FortiSIEM - Release Notes

Version 6.1.0

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

FORTINET®

08/15/2022
FortiSIEM 6.1.0 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
10/08/2020	Initial version of FortiSIEM 6.1.0 Release Notes
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 6.1.0 release. It also provides a list of resolved issues.

What's New in 6.1.0

FortiSIEM 6.1.0 is a foundational release with a new Linux OS. This document describes new and enhanced features for the release.

- Installation Notes
- Known Issues
- New Features
- Key Enhancements
- Bug Fixes and Enhancements
- New Reports
- New Rules
- Vulnerabilities Fixed

Installation Notes

1. In this release, the underlying OS is upgraded from CentOS 6.10 to CentOS 8.2. Consequently, the migration from older releases of FortiSIEM is significantly more involved. Details are in the platform-specific Installation and Migration Guides.
    - Migration is supported from FortiSIEM 5.3.0., 5.3.1, 5.3.2, to 6.1.0. If you are using an older version, first upgrade to FortiSIEM 5.3.2 and then migrate to 6.1.0. Migration from 5.3.3 to 6.1.0 is not supported because 6.1.0 does not have the pre-compute feature in 5.3.3. Customers running 5.3.3 will be able to upgrade to a future 6.2.0 release.
    - In-place migration procedures is provided, so you do not have to move out the data and bring it back.
    - Migration is hypervisor-specific and can be time consuming, so plan accordingly. Migration involves:
        i. Migrating the Supervisor.
        ii. Installing and registering new Workers.
        iii. Older Collectors and Agents will work with the 6.1.0 Super and Worker.
    - When you decide to migrate Collectors to 6.1.0, do the following steps. Details are provided in platform specific install and upgrade guides.
        i. You must install new Collectors and register them in a specific way by using the “--update” option.
        ii. If Agents are registered via this Collector, then you must copy the hashed http password file (`/etc/httpd/accounts/passwds`) from the old Collector to the new Collector. Make sure the permissions are the same.
        iii. Make sure that the new 6.1.0 Collector uses the same IP address as the old Collector.
    - Future upgrades from 6.1.0 to 6.2.0, etc., will work like before via rpm upgrades.
2. Release 6.1.0 requires at least ESX 6.5, and ESX 6.7 Update 2 is recommended. To install on ESX 6.5, see install in ESX 6.5.
3. Hardware requirements are the same, however, if you want to use the UEBA feature, then the Supervisor must be upgraded to 32vCPU and 64GB RAM.
4. During a fresh install and migration process, a separate disk called `OPT` is created for use by FortiSIEM. Unlike earlier releases, FortiSIEM 6.1.0 does not write own logs or dump files in the root partition.
5. If you were running FortiSIEM 5.x and were using custom SSL certificates for Apache created with a 1024-bit RSA key, then you will notice that Apache will be down. This is because FortiSIEM 6.1 requires a 2048-bit RSA key.

Follow these steps to obtain a 2048-bit RSA key:

a. Get your custom SSL certificates with the 2048-bit RSA key or create a new self-signed certificate by running the following command:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/httpd/conf.d/apache-selfsigned.key -out /etc/httpd/conf.d/apache-
selfsigned.crt
```

b. Add the following lines to the `/etc/httpd/conf.d/ssl.conf` file, then save it:

```
SSLCertificateFile /etc/httpd/conf.d/apache-selfsigned.crt
SSLCertificateKeyFile /etc/httpd/conf.d/apache-selfsigned.key
```

c. Restart Apache with the following command:

```
service httpd restart
```

For fresh installations and for migrating from existing FortiSIEM installations, see:

- AWS Installation and Migration Guide
- ESX Installation and Migration Guide
- HyperV Installation and Migration Guide
- KVM Installation and Migration Guide
- FortiSIEM 2000F Hardware Configuration Guide for 6.1
- FortiSIEM 500F Collector Configuration Guide for 6.1

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”`

Fresh Install and Migration Limitations

1. Fresh install limitations:
   a. Can not be installed on Azure, Alibaba Cloud, 3500F hardware appliance.
   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. Offline install is not supported.
   f. Disaster recovery is not supported as PostGreSQL BDR is not yet available on the CentOS 8.2 release.
   g. Report Server is not supported.
2. Migration limitations:
   a. Migration for the 500F Collector is not supported. If you have 500F Collectors, then you can upgrade the Super and Worker to 6.1 but let the Collectors remain on older releases. A future release will provide 500F Collector migration to 6.1.
   b. Migration to FortiSIEM installations running on Elasticsearch is not supported.
   c. The pre-compute feature in FortiSIEM 5.3.3 is not included in this release. Hence upgrade from 5.3.3 to 6.1.0 is not supported.
3. The built in certificates for the FortiSIEM 6.1 Image were generated during the build and will be the same across all installations. These certificates are used to secure inter-node communications between the Collector, Worker, and Supervisor nodes. You must change them for your installation as follows:

   You must decide whether you will use CA signed certificates or self-signed certificates. If you decide to continue with self-signed certificates, then you must run the following command to re-generate a self-signed certificate for your environment:

   ```
   openssl req -new -newkey rsa:4096 -days 3650 -nodes -x509 -subj
   "/C=<country>/ST=<state>/L=<city>/O=<organization>/CN=<hostname-or-FQDN>" -keyout
   /etc/pki/tls/private/localhost.key -out /etc/pki/tls/certs/localhost.crt
   ```

   For example, for Fortinet, located in Sunnyvale, California, the following command would be used:

   ```
   openssl req -new -newkey rsa:4096 -days 3650 -nodes -x509 -subj
   "/C=US/ST=CA/L=SunnyVale/O=Fortinet/CN=localhost" -keyout
   /etc/pki/tls/private/localhost.key -out /etc/pki/tls/certs/localhost.crt
   ```
4. 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`.

5. Fresh install may fail because of memory allocation issues, when Supervisor is installed on a VM with 24 GB RAM. This is likely caused by two issues: the swap size is not set correctly when configFSM.sh is run, and the App Server is forced to run on 12 GB virtual RAM via ulimit, even when physical memory is available.
   To resolve this issue, follow these steps:

   a. After deploying a 6.1.0 VM on any platform and booting up, download `swapon-ulimit-fixes.tgz` from here and copy it to the system.

      i. If the system comes up with a DHCP IP, then use that to copy the above file. If not, you will need to manually set up IP address in `/etc/sysconfig/network-scripts/ifcfg-eth0` and restart the network via systemctl restart NetworkManager (or reboot).

      ii. Login as `root`.

      iii. Run the command `sed -i -e 's/totalmem -lt 24000/totalmem -lt 20000/' /root/.bashrc`.

      iv. Logout.

   b. Log back in as `root`.

   c. Run `tar xzf <path-where-file-is-stored>/swapon-ulimit-fixes.tgz -C /`.

   d. Run `configFSM.sh` and it should succeed.

   If you did not do the above deployed system and it fails, then it is hard to manually fix and rerun configuration. Therefore, you will need to delete VM, redo the steps after patching above the yml files.

   If you did not do the above deployed system and it succeeds to the end, then do not worry about the swap issue since the swap will be set correctly after the reboot. Just run the following command `sed -i -e 's/totalmem -lt 24000/totalmem -lt 20000/' /opt/phoenix/bin/.bashrc /root/.bashrc` after logging in as root. Then reboot it again.

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
   ```

New Features

- Run on CentOS 8.2
- FIPS Enabled
- Inbuilt Windows UEBA

Run on CentOS 8.2

FortiSIEM 6.1.0 runs on CentOS 8.2. Both the install and migration procedures have been improved. There is now a single image for Collector, Supervisor and Worker nodes.

For fresh installations and for migrating from existing FortiSIEM installations, see:

- AWS Installation and Migration Guide
- ESX Installation and Migration Guide
- HyperV Installation and Migration Guide
- KVM Installation and Migration Guide
- FortiSIEM 2000F Hardware Configuration Guide for 6.1
- FortiSIEM 500F Collector Configuration Guide for 6.1

FIPS Enabled

FortiSIEM can run in FIPS mode. You can choose to install in FIPs mode during a fresh 6.1.0 installation. You can also disable or enable FIPS on an existing 6.1.0 system. The following features are added for FIPS mode, but some are also available for non-FIPS mode.

