## Firewall Configuration Guide

WiseMo Remote control can be used for connections locally on a LAN and over the internet by using WiseMo myCloud.

This document describes firewall configuration for LAN connections (see the paragraph Firewall Configuration for LAN Connections) and for myCloud based connections over the internet.

## WiseMo myCloud Overview

The WiseMo Guest and Host applications require access to the WiseMo myCloud infrastructure to establish and route remote control connections over the internet via myCloud.

WiseMo myCloud is designed to assure easy connectivity without any special firewall configurations being necessary. **The WiseMo Guests and Hosts only make outbound connections which are normally not blocked by firewalls**.

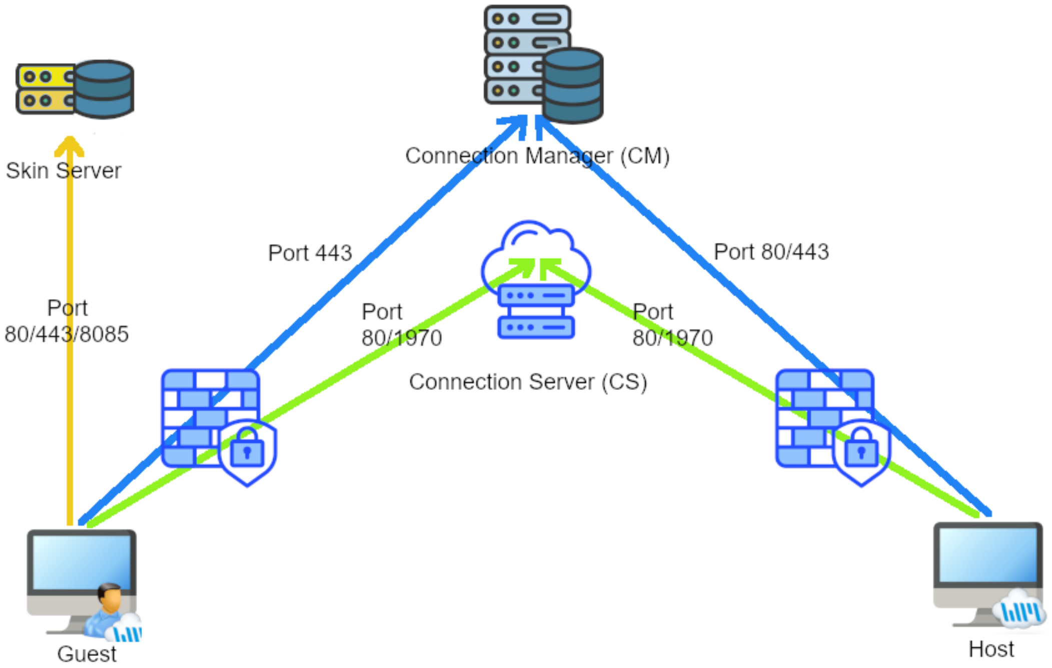
However, in environments with strict security policies, such as corporate networks, firewalls may block all unknown outbound traffic. In such cases, you must configure the firewall to permit WiseMo myCloud connections.

The myCloud infrastructure comprises of two key internet based server components:

1. **Connection Manager**: Handles authentication and assigns a Connection Server for each Guest-Host connection.
2. **Connection Servers**: Facilitate end-to-end encrypted connections while ensuring only authenticated connections are established. These servers are distributed globally for efficient routing.

plus, the auxiliary Skin Server:

3. **Skin Server**: The Skin server is a repository of device images that is used with mobile device remote control to show the remote control screen inside an image of the actual Host device.



## Firewall Configuration for WiseMo myCloud Connections

If firewall configuration is required, the next step is to determine whether the WiseMo ports need to be configured for specific IP addresses or if allowing the outbound ports generally will suffice.

### Connection Protocols

The underlying protocol for all connections to the WiseMo servers is TCP.

