

Default Ports for MAK Products

This document lists the default ports for MAK Products and their components.

MAK Legion

Port 6000 is the default port.

Table 1: MAK Legion Port Value

Default Port	To Use a Different Port...
6000	Change in command line or relevant config file (<i>./bin64/legionMonitor.lua</i> , <i>./bin64/legionServer.lua</i>)

MAK Data Logger

Table 2: MAK Data Logger Port Values

Default Port	Protocol / Usage	To Use a Different Port...
3000	DIS	Change in GUI, command line, or config file
4053	UDP: Remote Control	Change in command line or config file
5000	UDP: Video Streaming	Change in GUI or config file

MAK RTI

The MAK RTI ports are Modified in the RTI GUI or in *rid.mtl*. This information applies only to HLA connections

Table 3: MAK RTI Port Values

Default Port	Protocol / Usage	To Use a Different Port...
4000	UDP Port	Edit <i>rid.mtl</i> (setqb RTI_udpPort 4000)
4001	TCP Port	Edit <i>rid.mtl</i> (setqb RTI_tcpPort 4001)
5000	TCP: rtiForwarder	Edit <i>rid.mtl</i> (setqb RTI_distributedForwarderPort 5000)

Default Ports for MAK Products

Table 3: MAK RTI Port Values (Continued)

Default Port	Protocol / Usage	To Use a Different Port...
6001	Multicast Discovery Port	RTI_mcastDiscoveryPort
6003	UDP: RTI Assistant Port	RTI_ASSISTANT_PORT (environment variable)

VR-Link

Port 3000 is the default for all DIS protocols. For HLA, see MAK RTI above.

Table 4: VR-Link Port Value

Default Port	Protocol / Usage	To Use a Different Port...
3000	DIS	Change in command line

VR-Exchange

Table 5: VR-Exchange Port Values

Default Port	Protocol / Usage	To Use a Different Port...
3000	UDP: DIS Broker	Change in GUI, command line, or config file
5111	TCP: Brokers to heartbeat the portal	Change in GUI or config file

WebLVC

Table 6: WebLVC Port Values

Default Port	Protocol / Usage	To Use a Different Port...
8080	Port for Proxy	Change in GUI or config file
9101	Web Server Port	Change in GUI or config file
9102	TCP Server Port	Change in GUI or config file

Default Ports for MAK Products

VR-Vantage

Table 7: VR-Vantage Port Values

Default Port	Protocol / Usage	To Use a Different Port...
3000	DIS	Change in GUI or command line
22563	TCP: Remote Display Engines	Change in GUI or command line

VR-Forces

Table 8: VR-Forces Port Values

Default Port	Protocol / Usage	To Use a Different Port...
3000	DIS	Change in GUI or command line
9000	TCP: Transporting scenario files on load and save	Set --fileTransporterReceivePort on the front-end command line
Random	Port used by the DtCgfDispatcher's file transporter to receive order of battle and plan files from a DtVrfRemoteController. If the port requested cannot be opened, the next open port will be used. A value of zero indicates that VR-Link should choose an ephemeral port, which is automatically assigned by the system.	The only way to change the port is in the back-end. Edit: cgfDispatcherReceivePort in the <i>vrfSim.mtl</i> located in <i>../appData/settings/vrfSim</i> folder (setqb cgfDispatcherReceivePort0)

VR-Engage

Table 9: VR-Engage Port Values

Default Port	Protocol / Usage	To Use a Different Port...
3000	DIS	Change in GUI or command line

RadarFX

RadarFX can be used with VR-Vantage and VR-Engage.

Table 10: RadarFX Port Values

Default Port	Protocol / Usage	To Use a Different Port...
4567	Simple Client	Change in GUI
3000	DIS, RadarFX Server	Change in GUI

Default Ports for MAK Products

FLEXIm Licensing

Any edits must be made in your license file.

Table 11: FLEXIm Licensing Port Values

Default Port	To Use a Different Port...
27000	Edit SERVER hostname MAC_Address 27500 (27500 is the defined port)
Defined @ runtime	Set by adding port=xxxx, for example: VENDOR maklmgrd ./maklmgrd port=1234

Loopback Connections

When using a loopback connection for DIS or Legion, all executables must have the incoming and outgoing connection open for the loopback to work correctly.

To set up an inbound rule for a Windows program:

1. Run Windows Defender Firewall with Advanced Security.
2. Select Inbound Rules.
3. Choose **Action** → **New Rule**.
4. Select Program and then click Next.
5. Enter the path to the program executable and then click Next.
6. Select Allow the Connection and then click Next.
7. For the rule, select Domain, Private, and Public. Click Next.
8. Optionally, enter a name for the rule.
9. Click Finish.