GENERATED SUPPORT LOGS

To assist with troubleshooting, Security Validation support logs are helpful. There are various types of Director and Actor logs available when you create your support logs, as listed in the following tables. See **Checking Security Validation System Status and Collecting Logs (https://docs.mandiant.com/home/msv-support-settings)** for more information on how to collect and download log bundles.

- **Director Support Logs**
- **Actor Support Logs**
- **Integration Support Logs**

Director Support Logs

These logs are supplied if you export a log bundle that includes the Director as part of the log bundle scope.

Log Name	Description
verodin_alert_generator_log	Logs data relating to alerts that are generated from various triggers (for example, AEDA Monitors)
verodin_alert_processor_log	Logs related to the processing of various alerts generated from various triggers (AEDA Monitors). This log should be used with verodin_alert_generator_log
verodin_backup_log	Logs related to the generation of Director backups from the web user interface or API.
verodin_cleanup_log	Logs related to the routine function of the Director checking used disk space, license expiry, and service errors. For example, clearing out "support log downloads" that did not successfully finish generating, unneeded PCAP and hex files, and so on.

Log Name	Description

verodin_content_api_log	Logs messages relating to the Content Service. For every attempt (successful or not) the system makes when requesting a content update, the following messages are logged:
	• Timestamp
	• Destination Endpoint
	• Return Code
	• Return Body (at minimum, if request is not successful)
	
	Examples:
	
	• Timestamp:
	`2022-04-12 14:55:41`
	
	• Destination Endpoint:
	`https://update.validation.mandiant.com`
	
	• Return Code:
	`Response: 500`
	
	• Return Body (at minimum, if request not successful):
	`org_uuid: ca7f4641-230f-4c0b-b541-767b71c2d4b5] INFO 2022-04-12 14:55:45 +0000 content_api Response: 500 ( <html> <head> <title>Internal Server Error</title> </head> <body> <h1><p>Internal Server Error</p></h1> </body> </html> )`
	
	where:
	the HTML is the Response Body

verodin_content_log	Logs messages relating to the content import/export process
verodin_hex_handler_log	Logs error messages logged when generating hex from a PCAP
verodin_integration_dispatch_log	Contains logging that describes the starting and stopping of the Integrations service.
verodin_integration_utils_log	Contains logging around utilities that facilitate the function of Integrations (for example, tiny_tds)

Log Name	Description
verodin_jobs_log	Logs messages related to running jobs, including preparing jobs, sending action definitions to Actors, and checking job status
verodin_log_generator_log	Logs data when a user generates a support log download
verodin_migrations_log	Logs messages relating to migrations that ran, typically when updating director
verodin_node_log	Logs messages related to communications between the Director and Actors, including timeouts and errors on calls to Actors
verodin_node_info_handler_log	Contains logging around the updating of Network Info and CTTA Update processes.
verodin_notifications_log	Logs information about notifications that get sent from the director as a result of an alert being triggered
verodin_pcap_log	Logs information relating to uploading a PCAP into Director - primarily if any errors occurred
verodin_python_hex_log	Logs errors that occur due to invalid HTTP traffic when creating an Action from a PCAP
verodin_queue_log	Logs Actor calls and messages
verodin_schedule_log	Logs messages related to scheduling Jobs and Monitors. This log is only for the creation of the scheduled items; when Jobs are run, the logging goes to verodin_jobs_log.
verodin_sectech_log	Logs information regarding about what security technologies are found on Actors
verodin_shared_utils_log	Logs information with tools that are run in the background. Examples include commands that run when a PCAP is uploaded into the system.
verodin_system_log	Logs general system information
access_log, error_log	Logs messages from the Apache web server on Director. The access.log will only log request URLs, time, response status codes, and user-agent strings.
audit.log	Logs generated by the Linux Audit system when, which include SELinux violations, among other entries
config.enc	Encrypted Director configuration
development.log	Logs requests from and responses to the Director, templates rendered (for UI), SQL database calls, and Validation Platform-specific logging

Log Name	Description
Logs per integration service (for example, verodin_mcafee_log, verodin_splunk_test_log)	Logs messages from each integration service. See **Integration Support Logs** for more information.
production.log	Logs requests from and responses to the Director; indicates which templates were rendered and which parameters were sent with each request
verodin_actor_pull_comms_log	Log messages from the Director service responsible for communicating with pull actors
verodin_actor_push_comms_log	Log messages from the Director service responsible for communicating with push actors

Actor Support Logs

These logs are supplied if you export a log bundle that includes one or more Actors as part of the log bundle scope. These files are stored on the local file system of the selected Actors and are pulled by the Director as part of the log bundle generation process.

Log Name	Description
dmesg	Contains information that corresponds to the output of running `dmesg` on a given Actor.
messages	Contains information that corresponds to the content of /var/log/messages on a given Actor.
/var/log/nginx/access.log, /var/log/nginx/error.log	Logs for Nginx web server on the Actor
verodin_backend	Logs messages for Actor backend processes
verodin_integration_dispatch_log	Contains logging that describes the starting and stopping of the Integrations service for Remote Integrations.
verodin_network_monitor	Logs messages related to DHCP updates for the Actor, such as like notifying Director when the Actor's IP address has changed
verodin_node_web	(Push Actors) Logs messages between the Actor and Director
verodin_pull_check	(Pull Actors) Logs messages between the Actor and Director
verodin_upgrade_migration	On Protected Theaters, contains information related to the upgrade of the networking backend and crypto libraries.
verodin_vsetnet	Contains logging related to the restarting or reloading of nginx and sshd on Network Actors.

Log Name	Description
verodin_*INTEGRATION_NAME*_log	Logs with this format contain information around remote integrations hosted by the given Actor.
verodin_updater_log	Logs information related to the upgrade of Security Validation software on a Windows actor.
node_settings.conf	Actor settings file
node_version	Contains Actor version
server_settings.json	Contains port and protocol information
settings.json	Contains Actor information such as capabilities, OS, hostname, Director IP
upgrade_results.json	Contains status information for Actor upgrades.

Integration Support Logs

This table covers logs that are specific to a given integration. These logs are supplied if the following criteria are met:

- You export a log bundle that includes the Director as part of the log bundle scope
- That Director is configured with the given integration

Log Name	Description
verodin_splunk_log	Standard log file for the Splunk integration
verodin_symantec_dlp_log	Standard log file for the Symantec DLP integration
verodin_logrhythm_log	Standard log file for the LogRhythm integration
verodin_endgame_log	Standard log file for the Endgame integration
verodin_fireeye_log	Standard log file for multiple Trellix (formerly FireEye) integrations (CMS, NX, and so on.)

Log Locations

If you need to manually browse to the Director or Actor logs on the file system, reference the following paths to locate these logs.

Platform Component	Logs Location
Director	`/opt/apps/verodin/planner/log/`
Linux Actors	`/opt/apps/verodin/node/log/`
Linux Actors with Remote Integrations	`/opt/apps/verodin/integrations/log/`

Platform Component	Logs Location
Windows Actors	C:\Program Files\Verodin\node\log\