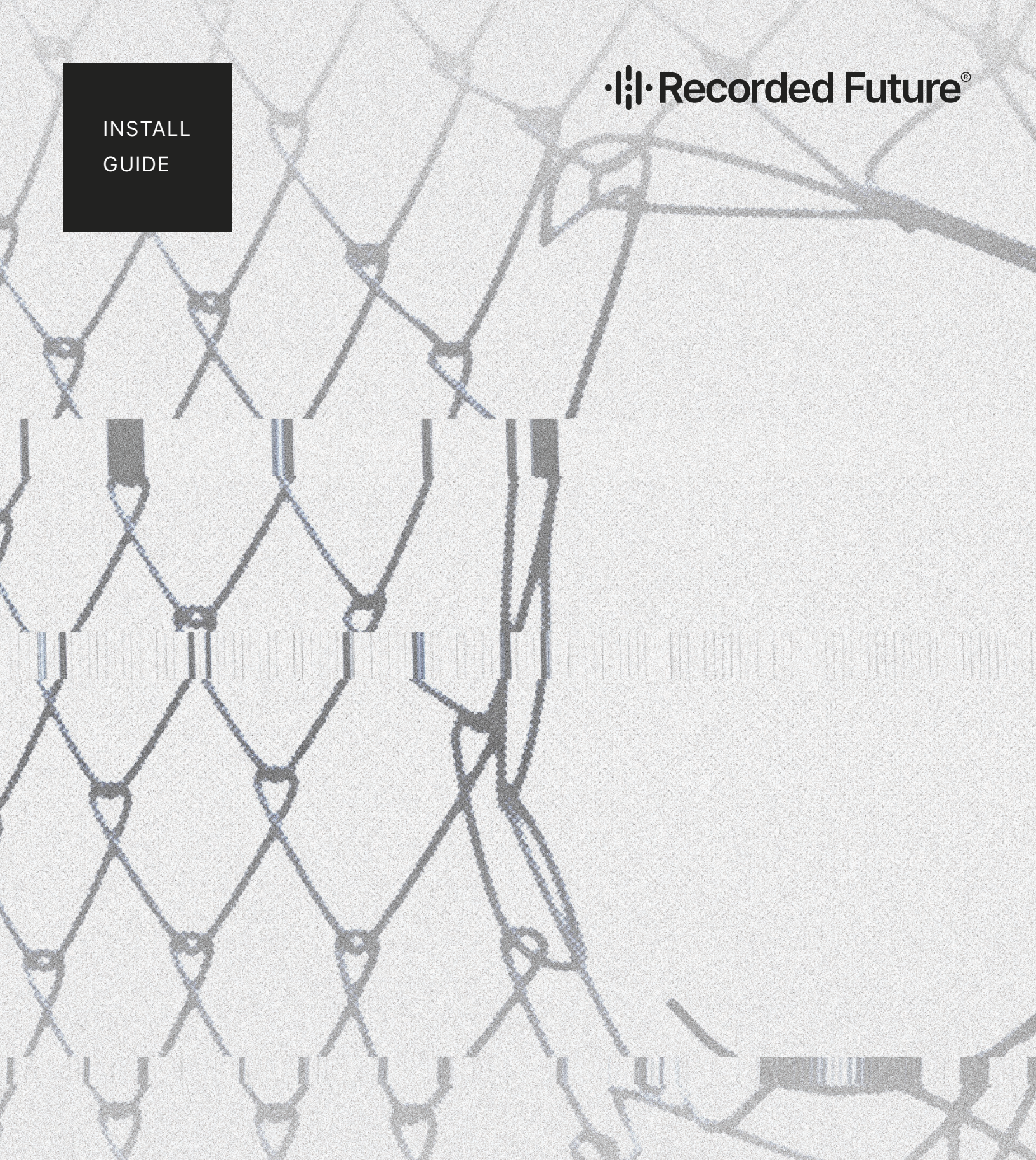
INSTALL
GUIDE

Recorded Future®



Recorded Future® for MISP, v2.0

Table of Contents

Overview

This guide describes the steps involved in integrating Recorded Future as both a Feed and Extension Module within MISP. Please note that expansive permissions are required within MISP to complete this integration.

Please contact your MISP administrator if you have insufficient permissions.

Prerequisites

Input your API Token

See Managing API Tokens on the Support Site for more information.