#### *Connection Manager*

Connections to the Connection Manager are based on http or https depending on configuration, module and task:

- The Guests always use https
- The Hosts use http for the myCloud presence poll and https for security related tasks. The Host can be configured to always use https (see below)

#### *Connection Server*

Connections to the Connection Servers are TCP but the communication might be encapsulated in http if necessary. The actual data that is sent is by default end-to-end encrypted using AES encryption.

#### *Skin server*

The connection to the Skin Server is based on WebDAV (Web Distributed Authoring and Versioning) that is an extension to the HTTP protocol.

## Allow outbound connections for port 80, 443 and 1970

The simplest configuration of the firewall would be to generally allow outbound connections on port 80, 443 and 1970 for all apps or specifically for the WiseMo Guest and Host apps.

On Windows the default full path and name of the Guest app is by default:

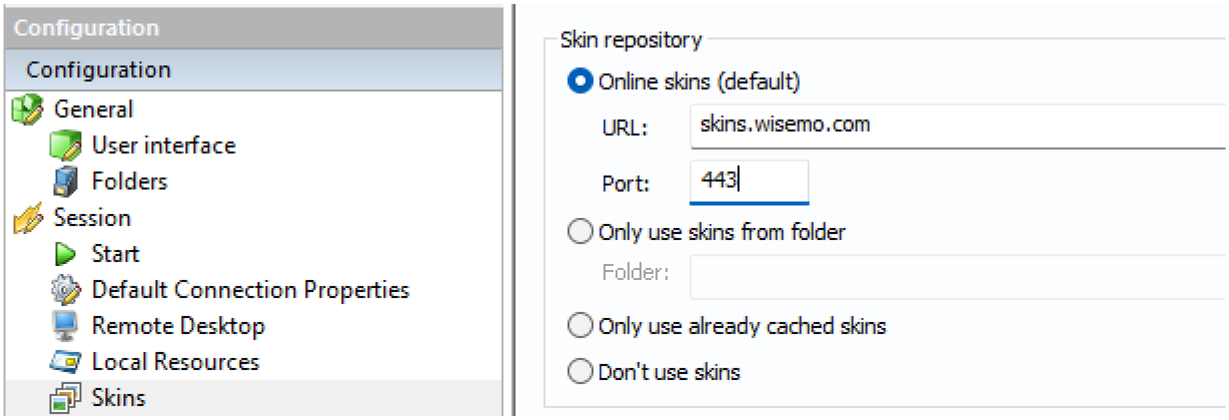
C:\Program Files (x86)\WiseMo\WiseMo RSM\Remote Desktop Guest\WsmGuest.exe

and for the Host app it is:

C:\Program Files (x86)\WiseMo\WiseMo RSM\Remote Desktop Host\WsmHostSvc.exe

### *Optimizing the necessary ports*

Newer Guests[1] only need access to port 443 and 1970. The Skin repository configuration in the Windows Guest might be configured to use port 80[2] but it can be changed to port 443, "Configuration > Session > Skins":



Skin repository

● Online skins (default)

URL: skins.wisemo.com

Port: 443

○ Only use skins from folder

Folder:

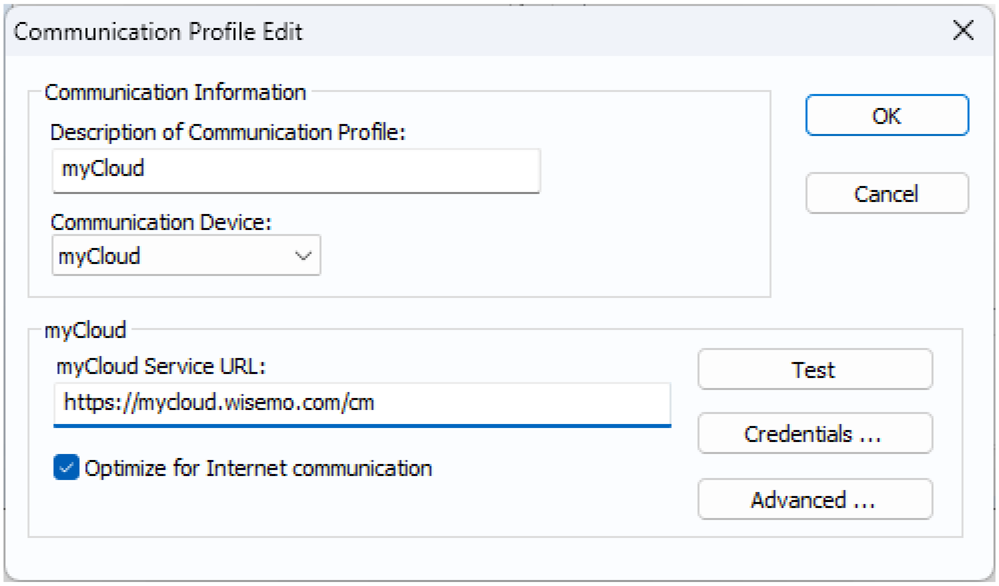
○ Only use already cached skins

○ Don't use skins

On Windows, the Host can be configured to use https (port 443) instead of http (port 80) in "Configuration > Communication Profiles > myCloud": Replace "http" with "https" in the "myCloud Service URL".

[1] Version 20 and newer.

[2] Version 20 build 2025016 and newer use port 443 by default.



Description of Communication Profile: myCloud

Communication Device: myCloud

myCloud Service URL: https://mycloud.wisemo.com/cm

☑ Optimize for Internet communication

It's also possible to use port 1970 (to use the same port as for Connection Server connections) by specifying:

http://mycloud.wisemo.com:1970/cm

in the “myCloud Service URL”.

These changes can also be made on other operating systems by editing the host.xml configuration file.

## Allow outbound connections for specific IP addresses on port 80, 443 and 1970

This is the more advanced firewall configuration case because it requires that you know the IP addresses of the WiseMo myCloud services.

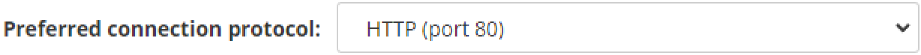
### *Connection Manager*

The Connection Manager is behind multiple load balancers, and you will need to add all load balancer IP addresses for Port 80 and 443. The above comments about Guest and Host port numbers are also applicable here. Please refer to the IP addresses paragraph below.

### *Connection Server*

A Connection Server is assigned to a connection based on its geographical proximity to the Guest and Host modules, as well as the load on Connection Servers in the area. Consequently, the IP address of the Connection Server may vary from one connection to another. The initial connection attempt through a Connection Server is made on port 1970, followed by port 80.

If connections are only permitted on port 80 (HTTP), it is recommended to configure myCloud accordingly (Settings > Connection > Preferred connection protocol):



**Preferred connection protocol:** HTTP (port 80)

Please refer to the IP addresses paragraph below for the pool of IP addresses for WiseMo Connection Servers.

The myCloud "Private Connection Server" feature in "Settings > Connection servers" allows you to set up dedicated Connection Servers for your domain. In this case you must of course add these IP addresses to the firewall.

### *Skin server*

The skin server uses by default port 443 but is also accessible via port 80 and 8085.

### *IP addresses*

The IP addresses the WiseMo myCloud services use are quite stable but especially Connection Servers might occasionally be added and in rare cases even removed. If a new Connection Server is added, it is necessary to add its IP address to the allowed list because your remote control connection risks being assigned to this new Connection Server and if it is not added, the connection will be rejected by your firewall.

The WiseMo myCloud IP addresses in use at any given time and their guaranteed validity period. Can be retrieved with DNS lookup as follows:

| Purpose | Ports | DNS lookup name | Validity days |
|---|---|---|---|
| **Connection Manager** | 80 or 443 | mycloudall.wisemo.com | 30 |
| **Connection Servers** | 80 or 1970 | csall.wisemo.com | 7 |
| **Skin server** | 80, 443 or 8085 | skinsall.wisemo.com | 30 |

To for example lookup the IP addresses in use by all Connection Servers, open a command prompt on Windows and write:

```
nslookup csall.wisemo.com
```

On Linux, macOS, Android or other UNIX variants, open a terminal window and write:

```
host csall.wisemo.com
```

And the list of IP addresses returned will remain valid for at least 7 days after you ran the command. If possible, you should look for a firewall feature that does that lookup automatically, as you will otherwise need to set up a procedure to repeat the lookup and possible firewall reconfiguration every 30 days (7 days for the connection server list).

