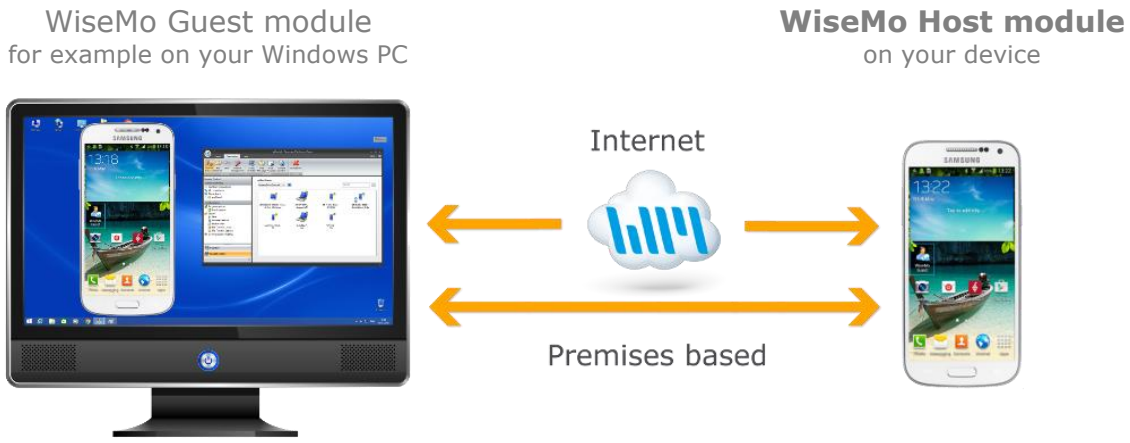
Remote Support & Management

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 devices running Android

This guide provides information on how to install, configure, use and uninstall the Android Host application – our Host module for use on Android devices. The Host module prepares the device 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/

1. Installation and first run of the Android Host application

The program is installed on the target device, so you can remote control it from computers and devices running a WiseMo Guest module. The program supports Android versions from 2.3.3, including v4, v5, v6, v7, v8, v9, v10 and v11.

There are various methods for download and installation of the WiseMo Android Host module, for example via App stores like Google Play, or via download link from WiseMo.

The aim for all installation methods is that program files are installed on the device, plus additionally a license file and a configuration file. If either of the latter two is missing, the program will prompt the user for input.

During first run of the Host app, there are various steps necessary to take to ensure that full remote control capability is installed and permitted. The specific steps may depend on Android version and WiseMo's cooperation with the device manufacturer. The steps generally involve granting the program specific permissions and perhaps also download and installation of a remote control add-on component specific to the device type.

1.1 Download and Install the Android Host

The Host is available for download from various stores, e.g. from Samsung Galaxy Store and from Google Play for Android devices in general. The Host can also be downloaded as and APK via the WiseMo myCloud Deploy page, and from WiseMo's download page.

1.1.1 Install from App Stores

A recommended method is to install the Android Host from an App store. For deployment to many devices, for example using an MDM tool, you may want to consider downloading the APK installation file from WiseMo.

When installation is done from an App store, the Host app comes with a trial license and is ready to communicate via TCP over your LAN / WAN.

You can later upgrade to a perpetual license via in-app purchase from the App store. As an alternative, you can acquire a perpetual license key from WiseMo or one of our partners, who also serve as an extra point of contact for any support questions. You can also switch to use WiseMo myCloud for licensing and connectivity, see about this later.

a. Locate the Host for example in Google Play. For Samsung devices, you can also find the Host in Galaxy Store.

b. Click Install and the Host will be downloaded and installed on the device. Click the Open button to start the Host.

Please continue to section 1.2 for first run information.

1.1.2 Install from WiseMo myCloud

You can download the installation file via the Deploy tab in a WiseMo myCloud domain. Notice that this method requires the device permits installation of non-App store apps. Alternatively the Host can be deployed with an MDM tool.

With the APK installation file from myCloud, the Host installation is pre-configured to join the myCloud domain, and it is myCloud licensed. Installing a license key is not necessary. You can connect to the Host via myCloud over the Internet or via TCP over your LAN / WAN. This installation method is also useful if you like an installation file that includes installation of a customized configuration file that you earlier may have uploaded to your myCloud domain.

a. Log on to your myCloud domain (trial or paid), from the browser on your device, and select the Mobile Host download link in the Deploy tab. You can also send the download link, for example via email or SMS (text), to the target device.

b. Download the APK file to the device.

c. Install the APK file on the device, and run it.

Please continue to section 1.2 for first run information.

1.1.3 Install from WiseMo download page

The installation file is also available from the WiseMo download page. This method is relevant if you do not want to install from an App store and you do not want to use WiseMo myCloud for internet connectivity. Notice that the device must permit installation of non-App store apps, alternatively the Host can be deployed with an MDM tool.

Select the Mobile Host via the download link from the email supplied after a purchase or after requesting a free trial. The email also contains a license key that you will need during installation.

The WiseMo download page contains the APK file for direct installation on the device.

a. Download the APK file to the device.

b. Install the APK file on the device, and run it.

During installation, if a license file (host.lic) is not already available in the target folder; the program will prompt for license info. Enter the license key (trial or purchased) and the program creates the license file, host.lic.

1.2 First run

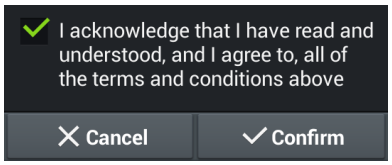
The Host will normally load automatically after installation. Otherwise locate the WiseMo Host app icon on your device and launch it.

On first run, you need to finish the installation and perhaps also provide a few configuration settings, as described below.

Notice: Do not launch the "Share my device" icon also installed, until after first run of the Host. This feature creates an invitation link, more about this in section 1.4.1.

1.2.1 – Finishing the installation

When the Host is run for the first time, you may be asked to accept that the program runs and gains access to capabilities protected by certain security policies. On some devices, you may need to set a checkmark, and press Confirm.

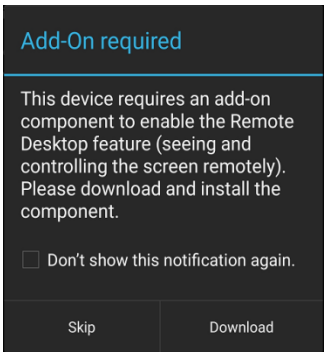


If you do not accept the requests, you may not be able to remotely view the screen and inject keys and touch input[1].

Full Remote Desktop control (i.e. viewing the screen and simulating keyboard and touch events) is provided via different methods depending on Android version and WiseMo's cooperation with the device manufacturer. Each method requires different setup steps and is described below.

