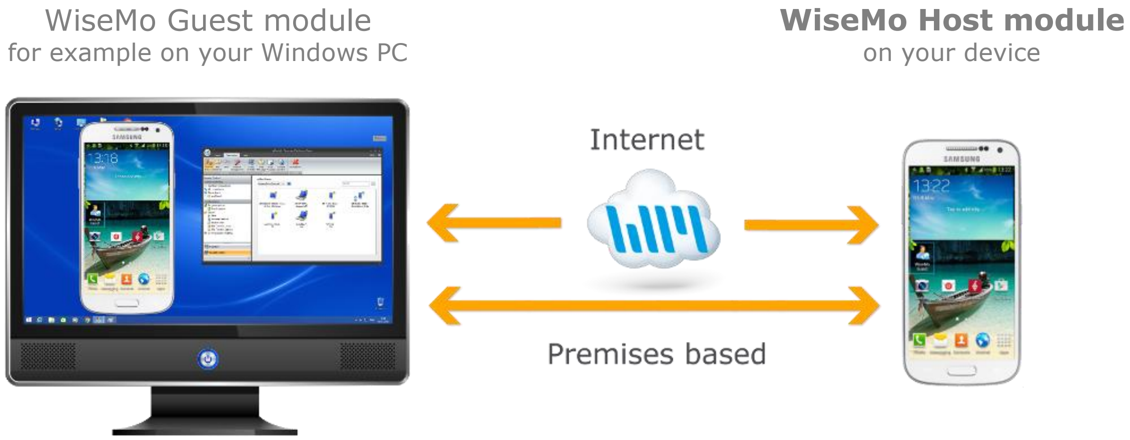
ANDROID HOST GUIDE

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 established either via WiseMo's myCloud solution (using the internet) or directly via your LAN/WAN network (using TCP/IP directly).

For Cloud connectivity (WiseMo myCloud), your computer or device must be able to access 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 access from both the Guest and Host computer / device.

For On-premises connectivity using TCP/IP via your LAN (Wi-Fi, cable) or WAN, you may avoid internet traffic and possible data charges from your mobile operator. You will have to manage any firewall settings to allow communication from the Guest module to reach the Host module.

The Android Host app, 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/

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 and first run

The program is installed on the target device, so you can remote control the device from computers and devices running a WiseMo Guest module.

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

The aim for all installation methods is that program files are installed on the device. Some installation methods also provide a license file and possibly also a configuration file. If already available, the program will during first run not prompt the user for such input.

During installation / first run of the Host app, there are also various steps necessary to take to ensure that full remote control capability is permitted. The specific steps depend on Android version and WiseMo's cooperation with the device manufacturer. The steps involve granting the program rights to access certain Android resources, perhaps via download and installation of a WiseMo add-on component or by accepting various user prompts.

In general, if you accept what the App proposes, such as permission prompts and downloads of extra modules, you are well prepared for remote control. If you do not accept the requests, you may not be able to remotely view the screen and inject keys and touch input.

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

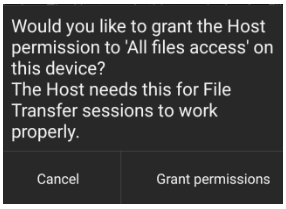
1.1 Install from an App Store

The Host app is available for download from various stores, e.g. from Samsung Galaxy Store and from Google Play. The Host app comes with a built-in trial license, which you later can upgrade to a perpetual license. You can also sign the Host into WiseMo myCloud, for cloud based licensing and connectivity. See more about myCloud later.

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

b. Click Install to download and install on the device. Click the Open button to start the Host.

c. Upon first run, you may be prompted for permissions, for example the permission to access certain files. All requested permissions are not required but they are necessary for full functionality.



Would you like to grant the Host permission to 'All files access' on this device?
The Host needs this for File Transfer sessions to work properly.

d. You will be met by the configuration wizard, where you can define security settings and configure for access to WiseMo myCloud. See section 1.6.

e. Finally, you may be met with requirements to prepare for remote view and control. See section 1.5.

The Host app is now ready to communicate via TCP over your LAN / WAN, and via the internet, if the Host app is signed into a myCloud domain.

1.2 Install via a WiseMo myCloud deployment link

You can download the Host app as an APK installation file from a myCloud domain. This method requires the device to permit installation of non-App store apps. The Host installation is pre-configured to join the myCloud domain, and it is myCloud licensed. 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 a customized configuration file that you may have created earlier and uploaded to your myCloud domain.

a. Log on to your myCloud domain (trial or paid) from a browser on your device. Go to Manage Devices > Deployment and select the **Mobile Host** download link. You can also send the download link, for example via email or SMS (text), to the target device.

b. From the Download page, select **Download Mobile Installer (APK)** which will download the file to the device. Alternatively, you can download the APK installation file to your computer and otherwise place it on the device.

Please notice, if you from the myCloud download page select Google Play or Samsung Galaxy, the Host app installation will not come pre-configured for your myCloud domain, will not be *myCloud licensed and will not include any customized configuration file you may have uploaded. Instead, the behavior is as described in 1.1 above.*

c. Execute the downloaded installation file. This step requires the device to have internet access.

d. Upon first run, you may be prompted for permissions, for example the permission to access certain files. All requested permissions are not required but they are necessary for full functionality.

e. Finally, you may be met with the requirements to prepare for remote view and control. See section 1.5.

1.3 Install from WiseMo shop or Trial download page

An APK installation file is also available from WiseMo's shop and trial download page(s). This method is relevant if you do not want to install from an App store and you do not want to use WiseMo myCloud.

Notice that the device must permit installation of non-App store apps, alternatively the Host can be deployed with an MDM tool.

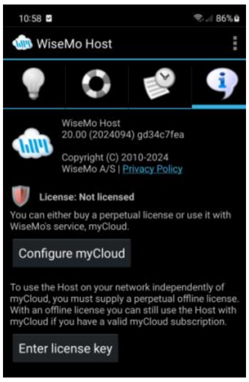
Select the Download button for the Mobile / Android Host, found on the email supplied after a purchase or after requesting a free trial. The button takes you to the download page. The email also contains a license key that you will need during installation.

a. From the download page, select the **APK link** to download the file.

   Please notice; from the Download page you can also select Google Play or Samsung Galaxy. This will take you to the selected store instead and behavior is as described in 1.1 above.

   You can also download the APK file directly from here: www.wisemo.com/d/a

b. Run the APK file on the device to install the Host.



WiseMo Host
20.00 (2024094) gd34c7fea

Copyright (C) 2010-2024
WiseMo A/S | Privacy Policy

License: Not licensed

You can either buy a perpetual license or use it with WiseMo's service, myCloud.

To use the Host on your network independently of myCloud, you must supply a perpetual offline license. With an offline license you can still use the Host with myCloud if you have a valid myCloud subscription.

c. Upon first run, you may be prompted for permissions, for example the permission to access certain files. All requested permissions are not required but they are necessary for full functionality.

d. You will be met by the configuration wizard, where you can define security settings and optionally configure for access to WiseMo myCloud. See section 1.6.

   Please notice, you can avoid the wizard by placing a pre-configured host.xml configuration file in the Host app's configuration folder, prior to installation.[1]

e. If you do not configure for access to myCloud, you will reach the Info screen and the Host is not running, as it is not yet licensed. Press the **Enter license key** and enter a license key, either a trial key or a purchased perpetual key.

   Please notice, you can avoid this step by placing a proper host.lic license file in the Host app's configuration folder prior to installation.[1]

f. Finally, you may be met with requirements to prepare for remote view and control. See section 1.5.

1.4 Install via MDM solution / using Android Managed configuration

For larger scale deployment, an MDM solution can be used. It takes care of deploying configuration file, license file and the app itself, perhaps including installation of an add-on module. The Android Host app also supports installation / configuration via Android Managed Configuration, often supported by MDM solutions. Please refer to separate document for details Click here

1.5 Preparing for remote view and control

The WiseMo Host app uses different techniques for capturing the screen and simulating input depending on the device manufacture and in some cases the Android version:

- Using a manufacturer specific Add-on component that is developed and provided by WiseMo but signed by the device manufacturer

[1] Configuration folder: [SDCard]/Android/data/com.wisemo.host.v10/files/WsmHost/

- Using WiseMo's Universal Add-on that's generic and uses Android's Accessibility Service.
- Using an API provided by manufacturer
- Using Android built-in method for capturing the screen
- A combination of the above
- Rooted devices

The Host app attempts to suggest best approach. Accepting the various permission prompts and download recommendations during setup will typically result in you being able to remotely view and control the device, provided the device is running recent version of Android.