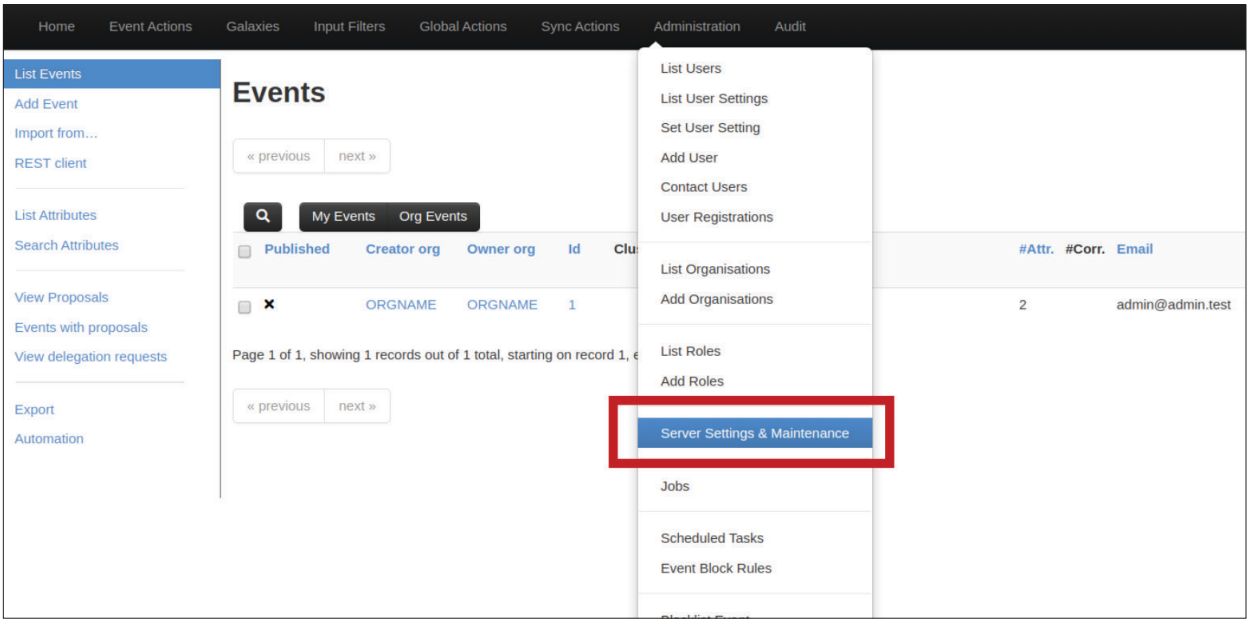
Software Versions

MISP 2.4.x

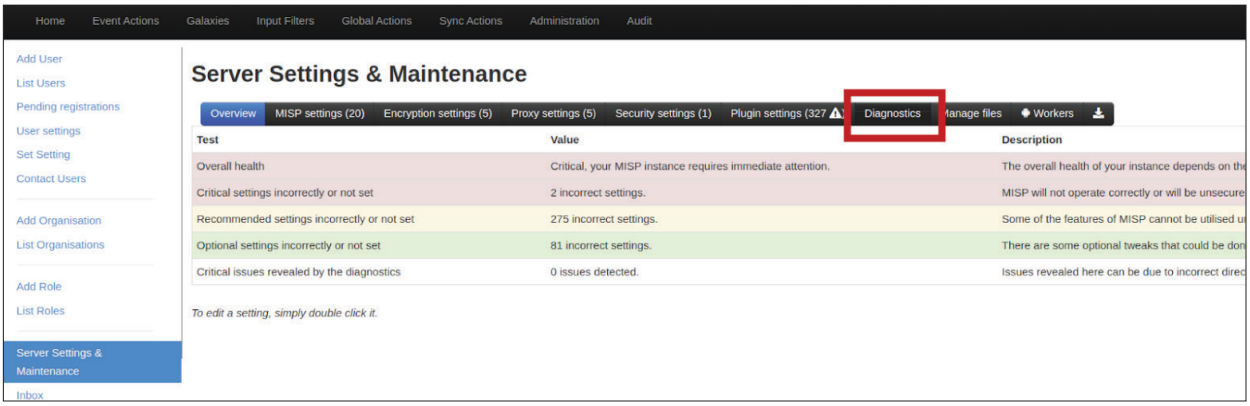
MISP Extension Module Installed

To confirm that the misp-modules services has been installed correctly and is running, follow these steps:

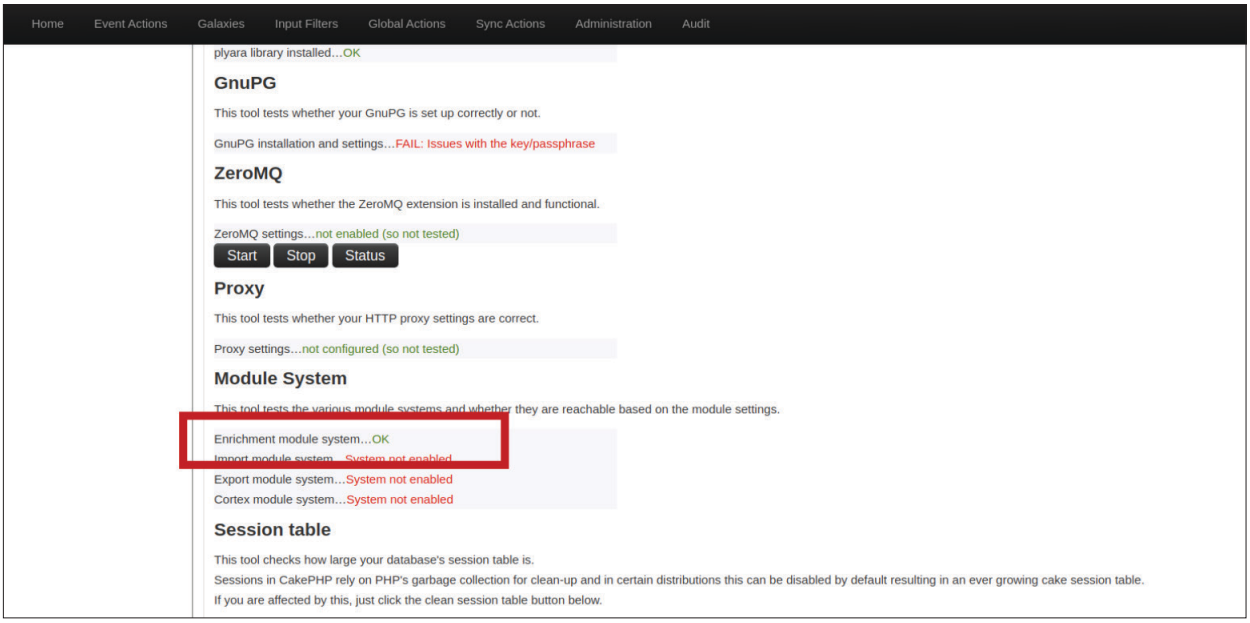
1. Go to Administration > Server Settings & Maintenance



