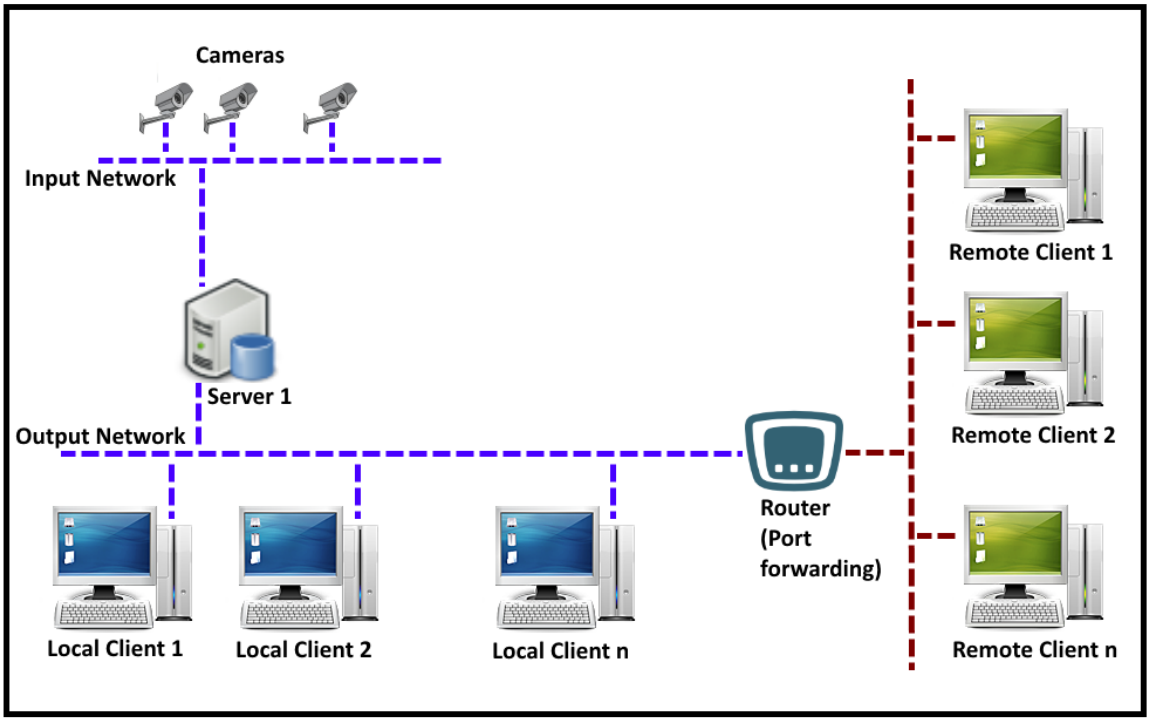
# Security Management System – Remote Client (22.11.28.01)

In most of the deployment scenarios, the server application is hosted on a computer which is in the internal network of an enterprise. Hence it is not accessible from the client applications running on computers outside this internal enterprise network. This is common practice followed for security of computers on the internal network.

However in some cases, it may be needed to grant access to a few client applications which are not in the local network – same network as server computer. Such client applications are called as 'remote clients'. Port forwarding on the router, is a commonly used method for allowing access to the remote clients, still maintaining the security of the network.




This document explains the configurations needed to expose the 'Security Management System Server software' to the remote client, running on an external network.

Note 1 – This document is applicable if the project requirement or solution design includes remote clients, running on external network; and connecting to the 'Security Management System Server software' hosted on internal enterprise network.
If the project requirement or solution design does not include remote clients, this document is not applicable and can be ignored

Note 2 – The configuration needed to expose the ‘Security Management System Server software’ to the remote client, running on an external network; is from the network side. It involves ‘port forwarding’ configuration in the router.