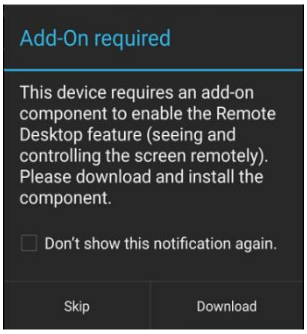
Each method requires different setup steps; below are a few typical examples, while you can find more details here

Add-on component method

The Add-on component comes in two fundamentally different versions, a manufacture specific add-on and a WiseMo generic add-on.

The Host will suggest downloading the Add-on component the first time the Host is launched.

Some Add-ons are available via Google Play. In such cases you will be sent to the Add-on in Google Play to install directly. Other Add-ons are only available from WiseMo. The Host app will send you to a WiseMo page where the suggested Add-on will be listed. Download and install the suggested Add-on.


Add-On required

This device requires an add-on component to enable the Remote Desktop feature (seeing and controlling the screen remotely). Please download and install the component.

□ Don't show this notification again.

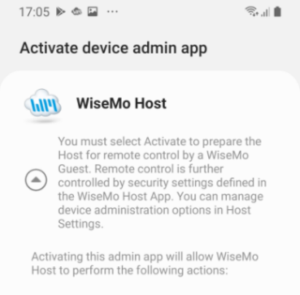
It is important to install only one Add-on and it must be the right one, so please use the one suggested. The Add-on component can also be installed later via the Host app menu > "Settings" > "Program Options" then click "Install Host Remote Control Add-on".

If a manufacture signed Add-on is not available, the generic Universal Add-on is suggested. Viewing and controlling the remote screen is generally supported from Android 8. Screen capture is supported in a combination of Android's built-in screen capture and the WiseMo Universal Add-on. The Universal Add-on uses Android's accessibility service to simulate input. Touch input is fully supported while injection of keyboard input is partly supported (depending on app and text input control) from the Guest app. Otherwise the Android onscreen keyboard can be opened and used remotely.

For larger scale distribution the Add-on component 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 KNOX method

When installing the Host on a Samsung device, the Host will by default use Samsung's Knox to provide remote viewing and remote input control. The Host will request 'device admin' privileges, which must be granted. See example screen to the right. Click 'Activate' to go to the Samsung Knox license screen and accept the terms to enable Full Remote Desktop control.



Activate device admin app

WiseMo Host

You must select Activate to prepare the Host for remote control by a WiseMo Guest. Remote control is further controlled by security settings defined in the WiseMo Host App. You can manage device administration options in Host Settings.

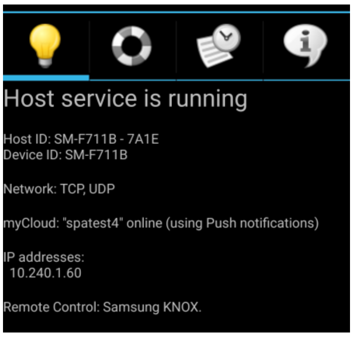
Activating this admin app will allow WiseMo Host to perform the following actions:

Zebra method

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".

Verify method applied

The Host app will show which method it has been configured for. See the Status view. In this example, it is using the Samsung Knox method.


Host service is running

Host ID: SM-F711B - 7A1E
Device ID: SM-F711B

Network: TCP, UDP

myCloud: "spatest4" online (using Push notifications)

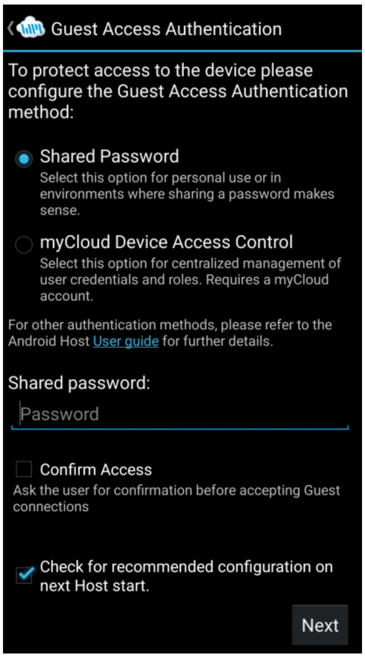
IP addresses:
10.240.1.60

Remote Control: Samsung KNOX.

Please check this status on your device if you are not able to remotely view or control it.

1.6 Configuration wizard

If the Host is not already configured after installation (e.g. via myCloud, Android Managed Configuration, configuration and license file copied to the configuration folder etc.), the configuration wizard is shown.



Guest Access Authentication

To protect access to the device please configure the Guest Access Authentication method:

● Shared Password
Select this option for personal use or in environments where sharing a password makes sense.

○ myCloud Device Access Control
Select this option for centralized management of user credentials and roles. Requires a myCloud account.

For other authentication methods, please refer to the Android Host User guide for further details.

Shared password:
Password

□ Confirm Access
Ask the user for confirmation before accepting Guest connections

☑ Check for recommended configuration on next Host start.

Next

It is possible to select Guest Access Authentication method and related settings and to configure access to a myCloud domain.

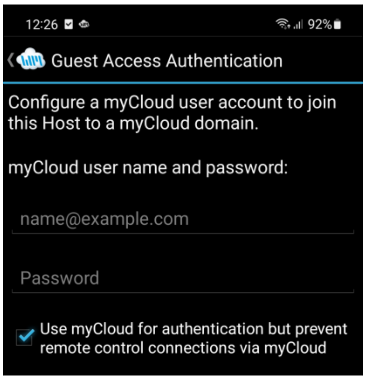
Start by selecting the authentication method which a remote Guest users accessing the device should be authenticated by. Select between the methods “Shared Password” and “myCloud Device Access Control”.

Shared Password method
IF Shared Password is selected; a password can be defined that a remote Guest user must be able to enter, to gain access.

It is also possible to enable Confirm Access, which is a feature that prompts a user on the device for permission prior to a remote user of a WiseMo Guest module gains access to the device. If the Host device is un-attended, the “Confirm Access” feature should be disabled.

When a remote Guest user is permitted access with the Shared Password option, the default access rights allow the use of all available features.

It is possible to restrict access rights and also to define individual User names / password instead of using a single password. See section 5.4.



12:26 92%

Guest Access Authentication

Configure a myCloud user account to join this Host to a myCloud domain.

myCloud user name and password:

name@example.com

Password

☑ Use myCloud for authentication but prevent remote control connections via myCloud

myCloud Device Access Control
myCloud Device Access Control (mDAC) is WiseMo’s solution for central management of authentication and access rights. IF mDAC is selected, the wizard will prompt for credentials to sign the Host into the myCloud domain that should manage authentication and access rights.

Pressing Next on the Wizard shows a screen where credentials should be specified to sign the Host into a myCloud domain. mDAC requires that myCloud access is configured.

The Host can be configured for mDAC authentication of TCP/IP connections only, so remote control is only possible via TCP/IP (LAN/WAN). Authentication is then done via access to myCloud. This method requires the Host to have a perpetual license, (initially perhaps a trial), and the method will also consume a myCloud license.

After finishing the Wizard, and if the Host is licensed, it is configured to load when the device is switched on. It is also configured to initialize itself for communication when it has loaded, so it is ready to service a remote connection from a WiseMo Guest app, subject to the security settings defined.

Please notice, the Host may not show the Configuration wizard on first run. For example, if the Host is deployed via a deployment link from a myCloud domain with mDAC enabled. The Host already has its security settings defined and already knows which myCloud domain to sign into. Likewise, if it otherwise already has a configuration file with these settings defined.

The Wizard can manually be run via the Host app menu > Settings > Guest Access Security.

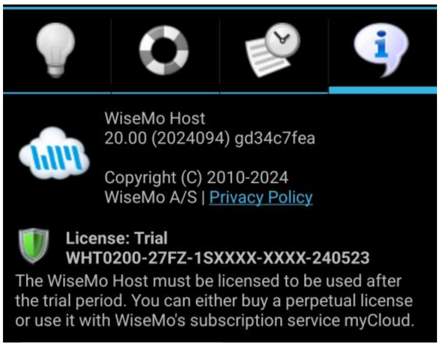
The Android Host module supports many configuration options. The user interface itself offer access to a subset of those, please see section 2.2 below. For access to the complete set of configuration options available, use the Windows based Host Manager to customize the configuration file host.xml (please refer to chapter 5 for details on configuration via the Host Manager).

