

OPERATIONAL READINESS

The Operational Readiness page provides you with information that tests your Security Validation Platform environment. This page includes a series of benign Actions geared toward ensuring adequate and correct configuration of various elements necessary for effective use of the platform. This page is also useful for troubleshooting issues that you may encounter, such as communication issues, while using the platform.

OPERATIONAL READINESS OF YOUR ENVIRONMENT ?

ENVIRONMENT

1
DIRECTORS

7
ACTORS

9
ZONES

3
CONTROLS

2
ACTION USER
PROFILES

1
PT

1
EMAIL

ⓘ The results below may not match the pass/fail status of the actual Jobs. They are intended to verify the Director can reach Actors and run Actions.

ENDPOINT ACTORS Incomplete

Name	Type	Zone	OS	Tested Actions	
mactors-5-192.168.1.14	endpoint	Desktop Users	macosx	Pass: 0 Fail: 0 Incomplete: 2	▶
vpa01	protected	Test Lab	windows	Pass: 0 Fail: 0 Incomplete: 5	▶
ubuntu-3-172.31.43.108	endpoint	Desktop Users	linux	Pass: 0 Fail: 0 Incomplete: 2	▶

NETWORK ACTORS Incomplete

Source	Destination	Tested Actions	
vna-servers	vna-internet	Pass: 0 Fail: 0 Incomplete: 3	▶
cloud-actor-2	cloud-actor-1	Pass: 0 Fail: 0 Incomplete: 3	▶

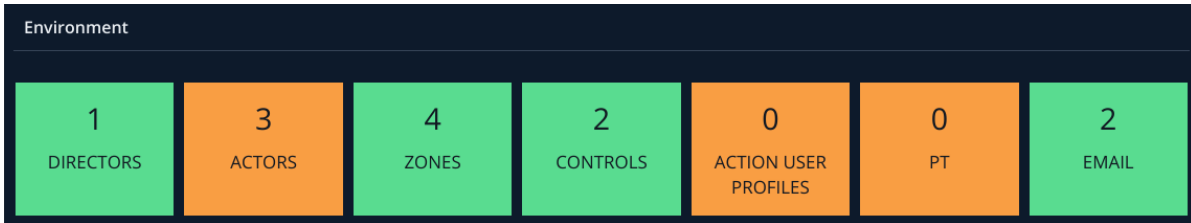
Operational Readiness page

To open the Operational Readiness page, select **Environment > Operational Readiness**. The two sections of the Operational Readiness page are:

- [Environment Table](#)
- [Actors Tables](#)

Environment Table

The tiles in the Environment table indicate the number of Directors, Actors, Zones, security technologies (Controls), Action User Profiles, Protected Theaters (PT) connected to your Director (when you have the Protected Theater module), and the number of Email profiles (Email) configured (when you have the Email Theater module).



Operational Readiness Environment table

Environment Status Indicator

The color of the tile indicates health based on the configured elements in the environment (for example, Actors) and on the tests run.

- **Green:** Indicates that the element in your environment is configured as expected and that all tests have passed
- **Orange:** Indicates a warning that requires attention
- **Red:** Indicates a problem that renders the system unusable (for example, no Actors registered)
- **Gray:** Indicates that a module, such as Protected Theater, is not included in your license

To see the test messages for an Environment element, move your cursor over the block. To expand the full list of messages, including tests that passed, click the tile.

Environment

1 DIRECTORS	4 ACTORS	4 ZONES	0 CONTR
----------------	-------------	------------	------------

Endpoint Actors

Name	Type
vna-endpoint	endpoint

- Actor vna-server time sync has never been checked
- Last received communication about 2 months ago from Actor vna-server (Actor info refresh rate: 24 hours)
- Actor vna-desktop time sync has never been checked
- Last received communication about 2 months ago from Actor vna-desktop (Actor info refresh rate: 24 hours)
- Actor vna-internet time sync has never been checked
- Actor vna-endpoint time sync has never been checked

Example of orange indicator messages for an Actor in the Operational Readiness tiles

Actors Tables

Network Actors and Endpoint Actors are shown in separate tables on the Operational Readiness page. The source and destination Actor pairs for the Network Actors table are populated based on the Actors in your environment and their Can Talk to Actors (CTTA) status. Benign Actions are populated in the appropriate table (Network or Endpoint) and associated with each Actor or Actor pair that can run the Action.

