

Arayüz Kullanılarak Yapılandırma

Server settings and maintenance

MISP sunucusunun yapılandırma ayarları ve bakım işlemleri, sunucu performansını optimize etmek, güncellemeleri uygulamak ve genel sunucu yönetimi ile ilgili diğer işlemleri içerir.

Site yöneticilerinin MISP kurulumlarını yönetmesine ve sorunları teşhis etmesine olanak tanır.

| Server Settings & Maintenance | | |
|--|--|---|
| Overview MISP (14) Encryption (5) Proxy (5) Security (6) Plugin (590) SimpleBackgroundJobs Correlations new Diagnostics Manage files Workers | | |
| Test | Value | Description |
| Overall health | Issues found, it is recommended that you resolve them. | The overall health of your instance depends on the most severe unresolved issues. |
| Critical settings incorrectly or not set | 0 incorrect settings. | MISP will not operate correctly or will be unsecure until these issues are resolved. |
| Recommended settings incorrectly or not set | 523 incorrect settings. | Some of the features of MISP cannot be utilised until these issues are resolved. |
| Optional settings incorrectly or not set | 97 incorrect settings. | There are some optional tweaks that could be done to improve the looks of your MISP instance. |
| Critical issues revealed by the diagnostics | 0 issues detected. | Issues revealed here can be due to incorrect directory permissions or not correctly installed dependencies. |

To edit a setting, simply double click it.

Tablodaki her satır bir ayarı temsil eder. Renkli satırlar, ayarın yanlış olduğunu / yapılmadığını belirtir ve renk, ciddiyeti belirler (kırmızı = kritik, sarı = önerilen, yeşil = isteğe bağlı).

Priority: Ayarın ciddiyeti.

Setting: Ayarın adı.

Value: Ayarın geçerli değeri. Belirli bir ayarın mevcut yapılandırılmış değeridir. Yani, sistemdeki bir ayarın şu anda ne olduğunu ifade eder. Örneğin, bir ayarın geçerli değeri "https://misp.example.com" ise, bu, o ayarın şu anda belirlenen değeridir ve sistem bu değeri kullanır. Bu değer, sistem ayarlarının yapılandırılması ve doğru çalışması için önemlidir.

Description: Ayarın ne işe yaradığının açıklamasıdır.

Error Message: Ayar yanlışsa/yapılmadıysa bu alan kullanıcıya neyin yanlış olduğunu bildirecektir.

• MISP

MISP'in kritik ayarlarını ve bu ayarların değerlerini içerir. MISP'in güvenli ve etkili bir şekilde çalışması için bu ayarların doğru bir şekilde yapılandırılması gerekmektedir. Her bir ayarın kritik olduğu ve işleyiş için önemli olduğu belirtilmektedir.

