Mandiant

PRODUCT UPDATE 4.14.7.0 - AUGUST 4, 2026

The Mandiant Security Validation (MSV) team is pleased to announce version 4.14.7.0 of the MSV platform.

Enhancements

- Added the option to set a default landing page (such as the Topology Map) upon sign in, improving load times for users who prefer to bypass the initial Simulations page.
- For Windows 10/11, added support for TPM 2.0 on Protected Theater.
- Added the ability to hide unselectable actors from the user interface, streamlining the actor selection process when running actions.
- Improved system memory efficiency and performance when downloading or exporting large datasets—including attachments, assessments, Bulk Job results, and suspect events.
- Enhanced the scaling and responsiveness of the Jobs interface through optimizations, including batched loading and database aggregation for event lists.

Bug fixes

This release includes a number of bug fixes and stability improvements. Key fixes are categorized as follows:

Actor and integration stability

- Fixed an intermittent issue where Actors would fail to execute actions and enter a polling loop after certain upgrades.
- Fixed an issue where in the Protected Actor environment, a Windows Actor did not appear in the select Endpoint Actor menu when running an action.
- Resolved connection stream errors that could occur when running certain actions.
- Corrected an error when retrieving Integration service statuses on updated Directors.
- Addressed time synchronization issues on Protected Actors that could interfere with accurate detection reporting.
- Prevented system instability that was caused by multiple asynchronous reboot or shutdown jobs being sent concurrently.

Security and authentication

- Addressed potential Cross-Site Request Forgery (CSRF) vulnerabilities to improve platform security.
- Updated the underlying Nginx component to address CVE-2026-1642.
- To help reduce exposure to Perl-related vulnerabilities, removed the Perl interpreter and associated packages from Director and Protected Theater appliances This removal reduces the system footprint and does not impact platform functionality.

Web interface

- Fixed an issue where events on jobs were being displayed in reverse chronological order rather than the correct chronological order.
- Resolved a date-offset issue where the SecOps integration test feature would query data from the previous day instead of the configured test date.
- Resolved an issue where the web interface could become inaccessible after updating NTP settings.

Known issues

- Local Event Filtering works as expected but is limited to Match Action, Match Integration, and Match Events (when the latter involves Raw Events). If a rule has a Match Event condition for any field other than Raw Event, the rule does not apply to Local Events. It only applies to events from standard local integrations in MSV.
- Network configuration may reset unexpectedly. To resolve the issue, run `vsetnet` after the upgrade with static IP addresses for one or more interfaces.

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 4.14.0.0 or higher is required to upgrade to version 4.14.6.1.

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).

Failed upgrade from Director web interface

If your Director fails to upgrade to this version after you attempt the upgrade from the web interface, check **Troubleshoot failed upgrades** (https://docs.mandiant.com/home/msv-failed-upgrade-41450) for additional self-help tips. That document contains which log file to check, for what specific content, and how to use the provided script to fix the issue.