

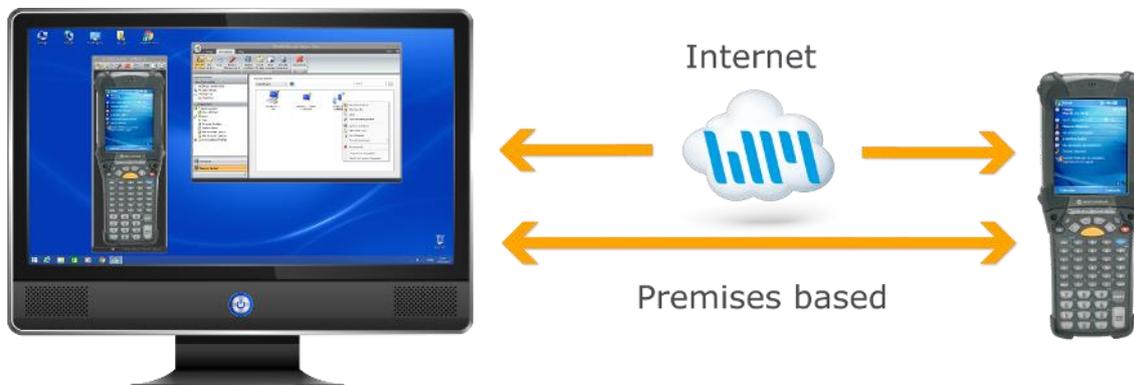
Remote Support & Management

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

Windows – macOS – Android – iOS – CE

WiseMo Guest module
for example on your Windows PC

WiseMo Host module
on your device



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 Windows Mobile / CE

This guide provides information on how to install, configure, use and uninstall the Windows Mobile/CE Host application – our Host module for use on Windows Mobile / Windows Compact Embedded 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: <http://www.wisemo.com/support/documents/>



1. Installation of the Windows Mobile / CE 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 a variety of older and newer operating system versions for Windows Mobile and CE devices, including v5, v6, v7, v8 (2013).

There are various methods for download and installation of the WiseMo Windows Mobile / CE Host module.

The aim for all 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 on first run prompt the user for input. So make sure to install to permanent storage, so those files always are available, also after e.g. a cold boot.

Our download pages contain multiple packages; you must select the correct package for your device for compatibility with CPU and operating system. Each package comes as a single CAB file for direct installation on the device or often also as part of an MSI installation package for installation via your PC. The program files can also be supplied un-packed for OEM installation.

1.1 Download and Install Host CAB files

A CAB file is installed on the device. The CAB file is available for download from WiseMo myCloud or from WiseMo's download page.

Use WiseMo myCloud if you want to remote control over the Internet or otherwise take advantage of the benefits of WiseMo myCloud, such as access to pre-configured deployment links and a subscription based license model.

Use the download page from WiseMo if you only want to remote control via your own controlled LAN / WAN network using WiseMo's perpetual license model.

If a Host package for your type of Windows CE device is not available via the download page, please contact us at: support@wisemo.com We can most likely build a special CAB installation package that works with your specific device.

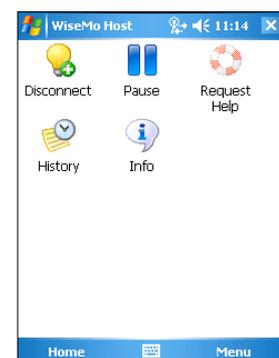
1.1.1 CAB file download from WiseMo myCloud

- Select the Mobile Host link in the Deploy tab of your [myCloud](#) domain (trial or paid). You can log on via the browser on your device¹, or via a Windows PC.
- Download the CAB file for the type of device operating system and CPU.
- Install the CAB file on the device.

During installation, if not already available in the target folder, a Host.lic license file is created and so is a Host.xml file that holds the default configuration settings. With default configuration, the user is prompted to define password protection. The default settings also cause the Host to load automatically and minimize, for example after a re-boot of the device.