| Overview | MISP (14) | Encryption (5) | Proxy (5) | Security (6) | Plugin (590) | SimpleBackgroundJobs | Correlations | new | Diagnostics | Manage files | Workers | | Filter the table(s) below |
|----------|-----------------------------------|--------------------------------------|--|---|--------------|----------------------|--------------|------------------|-------------|--------------|---------|--|---------------------------|
| Priority | Setting | Value | Description | Error Message | | | | | | | | | |
| Critical | MISP.baseurl | https://localhost | The base url of the application (in the format https://www.mymispinstance.com or https://myserver.com/misp). Several features depend on this setting being correctly set to function. | The currently set baseurl does not match the URL through which you have accessed the page. Disregard this if you are accessing the page via an alternate URL (for example via IP address). | | | | | | | | | |
| Critical | MISP.external_baseurl | https://localhost | The base url of the application (in the format https://www.mymispinstance.com) as visible externally/by other MISPs. MISP will encode this URL in sharing groups when including itself. If this value is not set, the baseurl is used as a fallback. | | | | | | | | | | |
| Critical | MISP.live | true | Unless set to true, the instance will only be accessible by site admins. | | | | | | | | | | |
| Critical | MISP.language | eng | Select the language MISP should use. The default is english. | | | | | | | | | | |
| Critical | MISP.correlation_engine | | Choose which correlation engine to use. MISP defaults to the default engine, maintaining all data in the database whilst enforcing ACL rules on any non site-admin user. This is recommended for any MISP instnace with multiple organisations. If you are an endpoint MISP, consider switching to the much leaner and faster No ACL engine. | | | | | | | | | | |
| Critical | MISP.correlation_limit | 100 | Set a value for the maximum number of correlations a value should have before MISP will refuse to correlate it (extremely over-correlating values are rarely useful from a correlation perspective). | | | | | | | | | | |
| Critical | MISP.enable_advanced_correlations | false | Enable some performance heavy correlations (currently CIDR correlation) | | | | | | | | | | |
| Critical | MISP.host_org_id | ORGNAME | The hosting organisation of this instance. If this is not selected then replication instances cannot be added. | | | | | | | | | | |
| Critical | MISP.uuid | 6a3f17e4-d268-4fc6-81f5-46febb3c07e3 | The MISP instance UUID. This UUID is used to identify this instance. | No valid UUID set | | | | | | | | | |
| Critical | MISP.showorg | true | Setting this setting to 'false' will hide all organisation names / logos. | | | | | | | | | | |

• Encryption

MISP'te kullanılan şifreleme yöntemlerini ve güvenlik protokollerini ifade eder. MISP, verilerin güvenliği için şifreleme sağlar ve bu nedenle şifreleme algoritmaları ve anahtar yönetimi gibi konuları içerir.

Overview

MISP (14)

Encryption (5)

Proxy (5)

Security (6)

Plugin (590)

SimpleBackgroundJobs

Correlations

new

Diagnostics

Manage files

Workers

Filter the table(s) below

| Priority | Setting | Value | Description | Error Message |
|-------------|-----------------------------|--|--|----------------|
| Critical | GnuPG.onlyencrypted | false | Allow (false) unencrypted e-mails to be sent to users that don't have a GnuPG key. | |
| Critical | GnuPG.email | admin@admin.test | The e-mail address that the instance's GnuPG key is tied to. | |
| Critical | GnuPG.homedir | /var/www/MISP/.gnupg | The location of the GnuPG homedir. | |
| Recommended | GnuPG.password | **** | The password (if it is set) of the GnuPG key of the instance. | |
| Optional | GnuPG.binary | /usr/bin/gpg | [CLI only] The location of the GnuPG executable. If you would like to use a different GnuPG executable than /usr/bin/gpg, you can set it here. If the default is fine, just keep the setting suggested by MISP. | |
| Optional | GnuPG.bodyonlyencrypted | false | Allow (false) the body of unencrypted e-mails to contain details about the event. | |
| Optional | GnuPG.sign | true | Enable the signing of GnuPG emails. By default, GnuPG emails are signed | |
| Optional | GnuPG.obscure_subject | false | When enabled, the subject in signed and encrypted e-mails will not be sent in unencrypted form. | |
| Optional | GnuPG.key_fetching_disabled | false | When disabled, user could not fetch his PGP key from CIRCL key server. Key fetching requires internet connection. | Value not set. |
| Optional | SMIME.enabled | false | Enable S/MIME encryption. The encryption posture of the GnuPG.onlyencrypted and GnuPG.bodyonlyencrypted settings are inherited if S/MIME is enabled. | |
| Optional | SMIME.email | | The e-mail address that the instance's S/MIME key is tied to. | Value not set. |
| Optional | SMIME.cert_public_sign | /var/www/MISP/.smime/email@address.com.pem | The location of the public half of the signing certificate. | Value not set. |
| Optional | SMIME.key_sign | /var/www/MISP/.smime/email@address.com.key | The location of the private half of the signing certificate. | Value not set. |
| Optional | SMIME.password | **** | The password (if it is set) of the S/MIME key of the instance. | Value not set. |

• Proxy

MISP'in arkasındaki proxy ayarlarını ve yapılandırmasını ifade eder. MISP sunucusunun arkasında bir proxy sunucusu kullanılıyorsa, proxy ayarlarının nasıl yapılandırıldığını ve yönetildiğini belirtir.