1.7 Ready for remote control

After installation / first run, the WiseMo Host module should be ready for remote control.

The WiseMo Host logo is shown in the Notification Bar on the Android device, when the Host service is initialized.

Expand the Notification Bar and select the Host icon for quick access to the Host app (or select the Host via Apps).



WiseMo Host
20.00 (2024094) gd34c7fea

Copyright (C) 2010-2024
WiseMo A/S | Privacy Policy

License: Trial
WHT0200-27FZ-1SXXXX-XXXX-240523
The WiseMo Host must be licensed to be used after the trial period. You can either buy a perpetual license or use it with WiseMo's subscription service myCloud.

Check licensing is OK
Select the Info screen, to verify the Host's license status is OK, indicated by a green shield symbol.

IF not licensed, please define license, for example by entering a license key (trial or purchased). You can also license the Host by signing it into a myCloud domain.

Check Host status is OK
Select the Status screen and check that it shows "Host service is running" and that at least one of the following two lines is shown:

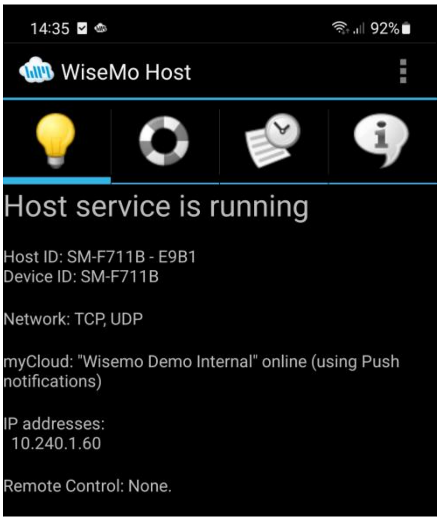
- "Network: UDP, TCP" indicating the Host is configured to be reached directly via TCP/IP on your LAN/WAN. Also check that the IP address shown is valid.

- "myCloud: <domain name> online". It is possible to connect via myCloud / LAN / WAN subject to security settings.

  IF the status is not showing "online" but showing "only myCloud Device Access Control", it is setup to authenticate LAN / WAN connections via this myCloud domain, while connection via myCloud is not possible.

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

Also check that the line "Remote Control:" does not state None, or another indication that remote control is not fully enabled. The line should show the mode the Host is configured for. Please see section 1.5 above.



Host service is running

Host ID: SM-F711B - E9B1
Device ID: SM-F711B

Network: TCP, UDP

myCloud: "Wisemo Demo Internal" online (using Push notifications)

IP addresses:
10.240.1.60

Remote Control: None.

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 2.2.2).

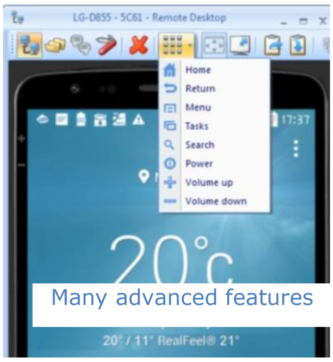
The "Device ID" (SM-F711B on the screen shot) is used by the Guest module to download the Skin file (a picture of the device) from WiseMo's Skin server, or from the local Guest computer or local server, if you have placed the skin file here, for example if the Guest computer does not have Internet access.

IF everything above is fine, your Host is now ready for remote control. Section 2 below explains more about the Host features and its user interface. Please refer to Section 3 for information on how to connect to the device from a browser / WiseMo Guest app.

2. Host features

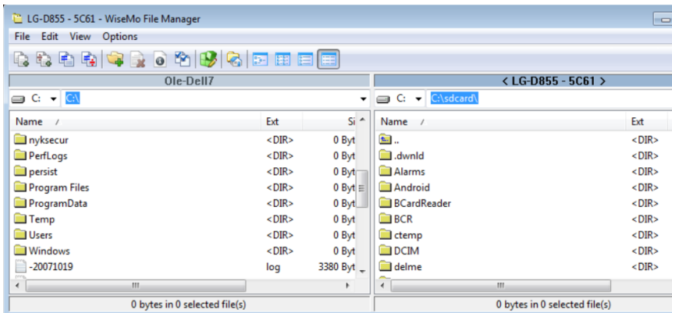
The Host prepares an Android device for remote access from users running the WiseMo Guest app, and it provides a number of features that greatly enhance the benefits and value. This irrespective of whether your purpose is to work remotely on the device as if you had it in front of you or it is to provide remote support and assistance to troubled users, or to transfer files and directories between the Android device and your Guest PC.

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, it is important 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 offers 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).



Many advanced features

Depending on the Guest module used, the Host offers features such as 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.



Name	Ext	Si
nyksecur	<DIR>	0 Byt
PerfLogs	<DIR>	0 Byt
persist	<DIR>	0 Byt
Program Files	<DIR>	0 Byt
ProgramData	<DIR>	0 Byt
Temp	<DIR>	0 Byt
Users	<DIR>	0 Byt
Windows	<DIR>	0 Byt
-20071019	log	3380 Byt

0 bytes in 0 selected file(s)

Name	Ext
..	<DIR>
.dwnld	<DIR>
Alarms	<DIR>
Android	<DIR>
BCardReader	<DIR>
BCR	<DIR>
ctemp	<DIR>
DCIM	<DIR>
delme	<DIR>

0 bytes in 0 selected file(s)

Advanced split-screen file transfer

2.1 The Host user interface

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

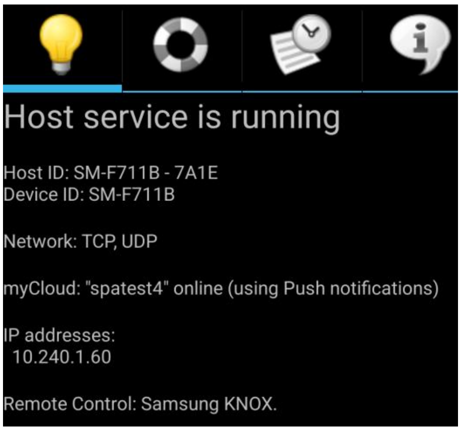
2.1.1 Status screen

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.

Finally, the status screen also shows which method is used, if any, for capturing screen and injecting input (touch, keyboard, and mouse).



Host service is running

Host ID: SM-F711B - 7A1E
Device ID: SM-F711B

Network: TCP, UDP

myCloud: "spatest4" online (using Push notifications)

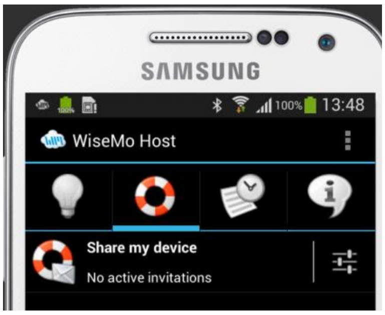
IP addresses:
 10.240.1.60

Remote Control: Samsung KNOX.

2.1.2 Share my device screen

This screen provides the Android device user with the possibility to create an invitation link, to allow another user access to the device via the Internet (myCloud).

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.

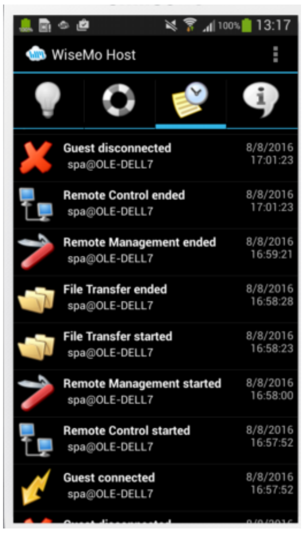


When created, pass the link to a third party, e.g. by emailing it. The third party can execute the link from a supported browser or from an installed WiseMo Guest (for example on Android, iOS, Mac, and Windows).

Notice: It is possible to place a Share my device icon on the desktop, for the user to easily create a link – please see section 2.2.1 on how to configure this option.