The Host will come on-line in your myCloud domain, ready for remote control, via the Internet and directly via your network using TCP/IP.

You can avoid the user prompt or override an existing host.xml configuration file, by customizing a configuration file and uploading it to your myCloud domain prior to download of the CAB file. The Host module supports many configuration options, while the user interface offers access to only a few. To access the complete set of configuration options, use the Windows based Mobile Host Manager to customize the configuration file, host.xml (please refer to chapter 4).



1.1.2 CAB file download from WiseMo download page

- Select the Mobile Host via the download link from the email supplied after a purchase or after requesting a free [trial](#).
- Download the CAB file for the type of device operating system and CPU.
- Install the CAB file on the device.

¹ Older Windows Mobile/CE devices may no longer have compatible Browser support. In such cases, log on to your myCloud domain from your PC. Download the installation file and transfer it to your device. If you have saved the CAB file on a PC, the easiest way to copy it to the device is usually with Windows Explorer.

During installation, if a license file is not already available in the target folder; the program will prompt for license info. Enter a license key. Alternatively, select myCloud subscription licensing and enter User Account credentials for a myCloud domain (https support required for this, or you will experience errors. If https is not available, please see section 1.5, Apply license, for workaround). After successful licensing, the file host.lic is created.

If a configuration file, host.xml, is not found in the target folder, the program will prompt the user to define password protection. Then a Host.xml file that holds the default configuration settings is created. With default configuration settings, the Host will load automatically and minimize, for example after re-boot of the device.

The Host is now ready for remote control via your network using TCP/IP and also via myCloud, if myCloud licensing was applied.

The Host module supports many configuration options, while the user interface offers access to only a few. To access the complete set of configuration options, use the Windows based Mobile Host Manager to customize the configuration file, host.xml (please refer to chapter 4).

1.2 Download and install MSI installation files

Downloading the MSI installation package to your PC and starting the installation will place the CAB file on your PC, install the Windows based Mobile Host Manager on the PC and install other files for use by Active Sync/Mobile Device Center for further installation of the CAB file onto the device.

MSI installation files are available both via myCloud and via the WiseMo download page. The CAB file being placed on the PC is the same as described in 1.1 above. For example, if downloaded from a myCloud link, the MSI installation file will contain the CAB file with license for myCloud and configuration to access the myCloud domain and customized configuration if applied.

After installation to the PC, you must transfer the CAB file to the device and run it. This can be done like you would normally transfer files to the device. The easiest way is usually to manually copy it to the device with Windows Explorer, if the device is connected via USB to the PC.

If your computer has Active Sync/Mobile Device Center installed, you can connect the device to the PC with a USB cable prior to running the MSI file. The MSI installation package will install both the Mobile Host Manager and the mobile device installation files on the PC. The installer will copy the CAB file to the device and launch the installation. Check your device display to see if you need to carry out additional steps to complete the installation. Notice, you may have to disconnect your device from your PC, to enable WiFi connectivity.

Otherwise, installation behaves as described in above section 1.1.1 and 1.1.2 respectively.

1.3 OEM installation

If you want to prepare and place all necessary files on an image for distribution, or perhaps build your own installation file, instead of using our MSI / CAB installation files, you are welcome to do so. Make sure to also place a valid license file (host.lic) and a configuration file (host.xml) in the target folder to avoid the program prompts for user input. One method to get those two files is to copy from a device where you have installed and configured the Host program to your liking.

Please contact info@wisemo.com to request delivery of a set of un-packed files for your specific CPU / operating system version or if you have any questions regarding OEM installation.

1.4 Ready for remote control

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

To verify this, you open the Host program, e.g. from menu > programs.

Check that the "Light bulb" icon on the Home screen shows "Running".

Select the Info button and verify that the Host is on-line in your myCloud domain, if it has been setup for myCloud communication.