Overview

MISP (14)

Encryption (5)

Proxy (5)

Security (6)

Plugin (590)

SimpleBackgroundJobs

Correlations

new

Diagnostics

Manage files

Workers

Filter the table(s) below

| Priority | Setting | Value | Description | Error Message |
|----------|----------------|-------|---|----------------------------------|
| Optional | Proxy.host | | The hostname of an HTTP proxy for outgoing sync requests. Leave empty to not use a proxy. | Value not set. |
| Optional | Proxy.port | | The TCP port for the HTTP proxy. | This setting has to be a number. |
| Optional | Proxy.method | | The authentication method for the HTTP proxy. Currently supported are Basic or Digest. Leave empty for no proxy authentication. | Value not set. |
| Optional | Proxy.user | | The authentication username for the HTTP proxy. | Value not set. |
| Optional | Proxy.password | **** | The authentication password for the HTTP proxy. | Value not set. |

• Security

MISP'in güvenliği ve güvenlik önlemlerini kapsar. Kullanıcı kimlik doğrulaması, erişim kontrolleri, güvenlik güncelleştirmeleri ve diğer güvenlik önlemleri bu kategoride yer alır.

| Priority | Setting | Value | Description | Error Message |
|----------|--|-------|---|--|
| Critical | Security.disable_form_security | false | Disabling this setting will remove all form tampering protection. Do not set this setting pretty much ever. You were warned. | This setting leaves your users open to CSRF attacks. Please consider disabling this setting. |
| Critical | Security.csp_enforce | true | Enforce CSP. Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. When disabled, violations will be just logged. | |
| Critical | Security.advanced_authkeys | true | Advanced authkeys will allow each user to create and manage a set of authkeys for themselves, each with individual expirations and comments. API keys are stored in a hashed state and can no longer be recovered from MISP. Users will be prompted to note down their key when creating a new authkey. You can generate a new set of API keys for all users on demand in the diagnostics page, or by triggering the advanced upgrade . | |
| Critical | Security.rest_client_enable_arbitrary_urls | false | [CLI only] Enable this setting if you wish for users to be able to query any arbitrary URL via the rest client. Keep in mind that queries are executed by the MISP server, so internal IPs in your MISP's network may be reachable. | |
| Critical | Security.syslog | false | Enable this setting to pass all audit log entries directly to syslog. Keep in mind, this is verbose and will include user, organisation, event data. | |
| Critical | Security.do_not_log_authkeys | false | If enabled, any authkey will be replaced by asterisks in Audit log. | |
| Critical | Security.disable_browser_cache | false | If enabled, HTTP headers that block browser cache will be send. Static files (like images or JavaScripts) will still be cached, but not generated pages. | |
| Critical | Security.check_sec_fetch_site_header | false | If enabled, any POST, PUT or AJAX request will be allow just when Sec-Fetch-Site header is not defined or contains "same-origin". | |
| Critical | Security.disable_local_feed_access | false | [CLI only] Disabling this setting will allow the creation/modification of local feeds (as opposed to network feeds). Enabling this setting will restrict feed sources to be network based only. When disabled, keep in mind that a malicious site administrator could get access to any arbitrary file on the system that the apache | |

- **Plugin**

MISP, eklentiler veya pluginler yoluyla genişletilebilir. Bu, MISP'e yeni özellikler eklemek veya mevcut işlevselliği özelleştirmek için kullanılır. Pluginler, farklı veri kaynaklarından veri almak, analiz yapmak veya çıktıları entegre etmek gibi çeşitli amaçlar için kullanılabilir.

