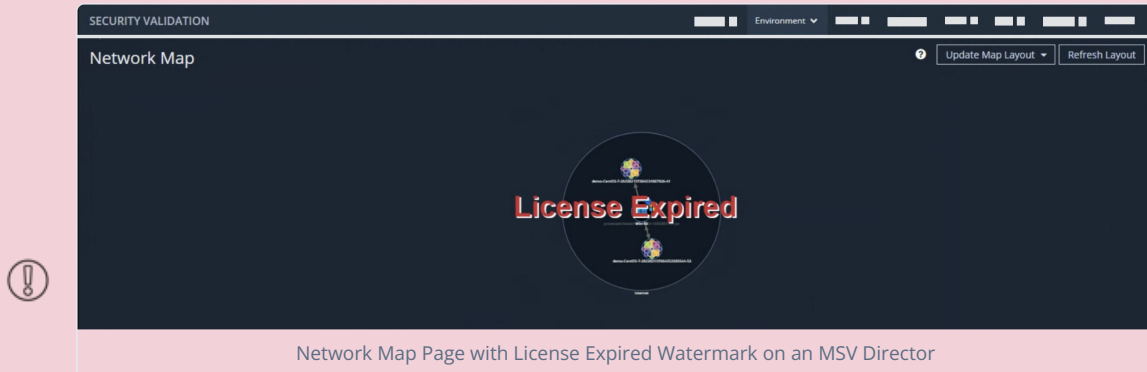


PRODUCT UPDATE 4.10.2.0 - MARCH 13, 2023

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.



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 \(https://docs.mandiant.com/home/manage-user-admin-account\)](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 4.10.2.0 of the MSV platform.

General Enhancements

- Additional improvements for Director memory usage to improve Director performance during upgrades and operation
- Users can now select Protected Action Types as a rule in Report Builder
- Provide a Director Installer option for privileged command escalation
- Cloud actions are now supported on Amazon Linux 2 Actors
- Added capability to complete a test, read-only run for MSV (on-prem) to MA-SV (SaaS) migrations in the MA-SV Migration Tool

Bug Fixes

- Fixed an issue when dzdo was used instead of sudo for Director or Actor installs
- Fixed an issue where Protected Theater snapshots were not updating on some Directors
- Fixed an issue where some Actions caused an error in the Job Processor
- Fixed an issue that prevented importing a new gold image OVA over existing Protected Actors
- Fixed an issue where NTP settings were not being properly applied to Network Actors when registering
- Fixed an issue where Defender ATP events were having issues inside of Protected Theater
- Fixed an issue where Splunk queries were not consistently working with Protected Theater
- Fixed an issue with Evaluation S100-081 that prevented being able to select an Endpoint Actor

- Fixed an issue where users were unable to see or delete their custom Evaluation
- Fixed an issue where the Job Status Page reporting did not display the correct errored group number
- Fixed an issue where users were unable to create a system backup of their Director
- Fixed an issue where Run Again was not properly working with Email Actions
- Additional minor bug fixes and improvements

API Changes

There are no API changes since the previous release.

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 latest platform security update can always be found on [Security Patch Downloads](#) (<https://docs.mandiant.com/home/msv-security-update-downloads>). This security update applies to all versions of the product.

Important Installation Notes

- Minimum Director version 4.8.4.0 or higher is required to upgrade to version 4.10.2.0.

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>).