2.1.3 History screen

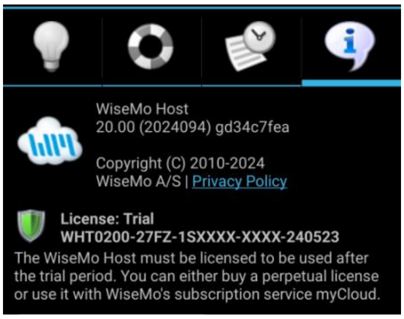
The history screen lists Guests connected / disconnected, with date and time stamp, since the Host app was started. Also shows main session types, Remote Desktop Control, File Transfer, Chat and Remote Management. The additional menu option *Clear History* will empty the history list. For more advanced logging to a file, please use the extensive logging features available (please see 2.2.6 Log setup).



Guest disconnected spa@OLE-DELL7 8/8/2016 17:01:23
Remote Control ended spa@OLE-DELL7 8/8/2016 17:01:23
Remote Management ended spa@OLE-DELL7 8/8/2016 16:59:21
File Transfer ended spa@OLE-DELL7 8/8/2016 16:58:28
File Transfer started spa@OLE-DELL7 8/8/2016 16:58:23
Remote Management started spa@OLE-DELL7 8/8/2016 16:58:00
Remote Control started spa@OLE-DELL7 8/8/2016 16:57:52
Guest connected spa@OLE-DELL7 8/8/2016 16:57:52

2.1.4 Info screen

The Info screen shows the Host version and build, how it is licensed (subscription, perpetual or 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.

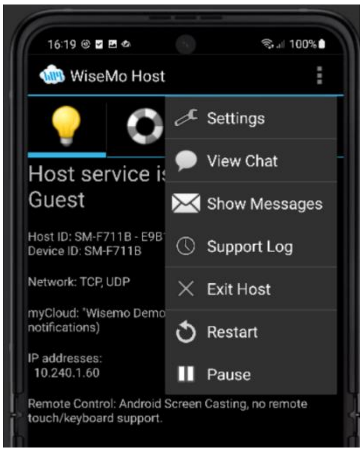


WiseMo Host
20.00 (2024094) gd34c7fea

Copyright (C) 2010-2024
WiseMo A/S | Privacy Policy

License: Trial
WHT0200-27FZ-1SXXXX-XXXX-240523
The WiseMo Host must be licensed to be used after the trial period. You can either buy a perpetual license or use it with WiseMo's subscription service myCloud.

2.1.5 The Menu



Host service i
Guest

Host ID: SM-F711B - E9B
Device ID: SM-F711B

Network: TCP, UDP

myCloud: "Wisemo Demo
notifications)

IP addresses:
10.240.1.60

Remote Control: Android Screen Casting, no remote touch/keyboard support.

Settings: Provides access to those configuration settings that can be defined from the Host itself. See section 2.2 for detailed description.

View Chat: A Guest user can Chat with the Host user. From a notification shown or via the menu option View Chat, the Host user reaches the Chat dialog. The Host user can end the Chat session and Clear the history showing the Chat dialog between Guest(s) and Host since the App was started.

Show Messages: Shows one-way messages from Guest(s) since start of Host app. Use the submenu *Clear messages,* or *Exit the Host* to clear all messages.

Support Log: Creates a troubleshooting log file, good to attach when reporting a problem to WiseMo. The file named wsmHostAndroid.log is placed here: [SDCard]/Android/data/com.wisemo.host.v10/files/WsmHost/

Uninstall: An option only available on older Samsung devices. A quick-access option to uninstall the Host, switching off the Activate Device Administrator setting, which otherwise prevents the usual method of removing Android apps on older devices.

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

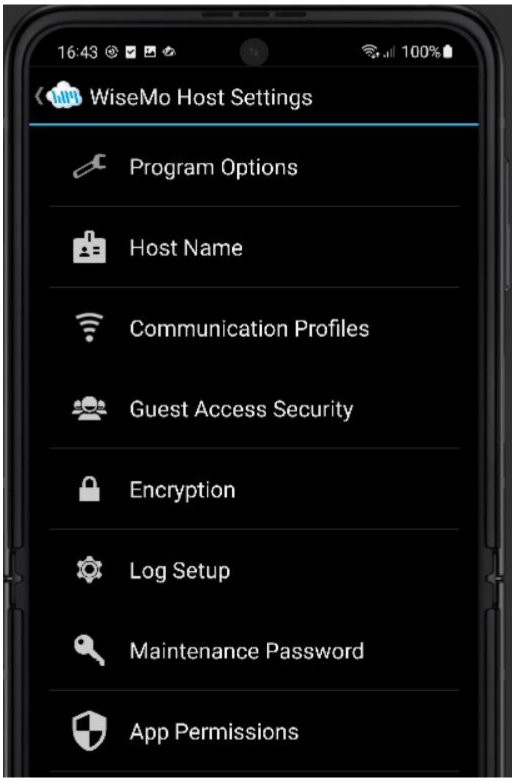
Restart: Re-initialize communication, typically used after applying a new configuration.

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

2.2 Configuration

Many of the Host's configuration settings can be controlled from the Host user interface itself. For additional configuration settings, for example Security Roles (Access rights) and definition of User credentials with individual password, the Host Manager module is used (please refer to section 5. Host Manager found later in this document).

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



2.2.1 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, which can wake-up the Host.

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 an authenticated Guest user.

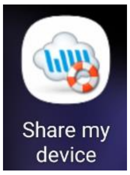
Activate device administration: Samsung specific setting, must be activated if no WiseMo remote control add-on is installed.

Screen density optimization: Available on devices with high screen resolutions to enhance performance. It can be switched on/off during a remote 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 menu item is only available if there is an Add-on component available for the device.

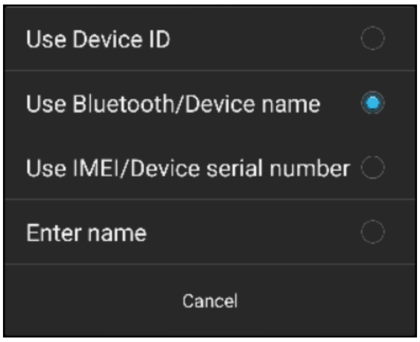
Use private configuration: License and configuration file is stored privately and cannot be accessed by the Host Manager or other file managers. On some devices / embedded systems, for example set-tops, the use of private configuration may be required.

"Share my device" icon: Show or hide an extra icon on the desktop, that creates a temporary invitation link. See also 2.1.2 Share my device screen.



2.2.2 Host Name

Select the source for the Host ID. As default, the Host uses the Device ID with an appended random number. Alternatively, you can use the Bluetooth/Device name or IMEI / device serial number, if they are available for the Android version you are using. You can also enter a name of your own choice. Make sure to use only a unique name, so you can identify the right device when you want to access it.



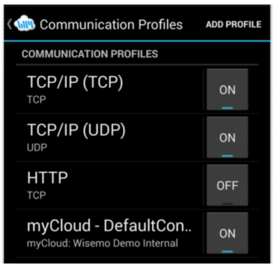
Use Device ID ○

Use Bluetooth/Device name ●

Use IMEI/Device serial number ○

Enter name ○

2.2.3 Communication Profiles



TCP/IP (TCP) – TCP – ON

TCP/IP (UDP) – UDP – ON

HTTP – TCP – OFF

myCloud - DefaultCon.. – myCloud: Wisemo Demo Internal – ON

Defines communication settings for various connection methods, and is mostly for skilled users. Click a profile to edit it. To disable / enable a profile, click the On / Off button. If you want remote access only via myCloud, disable the other methods. 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 whether the myCloud profile should use Push notifications

or polling when connecting over the Internet. It is a recommended default setting to use Push notification that often provides for quicker connection time.

2.2.4 Guest Access Security

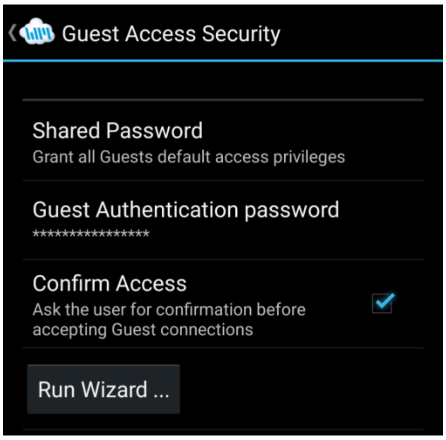
The Host has advanced authentication and authorization features, governing who may do what.