Add-on component

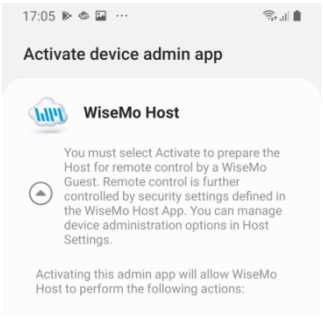
If full Remote Desktop control is provided via an Add-on component, the Host will suggest downloading the Add-on component the first time the Host is launched. Download and install the suggested Add-on.



Please note that different devices use different Add-ons so installing another Add-on than the suggested will cause malfunction of the Host. The Add-on component can also be installed later via the menu and choosing "Program Options". Click "Install Host Remote Control Add-on".

[1] Android 11, 10, 9, 8, 7, 6, 5, 4.x and some 2.3 versions supported. Features available for all devices include File Transfer, Chat, Remote Management and Inventory Collection. Full remote desktop support depends on the specific device, as the Host needs access to certain system resources, usually restricted by the manufacturer of the device. Support is available for Samsung, Sony, LG, Zebra, Lenovo and many others (plus Rooted devices). Also, the remote desktop can be viewed on all types of devices running Android 5 or newer. For more details click here

For larger scale distribution the Add-on can be requested from WiseMo and installed as a separate step before the Host itself is installed. For example if you use an MDM solution to deploy to your base of Android devices.

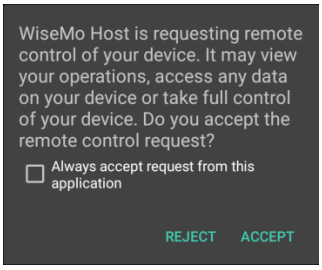


Samsung
When installing the Host on a Samsung device, the Host will request 'device admin' privileges and display the screen to the right. Click 'Activate' to enable Full Remote Desktop control.

Samsung devices with older Android versions also support Full Remote Desktop control via an Add-on component (see above). In this case you can choose either or both methods. If both methods are enabled the Host will use the Add-on method.

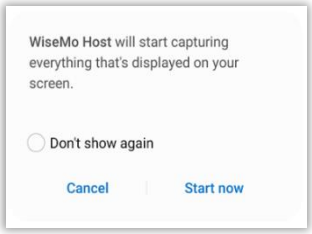
Zebra
A Zebra device running Android 5.0 or newer can be remotely viewed but it requires additional configuration for full remote control, where also keyboard and touch events can be emulated.

The configuration can be done via Zebra Stagenow on the device or via MDM solutions. The necessary configuration is described separately in this document "WiseMo remote control of Zebra scanner devices".



Sony
Full Remote Desktop control is supported on many Sony devices. Check the box "Always accept requests from this application" and click 'Accept' to avoid being prompted every time the Host starts.

Android 5 and newer
All Android devices from Android 5.0 can be remotely viewed.



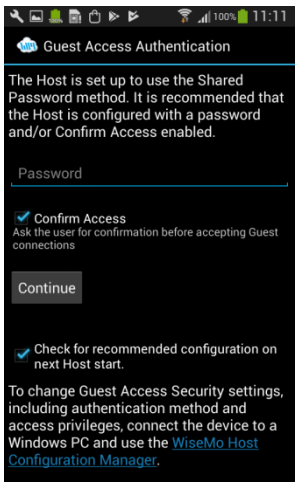
If your device is supported by one of the methods mentioned above, use such if you want remote keyboard and touch control.

If however this is the only supported method, you should check "Don't show again" and click "Start now", and you can view the device. View-only is often a better option than nothing, for example in case of providing user support.

Rooting
It is often possible to root a device, to provide the WiseMo Host the needed privileges, so both remote view and remote keyboard / touch control is possible. However, rooting is a method that should only be attempted if you are very skilled and know what you are doing. Many device manufacturers will not provide support if you have rooted the device. Use an APK downloaded from WiseMo, for a rooted device.

1.2.2 Completing default configuration

During installation / first run, if not already available in the target folder, a Host.xml file is created that holds the default configuration settings.



As default, the Host will load when the device is switched on, and it will initialize itself for communication when it is loaded.

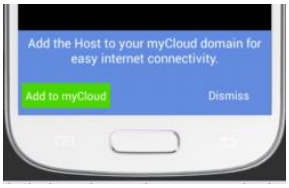
With default configuration, the Host prompts the user, recommending the use of Confirm Access and/or the use of password protection.

Confirm Access is enabled as default; this feature prompts the Host user for permission before allowing a remote user of a WiseMo Guest module access to the device. If the Host device is un-attended, the "Confirm Access" feature should be disabled and password protection should be used instead.

If you define a password, a remote Guest user must enter this password before access is granted.

When a remote Guest user is permitted access, the default security settings allow the use of all features available.

You can avoid the user prompt for security settings, or override an existing host.xml configuration file, by customizing a configuration file to be placed in the target installation folder prior to starting the Host. If you use myCloud, you can upload a customized configuration file to your myCloud domain. This configuration is then used when installing from WiseMo myCloud.



If the Host was not deployed from a myCloud domain, you may want to join the Host to a myCloud domain. Select the Status screen and press the "Add to myCloud" button and enter your myCloud User account credentials.

The prompt may not show on the Status screen, for example if you earlier have dismissed it. It that case, open the Host menu, select Settings/Communication Profiles, select the myCloud communication profile, and then select Domain. Enter credentials for your myCloud User account (typically an email address and a password) and press the "Add host to myCloud domain" button.

The Android Host module supports many configuration options. The user interface itself offer access to a subset of those, please see section 1.4.2 below. For access to the complete set of configuration options available, use the Windows based Mobile Host Manager to customize the configuration file host.xml (please refer to chapter 4 for details on configuration via the Mobile Host Manager).

1.3 Ready for remote control

The WiseMo Host logo is shown in the Action bar on the Android device, when the Host service is initialized. Expand the Action bar and select the Host icon for quick access to the Host app (or select the Host via Apps).

Check that the Status screen shows "Host service is running" and that at least one of the following two lines are shown:

- "Network: UDP, TCP" indicating the Host is configured to be reached directly via TCP/IP. Also check that the IP address shown is valid.

- "myCloud: <domain name> online" indicating the Host is configured to be reached via myCloud connectivity.

If the status does not show running, select the Host menu, and press "Start" or "Restart".

Also check the Info screen, to see whether the Host's license status is OK, indicated by a green shield symbol.