- For both FIPS and non-FIPS installation modes, you **must** change the default GUI and SSH passwords.
- GUI and SSH user passwords for both FIPS and non-FIPS modes are now required to contain at least 8 characters, and must include 1 letter, 1 numeric character, and 1 special character.
- For both FIPS and non-FIPS modes, you can zeroize the keys to ensure that there are no keys and critical security parameters left in the system. This is done before destroying a FortiSIEM installation. For details, see Erasing Disk Contents.
- In FIPS mode, FortiSIEM will use only FIPS-compliant cryptographic algorithms. For a full list of supported cryptographic algorithms, see Cryptographic Algorithms. Note that this list may change from version to version.
- During startup and reboot, FortiSIEM will run self-tests to ensure that proper FIPS-compliant algorithms are being used. These self-tests can also be run on-demand. Note that Redhat 8.1, being a new OS, has applied for FIPS certification.
- FIPS mode is displayed in GUI for all installations.
- In FIPS mode, FortiSIEM uses CPU Time Jitter Random Number Generator as the Non-deterministic Random Bit generator (NDRBG). This has been proven to provide strong keys (see https://www.chronox.de/jent/doc/CPU-Jitter-NPTRNG.html). This makes the cryptographic algorithms very secure as required by FIPS standards.

For key zeroization, see Erasing Disk Contents.

For cryptographic algorithms, see Cryptographic Algorithms.

FIPS requires a strict set of crypto algorithms. Therefore, when you enable FIPS on FortiSIEM, certain communications between FortiSIEM and external devices may break if the external device is not also FIPS enabled. This is especially true for migrating from FortiSIEM 5.3.x. Suppose you were collecting performance metrics and logs from a legacy network device. Before turning on FIPS, make sure that the device is also FIPS ready.

Inbuilt Windows UEBA

This release adds User Entity Behavior Monitoring for Windows users. The Windows Agent 4.0.0 has embedded a UEBA Kernel Agent that reports these user activity events:

- Logon/logoff
- Machine on/off
- File activity – create, delete, read, write, rename, move, print
- File upload/download
- Drive mount/un-mount

Based on these activities, an AI module running on the Supervisor, detects anomalous FortiSIEM incidents. The UEBA dashboard can be used to investigate these incidents.

You must have a new license to enable the UEBA feature. You can stack a UEBA license on top of a regular FortiSIEM Windows Agent license, or use the UEBA license independently. Therefore, 3 modes are possible:

- Windows logging and performance monitoring only.
- Windows UEBA only. In this mode the agent is not counted towards the CMDB license and UEBA events are not counted towards the licensed EPS
- Windows logging, performance monitoring and UEBA. In this mode, UEBA events are not counted towards licensed EPS.

To enable UEBA, you must complete the following steps:

1. Install Windows 4.0.0. The procedures are identical to Windows 3.3.0 and can be found in Configuring Windows Agent.
2. Install a new FortiSIEM license which contains UEBA telemetry.
3. Restart the `phFortiInsightAI` module by running the following command on the Supervisor node:
   ```
   systemctl restart phFortiInsightAI
   ```
4. 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 Configuring Windows Agents. Then in the CMDB tab, the Agent type becomes **Windows + UEBA**.
5. The windows Agent will start sending UEBA telemetry to FortiSIEM.

You may want to change UEBA Settings for the AI module: see UEBA Settings.

UEBA incidents created by the AI module can be seen on the UEBA dashboard, see UEBA View.

Key Enhancements

- EventDB Query Management
- Run Multiple Searches
- Report Bundle Export Progress

EventDB Query Management

This release adds the following enhancements for Event DB queries:

- New Adaptive Query Workload distribution algorithm
- Active Query visibility – Two dashboards are provided:
  - Query Status – the progress of each Query (Adhoc, Scheduled) at the Query Master and Worker levels.
  - Query Workload at each Worker

The Adaptive Query Workload distribution algorithm has these features:

- Query routing based on Worker workload
- Re-routing for failed Workers
- Reservation for Adhoc and Scheduled Queries

For details on the Query Status dashboard, see Query Status.

For details on the Worker Workload dashboard, see Query Workload.

Run Multiple Searches

You can now run multiple searches from the GUI without opening a new browser tab. Simply click the **+** tab to create a new search tab. If you leave a search tab, the query on that tab continues to run. For more information on this feature, see Run Multiple Searches Simultaneously.

Report Bundle Export Progress

A Report Bundle can take a long time to run if the bundle has multiple, complex reports. In earlier releases, there was no report-by-report progress indicator when you ran a Report Bundle from the GUI. This release provides visibility into the progress of Report Bundle processing and improves the user experience.

