FortiSIEM - Release Notes

Version 6.1.1

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 6.1.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
11/11/2020	Initial version of FortiSIEM 6.1.1 Release Notes
01/29/2021	Updated Known Issues - Migration limitations.
02/19/2021	Added Known Issues - bug discovery.
04/28/2021	Updated FortiSIEM 6.1.0 Release Notes - Installation Notes for ESX.
12/14/2021	Added Known Issues - Remediation Steps for CVE-2021-44228 to 6.x Release Notes.
05/12/2022	Added Known Issue - Elasticsearch Based Deployments Terms Query Limit.
08/15/2022	Added Known Issue - Shutting Down Hardware.

Introduction

FortiSIEM provides an all-in-one, seamlessly integrated and service-oriented IT infrastructure monitoring solution that covers performance, availability, change, and security monitoring aspects of network devices, servers, and applications.

This document describes the new and enhanced features for the 6.1.1 release. It also provides a list of resolved issues.

What's New in 6.1.1

This document describes new and enhanced features, bug fixes and device support for the FortiSIEM 6.1.1 release.

- New Features
- Installation and Usage Notes
- Upgrade Overview
- Known Issues
- Bug Fixes and Enhancements
- New Device Support

New Features

- Install and Upgrade on Microsoft Azure
- Migration for FortiSIEM Running on Elasticsearch

Install and Upgrade on Microsoft Azure

FortiSIEM 6.1.1 can be installed on Azure – see here. See the Upgrade Overview section for upgrading from older versions.

Migration for FortiSIEM Running on Elasticsearch

While FortiSIEM 6.1.0 can be installed fresh on Elasticsearch based deployments, installations running on the 5.3.2 version or earlier could not be migrated to 6.1.1 because of a bug. This release fixes that issue. See the Upgrade Overview section for more details.

Installation and Usage Notes

- Starting with 6.1.1, Windows UEBA Enablement does not require manual restart of `phFortiInsight` module. To enable UEBA, you must complete the following steps:
  - **a.** Install Windows 4.0.0. The procedures are identical to Windows 3.3.0 and can be found in Configuring Windows Agent.
  - **b.** Install a new FortiSIEM license which contains UEBA telemetry.
  - **c.** Create a monitoring template with UEBA enabled for the Agent and click **Apply**. You can create a single template for many hosts. For details on UEBA settings, refer to Define the Windows Agent Monitor Templates. Then in the CMDB tab, the Agent type becomes Windows + UEBA.
  - **d.** The windows Agent will start sending UEBA telemetry to FortiSIEM.

- During install or upgrade, FortiSIEM only needs to communicate to two external sites maintained by Fortinet: os-pkgs-cdn.fortisiem.fortinet.com and os-pkgs.fortisiem.fortinet.com to get the latest updates via HTTPS.
- Starting in 6.1.1, adhoc reports run from GUI and scheduled reports may time out after running for a long time. In a cluster environment with Worker nodes, the user may see partial results (indicated in the PDF), if some workers are able to finish their queries within the timeout. The default timeouts are specified (in seconds) in the `phoenix_config.txt` file on the Supervisor node.

  ```
  [BEGIN phQueryMaster]
  ...
  interactive_query_timeout=1800 # 30 mins
  ...
  scheduled_query_timeout=3600 # 60mins
  ...
  [END]
  ```

  To change the default timeout values, SSH to the Supervisor node, change the values, save the file, and restart the Query Master process.

Upgrade Overview

The following sections provide an overview of migration and upgrade instructions to the 6.1.1 release.

- Migrate from pre-5.3.0 to 6.1.1
- Migrate from 5.3.x or 5.4.x to 6.1.1
- Upgrade from 6.1.0 to 6.1.1
- Upgrade via Proxy
- Post Migration Health Check

Migrate from pre-5.3.0 to 6.1.1

1. Upgrade Supervisor to 5.4.0:
   a. Delete Workers from Supervisor.
   b. Upgrade Supervisor to 5.4.0: follow the instructions here.
   c. Perform health check: log on to the Supervisor and make sure that it is displaying the correct version and all processes are up.
2. Migrate to 6.1.1:
   a. Migrate the Supervisor from 5.4.0 to 6.1.1. Migration is platform-specific.
      - ESX
      - AWS
      - Azure
      - Hyper-V
      - KVM
   b. If you are using Elasticsearch, then go to **ADMIN > Setup > Storage > Elasticsearch** and click **Test and Save**.
   c. Install new 6.1.1 Workers and add them back to the Supervisor.
   d. Go to **ADMIN > Settings > Event Worker** and **Query Worker** and make sure that they are correct.
   e. Perform health checks. Old Collectors and Agents should work with 6.1.1 Supervisor and Workers.