Note that the commands above will sometimes also tell you the IP addresses of DNS servers used to retrieve the list, those are not part of the list.

If you set up your own private connection server somewhere, those will not be included in the IP lists returned by the above DNS lookups.

### *Additional information about firewall configuration*

If you block or restrict access to any ports likely to be used by WiseMo products (for example ports 80, 443 and 1970), please configure your firewalls to explicitly "reject" outgoing packets instead of silently "dropping" them. This allows WiseMo products, as well as other programs within your network, to handle the policy restriction more efficiently, either by reporting the error to the user or employing appropriate fallback behavior. Silently dropping inbound packets is effective for deterring known malicious actors and external port scans but silently dropping outbound packets is detrimental to the performance of your internal computers and users.

When using an "HTTPS inspection" system that requires web browsers within your network to trust a special CA certificate for the inspection system, ensure that the CA certificate is deployed to the system CA trust stores on internal machines, including those running WiseMo Host programs. For Windows machines, use the "Machine" part of group policy rather than the user part. Similarly, import it into the "Local Computer" certificate store for "Trusted Root Certification Authorities" on standalone Windows machines. Deploying the trust only to per user settings does not support system-wide services that operate independently of user login, such as WiseMo Hosts.

## Firewall Configuration for LAN Connections

When connecting directly to a Host IP address or DNS name, the LAN firewall configuration is simple. A firewall on the same computer/device (local firewall) rarely blocks outbound connections and it is hence only necessary to configure the firewall to allow inbound connections. The Guest only makes outbound connections so in the simple case, it’s only necessary to configure the Host for inbound connections.

### *Open for inbound connections to the Host application*

During the installation of the Host application (and Guest for that matter), the setup program automatically uses Windows functions to adjust the local firewall, enabling inbound connections for all ports on UDP and TCP to the Host application (and Guest, respectively). If you are not using Windows, similar configuration may have to be done manually in the firewall.

### *Opening for specific ports*

By default, the Guest and Host applications use port 80 and 1970 to establish LAN connections. The security can be tightened by only allowing incoming connections on these ports.

The Guest and Host can be configured to use different port and the firewall must hence be configured accordingly.

### *Open for outbound connections from the Guest application*

In environments with strict security, it might also be necessary to configure outbound connection for the Guest application. Connections should be allowed for port 80 and 1970 for UDP and TCP.

If you don’t make connections over UDP and http, you do not need to open the firewall up for UDP and port 80.

### *Using skins when remote controlling mobile devices*

The Skin server is a repository of device images that is used with mobile device remote control to show the remote control screen inside an image of the actual Host device.

The skin server uses by default port 443 but is also accessible via port 80 and 8085.

Please also refer to the relevant paragraphs for skin server access in Firewall Configuration for WiseMo myCloud Connections.

### *Using myCloud licensing*

If you license the WiseMo Guest and Host through a myCloud subscription, the Guests and Hosts need access to the Connection Manager just like when using myCloud. In such case, please refer to the relevant paragraphs about Connection Manager configuration in Firewall Configuration for WiseMo myCloud Connections.

### *Using myCloud Device Access Control service*

If you configure the WiseMo Host to use our centralized myCloud Device Access Control service, Guests and Hosts need access to the Connection Manager just like when using myCloud. In such case, please refer to the relevant paragraphs about Connection Manager configuration in Firewall Configuration for WiseMo myCloud Connections.

### *Crossing external firewalls*

In some cases, a connection might cross external firewalls for example in a VPN environment. In such case you must open for port 80 and 1970 either directly or by setting up a firewall port forward from a port number of your choice to port 1970 on each Host behind each firewall.