Address / Identify a Host from a Guest module

Notice the IP address and the Host ID on the Status screen. These are important ID's a Guest user may use to address or identify the Host with, depending on communication method. You can change the Host ID, if you prefer (see 4.3.2).

The "Device ID" (GT-I9100 on the screen shot) is used by the Guest module to download the Skin file (a picture of the device) from WiseMo's Skin server, or from the local Guest computer or local server, if you have placed the skin file here, for example if the Guest computer does not have Internet access.

Your Host is now ready for remote control. Refer to Section 2 for information on how to connect to the device. Section 1.4 below explains more about the Host features and its user interface.

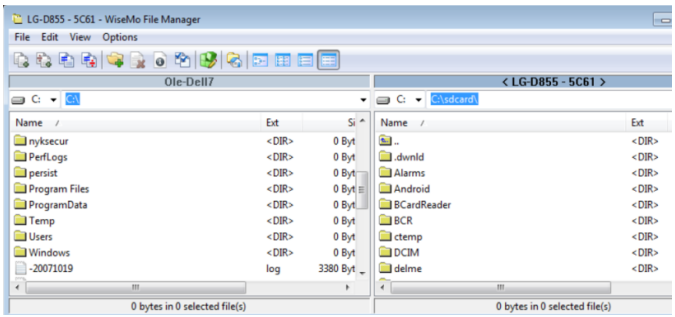
1.4 Host features

The Host prepares an Android device to be remotely reached by WiseMo Guest users, and provides a number of features that greatly enhance the benefits and value. This irrespective of whether your purpose is to remotely work on the device as if you had it in front of you, or it is to provide remote support and assistance to troubled users, or perhaps to remotely perform system management tasks on the device, like ending or starting tasks and processes, or to transfer files and directories between the Android device and your Guest PC.

Many advanced features

The WiseMo Android Host is developed for use in both un-attended situations and in situations where there is a user present at the device. For un-attended situations, you will want to have the app ready to respond, when you have a need to access it remotely. If a user is present, you may want the user to activate the program just prior to remote access, for example for security reasons, or to save battery and other resources. Even for the un-attended situation, WiseMo offer you some unique features to be able to reach the device, without having the program consume battery and other resources (the Automatic wake up feature, for example).

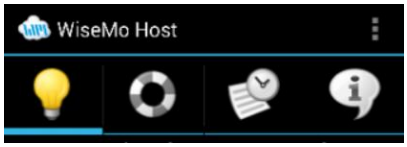
Subject to being supported by the Guest module used, the Host provides for features like Remote Desktop Control (view and control, including control of most device buttons), Remote clipboard transfer, File Transfer, Hardware / Software inventory collection, Chat, Remote execution of apps, Receipt of messages from Guest users, and more. It also allows for multiple Guest users to connect simultaneously to the same device.



Advanced split-screen file transfer

1.4.1 The Host user interface

The Host user interface contains 4 screens (Tabs), and a menu.



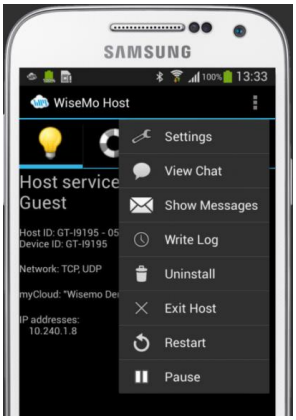
Status screen

The first screen (tab) shows the Host status, stopped, running or that a remote Guest is connected to it.

It shows the Host ID and the detected IP address, which a Guest user may use to identify the target device with, when connecting from Guest to the Host. The more generic Device ID is also shown.

It shows communication related info, and the status when prepared for myCloud communication. If not already configured to use myCloud, it provides a quick method for log on to a myCloud domain.

<u>Menu options</u>



Settings: Provides access to those configuration settings that can be defined from the Host itself. See section 1.4.2 for detailed description.

View Chat: Chat is possible between Guest and Host, initiated by the Guest user. A message pops up on the Host. The user on the Host device can end the Chat session. See chat dialog exchanged between Guest and Host since the Host was started. Use the sub-menu Clear history for clearing the chat history.

Show Messages: Shows messages received from Guests. Use the submenu *Clear messages,* or *Exit the Host* to clear all messages.

Support Log: Creates a troubleshooting log file:

Build 21-294 and later:
/storage/emulated/0/Android/data/com.wisemo.host.v10/files/WsmHost/wsmHostAndroid.log

Earlier builds:
/WsmHost/WsmHostAndroid.Log.

This file is good to include if you need to report a problem to WiseMo.

Uninstall: Available on some Android devices, e.g. Samsung, the menu provides a quick-access option to uninstall the Host, automatically switching off the Activate Device Administrator setting, which otherwise prevents the usual method of removing Android apps.

Exit Host: Closes the Host App. The "Automatic wake-up" feature is still active if enabled in "Program Options".

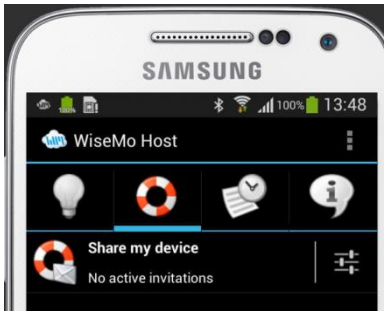
Restart: Re-initializes communication and typically is used after applying new configuration to the Host.

Start/Pause/Disconnect:

Depending on the Host status, you can start/pause communication, or disconnect from a Guest user.

Share my device / Help Request screen

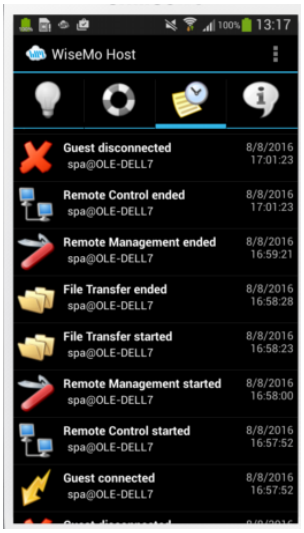
This screen provides the Android device user with the possibility to create an invitation link, to allow a third party easy access to the device via the Internet (myCloud). This is similar to clicking the "Share my device" WiseMo icon found in Apps.



Clicking on Share my device allows for the definition of duration of the invitation link, security settings and the actual creation or de-activation of an active link. By pressing the configuration button to the right of the "Share my device", the Host user can define the number of connections allowed and actions after the link has expired. 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). The Help Request option is provided as backwards compatibility to older PC Guest modules supporting this feature.

