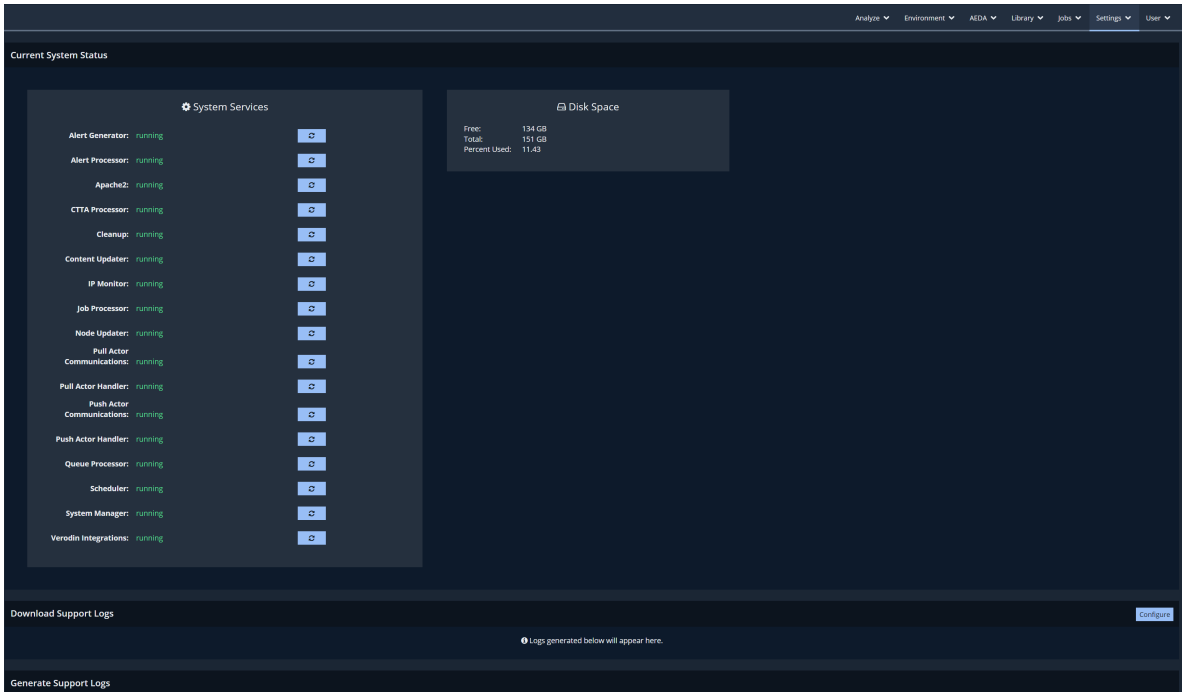


CHECKING SECURITY VALIDATION SYSTEM STATUS AND COLLECTING LOGS

If you want to check Security Validation's system status, view Disk Space usage, or generate support logs, you need to go to the Support Settings page.

Open the Support Settings page

1. Go to **Settings > Director Settings**.
2. Select **Support**.



The screenshot displays the 'Current System Status' page in the MSV (on-prem) Support Settings interface. The page is divided into three main sections:

- System Services:** A list of services with their status and a 'Configure' button. All services are shown as 'running'.
- Disk Space:** A summary of disk usage statistics.
- Support Logs:** A section for downloading and generating support logs.

Service Name	Status	Action
Alert Generator	running	Configure
Alert Processor	running	Configure
Apache2	running	Configure
CTIA Processor	running	Configure
Cleanup	running	Configure
Content Updater	running	Configure
IP Monitor	running	Configure
Job Processor	running	Configure
Node Updater	running	Configure
Pull Actor Communications	running	Configure
Pull Actor Handler	running	Configure
Push Actor Communications	running	Configure
Push Actor Handler	running	Configure
Queue Processor	running	Configure
Scheduler	running	Configure
System Manager	running	Configure
Verodin Integrations	running	Configure

Category	Value
Free	134 GB
Total	151 GB
Percent Used	11.4%

Download Support Logs [Configure](#)

● Logs generated below will appear here.

Generate Support Logs

MSV (on-prem) Support Settings - Current System Services, Disk Space, Support Logs

Analyze ▾ Environment ▾ AEDA ▾ Library ▾ Jobs ▾ Settings ▾ User ▾ Organizations ▾

Download Support Logs Configure

Filename	Includes	# of Days	Generated	Action
verodin_support_log_1652804362_7f3288d2-1f55-408a-b970-2d534769f46d.zip	Actor(s): PAN-Actor-Source-1-New	1	Tue, 17 May 2022 16:19:22 UTC	
verodin_support_log_1652804326_7f3288d2-1f55-408a-b970-2d534769f46d.zip	Actor(s): PAN-Actor-Source-1-New	1	Tue, 17 May 2022 16:18:46 UTC	

🔔 Generating more logs than the maximum will result in deletion of the oldest logs from the Downloads page. Click Configure to change the maximum.
🔔 Maximum support log downloads: 3

Generate Support Logs

Choose Log Options* ⌵

All Actors
 Selected Actors

Include Actor Logs Covering (days): * ⌵

Generate Logs

MA-SV (SaaS) Support Settings - Support Logs only

System services

If you are having issues with the platform, the first thing to check is the status of the system services. If any of the services aren't running, the platform will not function correctly. If you see **error** next to a service, click **restart** . If the service does not switch to **running**, contact **Support** (<https://docs.mandiant.com/home/mandiant-support-cases>). This table contains descriptions for each of the System Services.