2. Enter the Diagnostics tab



3. Scroll down to the Module System section and confirm the status is OK

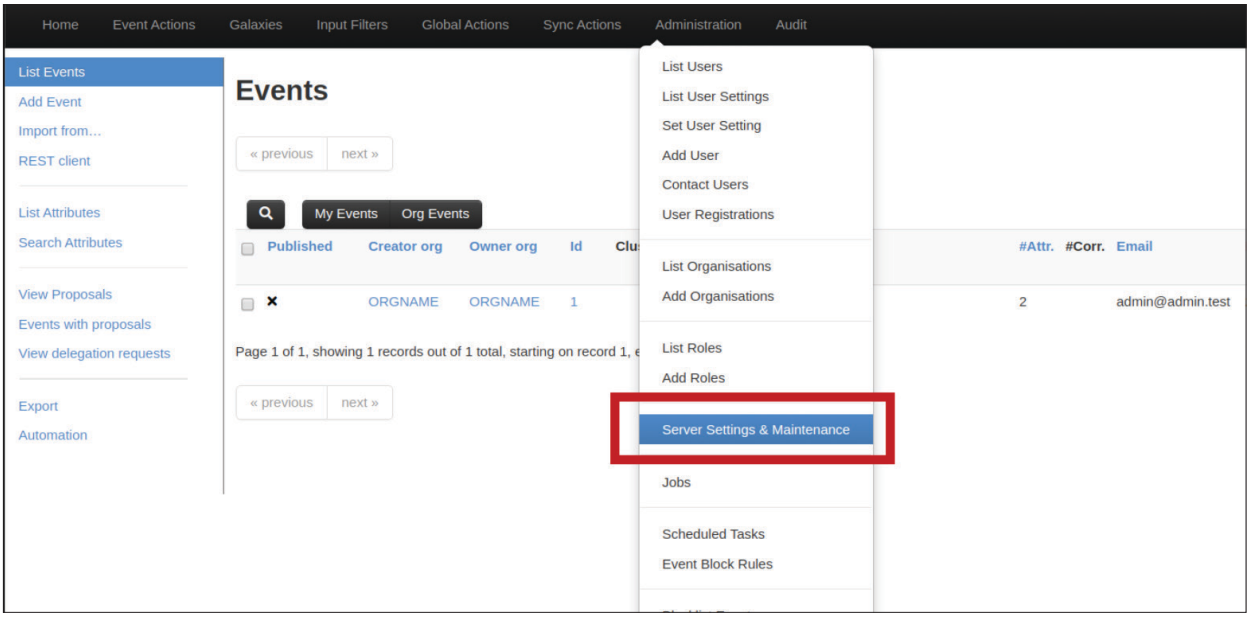


Enable Enrichment Module

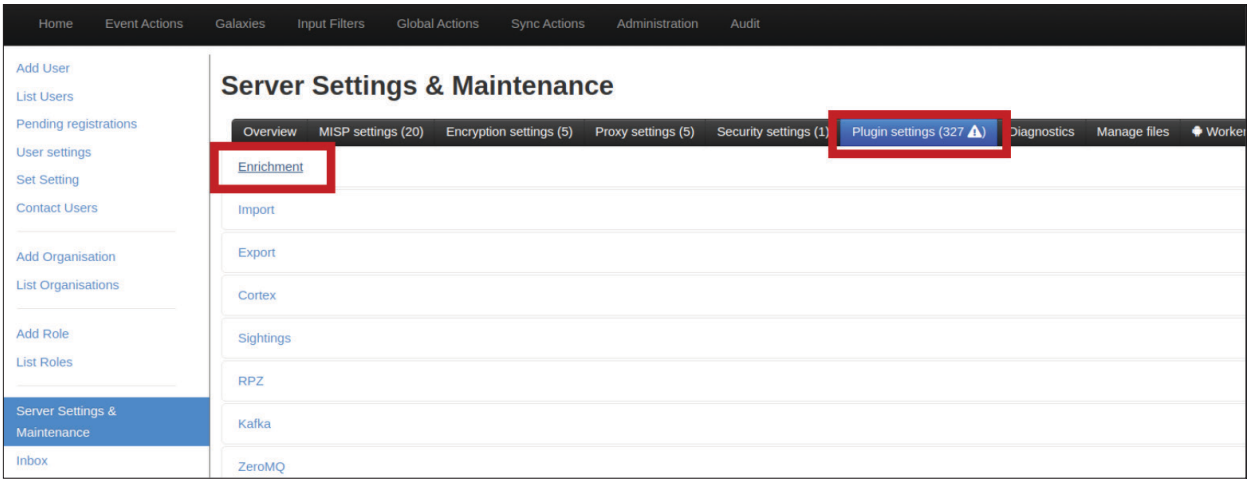
Running any type of extension module in MISP requires the misp-modules service to be installed. Instructions for installing the misp-modules service can be found in the official MISP modules documentation here. Installing the misp-modules service automatically installs the Recorded Future expansion module.

To confirm that the Recorded Future enrichment module is installed, follow these steps:

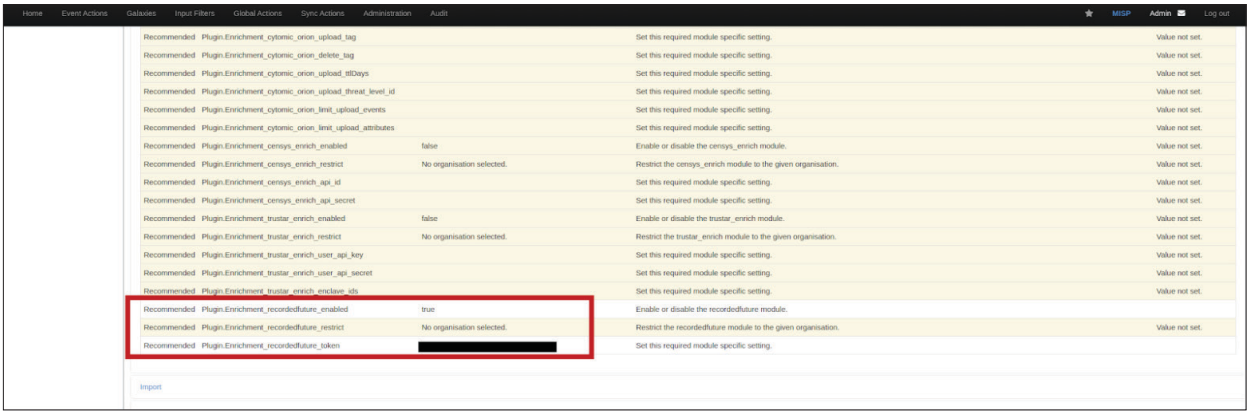
1. Go to Administration > Server Settings & Maintenance



2. Enter the Plugin settings tab and expand the Enrichment settings



3. Scroll down the expanded enrichment settings and look for the Recorded Future specific settings (such as Plugin.Enrichment_recordedfuture_enabled)

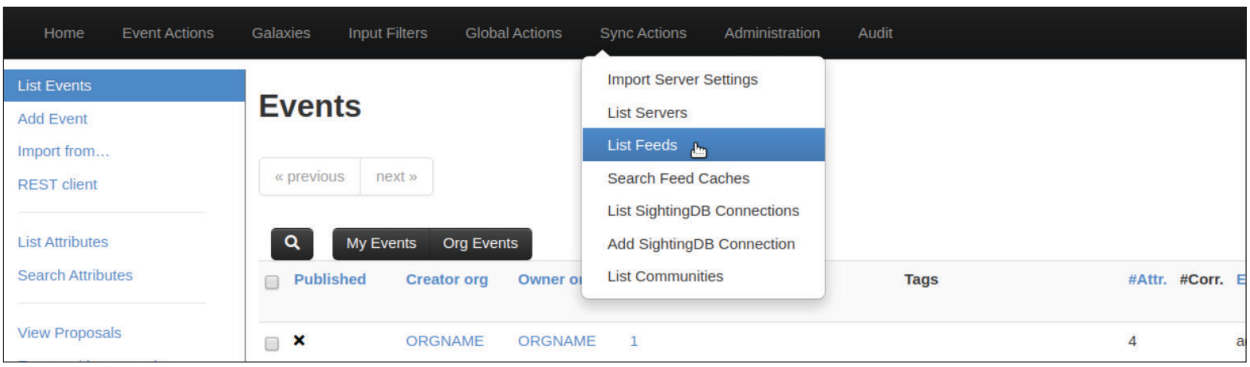


Configuring Feeds

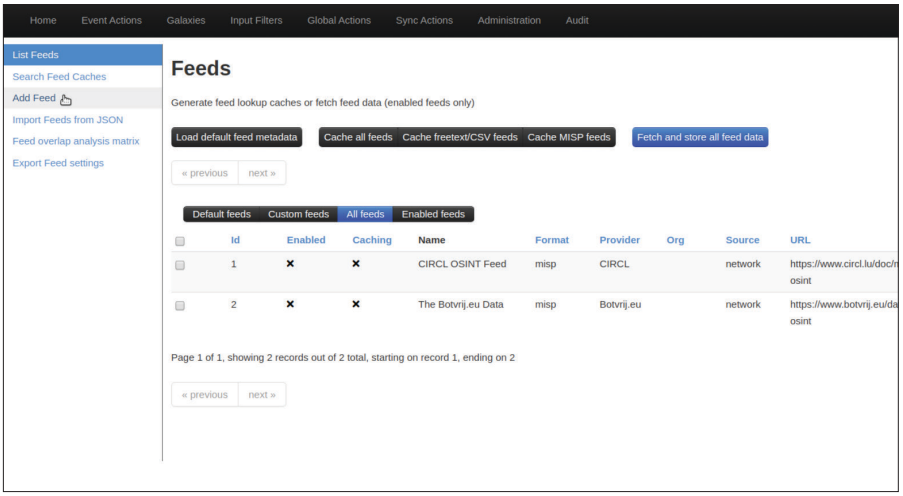
The Recorded Future MISP Feeds make use of the built in feeds functionality in MISP to allow anyone with a Recorded Future API key to download different lists of indicators and/or vulnerabilities associated with specific Recorded Future risk rules.