History screen

The history screen lists Guests connected / disconnected, with date and time stamp, since the Host was started. Also shows main session types, like Remote Desktop Control, File Transfer, Chat and Remote Management. The additional menu option *Clear History* allows you to clear the history list. For more advanced logging to file, please use the extensive logging features available (1.4.2 Log setup).



Info screen

The Info screen shows the Host version and build, how it is licensed (subscription, perpetual, trial) and copyright information. It also offers easy access to acquire or configure licensing, for example by signing the Host into a myCloud domain, or applying a trial or perpetual license key. If you cannot connect to the device, check this screen – a trial key may have expired.

1.4.2 Configuration

A subset of the Host's configuration settings can be controlled from the Host user interface. For other configuration settings, for example Security Roles and Guest authentication features, it is necessary to use our Host Mobile Manager module (please refer to section 4. Mobile Host Manager found later in this document).

Select "Settings" from the Host menu to see the configuration options available from the user interface:

Program Options

Automatic wake up: Connect to a device even when the Host app is not running. Also saves battery and other resources. This feature is available when using myCloud.

Load at boot: The host app will load when the device is started.

Start at load: The host service initializes communication and enters running state, ready to be controlled from a Guest.

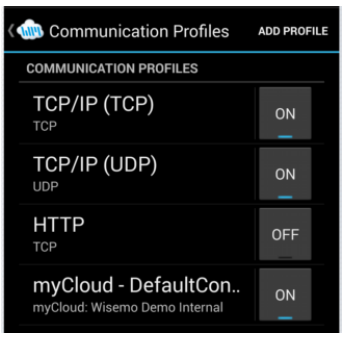
Activate device administration: Samsung specific setting, must be activated if no WiseMo remote control add-on is installed.

Screen density optimization: Available on devices with high screen resolutions to enhance performance. It can be switched on/off during a remote control session.

Host remote control add-on: Informs you if a Remote control add-on module is installed or provides for the installation of a needed add-on. This item is only available if there is an Add-on component available for the device.

Use private configuration: License and configuration file is stored privately, and cannot be accessed by the Host configuration manager or other file managers. On some devices / embedded systems, for example set-tops, the use of private configuration may be required.

Communication Profiles

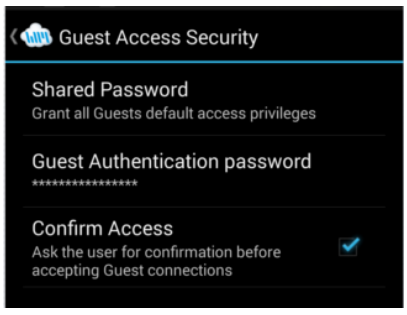


Defines communication settings for various connection methods, and is mostly for skilled users. Click a profile to edit it. To quickly disable / enable a profile, click the On / Off button. You can also add a new profile and remove an existing.

For TCP/IP profiles, you can for example configure port settings.

For myCloud profiles, you may want to log on to a myCloud domain or change to another domain. Click the myCloud profile, then click Domain setting, enter your myCloud user credentials for the domain, and press the button: "Add host to myCloud domain". You can also define if you want to use Google Play services for addressing the Host over the Internet. It is as default on, meaning the Host uses Google Play services if available on the device. If you experience problems establishing a connection to a Host listed in the myCloud list of enabled Hosts, it might be because the Google Play service is unavailable.

Guest Access Security



The Host has advanced authentication and authorization features, governing who may do what. This is organized via security roles; the name of the role used is shown on the first line. As default, the simpler Shared Password role is used, which as default allows for password protection and Confirm Access, and if a user is authenticated, permits the use of all features supported by the Guest module. The use and custom definition of security roles, including protection of the Host by two-factor authentication, is done via the Host Configuration Manager program, see later in this document.

Guest Authentication password: Touch to enter a password or to leave the device without any password protection. If password protected, a Guest user will be prompted to enter the correct password before being allowed access. Use a more advanced security role, if you for example want to require both a user ID and password prior to access.

Confirm Access: This feature will prompt the Host user to provide permission prior to a Guest user getting access. This is a strong security feature when a user is present at the device, but do not use it in situations where you need to access un-attended devices.

Encryption
The Host offers you very high level encryption and protection against spying on and tampering with the data stream. The Host configuration dictates ultimately which level of protection is used. If different levels are permitted by the Host settings (default), the Guest user has the option to decide its preferred encryption level, including No encryption. Especially when working over the Internet, encryption is strongly recommended, as you do not know which computers the data stream may pass through.

Log Setup
Here you can enable logging of events, and define the file to where the log should be written. To customize which events to log, use the Host Configuration Manager program (see Section 4).

2. Examples of Remote Control

Use a WiseMo Guest module to access and remote control an Android device that has the WiseMo Host module installed and running.

You can remote control your device 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 Mac computer, from a Chrome browser on Mac, Linux or Windows, from an IE browser or other Windows browsers using the WiseMo Guest module or supporting NPAPI components. The most feature rich Guest module is our Windows Remote Desktop Guest module, installed on a Windows PC.

In this chapter we show 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.

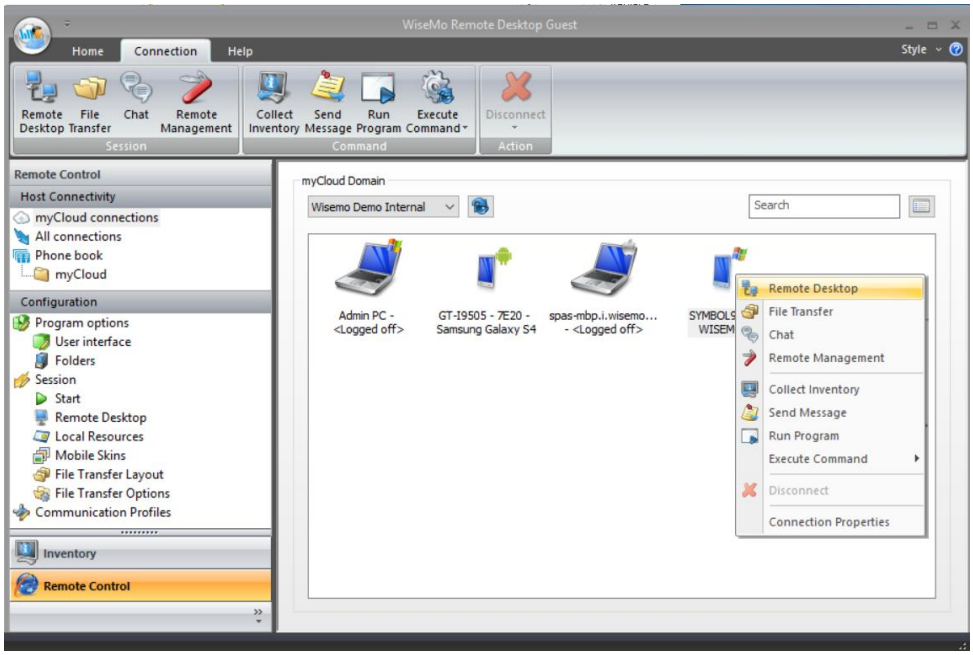
For more info on the use of this or other Guest types, please find the documentation relevant for each module here: https://www.wisemo.com/support/documents/

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 Android 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 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 and a Remote Desktop session will as default start.

