Mandiant

NETWORK COMMUNICATION REQUIREMENTS

The platform's management plane is a web service that is fully encrypted using TLS 1.2. No other management communications or ports are required for the management plane to communicate between the Director and Actors.

While it is recommended that you also enable SSH to the components of the platform, this is optional and not required.

Even though Security Validation Actors may communicate over any allowed protocol by the networks in place, this is only done when executing Attacker Behaviors to test the security controls in place on the network.

The following tables contain the minimum network communication requirements. Think about your environment and determine if other ports need to be open to permit communication between the Director and other systems (e.g., syslog servers, SIEMs, IDS).

Network Communication Requirements for the Validation Platform

Communication Type	Required Protocols	Optional Protocols	Required TCP Ports	Optional TCP Ports	Required UDP Ports	Optional UDP Ports
Browser client to Director	HTTPS	SSH	443	22	N/A	N/A
Browser client to Director	HTTPS	N/A	6080	N/A	N/A	N/A
Director to Actor	HTTPS	SSH	443	22	N/A	N/A
Actor to Actor	N/A	N/A	N/A	N/A	N/A	N/A
Director to Protected Theater Only required to use the optional Director Protected Actor console	N/A	N/A	5900, 5901	N/A	N/A	N/A
Director to Update and Content Services	HTTPS	SSH	443	N/A	N/A	N/A

Communication Details

Component	Port	Protocol	Direction	Info

Component	Port	Protocol	Direction	Info
Director	443	HTTPS, using TLS 1.2	Inbound to Director	Required for users to access the Director and for the Director to access the Update and Content Services
Actor (Network and Endpoint)	443	HTTPS, using TLS 1.2	• Push: Outbound from Director • Pull: Inbound to Director	Must be open in at least one direction to enable communication between the Director and Actor
Security Validation Admin	22	SSH	Inbound to Director / Actors	Required for users to SSH to the Director
Director	6080	HTTPS		Required to use the Director Protected Theater console  For more information, see **Connect to PT using VNC or the Console (https://docs.mandiant.com/home/msv-using-the-console-vs-vnc).**
Protected Theater (MSV on-prem)	5900 & 5901	RFB	Director to Protected Theater	

Mandiant Advantage Security Validation (MA-SV) Network Requirements

To allow traffic to and from MA-SV itself and receive any system-generated emails from MA-SV, you may need to address the following on your network:

- Inbound hostname and IP addresses for pull communication and UI access:
  - Name: `app.validation.mandiant.com`
  - Address: `162.159.240.125`
  - Address: `162.159.241.125`
- Outbound IP address for push communication: `34.135.50.52/32`
- Outbound IP address for email notification (Mandiant uses Amazon SES):

  ```
  199.255.192.0/22, 199.127.232.0/22, 54.240.0.0/18, 69.169.224.0/20, 23.249.208.0/20, 23.251.224.0/19, 76.223.176.0/20, 52.82.172.0/22, 54.240.64.0/19, 54.240.96.0/19, 76.223.128.0/19, 216.221.160.0/19
  ```

- MA-SV outbound email address: `admin@validation.mandiant.com`