The user interface offers two choices to protect access to the device, Shared Password or myCloud Device Access Control (mDAC). Click on the selected method to change to another.

Shared Password

The Shared Password method protects access to the device with a password and optionally requires confirmed access.

> 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.
>
> Confirm Access: This feature prompts the Host user for permission prior to a Guest user gains access (confirmed access). This is a strong security feature when a user is present at the device, but do not use it in situations for access to un-attended devices.



Guest Access Security

Shared Password
Grant all Guests default access privileges

Guest Authentication password
****

Confirm Access
Ask the user for confirmation before accepting Guest connections ☑

Run Wizard ...

The Shared Password method uses as default an access rights role, which permits the use of all features supported by the Guest module. It is possible to limit the rights by modifying the default access rights role. This is done via the Host Manager, see 5.4.1. Here you can also protect access by using two-factor authentication, where the user prior to gaining access must enter an ever changing passcode in addtion to the password.

If you press Run Wizard, you will presented with the configuration Wizard described in 1.6 above.

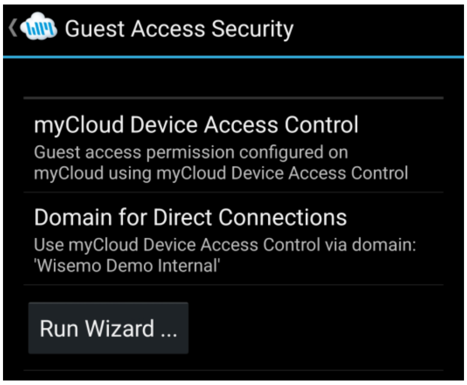
If you want to protect access with User ID / password, and perhaps define different access rights depending on which user, use the Host Manager program to do so (see section 5.4.1).

myCloud Device Access Control (mDAC)

The mDac method is centralized management of who may do what on which devices. Definitions of users (who), access rights (what), and which devices a user may access, are defined and managed centrally in a myCloud domain.

It is possible to configure to use mDAC for authentication of access via LAN / WAN (TCP/IP) only, so preventing access can happen via myCloud (the Internet).

If you press Run Wizard, you get the configuration Wizard described in 1.6 above.



Guest Access Security

myCloud Device Access Control
Guest access permission configured on myCloud using myCloud Device Access Control

Domain for Direct Connections
Use myCloud Device Access Control via domain: 'Wisemo Demo Internal'

Run Wizard ...

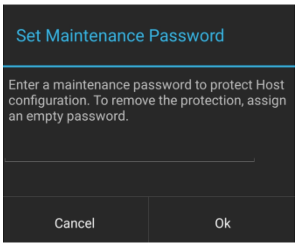
2.2.5 Encryption

The Host provides top-level encryption and safeguards to prevent data interception 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, 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.

2.2.6 Log Setup

You can enable logging of events and define the file the log is written to. To customize which events to log, use the Host Manager program (see Section 5.6).

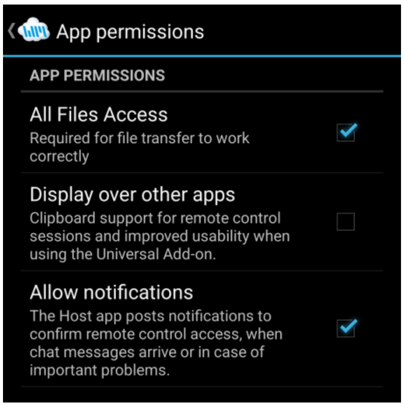
2.2.7 Maintenance password



Set Maintenance Password

Enter a maintenance password to protect Host configuration. To remove the protection, assign an empty password.

To protect against changes to the Host app’s configuration via the user interface, the configuration can be protected by a maintenance password. The user will have to know and enter the maintenance password to reach WiseMo Host Settings.



App permissions

APP PERMISSIONS

All Files Access ☑
Required for file transfer to work correctly

Display over other apps □
Clipboard support for remote control sessions and improved usability when using the Universal Add-on.

Allow notifications ☑
The Host app posts notifications to confirm remote control access, when chat messages arrive or in case of important problems.

2.2.8 App Permissions

This screen shows whether various Android permissions are enabled or not. Permissions may be needed for specific features to work.

Select / deselect a permission and you are taken to the Android location for enabling / disabling this permission.

3. 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, and from a Windows computer. The most feature rich Guest module is our Windows Remote Desktop Guest module, installed on a Windows PC.

You can also launch remote control from any Browser on Android, iOS, Mac or Windows. The browser will use the Guest module installed to establish the remote control session.

In this chapter we show examples of remote control from our Windows Remote Desktop Guest, via myCloud (internet communication) and directly via TCP/IP.

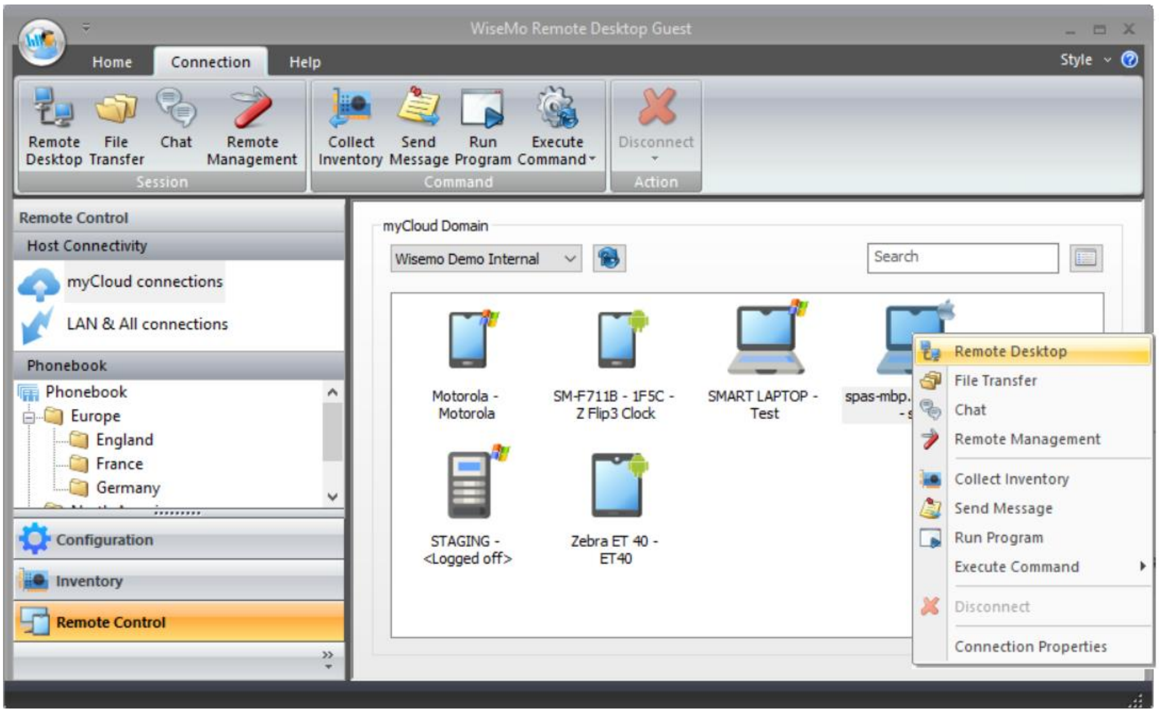
For more info on the use of this or other Guest types, please find the documentation relevant for each module here: https://www.wisemo.com/support/documents/

3.1 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. myCloud provides for central security management, who may do what on which devices. 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 Manage Devices > Deployment page found 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.



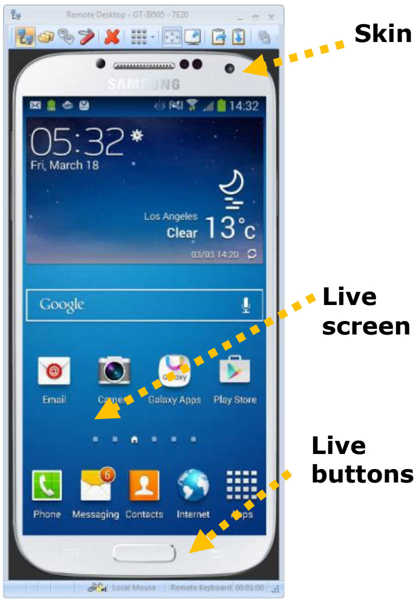
3. Double click on a Host and a Remote Desktop session will start (default). Alternatively, select a Host; in the Connection tab, click the button for the function you like, Remote Desktop, File Transfer, Chat, Remote Management, Send Message, Collect Inventory, Run program or Execute command. You can 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’s desktop.