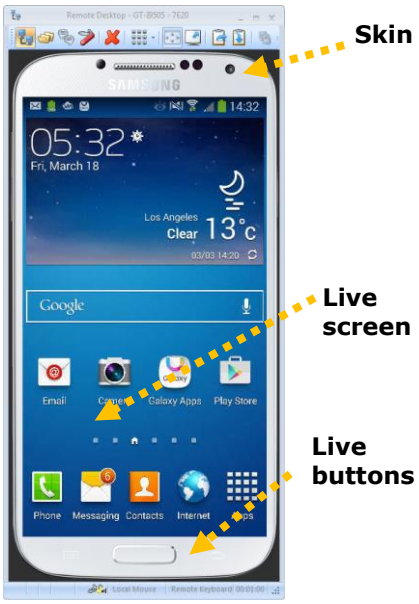
   Alternatively, select a Host; click the button for the function you like, Remote Desktop, File Transfer, Chat, Remote Management, Send message, Collect Inventory, Run program or Execute command. You can also right-click the Host and select from the menu.

4. For a Remote Desktop session, the program will connect to the remote device and open a separate remote desktop control window on your PC.

The first time you connect to a device, it will take a few seconds because the Guest is downloading a picture of the device, called a Skin (you can read more about Skins later in this document).

The window shows the device including live buttons and live screen. It has a menu at the top and info about the connection at the bottom. Select the window and start remote controlling the remote Host device – as if you were seated in front of it.

TIP: It is possible to show the device without the window (use "Show as transparent window"). You define this prior to connection, via the Connection Properties settings. When a transparent window is used, point the mouse on the device skin and right-click to access menu options. See the screen shot in 2.2.

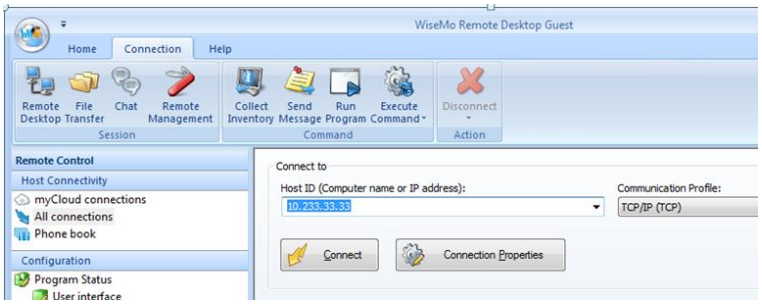


5. The remote control session can be ended by closing the window, or pressing the disconnect button.

2.2 Remote control on a LAN / WAN

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.

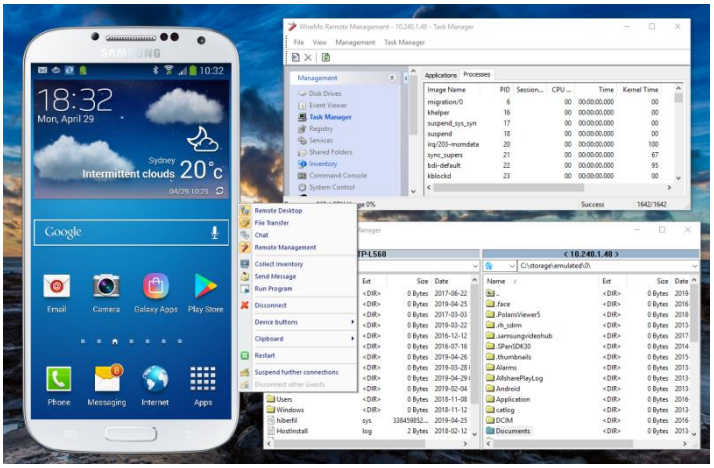
1. Start the Windows Remote Desktop Guest module on your PC.
2. Select "All connections" from the menu, found in the left pane.
3. Enter the IP address in the Host ID field. You can find the Host´s IP address by opening the Host module on the Android device. The IP address is shown in the Host´s Status screen.



4. Press the Connect button

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

5. The first time you connect to the device, it will take some seconds before the remote control screen is shown on your PC. This is because the Guest is downloading a picture of the device, called a Skin (read more about Skins later in this document).



6. You can simultaneously start other functions, for example the File Manager and the Remote Management console.

You can remote control the device, that is, you can inject keystrokes on the remote device, view how the screen of the remote device changes and use the various other features, such as file transfer, hardware / software inventory, chat, remote clipboard etc.

When using transparent skin as in the example above, you can right click on the skin to access the menu options.

3. Skins

By default on a Windows PC / Browser, the desktop of the Android device will be shown inside a picture of the device. This picture of the device is called a Skin.

The device buttons seen on the Skin (with some exceptions) are "live" and can be used to control the device, as if they had been pressed locally on the device.

WiseMo products are made to help eliminate distance by creating a feeling of being there. Using WiseMo's advanced Skin technology greatly improves this feeling of "being there". Besides using the mouse directly on the Skin, the Guest keyboard can also be used to execute keystrokes on the Host device.

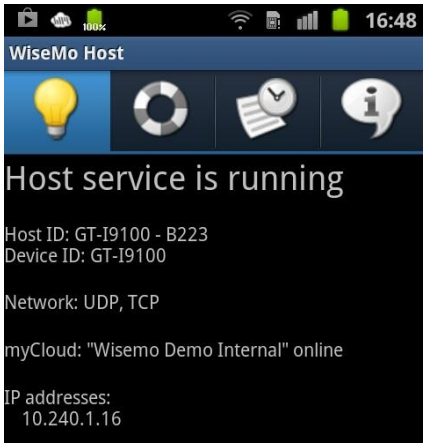
The Skin functionality is controlled from "Connection Properties" for the Host and from the Configuration pane, both found in the Guest module.

Transparent skin

Skin in a window

A skin is as default shown inside a window. The window provides you with menu options and status information at the bottom. Notice you can detach the menu bar; it may contain more options than can be shown.

