



Guide för att installera och driftsätta MISP

Denna guide är framtagen som ett stöd för organisationer som vill installera och driftsätta MISP. Det finns flera möjliga sätt att genomföra installation, konfiguration och förvaltning av MISP. Varje organisation ansvarar själv för de tekniska, organisatoriska och säkerhetsmässiga beslut som fattas i samband med införandet. Guiden ska inte ses som en komplett eller bindande rekommendation, utan ett komplement till organisationens egen analys.

Guiden bygger i hög utsträckning på CIRCL:s installationsguide och delar av innehållet är direkt översatt.

MISP och arkitektur

Kopplat till installation av MISP är frågan om arkitektur. Arkitektur handlar i detta sammanhang om hur olika komponenter placeras, kommunicerar och skalas för att uppfylla krav på prestanda, säkerhet och tillgänglighet. MISP består av flera komponenter som tillsammans bildar en modulär arkitektur.

Kärnan är en webbapplikation som hanterar användargränssnitt och API-anrop, tillsammans med en relationsdatabas där händelser och attribut lagras. Utöver detta används en in-memory-databas för cache, sessionshantering och bakgrundsjobb, medan Python-baserade moduler används för integrationer och databerikning.

Hur dessa komponenter placeras och dimensioneras påverkar både prestanda, skalbarhet och driftsäkerhet. En vanlig arkitektur är att använda separata Edge- och Internal-noder, där externa underrättelser först tas emot och granskas på en Edge-nod innan utvalda indikatorer förs vidare till interna system. För en mer detaljerad genomgång av arkitekturval och designrekommendationer, se MISP-Projects [webbsida](#).

Produktionsinstallation (fullständig installation och flexibilitet)

Källkod och dokumentation

MISP Project är open source och den officiella källkoden publiceras via projektets [GitHub-repository](#) tillsammans med dokumentation, installationsskript och uppdateringsrutiner.

Alla installationsmetoder – oavsett om de är skriptbaserade, containerbaserade eller konfigurationshanterade – bygger ytterst på denna officiella källkod.

Det är dock viktigt att skilja mellan:

- **Officiella komponenter** som underhålls direkt av MISP-projektet
- **Kompletterande distributionsprojekt** (exempelvis Docker-implementationer) som underhålls separat men använder den officiella källkoden som grund

[ChangeLog](#) innehåller en detaljerad lista över ändringar mellan versioner.

Systemkrav

MISP kan installeras på de flesta GNU/Linux-distributioner.

För MISP 2.5 rekommenderas starkt:

- Ubuntu 24.04
- [Installationsskripten](#) som tillhandahålls av projektet

Andra distributioner fungerar, men kan kräva manuell konfiguration.

Viktigt om äldre versioner

MISP 2.4 är i slutet av sin livscykel och får endast säkerhetsfixar.

Det rekommenderas inte att installera nya miljöer på denna version.

Om du redan kör 2.4:

- Uppgradera operativsystemet till Ubuntu 24.04
- Använd [uppgraderingsskriptet](#) till nyare version

Om din distribution inte stöds av installationsskripten rekommenderas en Docker-baserad installation.

Rekommenderad distributionsmodell

För produktion rekommenderas i första hand:

- Ubuntu 24.04 med officiella installationsskript eller
- misp-docker-projektet

Alternativa installationsmetoder

Docker

Det finns produktionsklara [Docker-images](#) för:

- MISP
- MISP-modules

De underhålls löpande och publiceras regelbundet.

Det finns även säkerhets- och prestandaoptimerade varianter baserade på [CentOS Stream 8](#).

Läs respektive projekts README för att välja rätt variant.

Puppet

Det finns en [Puppet-MISP](#) som kan installera och konfigurera MISP på CentOS 7.

Ansible

Det finns färdiga roller för att automatisera installation av [MISP](#).

RPM-paket

[RPM-baserade](#) paket finns tillgängliga för vissa miljöer.

Licens

MISP är fri och öppen källkod under AGPL-licensen.

[Taxonomier](#) och [Galaxy-data](#) är licensierade under:

- [CC0 1.0](#) (Public Domain) eller
- 2-clause BSD

Detta möjliggör integration med både öppna och proprietära system.