   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 can 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 3.2.

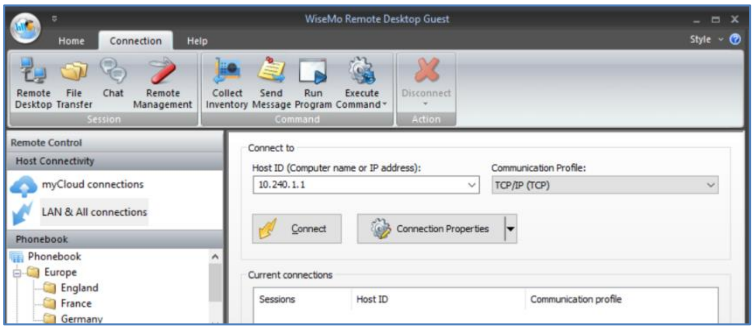


5. The remote control session can be ended by closing the window, or pressing the disconnect button.

3.2 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 “LAN & 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.



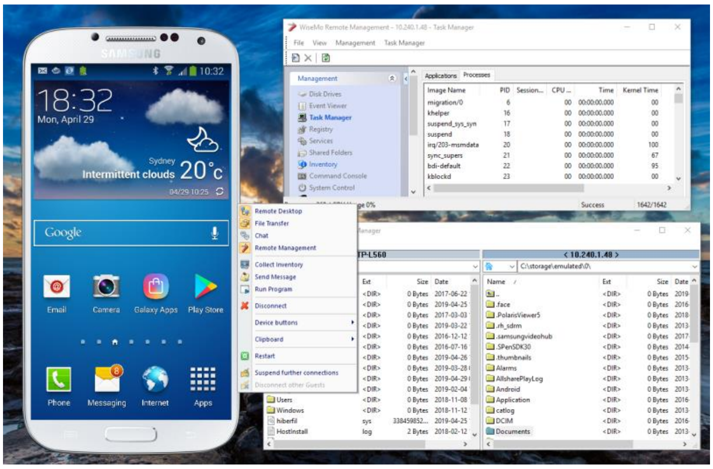
Host ID (Computer name or IP address): 10.240.1.1

Communication Profile: TCP/IP (TCP)

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.

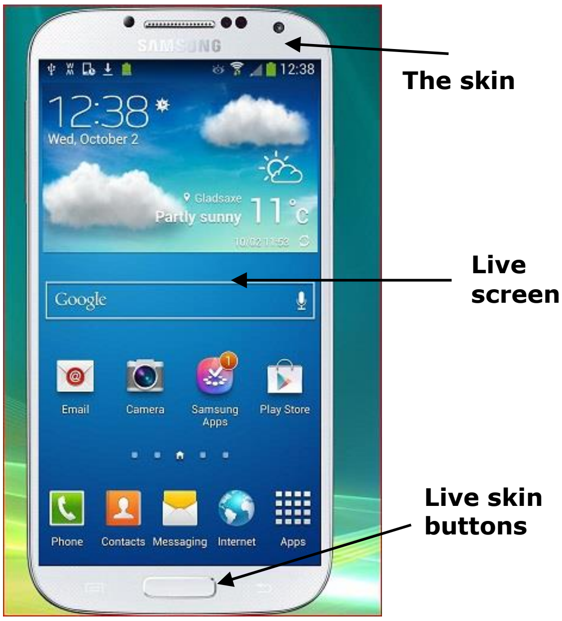
4. Skins

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

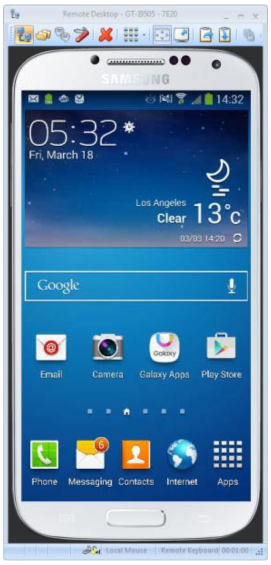
The device buttons seen on the Skin (with some exceptions) are "live" and can be used to control the device, as if they had been pressed locally on the device.

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 managed via "Connection Properties" for the Host and globally via Configuration, both found in the Windows Guest module.



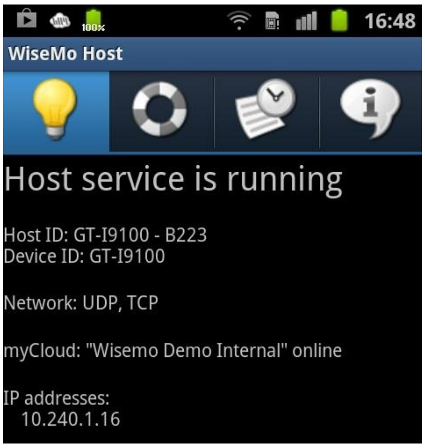
Transparent skin



Skin in a window

The 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 itself and right-click to access menu options.



Host service is running

Host ID: GT-I9100 - B223
Device ID: GT-I9100

Network: UDP, TCP

myCloud: "Wisemo Demo Internal" online

IP addresses:
10.240.1.16

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 specific Skin doesn't exist in the Skin repository, the 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.

5. Host Manager for editing configuration

The configuration settings are stored in a host.xml file, found 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.

Download the Host Manager here and install it on your Windows PC. IF you already have the Windows Host installed, it can also act as Host Manager for configuration of the Android Host. When installed, the Host Manager is found on the Windows Start menu in the WiseMo RSM folder. Open the Host Manager.

5.1 Accessing the Host.xml configuration file

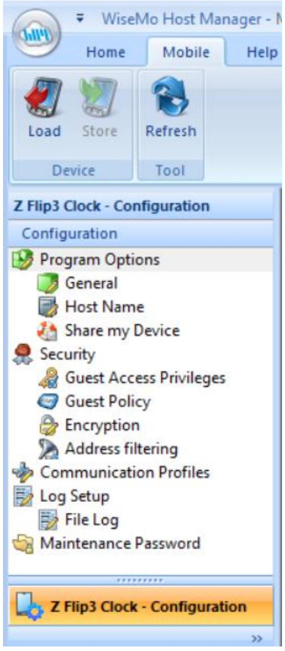
Connect your device to the PC with a USB cable. Make sure that the device allows file access from the PC ("Use USB for: File Transfer"). To verify this, open Windows File Explorer and locate the device and control that you can access the file system on the device.

If the device is detected, select it from the list found at the bottom in the left pane in the Host Manager. The program will retrieve the Host configuration file that's already on this device, if possible. IF NOT, select Open on the Home tab where the host.xml file can be opened from its location.

You can use the Store button to place a modified configuration file back to the device, but for later Android versions this may not be possible. Instead save the file on the Windows PC and use Windows' File Explorer to copy the file to the device.

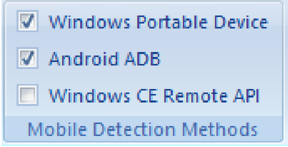
From Android version 12 and newer, it's often not possible for the Host Manager to access the configuration file on the device directly.

Instead, use Windows Explorer to copy the host.xml file from its location on the device to a folder on the Windows computer. Open it as a file with the Host Manager (on the Home ribbon tab, select Open). When you have made your changes to the configuration, save the file again (on the Home ribbon tab, select Save) and copy the host.xml file back to the folder on the device via Windows Explorer. Remember to select Restart via the Host menu on the device to load the new configuration.



In case the Host Manager cannot access the configuration on the device

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



☑ Windows Portable Device

☑ Android ADB

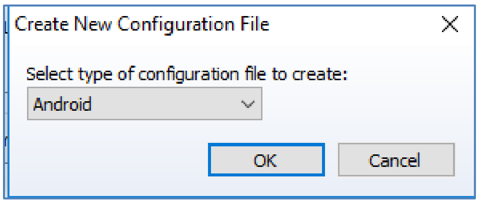
□ Windows CE Remote API

Mobile Detection Methods

Try to press the Refresh button on the 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".