Overview

MISP (14)

Encryption (5)

Proxy (5)

Security (6)

Plugin (590)

SimpleBackgroundJobs

Correlations

new

Diagnostics

Manage files

Workers

Enrichment

Import

Export

Action

Cortex

Sightings

Workflow

CyCat

CTInfoExtractor

RPZ

Kafka

ZeroMQ

ElasticSearch

S3

CustomAuth

• SimpleBackgroundJobs

MISP'in arka planda çalışan işleri yönetme yeteneğini ifade eder. Örneğin, otomatik veri senkronizasyonu, veritabanı temizliği veya veri işleme gibi görevler arka planda çalışır ve bu alan altında yönetilir.

Overview

MISP (14)

Encryption (5)

Proxy (5)

Security (6)

Plugin (590)

SimpleBackgroundJobs

Correlations

new

Diagnostics

Manage files

Workers

Filter the table(s) below

| Priority | Setting | Value | Description | Error Message |
|----------|--|-----------------|--|---------------|
| Critical | SimpleBackgroundJobs.enabled | true | Enables or disables background jobs with Supervisor backend. Please read this guide before setting this to `true`. | |
| Critical | SimpleBackgroundJobs.redis_host | redis | The host running the redis server to be used for background jobs. | |
| Critical | SimpleBackgroundJobs.redis_port | 6379 | The port used by the redis server to be used for background jobs. | |
| Critical | SimpleBackgroundJobs.redis_database | 1 | The database on the redis server to be used for background jobs. If you run more than one MISP instance, please make sure to use a different database or redis_namespace on each instance. | |
| Critical | SimpleBackgroundJobs.redis_password | ***** | The password on the redis server (if any) to be used for background jobs. | |
| Critical | SimpleBackgroundJobs.redis_namespace | background_jobs | The namespace to be used for the background jobs related keys. | |
| Critical | SimpleBackgroundJobs.max_job_history_ttl | 86400 | The time in seconds the job statuses history will be kept. | |
| Critical | SimpleBackgroundJobs.supervisor_host | 127.0.0.1 | The host where the Supervisor XML-RPC API is running. | |
| Critical | SimpleBackgroundJobs.supervisor_port | 9001 | The port where the Supervisor XML-RPC API is running. | |
| Critical | SimpleBackgroundJobs.supervisor_user | supervisor | The user of the Supervisor XML-RPC API. | |
| Critical | SimpleBackgroundJobs.supervisor_password | ***** | The password of the Supervisor XML-RPC API. | |
| Optional | SimpleBackgroundJobs.redis_serializer | JSON | Redis serializer method. WARNING: Changing this setting in production will break your jobs. | |

• Correlations

MISP'te kullanılan veri analizi ve ilişkilendirme işlemlerini yönetmek için kritik öneme sahip olan ayarları içerir. Bu ayarlar, veri analizi süreçlerini optimize etmek ve tehdit istihbaratı topluluğunun verimliliğini artırmak için kullanılır.

OverviewMISP (14)Encryption (5)Proxy (5)Security (6)Plugin (590)SimpleBackgroundJobsCorrelations (new)DiagnosticsManage filesWorkers

This is the correlation management interface. Its goal is to provide you with information about the currently used correlation engine as well as the data stores of currently dormant engines.

You will also find management tools for the various engines below, make sure that you keep an eye on the disk requirements as well as the exhaustion of IDs and recorelate the instance when needed.

| Field | Value |
|-----------------------|-------|
| Over correlations | 461 |
| Excluded correlations | 0 |

Active engine: Default correlation engine

| Table | # of rows | Size on disk | ID space saturation |
|----------------------|-----------|--------------|---------------------|
| default_correlations | 160569 | 49 MB | 0% |
| correlation_values | 15034 | 4 MB | 0% |

Recorelate

Dormant engine: No ACL correlation engine

| Table | # of rows | Size on disk | ID space saturation |
|---------------------|-----------|--------------|---------------------|
| no_acl_correlations | 0 | 0 MB | 0% |
| correlation_values | 15034 | 4 MB | 0% |

Activate engineTruncate

Dormant engine: Legacy correlation engine (< 2.4.160)

| Table | # of rows | Size on disk | ID space saturation |
|--------------|-----------|--------------|---------------------|
| correlations | 0 | 0 MB | 0% |

Truncate

To edit a setting, simply double click it.