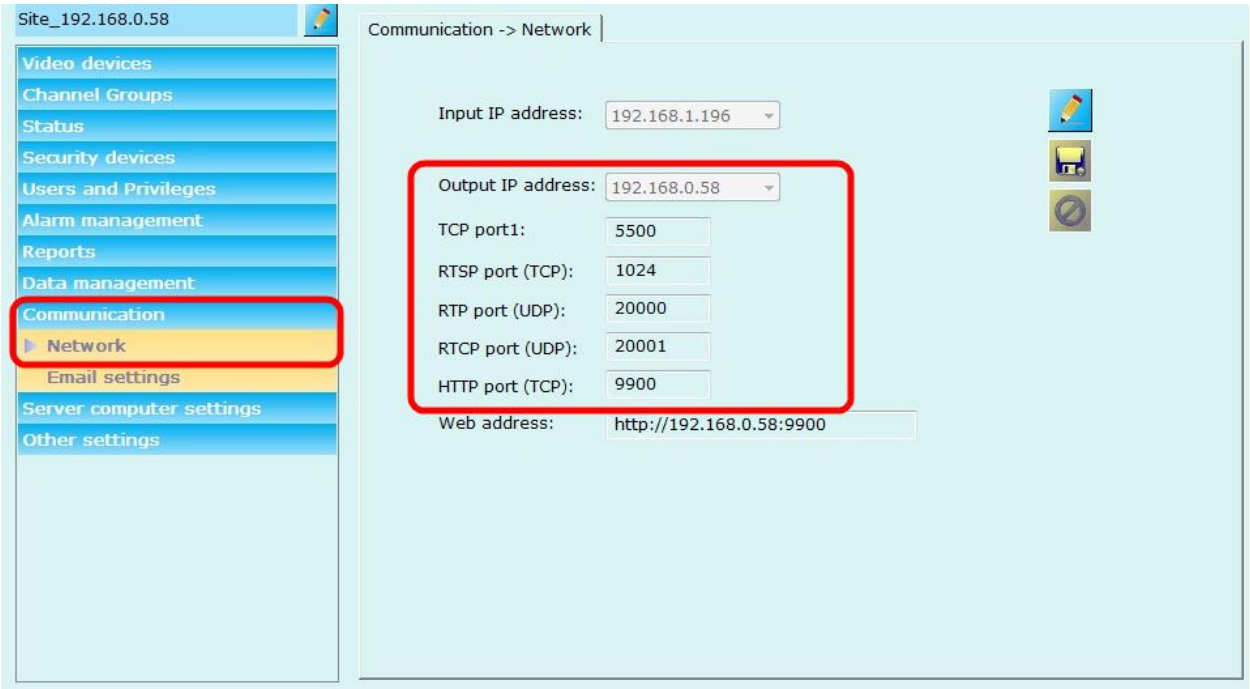
The ‘port forwarding’ configuration is external configuration. It is specific to router used and the network design. The port forwarding configuration needs to be performed by the network team at the site.

The ‘port forwarding’ configuration is outside the scope of the ‘Security Management System’ software and the 'Security Management System' software does NOT process the 'port forwarding'. The 'Security Management System Remote Client' only uses the port forwarding information, as configured by the network team at the site, for connecting to the ‘Security Management System Server software’.

## [A] Ports used by the 'Security Management System' Server software

1. In the server software, please navigate to the 'Communication' tab from the left side navigation menu. Navigate to the 'Network' sub-tab under it.

2. This will display the Network Settings page.




Please note following settings on this 'Network Configuration' page –

(a) Output IP address
(b) TCP port1
(c) RTSP port (TCP)
(d) RTP port (UDP)
(e) RTCP port (UDP)
(f) HTTP port (TCP)

Note – From these settings, TCP port1, RTSP port (TCP), RTP port (UDP), RTCP port (UDP), HTTP port (TCP) are read-only settings and can not be configured by the user.

## [B] Port forwarding information

1. Please configure the router in the network, to expose the 'Output IP address' and all the ports listed above, to external network. List the mapping table, as follows –

| Sr. No. | Port Type | Internal IP address | Internal port number | External IP address | External port number |
|---|---|---|---|---|---|
| 1 | TCP port1(TCP) | <IP address 1> | 5500 | <IP address 2> | <Port 1> |
| 2 | RTSP port (TCP) | <IP address 1> | 1024 | <IP address 2> | <Port 2> |
| 3 | RTP port (UDP) | <IP address 1> | 20000 | <IP address 2> | <Port 3> |

| | | | | | |
|---|---|---|---|---|---|
| 4 | RTCP port (UDP) | <IP address 1> | 20001 | <IP address 2> | <Port 4> |
| 5 | HTTP port (TCP) | <IP address 1> | 9900 | <IP address 2> | <Port 5> |

(a) '<IP address 1>' is the 'Output IP address', from 'Security Management System Server software' 'Network Settings' page (as described in point [A].2 in this document)
(b) 'Internal port number' values in the table are from 'Security Management System Server software' 'Network Settings' page (as described in point [A].2 in this document)
(c) '<IP address 2>' is the external IP address as configured in the router, by the site networking team.
(d) '<Port 1>', '<Port 2>', '<Port 3>', '<Port 4>' and ''<Port 5>' are the external port numbers as configured in the router, by the site networking team.