You can also create a completely new configuration file. From the Host Manager's System menu, select "New" and then "Android".



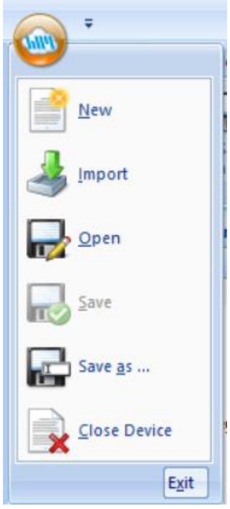
Create New Configuration File

Select type of configuration file to create:

Android

After making configuration changes, for example by using the Wizard, save the file, copy the host.xml file back to the configuration folder on the device via Windows Explorer and select Restart in the Host app menu on the device.

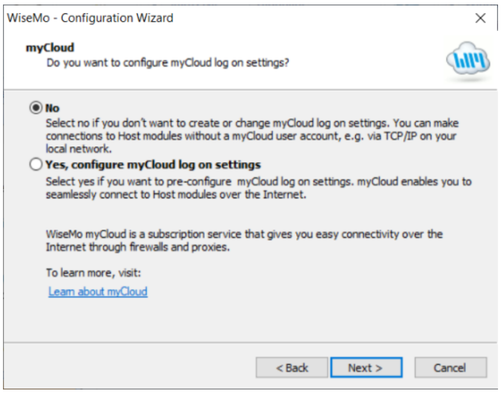
You can select "Close Device" to remove the file from the Host Manager interface.



System menu

5.2 The Configuration Wizard

The 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.



WiseMo - Configuration Wizard

myCloud
Do you want to configure myCloud log on settings?

● **No**
Select no if you don't want to create or change myCloud log on settings. You can make connections to Host modules without a myCloud user account, e.g. via TCP/IP on your local network.

○ **Yes, configure myCloud log on settings**
Select yes if you want to pre-configure myCloud log on settings. myCloud enables you to seamlessly connect to Host modules over the Internet.

WiseMo myCloud is a subscription service that gives you easy connectivity over the Internet through firewalls and proxies.

To learn more, visit:
Learn about myCloud

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.

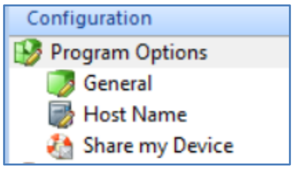
Now enter your myCloud user account credentials (email / password, and verification code if the myCloud User account is 2FA protected). Click next until the wizard has finished. Remember to store the new settings to your device (from the Mobile tab or by saving the host.xml file to the Windows computer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

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

5.3 Program Options

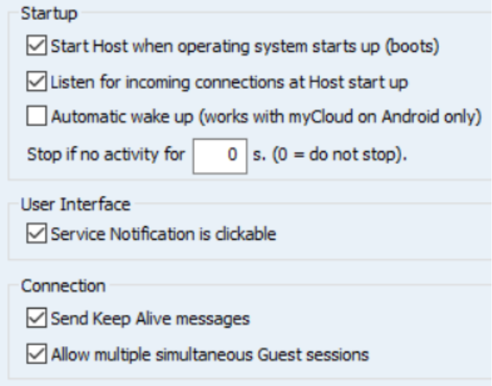
In this section program you can define general program settings.

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.



5.3.1 General

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.



Startup
☑ Start Host when operating system starts up (boots)
☑ Listen for incoming connections at Host start up
☐ Automatic wake up (works with myCloud on Android only)
Stop if no activity for 0 s. (0 = do not stop).

User Interface
☑ Service Notification is clickable

Connection
☑ Send Keep Alive messages
☑ Allow multiple simultaneous Guest sessions

User Interface: When the Host app is running it displays an entry within Android Notifications. The "Service Notification is clickable" feature controls whether a tap on the Host notification should open the Host app or not. This functionality is particularly useful in scenarios such as Kiosk mode, where restricting user access to view or interact with the host application is desired.

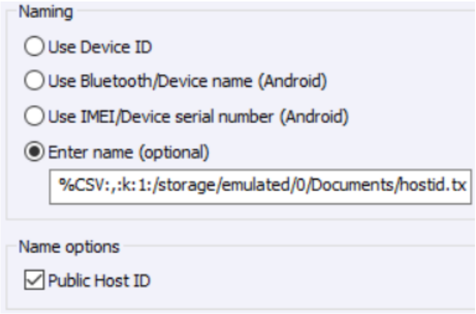
Connection: Control various connection settings. The "Send Keep Alive messages" ensures that the Host will detect if the Guest module suddenly is no longer available. The Host can be accessed by multiple Guests simultaneously, unless the setting "Allow multiple simultaneous Guest sessions" is unchecked.

5.3.2 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 appended for uniqueness.

You can change the Host ID to any unique ID of your liking.



Naming

○ Use Device ID

○ Use Bluetooth/Device name (Android)

○ Use IMEI/Device serial number (Android)

● Enter name (optional)

%CSV:,:k:1:/storage/emulated/0/Documents/hostid.tx

Name options

☑ Public Host ID

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]%

[DELIMITER]: Column delimiter. Can be '\t' for the tab character, '\:' for colon or any other printable character.

[LOOKUP KEY]: Text string to search for in column 0 (first column). Leading spaces are skipped.

[VALUE COLUMN]: Column number the value should be read in. Columns are separated by the delimiter character. Leading and trailing spaces of the Value are skipped.

[FILE NAME]: ANSI or ASCII text file. The file name can specify the full path. If no path is specified, the file must be in the same folder as Host executable.

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.

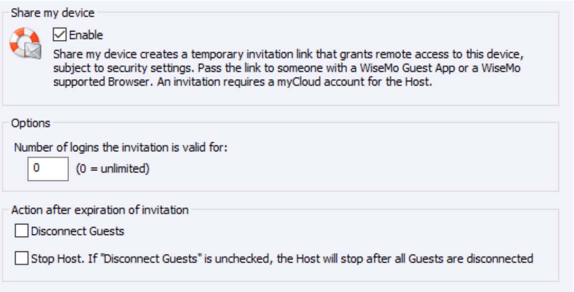
Hint for third-party integration: An API exist to obtain the actual Host ID used, see 8b.

5.3.3 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).



Share my device

☑ Enable

Share my device creates a temporary invitation link that grants remote access to this device, subject to security settings. Pass the link to someone with a WiseMo Guest App 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)

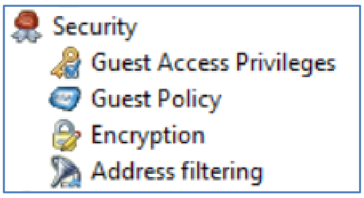
Action after expiration of invitation

☐ Disconnect Guests

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

5.4 Security

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



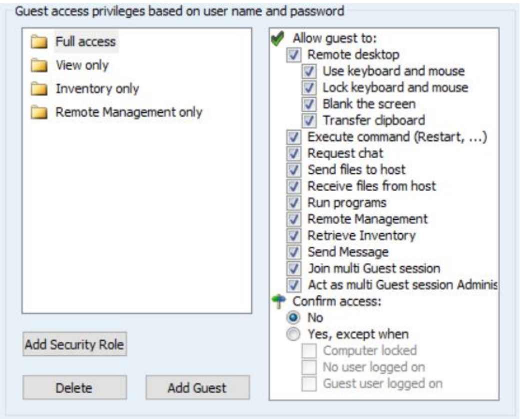
5.4.1 Guest Access Privileges

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.

<u>Access rights</u>

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.


Guest access privileges based on user name and password

- Full access
- View only
- Inventory only
- Remote Management only

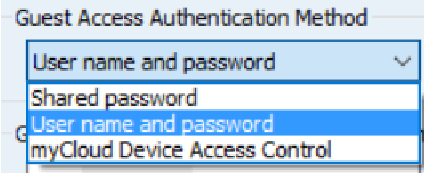
Allow guest to:
- ☑ Remote desktop
  - ☑ Use keyboard and mouse
  - ☑ Lock keyboard and mouse
  - ☑ Blank the screen
  - ☑ Transfer clipboard
- ☑ Execute command (Restart, ...)
- ☑ Request chat
- ☑ Send files to host
- ☑ Receive files from host
- ☑ Run programs
- ☑ Remote Management
- ☑ Retrieve Inventory
- ☑ Send Message
- ☑ Join multi Guest session
- ☑ Act as multi Guest session Adminis

Confirm access:
- ● No
- ○ Yes, except when
  - □ Computer locked
  - □ No user logged on
  - □ Guest user logged on

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 device grants access (use only this feature for situations with attended Host devices).

