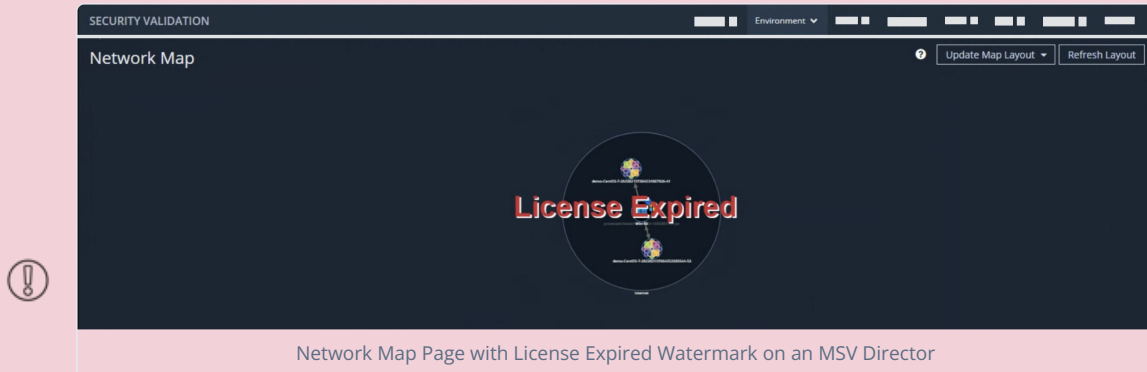


## PRODUCT UPDATE 4.11.1.0 - JULY 31, 2023

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.

The Mandiant Security Validation (MSV) team is pleased to announce version 4.11.1.0 of the MSV platform.

### General Enhancements

- Added support for Red Hat Enterprise Linux 8 Director installs. See the known issues section that follows for more information.
- Added ability to create a filter in Report Builder based on VID. This function allows users to create reports based on specific Actions.
- Added APIs for the following functionality:
  - Get the list of available OS security patches in the Director
  - Delete the list of available OS security patches in the director
  - Apply Security Updates to Actors
- Improved Integrations service reliability
- Improved Evaluations Library page loading performance
- Added support for PostgreSQL 13 for the external database
- Improved the MA-SV (Mandiant Advantage-Security Validation) Actor Migration Tool performance when Actor IDs are selected through the CLI
- Security enhancements

### Bug Fixes

- Fixed an issue where selecting the Events Box from the Jobs view would open a blank Job Status page
- Fixed an issue where event matching was not considering Virtual Addresses
- Fixed an issue where the correct count of Jobs on the Actor page was not displayed when "Run Recommended" was selected
- Fixed an issue where "Run-Ad-Hoc" was not honoring proxy settings and reverting to the default setting
- Fixed an issue where TAAM was referencing FireEye instead of Mandiant and updated the logo

- Fixed an issue where Director was allowing users to select actors for Captive IOC actions when the TAAM license is not enabled or purchased
- Fixed an issue where the product was not pulling correlated events for QRadar offenses
- Fixed an issue with the test integration query for Securonix SNYPR was not working
- Fixed an issue where the dialog window was not appearing when users tried to access the hyperlink of a VID's name from Library > Threat actors
- Fixed an issue where users were unable to create/save new Splunk Integrations
- Fixed an issue where errors would occur when attempting to configure director email to use the Gmail API

### Known Issues

- The Multisite Reporting feature and Preview Integrations service are not working properly with new RHEL8 Directors. We are working to resolve this issue as soon as possible.

### Appliance OS Security Update

The latest platform security update can always be found on the [Validation Section of the Docs Portal](#) (<https://docs.mandiant.com/home/msv-security-patch-downloads>). This security update applies to all versions of the product and is cumulative.

### Important Installation Notes

Minimum Director version 4.9.0.0 or higher is required to upgrade to version 4.11.1.0.