Setting Up a Feed

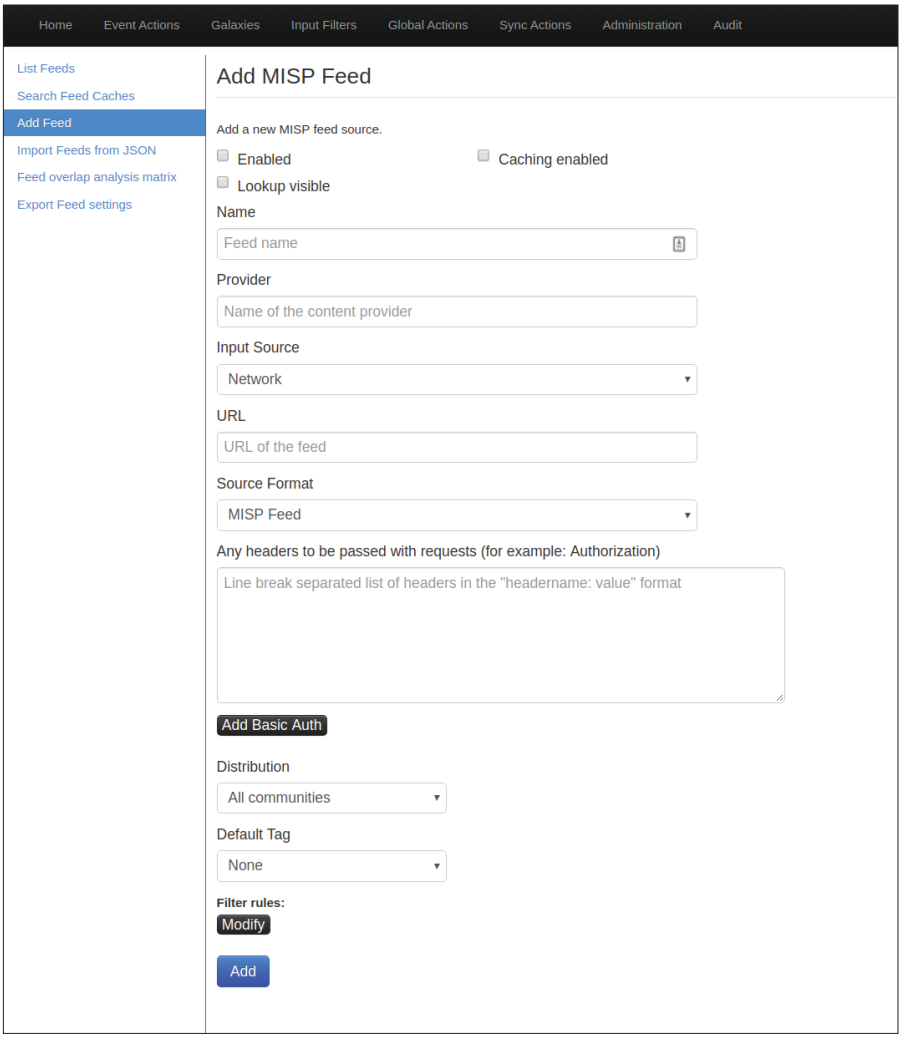
1. Go to Sync Actions → List Feeds



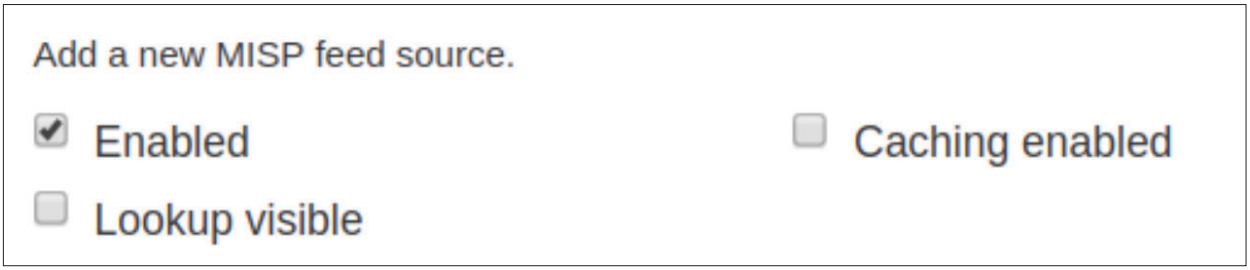
2. Go to Add Feed



3. This brings you to the feed configuration page



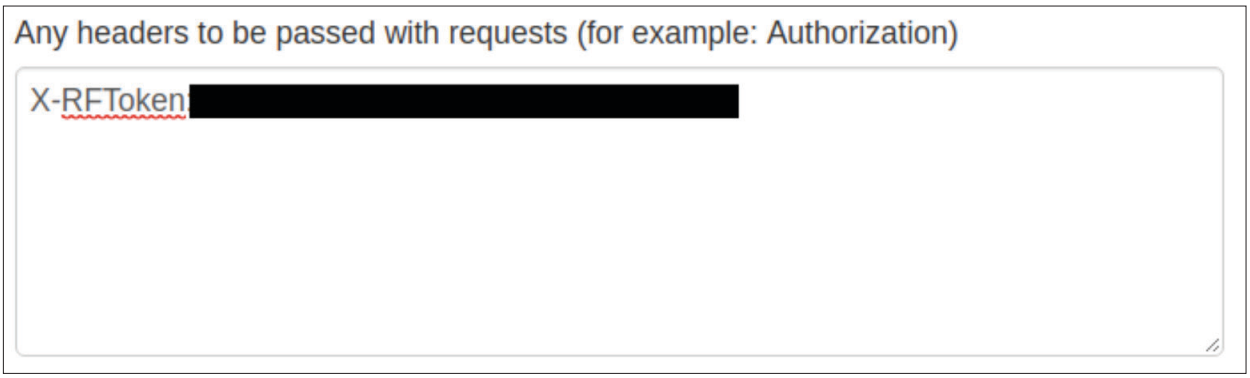
4. Toggle the Enabled box



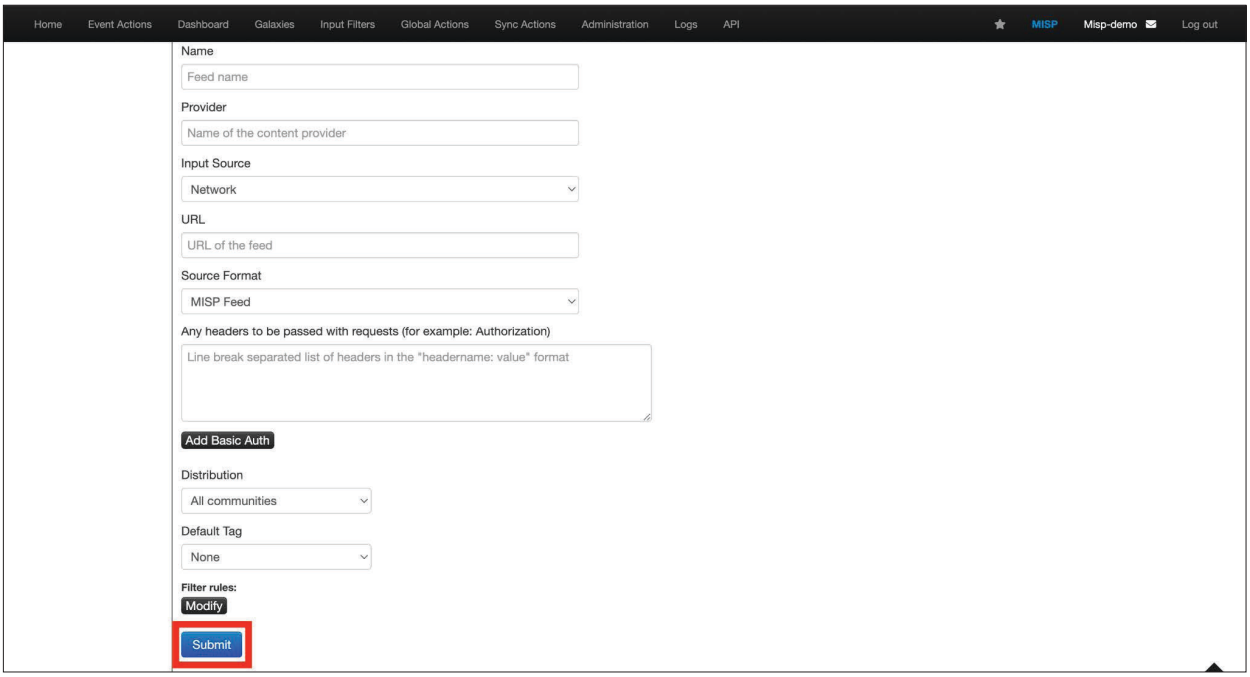
5. Enter feed name and provider (only cosmetic)