It is possible to show the device without the window (use transparent window). You define this prior to connection, via the Connection Properties settings. When a transparent window is used, point the mouse on the device skin and right-click to access menu options.



A Skin for a given device is automatically chosen based on the "Device ID".

The "Device ID" for a particular device can be seen in the Host App's Status screen.

WiseMo has created Skins for many devices but some devices don't have a Skin. If a Skin doesn't exist in the Skin repository, a default Skin will be used.

You can also setup the system to not use a Skin, but just display the "desktop" of the device.

If you like support for a specific skin, you are welcome to contact us, please email info@wisemo.com Please include the Device ID, found on the Status screen of the Host.

For customers who would want to create a Skin for their own device, WiseMo provides a Skin Designer. The Skin Designer is free of charge and the only requirement is that the Skin creator donates the Skin to WiseMo for the benefit of all other users. If you are interested in creating your own Skins, please contact us at info@wisemo.com

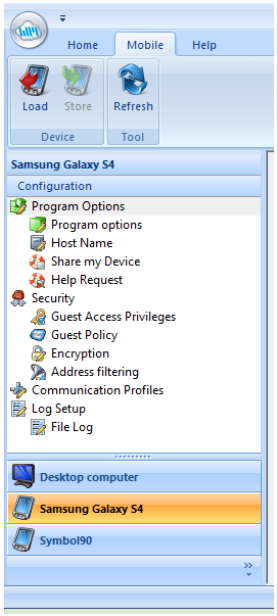
4. Host Configuration

The configuration settings for the Host are stored in the host.xml file, found in the /WsmHost directory. From Host build 21-294 this folder is located here:

/storage/emulated/0/Android/data/com.wisemo.host.v10/files/WsmHost/

Many settings can be changed from the Host app itself, but due to the abundance of different configuration options available, WiseMo has created a Host Manager program, which makes it easy to configure Host settings from a Windows PC.

The Mobile Host Manager, also termed Host Manager, can be installed to your Windows PC by downloading its installation package here. If your Windows PC already has the WiseMo Windows Host module installed, this Host module can also act as Host Manager for the Android Host.



When installed on Windows 8.0-10, the Mobile Host Manager is found in the Start menu > WiseMo RSM > Mobile Host Manager (or WiseMo Host Manager). For older Windows versions, it is found under 'Programs' or 'All Programs' in the folder 'WiseMo RSM'. Click Mobile Host Manager (or WiseMo Host Manager).

4.1 Accessing the Host.xml configuration file

Connect your device(s) to the PC with a USB cable and the Host Manager will automatically detect the device(s). If it does not detect the device(s) make sure that the device(s) allows file access from the PC. To verify this, open Windows File Explorer and locate the device(s) and control that you can access the file system on the device(s).

If the Host Manager still cannot access the configuration on the device, try to press the Refresh button on the Home tab.

Also make sure that the appropriate methods are enabled for detecting the device. You do this from the Host Manager's Home tab.

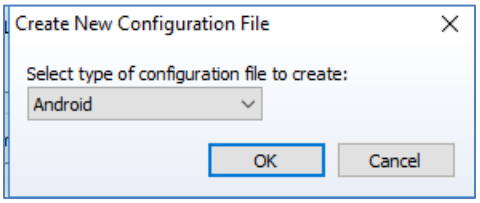
To use the "Android ADB" method, "USB debugging" must be enabled on the device. To do this, open Android settings on the device and search for 'Build number'. Go to the 'Build number' and tap it rapidly 5-6 times. Now search for "Developer options" and enable "USB debugging".

If the device is detected, select it from the list found at the bottom in the left pane. The program will retrieve the Host configuration file that's already on this device. IF NOT, you can from the Host manager use (File → Open) and select the file from its location. You can use the Store button to place a modified configuration file back to the device.

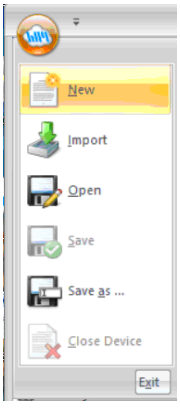
In case a device cannot connect to a Windows PC

If the manufacturer of the device manager software does not provide a standard way to work with the device from your PC, then the Host Mobile Manager cannot detect the connected device and is not able to load and store a configuration file.

Instead you can copy the host.xml configuration file to the PC desktop and then open it with the Mobile Host Manager (File → Open). When all required configuration changes have been made (remember to press the Apply button), the configuration has to be saved on the PC desktop (File → Save). Next the modified configuration file has to be copied back to the device again to the relevant path and the Host program has to be restarted.



You can also create a completely new configuration file. From the Mobile Host Manager's System menu, select "New" and then "Android".
After making configuration changes, for example by using the Wizard, save the file and place it on the device in the folder /WsmHost/ and restart the Host app on the device.



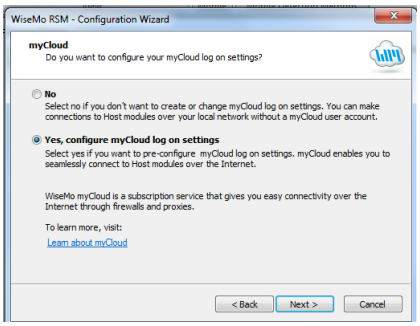
System menu

You can select "Close Device" to remove the file from the Host Manager interface.

4.2 The Configuration Wizard

The Mobile Host Manager offers a Configuration Wizard. Select it from the Home tab. It may also automatically load, when you connect the device to your PC. The wizard helps you to configure various settings, for example start-up settings and authentication as well as authorization options.

Use also the Wizard to configure the Host to connect to a specific myCloud domain, for example if the Host is not pre-configured via deployment from a myCloud domain, or if you later want to re-configure it to connect to another domain.



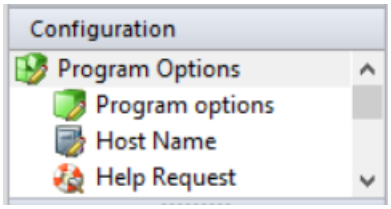
Press next until you reach the myCloud screen, then select "Yes" and press Enter.

Now enter your myCloud user account credentials (email / password, and verification code if the myCloud User account is 2FA protected). Click next until the wizard has finished. Remember to store the new settings to your device (from the Mobile tab or by saving the host.xml file and transferring it to the device). Re-start the Host module on your device in order to use the new configuration.

