.

Allow guest to:

- ☒ Remote desktop
 - ☒ Use keyboard and mouse
 - ☒ Blank the screen
 - ☒ Transfer clipboard
- ☒ Execute command (Restart, ...)
- ☒ Request chat
- ☒ Send files to host
- ☒ Receive files from host
- ☒ Retrieve Inventory
- ☒ Join multi Guest session
- ☒ Act as multi Guest session Administrator

Confirm access:

☒ No

☐ Yes, except when

- ☐ Computer locked
- ☐ No user logged on
- ☐ Guest user logged on

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 permissions.

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

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

Guest Access Authentication Method

User name and password

Shared password

User name and password

System Security Management

myCloud Device Access Control

Guest Access Authentication Method

System Security Management

No Multi-factor Authentication

Individual Guest access privileges based on System Security

Full access

- spa
- admin
- View only
- Inventory only

Allow guest to:

- ☒ Remote desktop
 - ☒ Use keyboard and mouse
 - ☒ Blank the screen
 - ☒ Transfer clipboard
- ☒ Execute command (Restart, ...)
- ☒ Request chat
- ☒ Send files to host
- ☒ Receive files from host
- ☒ Retrieve Inventory
- ☒ Join multi Guest session
- ☒ Act as multi Guest session Administrator

Confirm access:

☒ No

☐ Yes, except when

Add Security Role Add Group

Delete Add User

Guest Access Authentication Method

myCloud Device Access Control

myCloud Device Access Control

myCloud Connections

myCloud Device Access Control will be used.

Direct Connections

Use myCloud Device Access Control via domain:

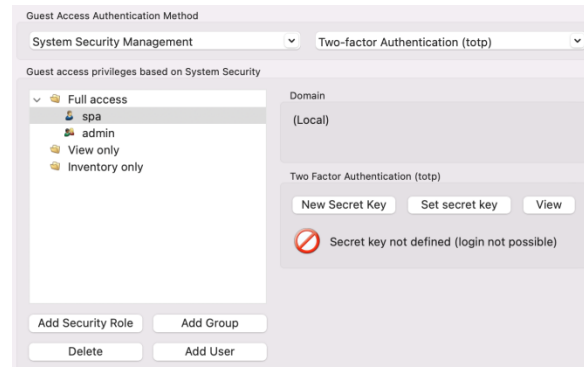
spatest

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

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 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 computer log out. It also controls how many password attempts are allowed and what should happen if the maximum is reached.

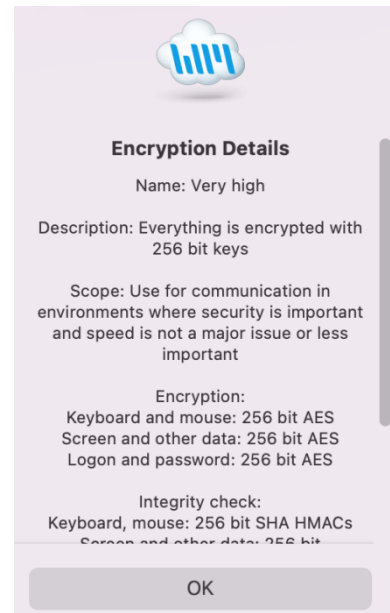
Encryption

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

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. 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 right 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. Current WiseMo Guest modules 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.

Using the Address filtering feature for myCloud connectivity should only be attempted by experienced users, because the applicable myCloud Connection Server(s) IP addresses must also be added to the permitted list. (see [Firewall Configuration Guide](#) for information about WiseMo Connection Servers).

Use the "Advanced Settings" button, to configure Address filtering.

4.3.3 Communication Profiles



The program supports communication via TCP, UDP, HTTP and via myCloud connectivity. From the user interface it is possible to disable / enable defined profiles.

Use the Advanced Settings button, to otherwise edit or create Communication Profiles.

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

For myCloud profiles, the myCloud 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 the myCloud User account credentials (email + password).

4.3.4 Log setup



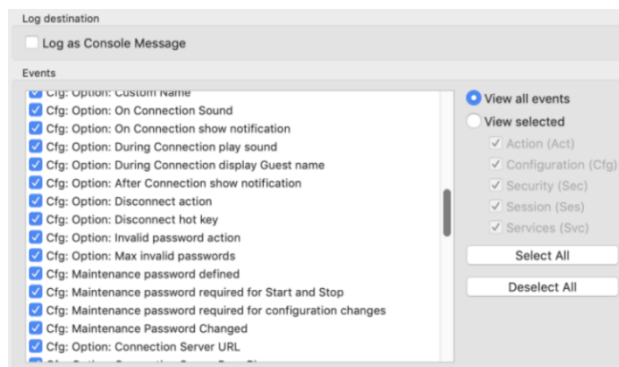
The Host provides for extensive logging of event activity related to the Host. This includes changes to configuration settings, specific

actions, security related events and session events.

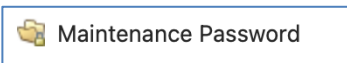
Logging can be made to a file and to the console log, either locally or to another computer/server.

Logging to a file is as default stored to:

..>etc>wsmhost>wsmhostevent.log



4.3.5 Maintenance Password



Use the Maintenance Password feature to protect against non-authorized users making changes to the configuration settings.

It is also possible to protect against the use of the Host's control buttons Start, Stop and Re-start.

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 starting WiseMo Host Uninstall.pkg app found in the folder "/Applications/WiseMo RSM".

Uninstalling the Host app 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 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 to the computer via myCloud Device Access Control. Signing a perpetual licensed Host into a myCloud domain 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 Manage Devices > Deployment page in your myCloud trial domain. If you already have a Host installed with a trial license key, you can from the Host user interface / the Host Manager configure the Host to use myCloud licensing by running the Wizard.

If you prior to installation locate and delete the file host.lic found in the "/etc/WsmHost" folder, 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. 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 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.