

Release Notes

FortiSIEM 6.3.3



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



08/15/2022

FortiSIEM 6.3.3 Release Notes

TABLE OF CONTENTS

- Change Log 4**
- What's New in 6.3.3 5**
 - New Features 5
 - Windows Discovery, Monitoring and Log Collection via OMI 5
 - Bug Fixes and Enhancements 5
 - Known Issues 6
 - Shutting Down Hardware 6
 - Linux Agent 6
 - Elasticsearch Based Deployments Terms Query Limit 6

Change Log

Date	Change Description
12/22/2021	Initial version of FortiSIEM 6.3.3 Release Notes.
05/12/2022	Added Known Issue Elasticsearch Based Deployments Terms Query Limit to Release Notes.
08/15/2022	Add Known Issue to 6.3.x Release Notes.

What's New in 6.3.3

This release includes a new feature, fixes, enhancements, and known issue.

- [New Features](#)
- [Bug Fixes and Enhancements](#)
- [Known Issues](#)

New Features

- [Windows Discovery, Monitoring and Log Collection via OMI](#)

Windows Discovery, Monitoring and Log Collection via OMI

This release adds Windows OMI method for discovery, monitoring and log collection for Windows Servers. Windows OMI can be used in cases where WMI has stopped working because of Microsoft Security Update KB5005573. (Bug 749146)

Windows OMI works just like WMI. In **ADMIN > Setup > Credentials**, choose OMI instead of WMI as the **Access Protocol**. Then all the relevant information, performance metrics and logs are collected as in WMI. The command line utility is `omic` instead of `wmic`, but the arguments are the same. The event types are identical except `PH_DEV_MON_WMI_PING_STAT` has analogous `PH_DEV_MON_OMI_PING_STAT`. All rules, reports and dashboards are modified if needed. Windows host names are now in FQDN format and existing servers will have the new name after re-discovery via OMI. OMI has been tested to run on all WMI supported servers. In addition, OMI works for Microsoft Windows Server 2022 while WMI does not.

Note: If FortiSIEM is set up in FIPS mode, then OMI based communication between FortiSIEM and Windows servers will not work. This is because current OMI code uses NTLM authentication via RC4 encryption which is not FIPS compliant. In future releases, Kerberos based authentication may be used to make it work in FIPS mode.

For details on OMI, see <https://github.com/microsoft/omi>.

Bug Fixes and Enhancements

1. Fix of the Log4J Remote command execution vulnerability ([CVE-2021-44228](#)). This is done by upgrading the log4j-core version to 2.17 for use by SVNLite module and deleting the appropriate log4j-core versions 2.13 and 2.6 from the system. These file deletions do not impact functionality, except potentially the logging functionality in the 3rd party ThreatConnect SDK, which will be upgraded at a later date. If you have already applied the CVE-2021-44228 mitigations recommended in 6.3.2 and earlier release notes, then you can safely upgrade to FortiSIEM 6.3.3.
2. Upgrade CentOS version to 8.5 to include more security fixes.

The fixes are listed here:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/

https://docs.rockylinux.org/release_notes/8-changelog/

3. Support for Windows OMI method for discovery, monitoring and log collection for Windows Servers. Windows OMI can be used in cases where WMI has stopped working because of Microsoft Security Update KB5005573. (Bug 749146)
4. Support for Windows 2022 discovery, monitoring and log collection via OMI. WMI does not work for Windows 2022 because of Microsoft Security Update KB5005573. (Bug 748011)
5. Report Bundle with duration 90 days does not produce results. (Bug 768020)
6. Fix the [slow upgrade issue](#) mentioned in [6.3.2 release notes](#). If you are running an earlier version other than 6.3.2, then you will not see the issue while upgrading to 6.3.3. (Bug 768720)

Known Issues

Shutting Down Hardware

On hardware appliances running FortiSIEM 6.6.0 or earlier, FortiSIEM `execute shutdown` CLI does not work correctly. Please use the Linux `shutdown` command instead.

Linux Agent

Linux Agent does not work for this release. Since Linux Agent is not vulnerable to log4j vulnerability ([CVE-2021-44228](#)), you can keep using Linux Agents from earlier versions (6.3.2 or earlier) to work with the Supervisor, Workers and Collectors in version 6.3.3. In other words:

- For 6.3.3 fresh install environments, use 6.3.2 Linux Agents.
- For upgrade situations, upgrade the Supervisor, Workers and Collectors to 6.3.3, but do not upgrade Linux Agents.

Elasticsearch Based Deployments Terms Query Limit

In Elasticsearch based deployments, queries containing "IN Group X" are handled using Elastic Terms Query. By default, the maximum number of terms that can be used in a Terms Query is set to 65,536. If a Group contains more than 65,536 entries, the query will fail.

The workaround is to change the "max_terms_count" setting for each event index. Fortinet has tested up to 1 million entries. The query response time will be proportional to the size of the group.

Case 1. For already existing indices, issue the REST API call to update the setting

```
PUT fortisiem-event-*/_settings
{
  "index" : {
    "max_terms_count" : "1000000"
  }
}
```

Case 2. For new indices that are going to be created in the future, update fortisiem-event-template so those new indices will have a higher max_terms_count setting

1. `cd /opt/phoenix/config/elastic/7.7`
2. Add `"index.max_terms_count": 1000000` (including quotations) to the "settings" section of the `fortisiem-event-template`.

Example:

...

```
"settings": {  
  "index.max_terms_count": 1000000,  
  ...  
}
```

...

3. Navigate to **ADMIN > Storage > Online** and perform **Test** and **Deploy**.
4. Test new indices have the updated terms limit by executing the following simple REST API call.
`GET fortisiem-event-*/_settings`



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.