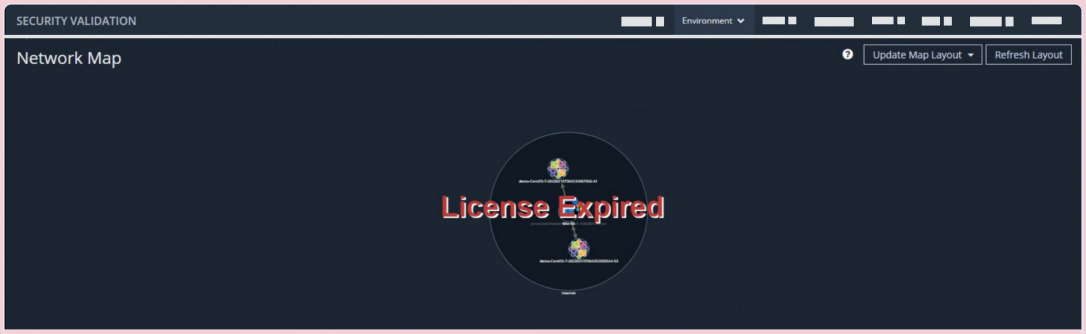
PRODUCT UPDATE 4.10.1.0 - FEBRUARY 14, 2023

If you're on a Mandiant Security Validation (MSV) release prior to 4.12.1.0, you may notice that a license expired watermark appears on the Network Map page on your Director.



Network Map Page with License Expired Watermark on an MSV Director

This watermark is related to the software that renders the Network Map and does not affect functionality of the product.
Use one of the following options to fix the watermark issue permanently:

- Update to the latest release (4.12.1.0 or later) or migrate to Mandiant Advantage Security Validation (MA-SV).
- As an additional option, you can upgrade to release 4.12.0.1, which provides a fix for this issue and if you need more time to complete the update to 4.12.1.0 or later.

MSV 4.10.2.2 contains defect resolutions and a critical security fix. We recommend you apply that update as soon as reasonably possible. If you're unable to upgrade at this time, use the instructions in **Manage User Admin Account (https://docs.mandiant.com/home/manage-user-admin-account)** to either set a password for the account or disable the account if it's not being used.

The Mandiant Security Validation (MSV) team is pleased to announce version 4.10.1.0 of the MSV platform.

General Enhancements

- Added Network Run-As feature

  All Actors need to be updated to 4.10.1.0 to use this feature.

- Added support for MSV (on-prem) to MA-SV (SaaS) migrations using the MA-SV Migration Tool
- Added option to include Actor information in Splunk base event queries to improve performance
- Updated Threat Intel API calls to latest versioning
- Email Theater Actions now report SMTP ID of emails sent by Jobs
- Added support for MITRE ATT&CK version 12.1
- Added support for Credential Cache for proxy configurations
- Enhanced file cleanup of the planner/tmp directory to improve performance
- Improved memory utilization for several processes to improve Director performance

Bug Fixes

- Fixed an issue where the heat map API documentation referenced incorrect field names
- Fixed an issue where the listed AEDA last run monitor was incorrect

- Fixed an issue that resulted in an incorrect status for Host CLI jobs run against French endpoints
- Fixed an issue where Windows Endpoint Actors were not always updating IP information in Director
- Fixed an issue regarding Host CLI timeout behavior
- Fixed an issue where Daylight Savings introduced a one-hour time skew for some jobs
- Fixed an issue where an Internal Server Error occurred when running some Evaluations
- Fixed an issue that caused bulk registration tokens to expire
- Improved DNS matching for some Evaluations
- Fixed an issue where Host CLI commands would disappear or be modified with cleanup
- Fixed an issue where AEDA webhook variable expansion was not JSON compliant
- Fixed an issue where Host CLI actions would error when run as an Active Directory user
- Fixed an issue where the Chronicle integration was missing the ability to select between version 1 and 2 for on-prem Directors
- Fixed an issue that caused Protected Theater Evaluations to error out after partial completion
- Fixed an issue where some security technologies would stop communicating with Protected Theater
- Fixed an issue where integration queries were being erroneously replicated and causing memory problems
- Fixed an issue where Actor communications were being interrupted by cleanup processes
- Made various improvements to MSFT Graph API calls
- Fixed an issue where SAML login was not working with Azure AD
- Fixed an issue where the date/time filter on the Jobs page would incorrectly work for “Today”
- Fixed an issue where integration events weren't matching to “updateTime”
- Improved Operational Status Graph performance and long load times
- Additional minor bug fixes and improvements

API Changes

- Creating an Action
  - JSON body: `sim_action.email_action_attributes.email_action_file_transfer_libraries` changed from required to optional (this field only applies to Email Actions)
  - Example payloads for Actions include: DNS, File Transfer, Host CLI, and Cloud
  - `POST /manage_sims/actions`
- Action User Profiles
  - `DELETE /action_user_profiles/:id`
  - Added error handling. On error cases, the json returned will be `{ result: 'error' }`

Known Issues

- There is a known issue where creating an AEDA monitor between zones, for a network action using a non-admin Action User Profile, can result in Actions being run on unsupported Actors.

Appliance OS Security Update

The Mandiant Advantage Security Validation Product team would like to announce the availability of a security update for the platform. This security update applies to Directors, Actors, and Protected Theaters that are virtual appliances.

Mandiant uses **Red Hat’s security ratings (https://access.redhat.com/security/updates/classification)** to determine the criticality of vulnerabilities identified and resolved. This rating system is a combination of a four-point scale and the Common Vulnerability Scoring System (CVSS) base scores. The criticality of the vulnerabilities resolved are listed below.

	Director	Actor	Protected Theater
Critical	0	0	0

	Director	Actor	Protected Theater
High	2	2	7
Medium	1	1	2
Low	0	0	0

Details for the vulnerabilities against the Director are as follows:

- CentOS 7: kernel (CESA-2023:0399)
- CentOS 7: sudo (CESA-2023:0291)
- CentOS 7: bind (CESA-2023:0402)

Details for the vulnerabilities against the Actor are as follows:

- CentOS 7: kernel (CESA-2023:0399)
- CentOS 7: sudo (CESA-2023:0291)
- CentOS 7: bind (CESA-2023:0402)

Details for the vulnerabilities against the Protected Theater are as follows:

- CentOS 7: firefox (CESA-2023:0296)
- CentOS 7: kernel (CESA-2023:0399)
- CentOS 7: libXpm (CESA-2023:0377)
- CentOS 7: sssd (CESA-2023:0403)
- CentOS 7: sudo (CESA-2023:0291)
- CentOS 7: tigervnc (CESA-2023:0045)
- CentOS 7: xorg-x11-server (CESA-2023:0046)
- CentOS 7: bind (CESA-2023:0402)
- CentOS 7: java-1.8.0-openjdk (CESA-2023:0203)

Important Installation Notes

- Minimum Director version 4.7.0.2 or higher is required to upgrade to version 4.10.1.0.
- Actor Compatibility. Actors must be upgraded to at least version 4.6.0.0 before updating their Director to 4.8.4.1.

To download documentation and software (appliance images, installers, and update packages) visit the **Validation Section of the Docs Portal (https://docs.mandiant.com/home/security-validation-on-prem-and-saas)**. For full details on how to upgrade, see **Updating Security Validation Components (https://docs.mandiant.com/home/msv-system-updates)**.