3. When you are ready to upgrade Collectors to 6.1.1, then do the following (details are in the documents listed in Step 2a):
   a. Copy the HTTP (hashed) passwords file from the old Collectors to the new Collector.
   b. Re-register with the update option and the same IP.
4. Perform health checks. See Post Migration Health Check.
5. Reinstall the Agents with the latest version when you are ready to upgrade them.
6. Perform health checks: make sure Agent events are being received.

Migrate from 5.3.x or 5.4.x to 6.1.1

1. Delete Workers from the Supervisor.
2. Migrate the Supervisor to 6.1.1:
   a. Migration is platform specific.
      - ESX
      - AWS
      - Azure
      - Hyper-V
      - KVM
   b. If you are using Elasticsearch, then go to **ADMIN > Setup > Storage > Elasticsearch** and click **Test and Save**.
   c. Install new 6.1.1 Workers and add them back to the Supervisor.
   d. Go to **ADMIN > Settings > Event Worker** and **Query Worker** and make sure that they are correct.
   e. Perform health checks. Old Collectors and Agents should work with 6.1.1 Supervisor and Workers.
3. When you are ready to upgrade Collectors to 6.1.1, then do the following (details are in the documents listed in Step 2a):
   a. Copy the HTTP (hashed) passwords file from the old Collectors to the new Collector.
   b. Re-register with the update option and the same IP.
4. Perform health checks. See Post Migration Health Check.
5. Reinstall the Agents with the latest version when you are ready to upgrade them.
6. Perform health checks: make sure Agent events are being received.

Upgrade from 6.1.0 to 6.1.1

1. Copy the `upgrade.py` script to the Supervisor. For instructions, see the *Pre-Upgrade* steps in the Upgrade Guide.
2. Upgrade the Supervisor to 6.1.1:
   - EventDB (local or NFS) case:
     i. Stop Workers.
     ii. Upgrade the Supervisor to 6.1.1.
   - Elasticsearch case:
     i. Delete Workers.
     ii. Upgrade the Supervisor to 6.1.1.
     iii. Go to **ADMIN > Setup > Storage > Elasticsearch** and click **Test and Save**.
3. Upgrade Workers to 6.1.1:
   - EventDB (local or NFS) case:
     i. Upgrade 6.1.0 Workers to 6.1.1.

- Elasticsearch case:
  1. Install new 6.1.1 Workers and add them back to the Supervisor.
  2. Go to **ADMIN > Settings > Event Worker** and **Query Worker** and make sure that they are correct.
4. Perform health checks: old Collectors should work with 6.1.1 Super and Workers.
5. When you are ready to upgrade Collectors to 6.1.1:
   - Pre-6.1.0 Collectors (details are in Upgrade Guide):
     1. Copy the HTTP (hashed) passwords file from old Collectors to the new Collector.
     2. Re-register with update option and the same IP.
   - 6.1.0 Collectors:
     1. Upgrade from the GUI.
6. Perform health checks. See Post Migration Health Check.
7. Reinstall the Agents when you are ready to upgrade them.
8. Perform health checks: make sure Agent events are being received.

Upgrade via Proxy

During upgrade, Super/Worker and Hardware appliances FSM-2000F and 3500F must be able to communicate with CentOS OS repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs.fortisiem.fortinet.com`) hosted by Fortinet, to get the latest OS packages. Follow these steps to set up this communication via proxy, before initiating the upgrade.

1. SSH to the node.
2. Edit `/etc/yum.conf` as follows:
   - If your proxy does not require authentication, then add a line like this:
     - `proxy=http://<proxy-ip-or-hostname>:<proxy-port>`
   - If your proxy requires authentication, then add `proxy_username=` and `proxy_password=` entries as well. For example, for squid proxy:
     - `proxy_username=<user>`
     - `proxy_password=<pwd>`
3. Test that you can use the proxy to successfully communicate with the two sites: `os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs.fortisiem.fortinet.com`.
4. Begin the upgrade.

Post Migration Health Check

1. Check Cloud health and Collector health from the FortiSIEM GUI:
   - Versions display correctly.
   - All processes are up and running.
   - Resource usage is within limits.
2. Check that Redis passwords match on Super and Workers:
   - Super: run the command `phLicenseTool -showRedisPassword`.
   - Worker: run the command `grep -i auth /opt/node-rest-service/ecosystem.config.js`.
3. Check that database passwords match on Super and Workers:
   - Super: run the command `phLicenseTool -showDatabasePassword`.
   - Worker: run the command `grep Auth_PQ_dbpass /etc/httpd/conf/httpd.conf`.