6. Enter feed URL (this is what decides what feeds you will download). A list with all available feeds is available in the Appendix Section.

7. Enter a Recorded Future API token in the format: X-RFToken:abc123**********



8. Press Submit once the feed has been configured



Importing All Feeds In Bulk

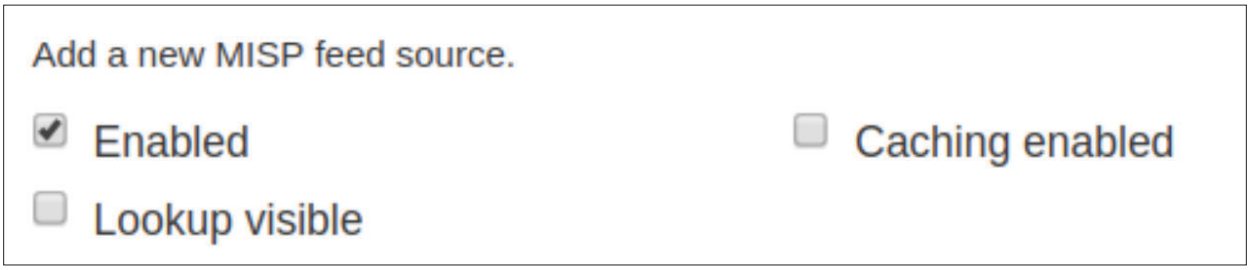
1. Recorded Future provides a dedicated JSON file to import all available feeds into MISP. The file is available at the following URL: https://api.recordedfuture.com/gw/misp/feed/import

The file can be downloaded by running the following command, where your Recorded Future token needs to be entered:

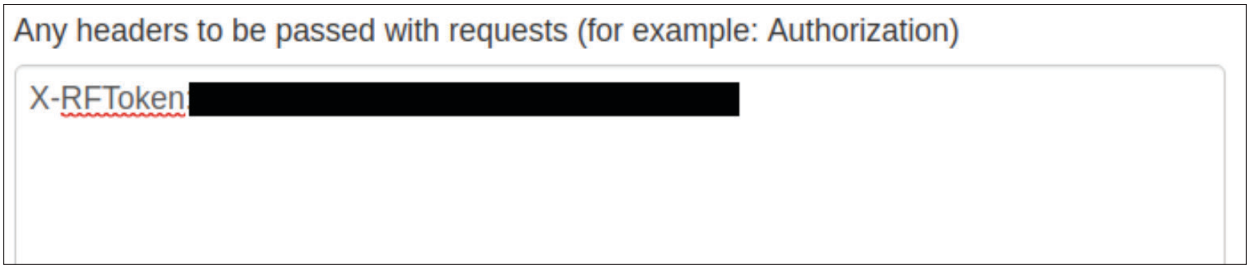
```
curl -X GET -H "Content-Type: application/json" -H "accept: application/json" -H "X-RFToken: XXX" 'https://api.recordedfuture.com/gw/misp/feed/import'
```

2. To import the Recorded Future feeds, select the Import Feeds from JSON option on the side menu. Paste MISP feed metadata JSON, that was previously downloaded, into the text box and click the Add button.