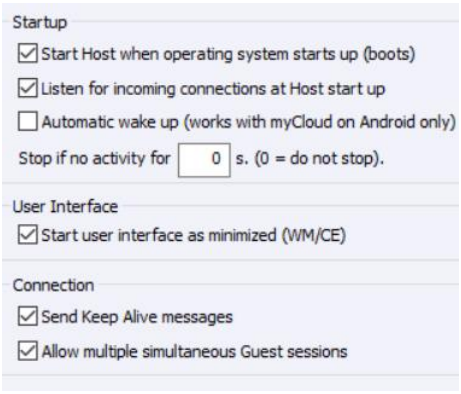
Instead of using the Wizard to configure your preferred settings, you can go directly to the Mobile Host Manager's configuration panel and make the specific changes you need.

4.3 Program Options

This section defines program type options. When changes are made, remember to press the Apply button, and subsequently save the configuration file back to the device, and restart the Host module.



4.3.1 Program options



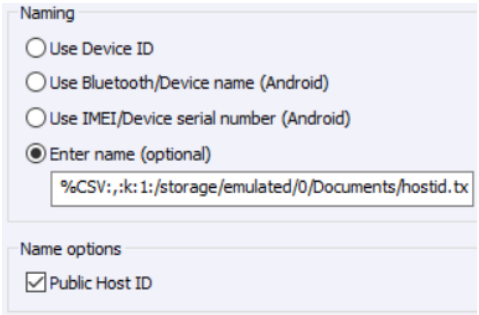
Startup: Define whether the Host starts when the device is booted up, and whether the Host should be ready to receive a connection from a Guest user, when it has started. Both settings should be checked for the un-attended situation. Otherwise you will manually have to press the Start button in the Host. You can define that the Host should automatically stop after a specified time of inactivity (no Guest user connected). The Host will not stop as long as a Guest is connected but will stop immediately after the Guest disconnects if the time has expired.

User Interface: Not applicable for Android Host.

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

4.3.2 Host Name

Settings to help you customize which IDs are available for Guest users, when they need to identify and reach the Host device.



As default, the Host ID is the device ID with a random number added for uniqueness.

You can change the Host ID to any unique ID of your liking (via the Host Configuration Manager).

You can also set the Host ID to use the IMEI (device serial number if no IMEI available). Or you can set it to use the Bluetooth name (device ID if Bluetooth name not available).

You can via the "Enter name" field define your own choice of value as Host ID. Select Enter name and specify the name you want to use.

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 the setting Public Host ID is checked, the Host will be shown in your myCloud list of Hosts. This list is shown to Guest users logged into your myCloud domain. If you un-check this setting, the Guest user must enter the Host ID manually to be able to connect to the Host via myCloud.

Hint for third-party integration: An API exist to obtain the actual Host ID used, see 7b.

4.3.3 Share my Device

Configuration options for the behavior of invitation links created by the Share my Device feature.

Options include how many connections are allowed from a link and defining the Action to take place after expiration of an invitation (for example to ensure Guests disconnects 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 is started, for example after re-boot of the device).

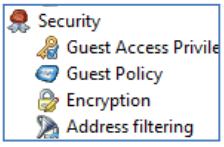
4.3.4 Help Request

The "Help request" feature is available for compatibility with older Windows Guest modules, and should normally not be used.

4.4 Security

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

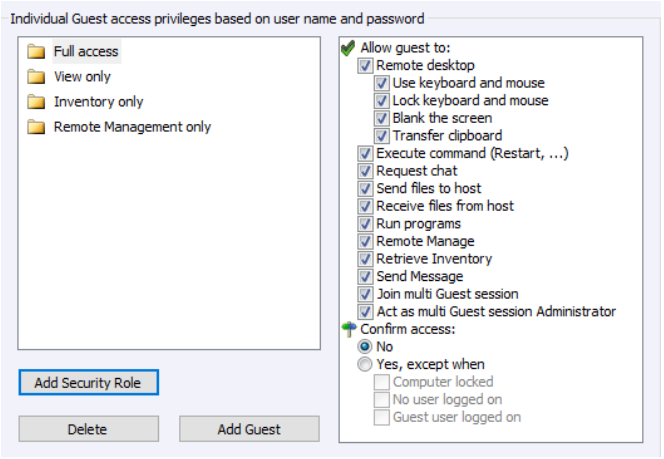
4.4.1 Guest Access Privileges



Defines 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.

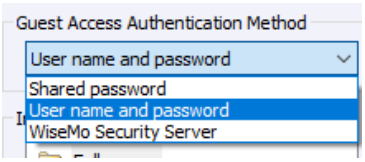


As default, WiseMo has created 4 different Security roles. You can define your own security roles, or modify the roles defined by WiseMo.

You can for example define whether Sending or Receiving files are permitted, or perhaps restrict the Guest user to only view the screen. (not permit use of keyboard / mouse to send touch input). The illustration shows the available permissions.

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

Authentication methods
There are 3 different authentication methods available:

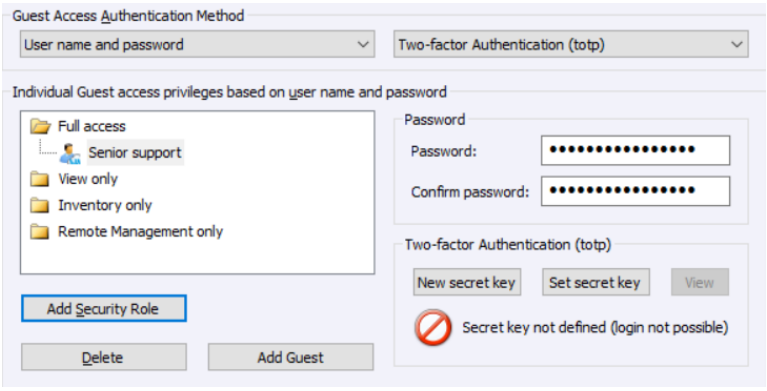


a. Shared password: Access is protected by a single password and the default security role specifies permissions.

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 permissions.

c. 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 other computers that only one or a few persons should be able to access.



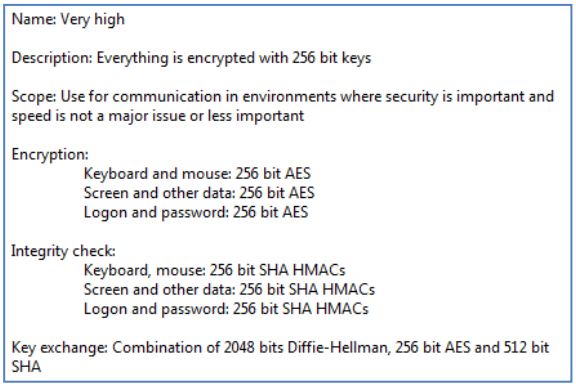
2FA protection is defined at Authentication method level, and all Guest users trying to get access must be able to provide the constantly changing verification code – or access will not be possible. The verification code is typically generated on a Smartphone (the second factor) for example via the Google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

4.4.2 Guest Policy
This section controls how many password attempts are allowed and what should happen if the maximum is reached.