<u>Authentication methods</u>
There are 3 different authentication methods available:


Guest Access Authentication Method

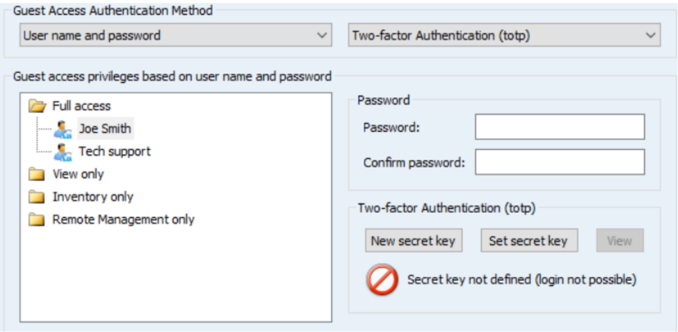
User name and password

a. Shared password: Access is protected by a single password. Select "Default user" in the left view to configure the password and select "Default Security Role" to configure permissions including the Confirm Access feature.

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. myCloud Device Access Control: Who (Guests) may do what (Access rights) on which computers and devices (Hosts) is centrally managed and controlled via myCloud. Using this method makes it easy to manage security for many devices, as users come and go.

<u>Two-factor Authentication (2FA)</u>
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.


Guest Access Authentication Method

User name and password | Two-factor Authentication (totp)

Guest access privileges based on user name and password

- Full access
  - Joe Smith
  - Tech support
- View only
- Inventory only
- Remote Management only

Password

Password:

Confirm password:

Two-factor Authentication (totp)

Secret key not defined (login not possible)

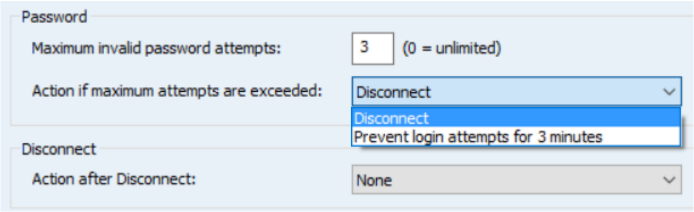
End-point 2FA protection is defined at Authentication method level, for either the Shared password or the User name and password authentication method. If using mDAC, 2FA is defined centrally for the myCloud user account.

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.

5.4.2 Guest Policy

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


Password

Maximum invalid password attempts: 3 (0 = unlimited)

Action if maximum attempts are exceeded: Disconnect

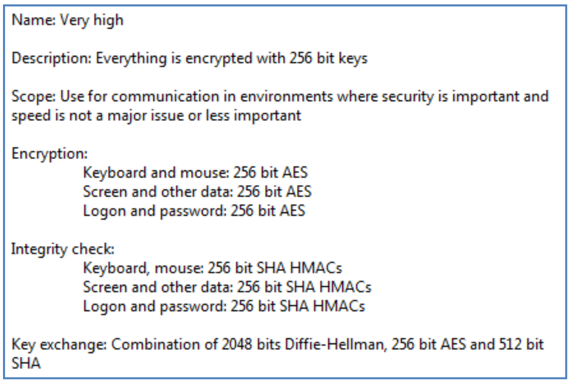
Disconnect

Action after Disconnect: None

5.4.3 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 High and Very High. The classic level is only relevant for compatibility with some special modules.



Name: Very high

Description: Everything is encrypted with 256 bit keys

Scope: Use for communication in environments where security is important and speed is not a major issue or less important

Encryption:
Keyboard and mouse: 256 bit AES
Screen and other data: 256 bit AES
Logon and password: 256 bit AES

Integrity check:
Keyboard, mouse: 256 bit SHA HMACs
Screen and other data: 256 bit SHA HMACs
Logon and password: 256 bit SHA HMACs

Key exchange: Combination of 2048 bits Diffie-Hellman, 256 bit AES and 512 bit SHA

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

If you are connecting via networks not controlled by you, e.g. the Internet, you should always use strong encryption. WiseMo Guest modules (from v.17) will as default attempt to use VERY HIGH.

5.4.4 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 a known range 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.

5.5 Communication Profiles

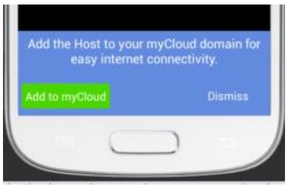
Allows advanced configuration of the communication profiles used by the program. The program supports communication via TCP, UDP, HTTP and via myCloud connectivity.

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

For myCloud profiles, the myCloud Connection Account can be defined manually. Also, if for example the Host device or company firewall doesn’t allow HTTP calls, you can change it to HTTPS.

In general, it is recommended to use the Wizard, for configuration of myCloud connectivity, as it uses myCloud User account credentials (email + password) to sign the Host into a myCloud domain.

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

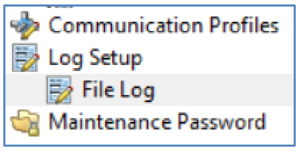


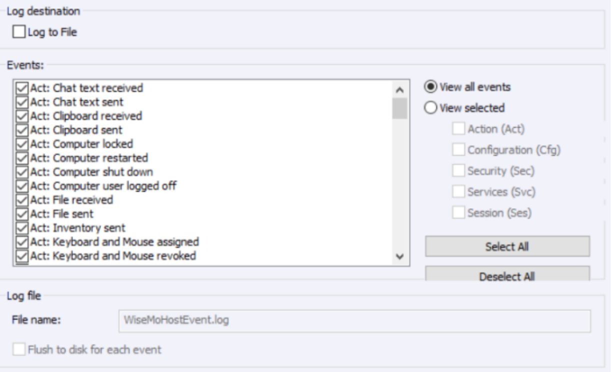
Add the Host to your myCloud domain for easy internet connectivity.

5.6 Log setup

The Host offers comprehensive logging capabilities of activity related to the Host and access to it.

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





Log destination

☐ Log to File

Events:

☑ Act: Chat text received
☑ Act: Chat text sent
☑ Act: Clipboard received
☑ Act: Clipboard sent
☑ Act: Computer locked
☑ Act: Computer restarted
☑ Act: Computer shut down
☑ Act: Computer user logged off
☑ Act: File received
☑ Act: File sent
☑ Act: Inventory sent
☑ Act: Keyboard and Mouse assigned
☑ Act: Keyboard and Mouse revoked

● View all events
○ View selected
☐ Action (Act)
☐ Configuration (Cfg)
☐ Security (Sec)
☐ Services (Svc)
☐ Session (Ses)

Log file

File name: WiseMoHostEvent.log

☐ Flush to disk for each event

5.7 Maintenance Password

To protect against changes to the Host app’s configuration via the user interface, the configuration can be protected by a maintenance password. The user will have to know and enter the maintenance password to reach WiseMo Host Settings.

6. 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.

This will preserve existing configuration settings found here:

/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 "Settings", "Apps", 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. Uninstall of the Host app also deletes configuration and license files.

TIP: *IF the Uninstall button is grayed out, open the Host App, select menu, and Uninstall. This may be true for Samsung devices on older Android versions.*

Removing the Host Manager

You can remove the 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.

7. License information for the Host program

The Host program, version 20, 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. An authenticated Guest user can as default 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 switch to use myCloud licensing, please un-install the Host, then re-install. From the Info screen, select "Configure myCloud", or if already signed in to a myCloud domain, press the "Use myCloud licensing" button.

8. 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, for example via support@wisemo.com for help with such issues.

8a. 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 app user interface or via the Host Manager on a Windows PC). 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, the 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.

8b. 3rd party API

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

8c. Advanced configuration

Please refer to this guide for an in-depth description advanced Host installation and configuration.

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.

8d. 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.

Please also refer to this guide for advanced Host installation.

8e. Microsoft Intune and Google Android Managed configuration

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

9. Glossary

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

Device – Any Smartphone, Tablet, Set-top box, Scanner, or other handheld or un-attended device that runs an operating system supported by the Guest or Host module.

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

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

Host 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.