The Info screen also shows if the Host can be reached via UDP, TCP or both. Verify that a valid IP address is shown.



You may also want to check the About box to verify the program is properly licensed, click Menu > About. Perhaps a trial key has expired.

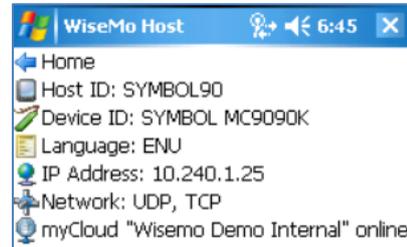
Address / Identify a Host from a Guest module

Notice the IP address and the Host ID (Symbol90 on below screen shot). Both are shown on the Info screen. These are important ID's a Guest user may use to address or identify a Host. The Host ID must be kept unique.

As default, the Host ID is taken from the "device / computer name" as defined on the device.

To get another Host ID, you can modify the device name on the device, e.g. via: settings/systems/about/Device ID

You can also set the Host ID value to your preference via configuration of the WiseMo Host, use the Mobile Host Manager (see 4.3 for various options).



In the myCloud list of Hosts, the "User name" field will show the "Owner" information, if defined on the device, else it shows the "device / computer name" if available. Otherwise it will show the "System model".

The Device ID in the Host info screen shows the "System model" (SYMBOL MC9090K) which is also used by the Guest module to identify and download the Skin file (a picture of the device) from the 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.

1.5 Host features

The Host module prepares a Windows Mobile/CE device to be remotely reached by users with a WiseMo Guest module, and provides a number of features and functions 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 Windows Mobile/CE device and your PC.

The WiseMo 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.

Subject to being supported by the Guest module used, the Host provides for Remote Desktop Control (remote view and control, including control of most device buttons), Remote clipboard transfer, File Transfer, Hardware / Software inventory collection, Chat dialog, 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.

Typically, the Host program is not used much by the device user, but prepares the device for remote control by a remote Guest user, for example support staff, who, when permitted, remotely can view the screen of the device and enter keystrokes / mouse input, plus perform other support and management actions supported by the Guest / Host module.

Some features that the device user may benefit from knowing are listed below.

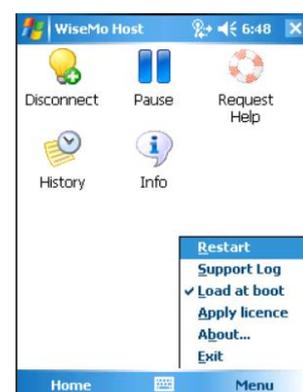
Home screen

The home screen shows the Host status, for example that it is running, or paused and whether a remote Guest user is connected to the device or not. It offers a menu and a number of buttons.

Menu

"Restart" reloads license and configuration and re-initializes communication if in running state. Restart is typically used after applying new configuration to the Host, perhaps done remotely.

"Support Log" creates a troubleshooting log file: \WsmHostWMCE.log
A file which is good to include if you need to report a problem to



WiseMo. The Support Log file can also be saved via a "SendMessage" command from a third party application.

"Load at boot" define if the Host automatically should load when the device is booted up.

"Apply license" permits you to select license method. See below for details.

"About" provides info on program version and licensing. If you cannot connect to the device, check this screen – a trial key may have expired.

"Exit" ends the program.

Apply license

Define perpetual licensing by entering a license key or myCloud subscription licensing via log on to a myCloud domain, using a myCloud user account. The Host also supports log on with a myCloud user account that is protected by two-factor authentication (2FA).

For myCloud licensing, make sure the device has internet connectivity with support for https, as it needs this to communicate securely with the myCloud domain for the sign-in / 2FA process.

If your device does not support https you can use the myCloud Connection Account instead. You'll find the Connection Account by logging in to your myCloud domain from a browser. Go to the Settings tab and select the Connection submenu. The Account name is always "DefaultConnection" and the password can be shown by clicking 'show'.