4.4.3 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 dictates which encryption methods 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.

4.4.4 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.

4.5 Communication Profiles

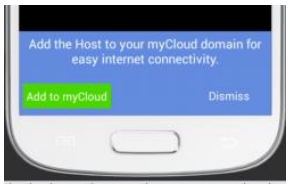
Allows advanced configuration of the communication profiles used by the program. The program supports communication via TCP, UDP and via myCloud connectivity.

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 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 myCloud User account credentials (email + password).

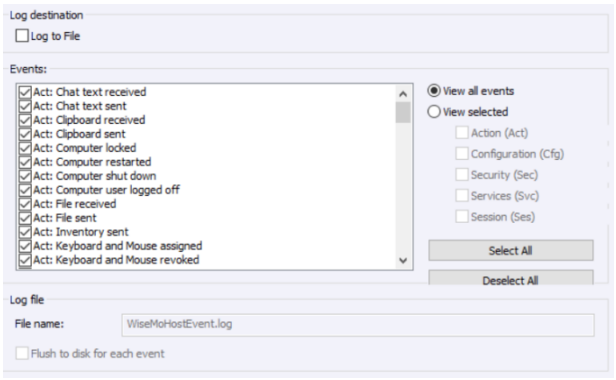
Or use the options available on the device after installation, if the device is not already configured to use myCloud.



4.6 Log setup

The Host provides for extensive logging of activity related to the Host.

This includes changes to configuration settings, specific actions, security related events and session events. Logging is made to a local file.



5. Updating or removing the Android Host module

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

For build 21-294 and later, this will preserve existing configuration settings, which are found in the Host.xml file in the folder \WsmHost.

For older builds, you can install Host build 21-294, which will move the files from the old location:

/storage/WsmHost/

to the new location for build 21-294 or later:

/storage/emulated/0/Android/data/com.wisemo.host.v10/files/WsmHost/

You can delete the host.xml file prior to installation, if you want to start with default configuration settings.

Notice: If you install via a myCloud deployment link, for example sent via SMS, 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 used, replacing any existing configuration file on the device. This allows for deployment of configuration settings via the use of myCloud deployment links.

Removal of the WiseMo Host application from an Android device is done from the device as you would remove any other App. For example, select "Applications", "Settings", "Application Manager", and find the Host App in the list and select it. Then press Uninstall. If a Host Add-on module is installed, follow the same procedure. To remove the Host configurations and other supporting files, delete the folder: \WsmHost.

TIP: *IF the Uninstall button is grayed out, open the Host App, select menu, and Uninstall.*

Removing the Mobile Host Manager

You can remove the Mobile Host Manager on the Windows PC by using "Add or Remove Programs / Program and Features" from the Windows Control Panel or you can use the Remove functionality in the installation MSI package.

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 if you need to reach the Host via the Internet, or if you prefer a subscription based payment model for direct TCP/IP connectivity between a Guest and the Host.

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 the Host was downloaded from an authorized App store, e.g. Google Play, or 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).

If a Host downloaded from an App store is signed into a myCloud domain, it will switch to myCloud licensing.

If you have entered a trial license key, and you want to test or switch to myCloud licensing, locate and delete the file host.lic and re-start the program. You will be prompted for licensing, select Configure myCloud and add the Host to a myCloud domain.

7. For the advanced user

The program contains various options and settings to help ease addressing target devices from Guest modules / 3rd party applications and to help ease larger scale deployment. You are always welcome to contact WiseMo on support@wisemo.com for help with such issues.

7a. Address the device from Guest computers

The IP address and the unique Host ID shown in the Status screen are important ID's a Guest user can use to identify a Host and to address a Host depending on the communication method used.

As default, the Host ID is the device ID with a random number added for uniqueness.
You can change the Host ID to any unique ID of your liking (via the Host Configuration Manager). Here you can also set the Host ID to use the IMEI (device serial number if no IMEI available). You can also set it to use the Bluetooth name (device ID if Bluetooth name not available).

The table below shows which IDs are available to use depending on type of communication profile.

Addressing the Host from a Guest, via Quick Connect, Phonebook, or from a myCloud list

Communication profile	IDs for Host addressing	Default value	Comment
TCP direct	IP address		
UDP direct	IP address		
UDP direct	Host ID	Device ID + number	Define your own Host ID, via Host Conf. Mng.
myCloud direct	Host ID	Device ID + number	Define your own Host ID, via Host Conf. Mng.
myCloud, from list	Host ID	Device ID + number	Define your own Host ID, via Host Conf. Mng.
myCloud, from list	User name	Bluetooth name	If no Bluetooth name, the Device ID will be shown

Note: The Bluetooth name can usually be changed via Settings on your device.

7b. API to query the Host ID / restart the Host

For use by third party Android applications (MDM solutions, for example), an API exists so the third party application can query the Host ID and also issue a command to re-start the Host. The API is implemented as Android AIDL-based service. Please contact WiseMo at support@wisemo.com for more information on this.

7c. Use of "opt." flags

It is possible to define "opt." flags to control certain behavior. The "opt." flags are set by creating an empty file with the flag name and place it in the Host configuration folder /WsmHost. The options flags are case sensitive and should be lower case file names.

opt.no-device-admin	suppress device admin User Input request on Samsung devices.
opt.no-rcbridge-ui	suppress User Input request for installation of Host add-on module.

7d. Deployment

For deployment, where you want to prepare the devices with license and configuration, and have the Host load with as little user interface requests as possible, you can consider this approach.

1. Create the folder:
   /storage/emulated/0/Android/data/com.wisemo.host.v10/files/WsmHost/
2. Place the license file (host.lic) in the folder
3. Place the configuration file (host.xml) in the folder
4. When the Host application is launched, it will detect license and configuration, and thus not request such input from the user.

7e. Microsoft Intune and Google Android Managed configuration

Check here for further info on using the Host with Intune and Android Managed configuration.

8. 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.

Mobile Host Manager – also termed Host Manager. A tool used for configuring a WiseMo Host application. It is installed on a Windows desktop computer and can create and modify the host.xml file that contains the Host configuration. It can also communicate with the host.xml file on your device when the device is USB connected to your PC.

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.