4. Elasticsearch case: check the Elasticsearch health
5. Check that events are received correctly:
   a. Search All Events in last 10 minutes and make sure there is data.
   b. Search for events from Collector and Agents and make sure there is data. Both old and new collectors and agents must work.
   c. Search for events using CMDB Groups (Windows, Linux, Firewalls, etc.) and make sure there is data.
6. Make sure there are no SVN authentication errors in CMDB when you click any device name.
7. Make sure recent Incidents and their triggering events are displayed.

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.

Remediation Steps for CVE-2021-44228

Two FortiSIEM modules (phFortiInsightAI and 3rd party ThreatConnect SDK) use Apache log4j version 2.11 and 2.8 respectively for logging purposes, and hence are vulnerable to the recently discovered Remote Code Execution vulnerability (CVE-2021-44228) in FortiSIEM 6.1.x.

These instructions specify the steps needed to mitigate this vulnerability without upgrading Apache log4j to the latest stable version 2.16 or higher. Actions need to be taken on the Supervisor node only.

On Supervisor Node

1. Logon via SSH as root.
2. Mitigating 3rd party ThreatConnect SDK module:
   a. Delete these log4j jar files under `/opt/glassfish/domains/domain1/applications/phoenix/lib`
      i. log4j-core-2.8.2.jar
      ii. log4j-api-2.8.2.jar
      iii. log4j-slf4j-impl-2.6.1.jar
3. Mitigating phFortiInsightAI module:
   a. Delete these log4j jar files under `/opt/fortiinsight-ai/lib/`
      i. log4j-api-2.11.1.jar
      ii. log4j-core-2.11.1.jar
4. Restart all Java Processes by running: `“killall -9 java”`

Migration and Fresh Install Limitations

1. Migration limitations: If migrating from 5.3.3 or 5.4.0 to 6.1.1, please be aware that the following features will not be available after migration.

   a. Pre-compute feature
   b. Elastic Cloud support

   If any of these features are critical to your organization, then please wait for a later version where these features are available after migration.

2. Fresh Install limitations:
   a. Can not be installed on Alibaba Cloud.
   b. Linux ISO image is not available.
   c. Does not install on IPV6 networks .
   d. Collector to Supervisor/Worker communication via Proxy is not supported.
   e. Disaster recovery is not supported as PostGreSQL BDR is not yet available on the CentOS 8.2 release.
   f. Report Server is not supported.
3. STIX/OTX Malware IOC Integration Error: If you see the error below when you log in to Glassfish, it is likely caused by the `jsse.enableSNIExtension` flag that was added to resolve a `httpd` issue in Java JDK 7. In JDK8, there is no need to set this flag.

   Error:

   ```
   #|2020-09-
   10T12:30:00.535+0200|SEVERE|glassfish3.1.2|com.accelops.service.threatfeed.BaseOTXU
   pdateService|_ThreadID=218;_ThreadName=Thread-
   2;|org.springframework.web.client.ResourceAccessException: I/O error on GET request
   for "https://otx.alienvault.com/api/v1/pulses/subscribed?limit=20&modified_
   since=2020-09-03T12:30:00%2B02:00&":Unsupported record version Unknown-0.0; nested
   exception is javax.net.ssl.SSLException: Unsupported record version Unknown-0.0
   ```

   To resolve this issue, follow these steps:
   a. Log in to the Supervisor node.
   b. Run the command `su - admin`.
   c. Enter your Glassfish password and run this command `/opt/glassfish/bin/asadmin delete-jvm-options -Djsse.enableSNIExtension=false`
   d. Run the command `Killall -9 java`.
4. Changing Worker IP via configFSM.sh does not work. To change Worker IP, delete the Worker from Supervisor, change the IP using Linux commands and add it back.
5. A newly installed 5.x Collector cannot be registered to a 6.x Supervisor. Old Collectors will continue to work. For new installations, install 6.x Collectors.
6. The following bugs have been discovered.
   - Malware Hash import from a CSV file fails when the CSV file contains 75,000 or more Malware Hash entries.
   - Scheduled bundle reports fail after migration.
   - Update Malware Hash via API does not work as expected, producing "duplicate" errors.
   - Cisco Meraki log discovery does not add devices to CMDB.
   - FortiSIEM does not recognize a UEBA perpetual license, so users with a UEBA perpetual license are unable to add UEBA for their devices.
   - For Elasticsearch cases with inline report mode set to 2, the ReportMaster memory may grow quickly.
   - Malware IP, Domain, and URL Group lookup performance slower than expected.
   - Security incidents always indicate "System Cleared" after 24 hours, even if `auto_clear_security_incidents=0` is set.
   - SSL communication sockets between rule worker and rule master are not always closed properly, leading to rules not triggering.