3. Edit the created feed and enable the ones that are relevant for the organization.

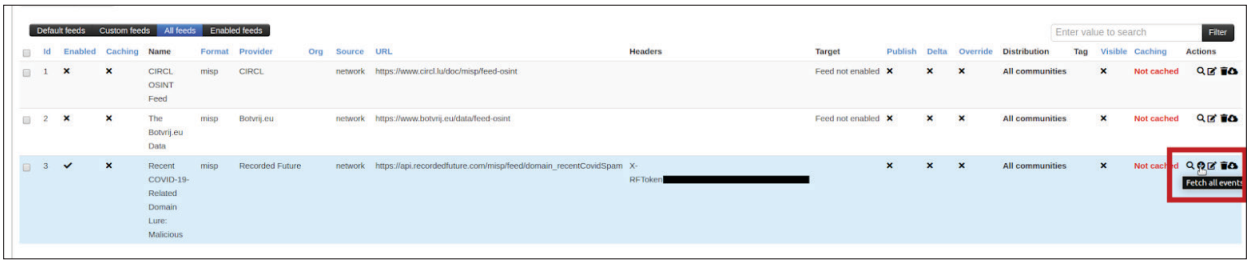


4. For each on of the enabled feed and enter a Recorded Future API token in the format: X-RFToken:abc123**********

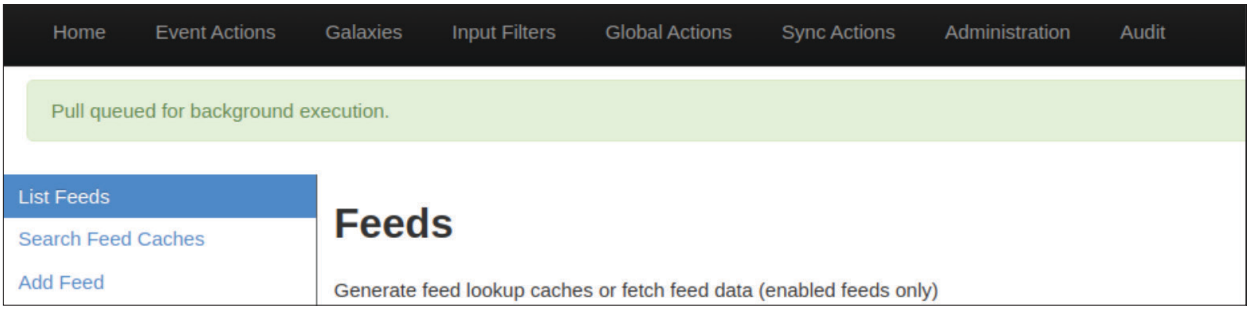


Creating an Event from a Feed

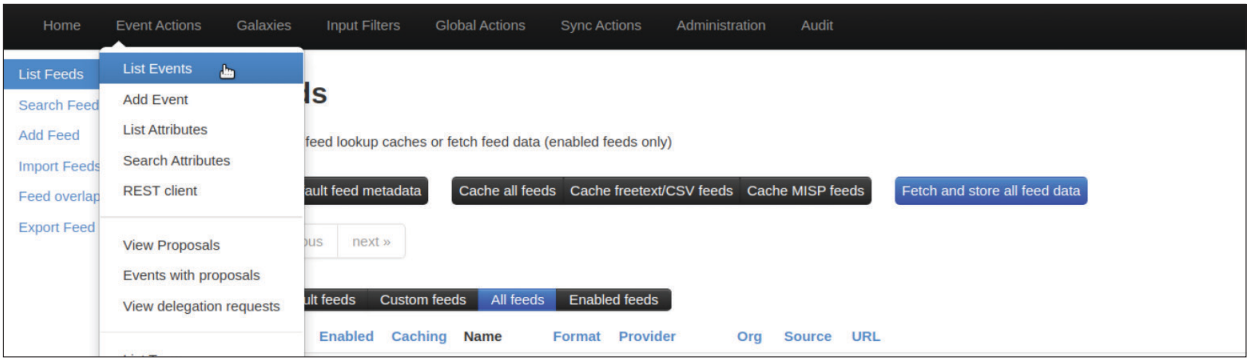
1. Click the fetch all events button on the newly added feed



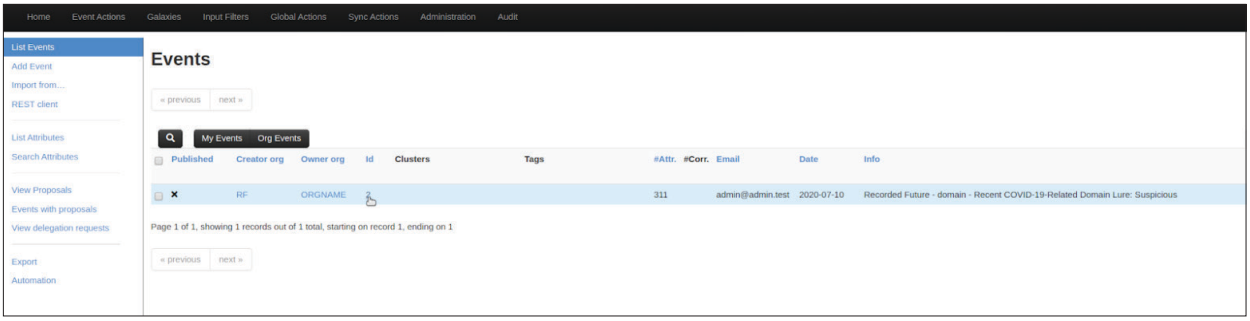
2. If the feed has been configured correctly it will start downloading



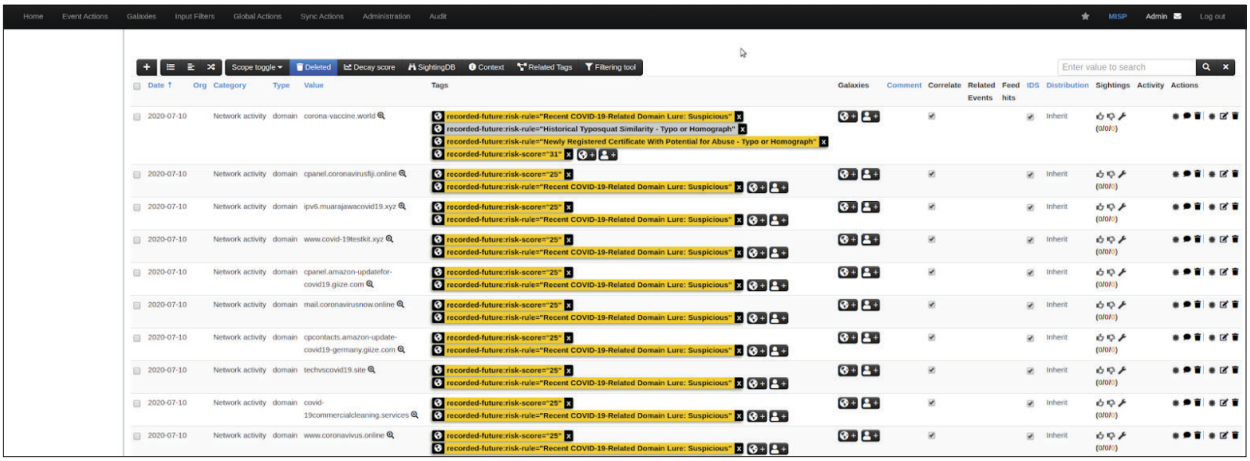
3. Go to Event Actions → List Events



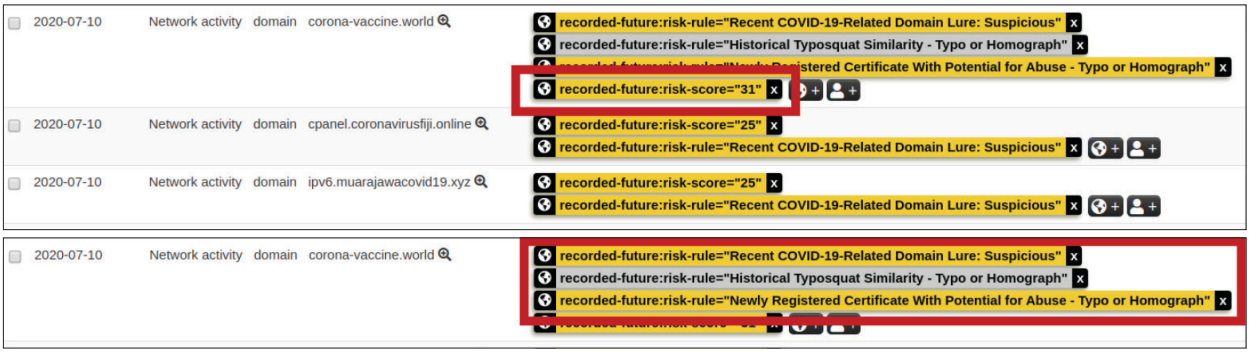
4. The event created by the feed should now be present in the list of events (it can take a few minutes for the event to populate)



5. Clicking the event will show all the attributes (indicators) included in the specific feed



6. Each attribute is tagged with Recorded Future risk scoring and triggered risk rules



IDS Flag

According to the MISP core format data standard, the to_ids flag represents whether the attribute is meant to be actionable. The following list of feeds will have the to_ids flag enabled by default which we recommend to be used for detection or correlation actions:

- Default Domain Risk List: Risk Score 90+
- Recent C&C DNS Name
- Actively Communicating C&C Server
- Default IP Risk List: Risk Score 90+
- Recently Active Targeting Vulnerabilities in the Wild
- SCF - C2 Communicating Ips
- SCF - Weaponized Domains
- SCF - Exploits Itw Hashes
- Validated C&C Server

Troubleshooting

Extension Module

If you can't find the Recorded Future app settings this means that you either have an older version of the misp-modules service installed. To manually install the Recorded Future expansion module on top of an existing misp-modules installation, follow these steps:

1. Locate the misp-modules directory on your MISP server

```
root@misp-int-dev-01:/opt/misp/misp-modules# pwd
/opt/misp/misp-modules
```