In the 'Apply License' dialog enter "[Domain name]/DefaultConnection" in the user name field and enter the password you have looked up in myCloud, please see the screen shot example above, where the domain name is WiseMo.

Press Ok and restart the Host from the menu.

Another possibility to configure the Host for myCloud, if the device doesn't support https, but only http, is to use the Mobile Host manager on a PC for configuration, please see chapter 4.

Buttons

Disconnect Allows the Host user to disconnect the session with a Guest. When no user is connected, it will show the Host status, for example "Running" indicating the Host is ready.

Run/Pause Pause the Host (not listening for incoming calls) or start it if paused.

Info The Info screen shows communication info, such as detected IP addresses and the status when prepared for myCloud communication. It also lists the Host ID, which a Guest user may use to identify / connect to the Host, and the Device ID is also shown.

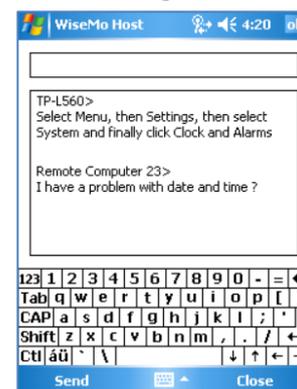
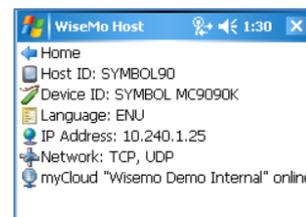
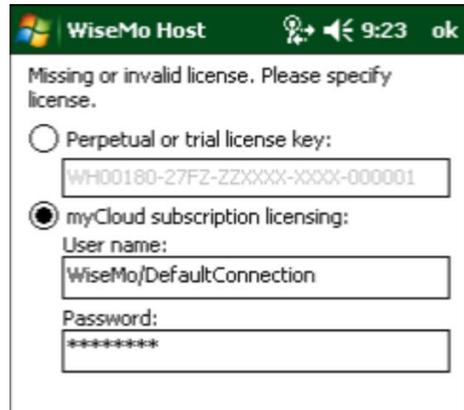
Help Request The Help Request screen is provided as backwards compatibility to older Guest modules supporting this.

History The history screen lists Guests connected / disconnected, with date and time stamp, since the Host module was started. For more advanced logging features, please use the logging feature, which can be configured via the Mobile Host Manager, described later in this document.

Chat is possible between Guest and Host, initiated by the Guest user. The user on the Host device can also end the Chat session.

With the Confirm Access security feature activated, the device user is prompted to accept or deny access from a Guest user.

A Guest user may show a message on the device screen. A Guest user may perform File Transfer, Hardware / Software Inventory and other actions on the Host device, without interrupting the device user.



2. Examples of Remote Control

Use a WiseMo Guest module to access and remote control a Windows Mobile / CE 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 Chrome browser on Mac, Linux or Windows, from an IE browser or Windows browsers supporting NPAPI components. The most feature rich Guest module is our Windows Remote Desktop Guest, a program 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.