Following is the example table with example values –

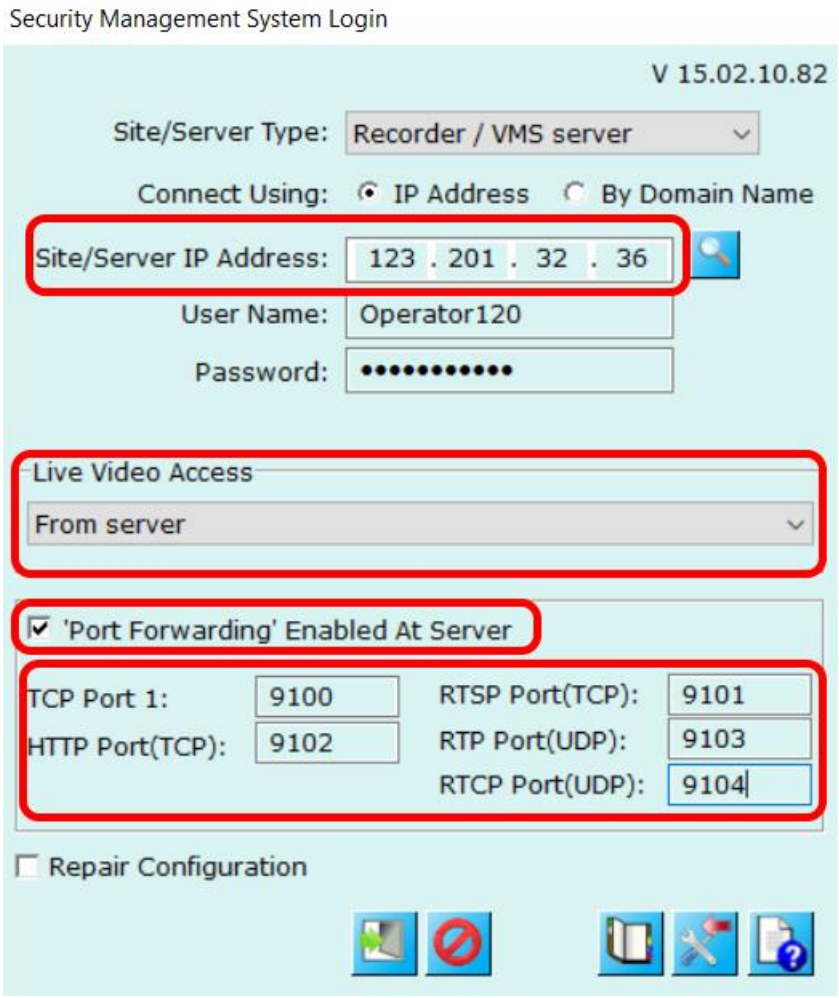
| Sr. No. | Port Type | Internal IP address | Internal port number | External IP address | External port number |
|---|---|---|---|---|---|
| 1 | TCP port1(TCP) | 192.168.0.58 | 5500 | 123.201.32.36 | 9100 |
| 2 | RTSP port (TCP) | 192.168.0.58 | 1024 | 123.201.32.36 | 9101 |
| 3 | RTP port (UDP) | 192.168.0.58 | 20000 | 123.201.32.36 | 9102 |
| 4 | RTCP port (UDP) | 192.168.0.58 | 20001 | 123.201.32.36 | 9103 |
| 5 | HTTP port (TCP) | 192.168.0.58 | 9900 | 123.201.32.36 | 9104 |

Notes –
(a) This table is only an example and actual values, will change depending on the network configuration at the deployment site
(b) The values in this table related to the Router, should be the values configured in the router for port forwarding
(c) During port forwarding configuration on the router, please allow incoming as well as outgoing traffic and for both TCP and UDP, for all ports being configured for port forwarding.

2. Please make sure that the remote computer is able to access the computer where Management System Server Software is running, through the port forwarding.
Using the standard 'Ping' command to ping the router IP address, can be a good initial test. However, advance tools available with the network team need to be used to confirm the port forwarding configuration and access to all exposed ports through port forwarding.

## [C] 'Security Management System' Remote Client software

1. Please install the Security Management System Client Software on the remote computer and execute it. It will pop up the 'Server Connection / Login' dialog box.




2. In the 'Site/Server IP Address' input, please type 'External IP address' as per the port forwarding configuration performed and captured in the table (as described in point [B].1 in this document)

3. Please type 'User Name' and 'Password'. These credentials are for 'Operator' privilege user configured in the target 'Security Management System Server software'

4. Please enable the "'Port forwarding' enabled on the server" check-box.
   Type the values for TCP port1, RTSP port (TCP), RTP port (UDP), RTCP port (UDP), HTTP port (TCP). These values are as per the port forwarding configuration performed and captured in the table (as described in point [B].1 in this document)

5. Click on the 'Login' button to login to the server. After successful connection and login, 'Security Management System Client software' main screen will be displayed.

## Notes –

(a) It is very important to have sufficient and consistent network throughput available between the server and the remote client.
   i. In the direction from remote client to server – minimal network throughput 32 kbps is required

ii. In the direction from server to remote client – higher network throughput is required. Exact value can be calculated based on multiple parameters including live video stream bitrate, maximum simultaneous number of live videos viewed in remote client, recorded video bitrate, maximum simultaneous number of recorded videos viewed in remote client etc

(b) If sufficient and consistent network throughput is not available, 'Security Management System Client software' running on the remote client workstation may not be able to finish the initial handshaking after communication and may keep trying to complete it. The 'Security Management System Client software' user interface will not be displayed till the initial handshaking is successful.

(c) The initial handshaking network throughput requirement varies depending on the cameras authorized for the user logging in from the remote client. Hence for initial tests, during the configuration, it is recommended to create a new privilege in the 'Security Management System server software', with authorization for only a few cameras; and creating a new user with this new privilege; and using the new user credentials for logging in from the remote client.

(d) After initial handshaking, remote client will start displaying videos. If sufficient network throughput is not available, the videos may not be displayed properly