Bug Fixes and Enhancements

The current release includes the following bug fixes and enhancements:

ID	Severity	Module	Summary
644410	Minor	App Server	Widget Dashboard Imported in Super Global is not shared in organizations.
644090	Minor	App Server	Custom Event Attribute names do not display in CSV reports.
643967	Minor	App Server	Handle the Null pointer exception in App Server to Query Master communication.
643648	Minor	App Server	Query time interval is not saved properly in Report Bundle scheduled for organizations.
643249	Minor	App Server	An exception occurs during app server start up while loading namedValue to Redis.
640569	Minor	App Server	After upgrade, Shared dashboards created in Super Global are

ID	Severity	Module	Summary
			invisible if su to organizations.
637264	Minor	App Server	Failed to save location for device when city/state has a single quote (after it already triggered an incident).
635420	Minor	App Server	Device hostnames containing a single quote cause incident insert errors.
527733	Minor	App Server	LDAP user discovery merge is logging excessive user contact update.
497314	Minor	App Server	LDAP OU discovery is aborted because of long OU name.
647601	Minor	Data	"System License Warning: Max Number of Devices Exceeded License" rule does not trigger.
644155	Minor	Data	Some attributes are not correctly parsed by NetBotzCMCTrap.
641317	Minor	Event Pulling	Logon Events are not pulling from Google App Suite.
649152	Minor	GUI	Home Setting does not show on UI after an upgrade.
648413	Minor	GUI	winexe is enabled in Discovery once you edit a Discovery template.
647769	Minor	GUI	You can select any attribute in a rule exception. It should only allow those attributes in "Incident attribute".
644073	Minor	GUI	New schedule for FortiGuard IOC Service does not show the created schedule after saving.
643888	Minor	GUI	Losing the connection to Super during a Dashboard slideshow causes a user log out after 10 minutes.
640894	Minor	GUI	Pull Events tab shows an error from another organization.
638148	Minor	GUI	The GUI displays 0xA0 characters in Raw events as 0x20.
633235	Minor	GUI	GUI Error occurs when saving Access Method configuration for FortiGate Rest API.
632413	Minor	GUI	During GUI login, DOMAIN is not displayed until the Log On button is pressed.
612331	Minor	GUI	Dashboard Slideshow times out after 1 day.
611930	Minor	GUI	Generating two reports that attempt to show average and max value only shows max.
602326	Minor	GUI	CMDB Reports with Report Type generate a PSQLException.
598485	Minor	GUI	Parser Validation cannot handle parsers with an "&" symbol.
639744	Minor	GUI, App Server	Login drop down has to convert to text box in order to protect end client from exposure of other domains.
637664	Minor	H5_Analytics	In Rule Exception, the Value field cannot be edited when values are added from the CMDB.

ID	Severity	Module	Summary
596560	Minor	Parser	The character "<" in the test event breaks attributes display in Parser testing
629489	Minor	Performance Monitoring	Cisco ASA memory utilization polling fails as vendor has changed SNMP OID.
517105	Minor	Performance Monitoring	Memory utilization on Cisco Nexus 9k is stuck at 100%.
637631	Minor	Query Master	CSV Export from the date before daylight saving change shows a one hour difference.
648971	Minor	System	phDataPurger crashes when archiving from Elasticsearch to NFS if the raw event size is more than 64KB.
643027	Minor	System	FSM collector nodes contain passwords in plain text based on the API cache.
632883	Minor	System	Elastic Search Disaster Recovery does not sync the Redis Password correctly.
630634	Minor	System	Elasticsearch snapshot creation fails during disaster recovery.
644882	Enhancement	App Server	Support device names with single quote.
632976	Enhancement	App Server	Malware IP download - does not handle CIDR notation.
644104	Enhancement	Data	Need additional JunOS event types to the data-definition file.
643874	Enhancement	Data	Watchguard Firewall Parser needs an update.
643780	Enhancement	Data	Trend Micro Apex Central Parser for Antivirus doesn't create a correct Event Type.
643015	Enhancement	Data	Sophos Event parser does set the reporting IP or host name.
639125	Enhancement	Data	Windows WMI events in French are not fully parsed.
637703	Enhancement	Data	Citrix Netscaler Parser does not parse certain VPN logs.
632767	Enhancement	Data	Spanish Windows parser needs more translations.
615340	Enhancement	Data	Citrix Netscaler Parser does not parse out Group Names with a space.
612914	Enhancement	Data	Infoblox parser - Parser does not pick up client hostname in the syslog field. Instead, it picks up the IP address.
609725	Enhancement	Data	Windows Custom Log Parser does not parse out two fields for event ID 411: Client IP and Error Message.
603557	Enhancement	Data	Nessus Parser Host Field must also parse the hostname.
599955	Enhancement	Data	Windows Event Parsing - Language translation update.
643287	Enhancement	GUI	Domain part of O365 Endpoints need to be configurable.