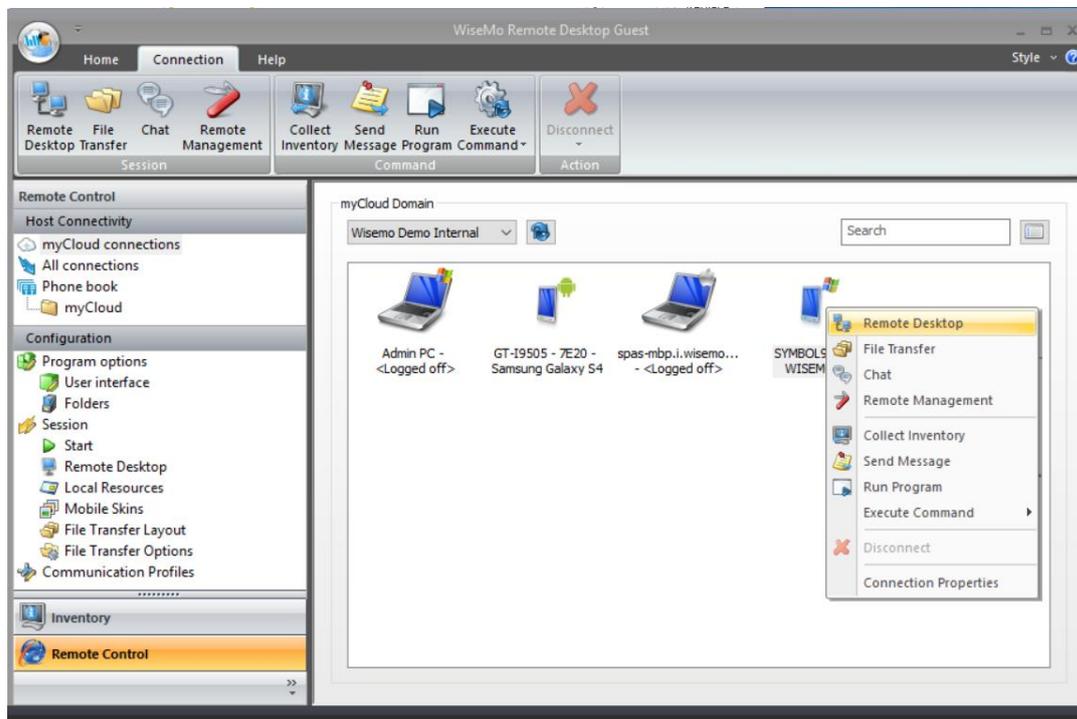
For more info on the use of these or other Guest types, please find the documentation relevant for each module here: <http://www.wisemo.com/support/documents/>

2.1 Remote control over the Internet (using WiseMo myCloud)

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

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

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



3. Double click on a Host 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.

- 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.

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

Live Remote Control screen

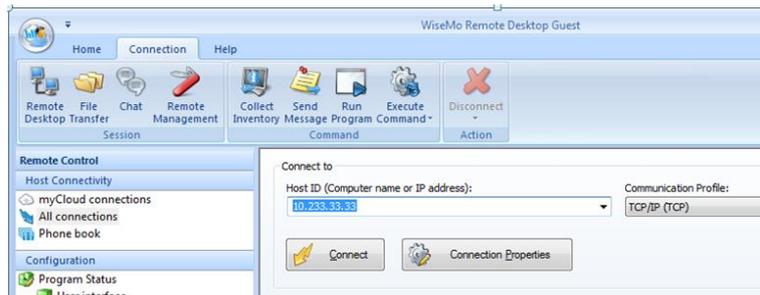


Skin

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.

- Start the Windows Remote Desktop Guest module on your PC.
- Select “All connections” from the menu, found in the left pane.
- Enter the IP address in the Host ID field. You can find the Host’s IP address by opening the Host module on the Windows Mobile/CE device. The IP address is shown in the Host’s Info screen.



- Press the Connect button

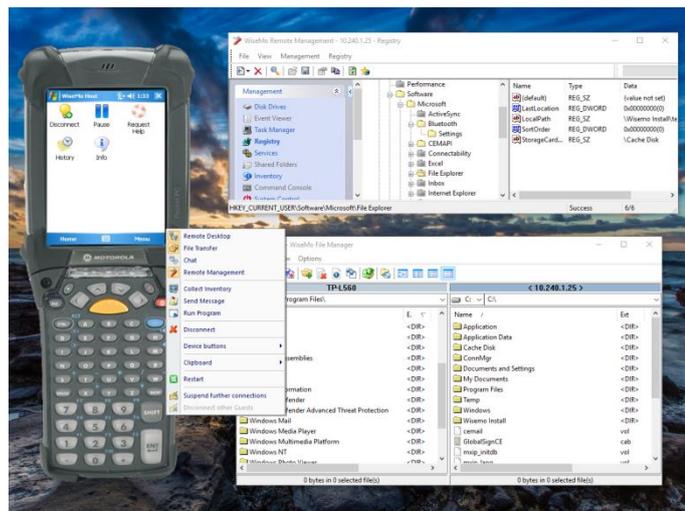


(or click the Remote Desktop button on the Connection tab)

- 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).