• Diagnostics

MISP sisteminin teşhis ve hata ayıklama işlevselliğini ifade eder. Özellikle sistem sorunlarını tespit etmek ve çözmek için teşhis araçlarını içerir.

OverviewMISP (14)Encryption (5)Proxy (5)Security (6)Plugin (590)SimpleBackgroundJobsCorrelationsnewDiagnostics (2)Manage filesWorkers

MISP version

Every version of MISP includes a JSON file with the current version. This is checked against the latest tag on GitHub, if there is a version mismatch the tool will warn you about it. Make sure that you update MISP regularly.

Currently installed version... v2.4.187 (661b238b3f4b8aecc25f32915a74a8eb0514f775)
Latest available version... v2.4.189 (04100d13d3963ccaa35ad4442090f7b625b378cc)
Status... Outdated version
Current branch... You are not on a branch, but since MISP self-update is disabled this is expected.

Update MISP

You are using a MISP installation method that does not support or recommend using the MISP self-update, such as a Docker container. Please update using the appropriate update mechanism.

Writable Directories and files

The following directories and files have to be writeable for MISP to function properly. Make sure that the apache user has write privileges for the directories below.

Directories

/tmp...OK
/var/www/MISP/app/tmp...OK
/var/www/MISP/app/files...OK
/var/www/MISP/app/files/scripts/tmp...OK
/var/www/MISP/app/tmp/csv_all...OK
/var/www/MISP/app/tmp/csv_sig...OK
/var/www/MISP/app/tmp/md5...OK
/var/www/MISP/app/tmp/sha1...OK
/var/www/MISP/app/tmp/snort...OK
/var/www/MISP/app/tmp/suricata...OK
/var/www/MISP/app/tmp/text...OK
/var/www/MISP/app/tmp/xml...OK
/var/www/MISP/app/tmp/files...OK
/var/www/MISP/app/tmp/logs...OK
/var/www/MISP/app/tmp/bro...OK

Writeable Files

/var/www/MISP/app/Config/config.php...OK
/var/www/MISP/.git/ORIG_HEAD...OK

Readable Files

/var/www/MISP/app/files/scripts/stixtest.py...OK

• Manage files

MISP'in dosyaları yönetme yeteneğini ifade eder. Özellikle tehdit verileri veya analiz sonuçları gibi dosyaları yüklemek, saklamak ve yönetmek için kullanılır.










Below you will find a list of the uploaded files based on type.

Organisation logos

Description: The logo used by an organisation on the event index, event view, discussions, proposals, etc. Make sure that the filename is in the org.png format, where org is the case-sensitive organisation name.

Expected Format: 48x48 pixel .png files or .svg file

Path: /var/www/MISP/app/files/img/orgs

| Filename | Used by | Size | Permissions | Actions |
|-------------|---------|---------|-------------|---|
| ADMIN.png | N/A | 4.6 kB | rwX |  |
| CERT.at.png | N/A | 2.4 kB | rwX |  |
| CERT.at.png | N/A | 2.4 kB | rwX |  |
| CIRCL.png | N/A | 1.8 kB | rwX |  |
| MIL.be.png | N/A | 6.8 kB | rwX |  |
| MISP.png | N/A | 842.0 B | rwX |  |
| NATO.png | N/A | 5.1 kB | rwX |  |
| NCIRC.png | N/A | 5.1 kB | rwX |  |
| RISKIQ.png | N/A | 6.1 kB | rwX |  |

Dosya seçilmedi

Additional image files

Description: Image files uploaded into this directory can be used for various purposes, such as for the login page logos

Expected Format: PNG or SVG file

Path: /var/www/MISP/app/files/img/custom

Files set for each relevant setting:

- MISP.footer_logo:
- MISP.home_logo:
- MISP.welcome_logo:
- MISP.welcome_logo2:

| Filename | Used by | Size | Permissions | Actions |
|----------|---------|------|-------------|---------|
|----------|---------|------|-------------|---------|

Dosya seçilmedi

• Workers

MISP sistemindeki çalışan süreçlerini ifade eder. Özellikle veri işleme, analiz veya diğer görevler için ayrılmış çalışan süreçlerinin yönetimini içerir.