- Rules with a pattern-based clearing condition do not always clear even if the condition is met. This is because the clear rule's time window is sometimes read incorrectly.

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
   ```

Bug Fixes and Enhancements

The current release includes the following bug fixes and enhancements:

Bug ID	Severity	Module	Description
664708	Major	App Server	All Super Global users can see all Incidents for all Organizations, regardless of their role restrictions.
655557	Major	Query	Real time Query results not shown if there is no overlap between Event workers and Query workers.

Bug ID	Severity	Module	Description
665994	Minor	App Server	Selecting a incident category first in search panel will cause aggregation count of other criteria to be blank.
665387	Minor	App Server	Analytics filter operator IN / NOT IN doesn't work for individual CMDB selections.
664245	Minor	App Server	Incident comments filled with debug messages when running CVE Integration.
659678	Minor	App Server	Geo Maps do not show location on Dashboard map widget.
653426	Minor	App Server	Dashboard using Google API does not work for Org if the Org user does not have read permission of Google key (in Admin).
651528	Minor	App Server	FortiSIEM CMDB to ServiceNow Duplicates.
660734	Minor	Device Support	Aruba Parser parses causes high CPU because of excessive use of regular expression.
659163	Minor	Device Support	Fortigate on AWS logs are not recognized in FortiSIEM because of new devices.
652184	Minor	Device Support	Update Unix Parser with a new time stamp format.
652182	Minor	Device Support	Update F5BigIP Parser Update for Unsupported (New/Custom) Syslog Header.
649906	Minor	Device Support	CentOS CROND events incorrectly parsed as McAfee-WebGw-Run-Cmd because logs are too similar.
647216	Minor	Device Support	Not all attributes for Windows Security Events 4754, 4759, 4749 are parsed.
640196	Minor	Device Support	Not all attributes for Windows Security Event Parsing for Event ID 4625 is incorrect.
634374	Minor	Device Support	Windows Security Event ID 4688 is not parsed fully.
634372	Minor	Device Support	Windows Sysmon Parser needs to be extended.
607339	Minor	Device Support	Sysmon PowerShell Commands not correctly parsed if .exe is called from within Powershell.
594078	Minor	Device Support	Rule "Windows Audit Log Cleared" does not include user as an incident attribute.
592946	Minor	Device Support	Set Windows Event ID, Category, Subcategory and Login failure reason as description in Windows Security logs.
659018	Minor	Elastic Search	Many phDataManager errors may occur in some situations, caused by FortiSIEM sending malformed JSON to Elastocsearch.
662556	Minor	Event Pulling	AWS CloudTrailParser.xml parses event time incorrectly, which can

Bug ID	Severity	Module	Description
			cause event collection delay.
662540	Minor	Event Pulling	Azure CLI: mLastPollTime is not updated when job failed, causing data collection errors.
662450, 661806, 655562	Minor	Event Pulling	Azure Event Hub event collection errors can cause data collection to stop after running for some time.
660938	Minor	Event Pulling	Guard Duty max count event sometimes does not get picked up.
654551	Minor	Event Pulling	AgentManager can consume memory after running for a while, causing process to stop functioning.
656337	Minor	GUI	Analytics tab - Trend Bar Graph does not show continuity with time and results.
663683, 638773	Minor	Integration	Alienvault STIX OTX Integration may not work for pulling IOCs.
662899	Minor	Parser	Parser function for resolving Hostname to IP address does not work correctly.
659180	Minor	Parser	Collector caches time stamp when rejected from Appserver from Check-in.
659171	Minor	Parser	Two events attributes exist with same name Total Connections.
598471	Minor	Parser	Parse MITRE mapping event attributes in Windows Sysmon events.
516477	Enhancement	App Server	Cannot Discover Multiple Devices through Multiple Collectors through API.
665694	Enhancement	Data	The list of public DNS Servers need to be updated.
530467	Enhancement	Device Support	FortiSIEM not detecting certain event SSH/Audit events using UnixParser.
521230	Enhancement	Device Support	Need to support Barracuda F Series Log.
661711	Enhancement	Event Pulling	Parse out SQS log of when Cloudtrail package is logged.
544522	Enhancement	GUI	Cannot delete many credentials at one time.

New Device Support

- Tigera Calico - K8 log analysis
- Alcide.io Kubernetes and Microservices Audit log
- Stormshield Network Security