Test, utbildning och utvärdering (förkonfigurerad VM)

Den här delen är avsedd för:

- Test
- Proof-of-Concept
- Utbildning

- Demo-miljöer

Den ska inte ses som en produktionsinstallation.

Färdig virtuell MISP-miljö

CIRCL tillhandahåller en färdig virtuell maskin med MISP installerat. Den:

- Uppdateras automatiskt efter varje commit till huvudprojektet
- Är optimerad för utbildning och utvärdering
- Kräver minimal installationstid

Hämta VM-imagen

VM-imagen finns på CIRCL:s sida för utbildningsmaterial.

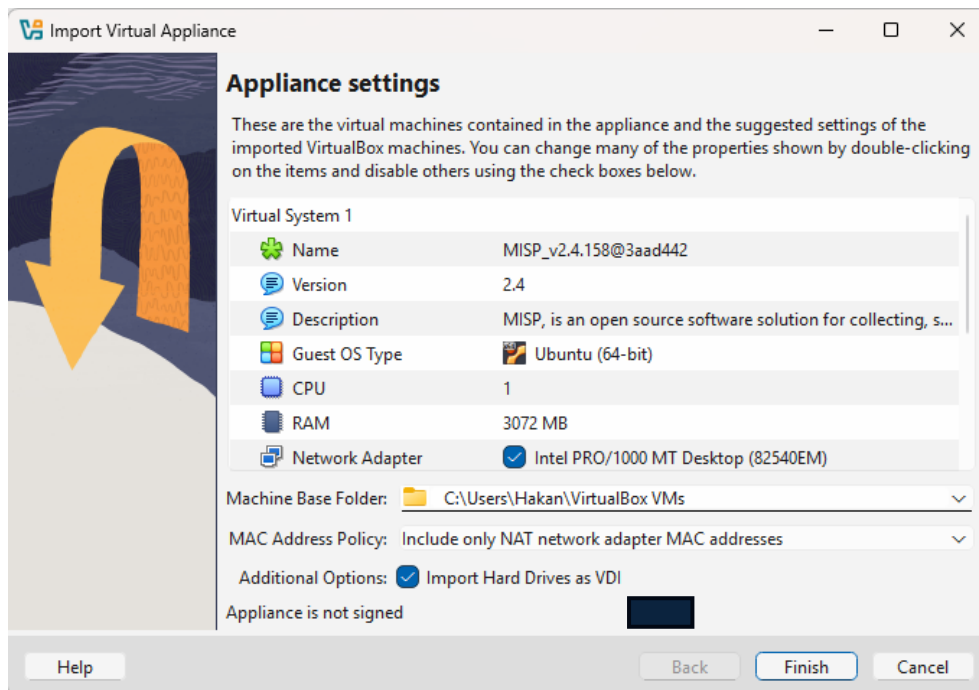
Steg:

1. Gå till [CIRCL:s webbplats](#)
2. Navigera till [Training-området](#)
3. Välj [MISP Malware Information Sharing Platform – Threat Sharing](#)
4. Ladda ned:
 - [VM-image](#)
 - [Utbildningsmaterial](#)
5. Verifiera SHA512-fingeravtrycket

Importera i VirtualBox

Använd funktionen:

- "Import Appliance..."



[Manualen](#) täcker främst VirtualBox.

VMware fungerar också, men där krävs ingen port-forwarding och vissa mindre justeringar kan behövas.

ESXi har testats och fungerar, men kan kräva ändring av ATA-bus.

Standardåtkomst till VM

Förkonfigurerade adresser:

- GUI:
<http://localhost:8080>
- SSH:
localhost port 2222

Standardkonton:

- GUI admin:
admin@admin.test / admin
- SSH:
användare: misp
lösenord: Password1234
- MySQL-uppgifter:
finns i:
~misp/mysql.txt

Nätverksinställningar

VirtualBox-konfigurationen bör ha två nätverkskort:

- NAT

- Host-only

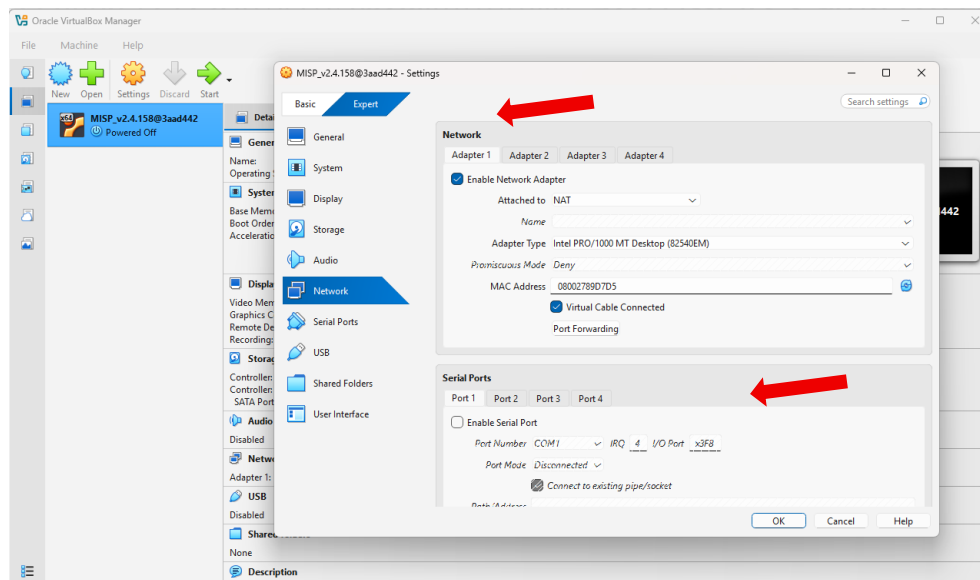
Port-forwarding (standard):

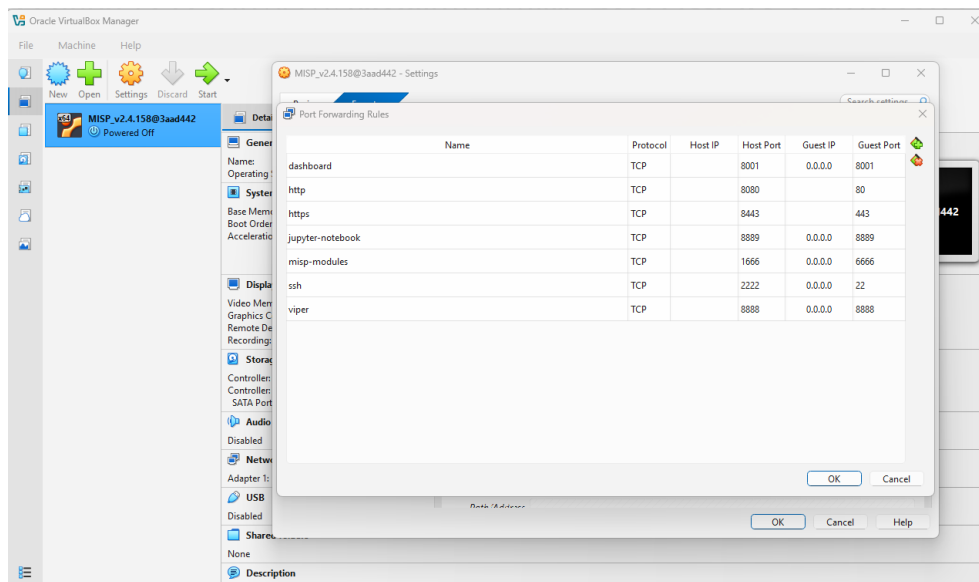
- 2222 → 22 (SSH)
- 8080 → 80 (Web GUI)
- 8443 → 443 (HTTPS – normalt ej aktivt)
- 8001 → Dashboard
- 8888 → Viper UI
- 1666 → MISP modules API

Om en port redan används startar VM ändå, men just den porten fungerar inte.

Port-forwarding kan ändras via:

Settings → Network → Advanced → Port forwarding





VMware-användare ansluter direkt till VM:ens IP-adress eftersom ingen port-forwarding sker där.

Ändra base URL

Om du behöver nå MISP från andra system kan du ändra bas-URL:

Via CLI:

```
sudo -u www-data /var/www/MISP/app/Console/cake Baseurl [baseurl]
```

Verifiera:

```
grep baseurl /var/www/MISP/app/Config/config.php
```

Extern base URL kan sättas senare via GUI eller CLI:

```
sudo -u www-data /var/www/MISP/app/Console/cake Admin setSetting  
external_baseurl [external_baseurl]
```

Detta är inte nödvändigt för lokal åtkomst.