Worker type: cache

Jobs in the queue: 0
Queue status: OK

| Worker PID | User | Worker process | Information | Actions |
|------------|----------|----------------|-----------------------------------|---|
| 1098 | www-data | OK | The worker appears to be healthy. |  |
| 1105 | www-data | OK | The worker appears to be healthy. |  |
| 1113 | www-data | OK | The worker appears to be healthy. |  |
| 1120 | www-data | OK | The worker appears to be healthy. |  |
| 1128 | www-data | OK | The worker appears to be healthy. |  |

Start a worker

Worker type: default



Jobs in the queue: 0
Queue status: OK

| Worker PID | User | Worker process | Information | Actions |
|------------|----------|----------------|-----------------------------------|---|
| 1040 | www-data | OK | The worker appears to be healthy. |  |
| 1041 | www-data | OK | The worker appears to be healthy. |  |
| 1042 | www-data | OK | The worker appears to be healthy. |  |
| 1043 | www-data | OK | The worker appears to be healthy. |  |
| 1046 | www-data | OK | The worker appears to be healthy. |  |

Start a worker

Worker type: email

Jobs in the queue: 0
Queue status: OK

| Worker PID | User | Worker process | Information | Actions |
|------------|----------|----------------|-----------------------------------|---|
| 1052 | www-data | OK | The worker appears to be healthy. |   |

"worker" terimi, yazılım veya bilgisayar sistemlerindeki arka plan süreçlerini ifade etmektedir. Yani, "workerlar", MISP'in arka planda çalışan parçalarıdır ve genellikle farklı görevleri yerine getirirler. Örneğin, veri senkronizasyonu, analiz işlemleri veya diğer veri işleme görevleri için workerlar kullanılabilir.

Workerlar, MISP'in verimli çalışmasını sağlamak için önemlidir ve genellikle otomatik olarak başlatılır ve durdurulur. Bu bağlamda "worker", genellikle bir bilgisayar sistemine ait olan, belirli bir görevi yerine getiren ve arka planda çalışan bir yazılım bileşeni olarak anlaşılır.

Worker Types:

Cache: Önbellek işlemlerini gerçekleştiren worker türüdür. Genellikle MISP'in performansını artırmak için kullanılır.

Default: Varsayılan worker türüdür ve genel sistem işlevselliğini destekler.

Email: E-posta gönderme işlemlerini yöneten worker türüdür.

Update: Veri güncelleme işlemlerini gerçekleştiren worker türüdür.

Prio: Öncelikli işlemleri yöneten worker türüdür.

Scheduler: Zamanlanmış görevleri yöneten worker türüdür.

Çalışmayan Workerlar:

Eğer workerlar çalışmıyorsa, bu durumda bile, onlarla ilgili herhangi bir işlem askıya alınır ve hiçbir veri kaybolmaz. Workerları yeniden başlatmak, askıya alınan işlemleri yeniden başlatacaktır.

Workerların Yeniden Başlatılması:

Kullanıcı arayüzü üzerinden veya komut satırından manuel olarak yapılabilir.

Komut satırından workerları manuel olarak başlatmak için,

```
sudo -u www-data bash /var/www/MISP/app/Console/worker/start.sh
```

komutu kullanılabilir.

• Download report

Araçta görünen tüm ayarların JSON formatında bir raporunu indirilebilir.

Revision #6

Created 9 April 2024 17:24:54 by İlayda Durlanık

Updated 14 April 2024 12:04:38 by İlayda Durlanık