ENDPOINT ACTORS					Fail
Name	Type	Zone	OS	Tested Actions	
vea01	endpoint	Desktop Users	windows	Pass: 0 Fail: 1 Incomplete: 9	⌵
Host CLI - Benign: Check Internet Connectivity in Windows via Command Prompt (VID: A104-320)				2019-5-13 13:25 UTC	⏹ ⬇ ▶
Host CLI - Benign: whoami in Windows via Command Prompt (VID: A104-319)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Batch File Execution via PowerShell (VID: A104-321)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: whoami in Windows via PowerShell (VID: A104-323)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Check Internet Connectivity via PowerShell (VID: A104-324)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: whoami in Bash (VID: A104-325)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Check Internet Connectivity in Bash (VID: A104-327)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Script Execution in Bash (VID: A104-326)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Batch File Execution via Command Prompt (VID: A104-318)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Check PowerShell Version (VID: A104-322)				Not yet run	⏹ ⬇ ▶
vpa01	protected	Test Lab	windows	Pass: 0 Fail: 0 Incomplete: 10	⏹

Operational Readiness - Endpoint Actors table

Job Status Indicator

An indicator at the top of the Actors tables provides a status of the tests listed in the table based on the greatest severity - Fail, Incomplete, or Passed. Status is indicated by color and a label .

ENDPOINT ACTORS					Fail
Name	Type	Zone	OS	Tested Actions	
vea01	endpoint	Desktop Users	windows	Pass: 0 Fail: 1 Incomplete: 9	⌵
Host CLI - Benign: Check Internet Connectivity in Windows via Command Prompt (VID: A104-320)				2019-5-13 13:25 UTC	⏹ ⬇ ▶
Host CLI - Benign: whoami in Windows via Command Prompt (VID: A104-319)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Batch File Execution via PowerShell (VID: A104-321)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: whoami in Windows via PowerShell (VID: A104-323)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Check Internet Connectivity via PowerShell (VID: A104-324)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: whoami in Bash (VID: A104-325)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Check Internet Connectivity in Bash (VID: A104-327)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Script Execution in Bash (VID: A104-326)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Batch File Execution via Command Prompt (VID: A104-318)				Not yet run	⏹ ⬇ ▶
Host CLI - Benign: Check PowerShell Version (VID: A104-322)				Not yet run	⏹ ⬇ ▶
vpa01	protected	Test Lab	windows	Pass: 0 Fail: 0 Incomplete: 10	⏹

Operational Readiness - Tests Failed

- **Blue:** Pending. Indicates that at least one Job in the table is in a Pending state (see for an example).
- **Green:** Passed. Indicates that all tests passed.
- **Orange:** Incomplete. Indicates that Jobs in the table were not completed or that some tests have not been run.

- **Red:** Fail. Indicates that at least one test failed.

Each Action listed also has a color-coded status in the Tested Actions column. This status updates each time an Action runs, whether from this page, from the Action library, or as part of an Evaluation or Sequence.