2. Copy the Recorded Future script into the expansion modules folder

```
root@misp-int-dev-01:/opt/misp/misp-modules# cp /tmp/recordedfuture.py misp_modules/modules/expansion/
root@misp-int-dev-01:/opt/misp/misp-modules# ls misp_modules/modules/expansion/
apiosintds.py           cve_advanced.py         google_search.py                macvendors.py       ransomcoindb.py                urlhaus.py
apivoid.py              cve.py                  greynoise.py                    malwarebazaar.py    rbl.py                         urlscan.py
assemblyline_query.py   cytomic_orion.py       hashdd.py                       module.py.skeleton  recordedfuture.py              virustotal_public.py
assemblyline_submit.py  dbl_spamhaus.py        hibp.py                         ocr_enrich.py       reversedns.py                  virustotal.py
backscatter_io.py       _dnsdb_query            __init__.py                     ods_enrich.py       securitytrails.py              _vmray
bgpranking.py           dns.py                  intel471.py                     odt_enrich.py       shodan.py                      vmray_submit.py
btc_scam_check.py       docx_enrich.py          intelmq_eventdb.py.experimental onyphe_full.py      sigma_queries.py               vulndb.py
btc_steroids.py         domaintools.py          ipasn.py                        onyphe.py           sigma_syntax_validator.py      vulners.py
censys_enrich.py        eql.py                  iprep.py                        otx.py              sophoslabs_intelix.py          whois.py
circl_passivedns.py     eupi.py                 joesandbox_query.py             passivetotal.py     sourcecache.py                 wiki.py
circl_passivessl.py     farsight_passivedns.py  joesandbox_submit.py            pdf_enrich.py       stix2_pattern_syntax_validator.py xforceexchange.py
countrycode.py          geoip_asn.py            lastline_query.py               pptx_enrich.py      threatcrowd.py                 xlsx_enrich.py
crowdstrike_falcon.py   geoip_city.py           lastline_submit.py              qrcode.py           threatminer.py                 yara_query.py
cuckoo_submit.py        geoip_country.py        macaddress_io.py                _ransomcoindb       trustar_enrich.py              yara_syntax_validator.py
root@misp-int-dev-01:/opt/misp/misp-modules#
```

3. Modify the __init__.py script located in the expansion modules folder by adding recordedfuture to the __all__ list

```
root@misp-int-dev-01:/opt/misp/misp-modules# vi misp_modules/modules/expansion/__init__.py
```

```
from . import _vmray  # noqa
import os
import sys

sys.path.append('{}/lib'.format('/'.join((os.path.realpath(__file__)).split('/')[:-3])))

__all__ = ['cuckoo_submit', 'vmray_submit', 'bgpranking', 'circl_passivedns', 'circl_passivessl',
           'countrycode', 'cve', 'cve_advanced', 'dns', 'btc_steroids', 'domaintools', 'eupi', 'eql',
           'farsight_passivedns', 'ipasn', 'passivetotal', 'sourcecache', 'virustotal',
           'whois', 'shodan', 'reversedns', 'geoip_asn', 'geoip_city', 'geoip_country', 'wiki', 'iprep',
           'threatminer', 'otx', 'threatcrowd', 'vulndb', 'crowdstrike_falcon',
           'yara_syntax_validator', 'hashdd', 'onyphe', 'onyphe_full', 'rbl',
           'xforceexchange', 'sigma_syntax_validator', 'stix2_pattern_syntax_validator',
           'sigma_queries', 'dbl_spamhaus', 'vulners', 'yara_query', 'macaddress_io',
           'intel471', 'backscatter_io', 'btc_scam_check', 'hibp', 'greynoise', 'macvendors',
           'qrcode', 'ocr_enrich', 'pdf_enrich', 'docx_enrich', 'xlsx_enrich', 'pptx_enrich',
           'ods_enrich', 'odt_enrich', 'joesandbox_submit', 'joesandbox_query', 'urlhaus',
           'virustotal_public', 'apiosintds', 'urlscan', 'securitytrails', 'apivoid',
           'assemblyline_submit', 'assemblyline_query', 'ransomcoindb', 'malwarebazaar',
           'lastline_query', 'lastline_submit', 'sophoslabs_intelix', 'cytomic_orion', 'censys_enrich',
           'trustar_enrich', 'recordedfuture']
~
~
~
~
```

4. Stop the misp-modules service

```
root@misp-int-dev-01:/opt/misp/misp-modules# service misp-modules stop
root@misp-int-dev-01:/opt/misp/misp-modules#
```

5. Re-install the misp-modules (command depends on your environment and distribution, see misp-modules documentation)

```
root@misp-int-dev-01:/opt/misp/misp-modules# /opt/misp/venv/bin/pip3.6 install -I -r REQUIREMENTS
```

```
root@misp-int-dev-01:/opt/misp/misp-modules# /opt/misp/venv/bin/pip3.6 install .
```

6. Start the misp-modules service

```
root@misp-int-dev-01:/opt/misp/misp-modules# service misp-modules start
root@misp-int-dev-01:/opt/misp/misp-modules#
```

APPENDIX A: Supported Security Control Feeds

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
SCF - C2 Communicating Ips	https://api.recordedfuture.com/gw/misp/feed/scf_c2_communicating_ips	Very Malicious	Recorded Future Internet Scanning collects live information about internet hosts and Network Traffic Analysis observes the midpoint between the adversary and their victims as they build, stage, and launch attacks. The Command and Control dataset fuses those two methods to identify and track IPs that we have scanned as positive C2 and then observed communications to understand how the C2 is interacting with infected machines as well as being controlled by the adversary. This method has been used to produce unique Intelligence where we can observe and track Command and Control activity at Internet scale.
SCF - Weaponized Domains	https://api.recordedfuture.com/gw/misp/feed/scf_weaponized_domains	Very Malicious	Recorded Future Domain Analysis observes the entire Domain Weaponization lifecycle from Domain registration, resolution to IP address, Certificate provisioning, Mail Server configuration, and URL propagation to assess risk of malicious activity. There are pockets of the Internet that allow adversaries to enjoy economies of scale due to free, anonymous, and unmonitored services. The Weaponized Domains and URLs datasets identifies domains and URLs with live activity in those Service Providers and connects them with a Bad Actor threat model to present a set of Domains that have a risk of being malicious even before a URL has ever been seen in the wild and as well as a set of Domains and URLs that been verified as malicious.
SCF - Exploits Itw Hashes	https://api.recordedfuture.com/gw/misp/feed/scf_exploits_itw_hashes	Very Malicious	Recorded Future Malware Hunting analyzes billions of malware samples to identify important samples that have static and behavioral characteristics that make them important to Intelligence and Security teams. The Exploits in the Wild dataset identifies SHA-256 hashes and vulnerabilities where we have observed recent malware activity in the wild. This technique uses submissions to popular malware repositories as a rough proxy for propagation in the wild since we believe that the majority of the submission activity to malware repositories is done automatically by security tools and Antivirus vendors as samples are discovered on endpoints, in email, or on networks. This method has been used to produce unique Intelligence where we have observed Malware known to exploit Vulnerabilities activity In the Wild (ITW).