Description of Security Validation services

Service	Description
Alert Generator	Processes Monitors (AEDA) to determine if email/syslog messages need to be sent out
Alert Processor	Delivers email/syslog Alert messages for Monitor (AEDA) notifications
Apache2	Web Server used for the Web console of the Director
CTTA Processor	Kicks off the queue actions to have Actors attempt port scans against each other to identify which Actors can communicate
Cleanup	Responsible for the log rotation and general system cleanup of Jobs, files, and other stateful items
Content Updater	Manages content updates. When the Content Service has been enabled, you can click restart on the Support page to check for content updates immediately. Otherwise, the Director checks once an hour after enabling the Content Service without a full restart of the server.
IP Monitor	Checks for IP changes on the Director and updates network values when necessary.
Job Processor	Processes Jobs, Evaluations, and Sequences
Node Updater	Polls Actors for any needed updates on a user-configurable interval
Pull Actor Handler	Part of the web services, handles incoming connections from Pull Actors; Delivers Actions and returns the results to the Director

Service	Description
Push Actor Handler	Handles connecting out to Push Actors to deliver Actions and return the results to the Director
Queue Processor	Processes Upgrades, Updates, CTTA, and other Actor-related processes
Scheduler	In charge of running scheduling and repeating Jobs and Monitors and other scheduled processes
System Manager	Applies security updates (os packages), and checks the updater service
Verodin Integrations	Responsible for the management of the platform's integrations

Disk space usage

As a general administrative action, you may want to see how much disk space is in use by the Director. To do this, review the Disk Space table on the Support Settings page. This table lists the quantity of Free space, Total space (consisting of free + used space), and Percent Used.

The platform performs regular cleanup:



- Unnecessary temporary files are automatically removed from the disk once every 24 hours.
- Old push notifications are automatically removed from the disk every 14 days by default. You can configure the frequency of push notification clean-up in **Advanced Settings**.

Obtain support logs

1. Go to **Settings > Director Settings**. The Systems Settings page opens.
2. Select **Support**.
3. Under **Generate Support Logs**, use the radio buttons to select the appropriate option: Director Only, Director and All Actors, or Director and Selected Actors.
4. In **Include Director Logs Covering (days)**, specify the number of days (from 1 to 30, or All) for which you want to collect support logs. All Job Actions are included in the log for the specified time frame, even for those Actors that have been disabled. Leave the selection at None if you do not need the Job Action Logs.



If you set the number of days to "All" then no Job Action Logs will be included, as this could represent a significant amount of data.

5. Click **Generate Logs**. The logs will populate in the Download Support Logs section.

Download Support Logs
Configure

Filename	Includes	# of Days	Generated	Action
verodin_support_log_1660842572_31257.zip	Director Only	1	Thu, 18 Aug 2022 17:09:32 UTC	
verodin_support_log_1649914392_30125.zip	Director Only	1	Thu, 14 Apr 2022 5:33:12 UTC	
verodin_support_log_1649699220_31933.zip	Director and Actor(s): vna-desktop	all	Mon, 11 Apr 2022 17:47:00 UTC	

Generating more logs than the maximum will result in deletion of the oldest logs from the Downloads page. Click Configure to change the maximum.
 Maximum support log downloads: 3

Generate Support Logs

Choose Log Options* Director Only
 Director and All Actors
 Director and Selected Actors

Include Director Logs

Covering (days): *

Generate Logs

MSV (on-prem) Download and Generate Support Logs view

Long-running migration status

Sometimes a release or patch includes a long-running process, such as updating the Director's database schema. When this occurs, you will see a notification in the release notes. After installation of that release or patch, you can monitor the progress of that process from the Support Settings page.

Long-Running Migration Status

Name	Status	Started At	Completed At	Duration
████████████████████	Completed	2021-03-31 03:39:15 UTC	2021-03-31 03:39:26 UTC	less than a minute
████████████████████	Completed	2022-01-05 15:06:31 UTC	2022-01-05 15:11:11 UTC	5 minutes
████████████████████	Completed	2022-01-05 15:11:11 UTC	2022-01-05 15:11:11 UTC	less than a minute
████████████████████	Completed	2022-07-20 22:06:58 UTC	2022-07-20 22:30:23 UTC	23 minutes

Long-Running Migration Status table in Support Settings