- 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 Windows Mobile/CE 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, a very efficient method for remotely entering input on the device.

The Skin functionality can be controlled from the "Connection Properties" and from the Configuration pane, both found in the Guest module.



Transparent skin



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 on a narrow window.



Skin in a window

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

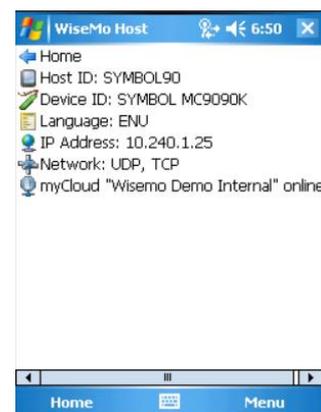
A Skin for a device is automatically chosen based on the "System model".

The "System model" for a particular ID device can be seen in the Host's Info screen, where it is called Device ID. In this example, the Device ID in the Host info screen shows "SYMBOL MC9090K". This is the name of the System model.

WiseMo has created Skins for many devices. If a Skin doesn't exist in the Skin repository, a default Skin will be shown.

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 Host user interface offer few configuration options but there are an abundance of different configuration options available via the Mobile Host Manager program.

The Mobile Host Manager, also termed Host Manager, is installed on your PC desktop computer when running the Windows Installer (.MSI) package for the Host. You can also download it separately [here](#). If your Windows PC has the WiseMo Windows Host module installed, this Host module also act as Host Manager for the Windows Mobile/CE Host, when you connect your device to the PC or load / create a Windows Mobile / CE host.xml file.

When installed, the Mobile Host Manager is found in **Start > All Programs > WiseMo RSM > Mobile Host Manager** (or WiseMo Host Manager).

4.1 Accessing the Host.xml configuration file

If the Windows PC has Active Sync/Mobile Device Center installed, connect your device(s) to the PC via a USB cable and the Mobile Host



Manager will try to automatically detect the device. If not, try to press the Refresh button on the Mobile tab. Make sure that the appropriate methods are enabled for detecting the device. You do this from the Mobile Host Manager's Home tab.

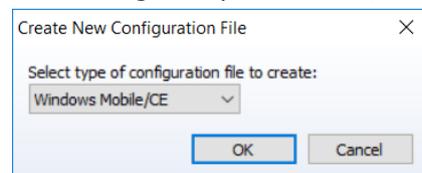
If the device is detected, select it from the list found at the bottom in the left pane. The program will retrieve the Host configuration file that's already on this device. Later you can use the Store button to place a modified configuration file back to the device.

In case a device cannot connect to a Windows PC



If the program cannot automatically retrieve the host.xml configuration file, you can instead copy it to the desktop PC and then open it by the Mobile Host Manager (File → Open). When all required configuration changes have been made, the configuration has to be saved on the desktop PC (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 default configuration file. From the Mobile Host Manager's System menu, select New and then Windows Mobile/CE.

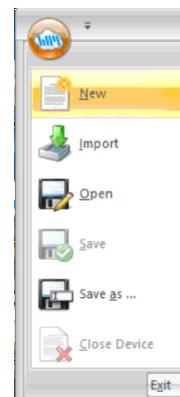


After making configuration changes, save the file and place it on the device in the WiseMo Host folder and restart the Host.