Run an Action on the Operational Readiness page

1. Go to **Environment > Operational Readiness**.
2. Click to expand an Actor or Actor Pair in the table.

ENDPOINT ACTORS					Pending
Name	Type	Zone	OS	Tested Actions	
vea01	endpoint	Desktop Users	windows	Pass: 0 Fail: 0 Incomplete: 9 Pending: 1	⌵
Host CLI - Benign: Check Internet Connectivity in Windows via Command Prompt (VID: A104-320)					Waiting... ⚙️ ⏴ ⏵
Host CLI - Benign: whoami in Windows via Command Prompt (VID: A104-319)					Not yet run 🟡 ⏴ ⏵
Host CLI - Benign: Batch File Execution via PowerShell (VID: A104-321)					Not yet run 🟡 ⏴ ⏵
Host CLI - Benign: whoami in Windows via PowerShell (VID: A104-323)					Not yet run 🟡 ⏴ ⏵
Host CLI - Benign: Check Internet Connectivity via PowerShell (VID: A104-324)					Not yet run 🟡 ⏴ ⏵
Host CLI - Benign: whoami in Bash (VID: A104-325)					Not yet run 🟡 ⏴ ⏵
Host CLI - Benign: Check Internet Connectivity in Bash (VID: A104-327)					Not yet run 🟡 ⏴ ⏵
Host CLI - Benign: Script Execution in Bash (VID: A104-326)					Not yet run 🟡 ⏴ ⏵
Host CLI - Benign: Batch File Execution via Command Prompt (VID: A104-318)					Not yet run 🟡 ⏴ ⏵
Host CLI - Benign: Check PowerShell Version (VID: A104-322)					Not yet run 🟡 ⏴ ⏵
vpa01	protected	Test Lab	windows	Pass: 0 Fail: 0 Incomplete: 10	⏴

Expanded row for an Actor

3. Navigate to the Action that you want to run (for example, "Benign File Transfer - Upload of text.txt via HTTP" on a network Actor pair).
4. Click ▶ **Run**.
5. Set runtime parameters as needed then click **Run Now**.



















See [Running Actions \(https://docs.mandiant.com/home/running-actions\)](https://docs.mandiant.com/home/running-actions) for more information.



When you use the default Actors, you are not redirected to the Job Status page. If you use Run Recommended or Run Bulk, you're redirected.

View the Job results for a benign Action

After an Action has completed, you can go directly to its Job page by clicking the timestamp or the status indicator of the Job.

cloud-actor-2	cloud-actor-1	Pass: 1	Fail: 0	Incomplete: 5	
Benign File Transfer - Upload of test.txt via HTTP (VID: A100-363)					2019-5-13 13:38 UTC   
Benign Email Test (VID: A100-367)					Not yet run  Pass  
Benign TCP Scan of Common Ports (VID: A100-365)					Not yet run   
Benign DNS Query - Google.com (VID: A100-364)					Not yet run   
Benign Web Activity - Google.com (VID: A100-366)					Not yet run   
Benign File Transfer - Download of test.txt via HTTP (VID: A100-362)					Not yet run   

Operational Readiness - Go to Job Results



If the Download icon is unavailable, the Job has not completed successfully.

For more information, see [Jobs \(https://docs.mandiant.com/home/msv-jobs\)](https://docs.mandiant.com/home/msv-jobs).

Determine Pass/Fail Results for Benign Actions



The Pass/Fail status displayed on the Operational Readiness dashboard may differ from what is displayed on the Job page. The intent of the dashboard is only to ensure that the test can be run.

The Operational Readiness dashboard reports pass/fail for the two types of benign Actions:


- **Benign Port Scan Action**: Reports as Passed if the Job ran successfully.
- **All other benign Actions**: Reports as Passed if the Job ran successfully and the Job Action was not blocked.

Two other statuses are possible on the Operational Readiness dashboard for benign Actions:

- **Incomplete**: Indicates that the test has not been run.
- **Pending**: Indicates that the test is running but has not yet completed.

To export the Job log for an Action on the Operational Readiness page

After an Action completes, you can export the Job log to a CSV file using the following procedure.

1. Go to **Environment > Operational Readiness**.
2. Navigate to the Action that you want to export in the Endpoint Actors or Network Actors table.
3. Click **Download Job Log**  .