ID	Severity	Module	Summary
641357	Enhancement	GUI	Country Groups must be editable only from the left tree.
640064	Enhancement	GUI	Cannot clear multiple incidents under the Incident Explorer dashboard.
612285	Enhancement	Parser	O365 Event Type MS_OFFICE365_SecurityComplianceCenter_AlertTriggered is missing details.

New Reports

- FortiSIEM UEBA detected hacking tool usage
- FortiSIEM UEBA detected ransomware
- FortiSIEM UEBA detected backup applications
- FortiSIEM UEBA detected ransomware file types
- FortiSIEM UEBA detected MTP write
- FortiSIEM UEBA detected potential pirated media
- FortiSIEM UEBA detected file printed
- FortiSIEM UEBA detected removable media read
- FortiSIEM UEBA detected snipping tool
- FortiSIEM UEBA detected encryption tools
- FortiSIEM UEBA detected email upload
- FortiSIEM UEBA detected cloud upload
- FortiSIEM UEBA detected potential leaver editing a CV at work
- FortiSIEM UEBA detected email download
- FortiSIEM UEBA detected NFS write
- FortiSIEM UEBA detected browser download
- FortiSIEM UEBA detected hacking tool and footprints
- FortiSIEM UEBA detected ransomware file names
- FortiSIEM UEBA detected gaming application
- FortiSIEM UEBA detected removable media write
- FortiSIEM UEBA detected NFS read
- FortiSIEM UEBA detected files copied over remote desktop
- FortiSIEM UEBA detected browser upload
- FortiSIEM UEBA detected software installation
- FortiSIEM UEBA detected MTP read
- FortiSIEM UEBA detected file archiver application

New Rules

There are 846 built-in correlation rules in the system. The following rules have been added to 6.1.0 release.

- FortiSIEM UEBA AI detects unusual file movement
- FortiSIEM UEBA AI detects unusual process created
- FortiSIEM UEBA AI detects unusual file download
- FortiSIEM UEBA AI detects unusual file upload
- FortiSIEM UEBA AI detects unusual machine on
- FortiSIEM UEBA AI detects unusual machine off
- FortiSIEM UEBA AI detects unusual host logon
- FortiSIEM UEBA AI detects unusual machine logoff
- FortiSIEM UEBA AI detects unusual file renamed
- FortiSIEM UEBA AI detects unusual file printed
- FortiSIEM UEBA AI detects unusual new drive mounted
- FortiSIEM UEBA AI detects unusual drive unmounted
- FortiSIEM UEBA AI detects unusual process not restarted
- FortiSIEM UEBA Policy detects antivirus not started
- FortiSIEM UEBA Policy detects antivirus stopped
- FortiSIEM UEBA Policy detects malicious powershell execution
- FortiSIEM UEBA Policy detects suspicious applications
- FortiSIEM UEBA Policy detects Tor client usage
- FortiSIEM UEBA Policy detects uncommon VPN client
- FortiSIEM UEBA Policy detects hacking tool usage
- FortiSIEM UEBA Policy detects ransomware
- FortiSIEM UEBA Policy detects backup applications
- FortiSIEM UEBA Policy detects ransomware file types
- FortiSIEM UEBA Policy detects MTP write
- FortiSIEM UEBA Policy detects potential pirated media
- FortiSIEM UEBA Policy detects file printed
- FortiSIEM UEBA Policy detects removable media read
- FortiSIEM UEBA Policy detects snipping tool
- FortiSIEM UEBA Policy detects encryption tools
- FortiSIEM UEBA Policy detects email upload
- FortiSIEM UEBA Policy detects cloud upload
- FortiSIEM UEBA Policy detects potential leaver editing a CV at work
- FortiSIEM UEBA Policy detects email download
- FortiSIEM UEBA Policy detects nfs write
- FortiSIEM UEBA Policy detects browser download
- FortiSIEM UEBA Policy detects hacking tool and footprints
- FortiSIEM UEBA Policy detects ransomware file names
- FortiSIEM UEBA Policy detects gaming application
- FortiSIEM UEBA Policy detects removable media write
- FortiSIEM UEBA Policy detects NFS read
- FortiSIEM UEBA Policy detects files copied over remote desktop
- FortiSIEM UEBA Policy detects browser upload
- FortiSIEM UEBA Policy detects software installation
- FortiSIEM UEBA Policy detects MTP read
- FortiSIEM UEBA Policy detects file archiver application

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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.