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

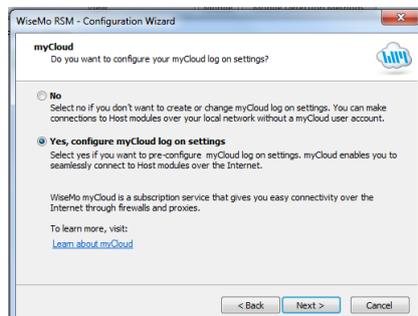


System menu



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.

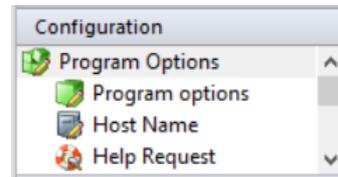
Press next until you reach the myCloud screen, then select Yes and press Enter.

Now Enter your myCloud user account credentials (email / password, and verification code if the User account is 2FA protected). Click next until the wizard has finished. Remember to store the new settings to your device (for example 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.

Use the Wizard to configure / re-configure connection to myCloud using a myCloud user account. All other configuration settings can be defined via the Mobile Host Manager's configuration panel.

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

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 s. (0 = do not stop).

User Interface

Start user interface as minimized (WM/CE)

Connection

Send Keep Alive messages

Allow multiple simultaneous Guest sessions

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 unattended 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).

User Interface: Define whether the Host user interface is shown minimized after start of the 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.

Naming

Use Device ID

Use Bluetooth/Device name (Android)

Use IMEI/Device serial number (Android)

Enter name (optional)

Name options

Public Host ID

As default, the Host ID will be the device name / computer name as defined on the device. When you have multiple devices, it is important the Host ID is unique. IF the device name is the original generic device name, the Host will add a random number to the device name to make it unique – but only IF the device name is the original generic device name (this condition to permit you to modify the device name on the device, to your own liking, without the Host interfering).

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: The Host report its actual Host ID to the WiseMo.ini file found in the Windows folder.

4.3.3 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, but not allow control of keyboard and mouse. 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 computers).

Authentication methods

There are 3 different authentication methods available:

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

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

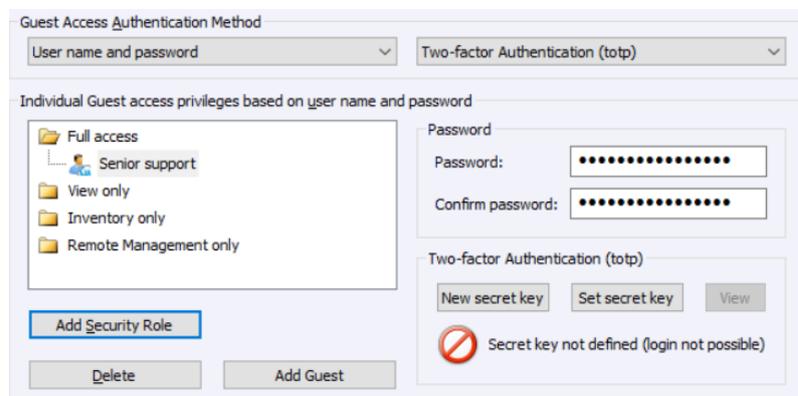
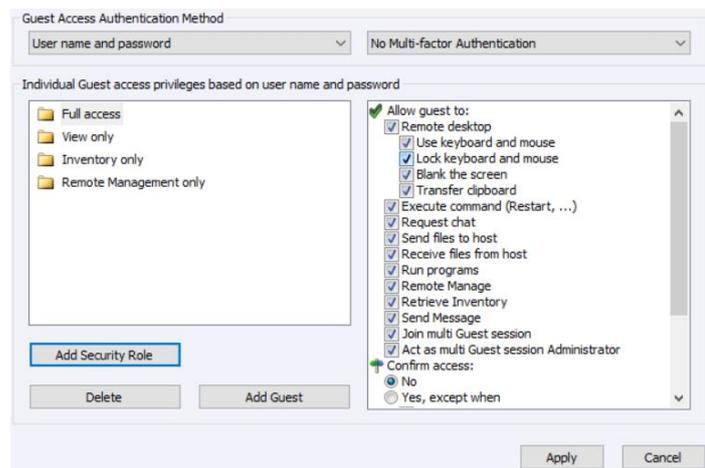
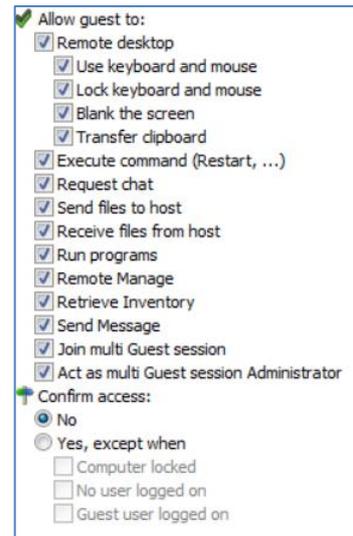
c. WiseMo Security Server: Individual Guest access privileges based on a WiseMo Security Server, which is an extra cost module for centralized management of security between Guests and Hosts.

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 secret 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 what should happen after a Guest disconnects, for example lock of the device. It also 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.

NOTICE: The Windows Mobile/CE Host module currently support Classic, None and Very High, although the Host Manager list other options. Make sure that at least one of those 3 supported modes is enabled. Very High is recommended, perhaps None if the network otherwise is secure. The classic level is only relevant for compatibility with some special modules.

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 permit None and Very High.

Name: Very high

Description: Everything is encrypted with 256 bit keys

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

Encryption:

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

Integrity check:

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

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

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

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

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.

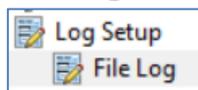
4.5 Communication Profiles

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

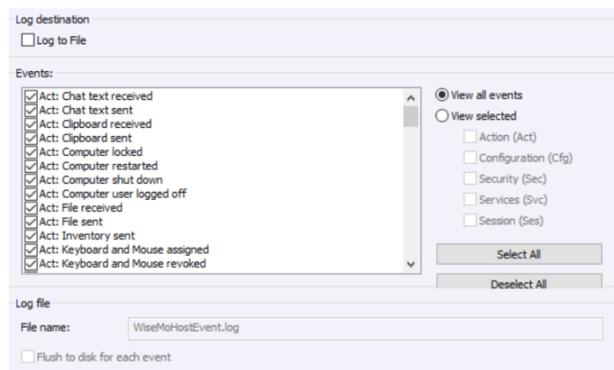
For TCP/IP profiles, you can for example change the send/receive port numbers the Host use as default (1970/1970).

For myCloud profiles, the 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 or the "Apply license" option found in the Host menu, for configuration of myCloud connectivity, as it uses myCloud User account credentials (email + password).

4.6 Log setup



The Host provides for extensive logging of event activity related to the Host. This includes changes to configuration settings, specific actions, security related events and session events. Logging is made to a local file.



5. Updating or removing the Windows Mobile / CE module

A newer version or service release of the Host application can be installed on top of the previous one. Updating an existing installation will as default preserve configuration settings, which are found in the Host.xml file located in the folder \WiseMo Host.

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

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

Removal of the WiseMo Host application from a Windows Mobile/CE device is done like you would remove any other program. You can for example do it from the device's Settings | System | Remove programs. Select the Host module, and click the "Remove" button.

Uninstalling the Host program does not remove the configuration and license files found in the "\\WiseMo Host" folder.

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 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 the Host is licensed with a trial license key, and it is configured for myCloud connectivity, then the Host module will NOT automatically use myCloud licensing, when the trial key expire !!

To test the Host with myCloud licensing only, you can download and install the Host installation file from the Deploy tab in your myCloud trial domain. If you already have a Host installed, you can also from the Host user interface switch the Host to use myCloud licensing instead.

If you locate and delete the file host.lic prior to installation / start of the Host, you will be prompted for licensing.

7. Glossary

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

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

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

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

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 communicates with 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.