APPENDIX B: Supported IP Risk Lists

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default IP Risk List: Risk Score 90+	https://api.recordedfuture.co m/gw/misp/feed/ip_default	Very Malicious	Indicators with a Risk Score of 90 and higher
Actively Communicating C&C Server	https://api.recordedfuture.co m/gw/misp/feed/ip_recentActiveCnc	Very Malicious	Observing C2 communications with infected machines or adversary control by Recorded Future Network Traffic Analysis [ATT&CK] Tactic: Command and Control Mitigated to Suspicious level by whitelisting of the IP Address. Also mitigated to Suspicious level by metadata published in the threat list indicating low confidence in the finding.
Validated C&C Server	https://api.recordedfuture.com /gw/misp/feed/ip_recentValidatedCnc	Very Malicious	Recently detected or reported C2 that was further validated as a running C2 by Insikt Group using proprietary methodology. [ATT&CK] Tactic: Command and Control
Recently Reported by Insikt Group	https://api.recordedfuture.com/gw/misp/feed/ip_recentAnalystNote	Malicious	Primary Indicator in an Insikt Group Note [ATT&CK] Tactic: Command and Control
Phishing Host	https://api.recordedfuture.com/gw/misp/feed/ip_phishingHost	Malicious	Reported as host of an active phishing URL [ATT&CK] Technique: Spear Phishing Link Mitigated to Suspicious level by whitelisting of the IP Address

APPENDIX C: Supported DOMAIN RiskLists

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default Domain Risk List: Risk Score 90+	https://api.recordedfuture.com/gw/misp/feed/domain_default	Very Malicious	Indicators with a Risk Score of 90 and higher
Recent C&C DNS Name	https://api.recordedfuture.com/gw/misp/feed/domain_recentCncSite	Very Malicious	DNS Name associated with malicious Command and Control [ATT&CK] Technique: Application Layer Protocol, DNS
Recently Detected Malware Operation	https://api.recordedfuture.com/gw/misp/feed/domain_recentMalwareSiteDetected	Malicious	This rule provides high confidence that the domain distributed or was connected to malware. [ATT&CK] Tactic: Initial Access, Tactic: Command and Control
Recently Detected Phishing Techniques	https://api.recordedfuture.com/gw/misp/feed/domain_recentPhishingSiteDetected	Malicious	This rule provides high confidence that the domain was involved in phishing activities. [ATT&CK] Technique: Spearphishing Link
Recently Reported Fraudulent Content	https://api.recordedfuture.com/gw/misp/feed/domain_recentFraudulentContent	Malicious	Domain has been reported to convince victims to send money/bitcoin for items that look legitimate. [ATT&CK] Technique: Spearphishing via Service
Recently Active Weaponized Domain	https://api.recordedfuture.com/gw/misp/feed/domain_recentWeaponizedDomain	Malicious	Domain activity observed in connection to Bad Actor tracked by Recorded Future Domain Analysis [ATT&CK] Technique: Spearphishing Link, Tactic: Command and Control
Recently Reported by Insikt Group	https://api.recordedfuture.com/gw/misp/feed/domain_recentAnalystNote	Malicious	Involved in an Insikt Group Note [ATT&CK] Tactic: Initial Access, Tactic: Command and Control, Technique: Malicious Link
Recent COVID-19-Related Domain Lure: Malicious	https://api.recordedfuture.com/gw/misp/feed/domain_recentCovidLure	Malicious	Domain with COVID-19 related naming characteristics which is convicted as malicious by technical analysis. [ATT&CK] Tactic: Initial Access, Tactic: Execution
Recent Phishing Lure: Malicious	https://api.recordedfuture.com/gw/misp/feed/domain_recentPhishingLureMalicious	Malicious	This rule provides high confidence conviction for active domains that appear to be phishing lures. This is a recently changed domain that contains an internet service brand names within the last 90 days. [ATT&CK] Tactic: Initial Access, Tactic: Execution

APPENDIX D: Supported URL RiskLists

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default URL Risk List: Risk Score 70+	https://api.recordedfuture.com/gw/misp/feed/url_default	Very Malicious & Malicious	Indicators with a Risk Score of 70 and higher
Recently Detected Malware Distribution	https://api.recordedfuture.com/gw/misp/feed/url_recentMalwareSiteDetected	Malicious	Site distributes malware [ATT&CK] Technique: User Execution
Recently Detected Phishing Techniques	https://api.recordedfuture.com/gw/misp/feed/url_recentPhishingSiteDetected	Malicious	Site contains logos, images, text, and other attributes to steal user credentials. [ATT&CK] Technique: Spearphishing Link
Recently Reported by DHS AIS	https://api.recordedfuture.com/gw/misp/feed/url_recentDhsAis	Malicious	Reported by DHS Automated Indicator Sharing
Recently Reported by Insikt Group	https://api.recordedfuture.com/gw/misp/feed/url_recentAnalystNote	Malicious	Recently Reported as a Threat in Insikt Group Reporting
Active Phishing URL	https://api.recordedfuture.com/gw/misp/feed/url_phishingUrl	Malicious	URL reported as an active phish [ATT&CK] Technique: Spearphishing Link

APPENDIX E: Supported HASH RiskLists

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default Hash Risk List: Risk Score 80+	https://api.recordedfuture.com/gw/misp/feed/hash_default	Very Malicious & Malicious	Indicators with a Risk Score of 80 and higher
Recently Active Targeting Vulnerabilities in the Wild	https://api.recordedfuture.com/gw/misp/feed/hash_recentActiveMalware	Malicious	Malware known to exploit a vulnerability observed in the wild by Recorded Future Malware Hunting in the last 28 days [ATT&CK] Tactic: Execution
Observed in Underground Virus Testing Sites	https://api.recordedfuture.com/gw/misp/feed/hash_observedMalwareTesting	Malicious	Potentially undetectable malware observed on darkweb, collected from No-Distribute Scanners [Pre-ATT&CK] Technique: Test malware to evade detection
Malware SSL Certificate Fingerprint	https://api.recordedfuture.com/gw/misp/feed/hash_malwareSsl	Malicious	Fingerprint hash for an SSL Certificate that is linked to Malware [Pre-ATT&CK] Technique: SSL certificate acquisition for domain
Reported by Insikt Group	https://api.recordedfuture.com/gw/misp/feed/hash_analystNote	Malicious	Involved in an Insikt Group Note [ATT&CK] Tactic: Execution, Tactic: Persistence

APPENDIX F: Supported Vulnerability RiskLists

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default Vuln Risk List: Risk Score 90+	https://api.recordedfuture.com/gw/misp/feed/vulnerability_default	Very Critical	Vulnerabilities with a Risk Score of 90 and higher
Exploited in the Wild by Recently Active Malware	https://api.recordedfuture.com/gw/misp/feed/vulnerability_recentMalwareActivity	Very Critical	Malware known to exploit a vulnerability recently observed in the wild by Recorded Future Malware Hunting or by Recorded Future Vulnerability Analysis [ATT&CK] Tactic: Execution
NIST Severity: Critical	https://api.recordedfuture.com/gw/misp/feed/vulnerability_nistCritical	Critical	Assigned a Critical CVSS score in the National Vulnerability Database [Pre-ATT&CK] Technique: Research relevant vulnerabilities/CVEs Note: For normalization, Risk Scoring assumed the minimum Temporal Score for CVSSv3 since our other Risk Rules will provide the Temporal component
Exploited in the Wild by Malware	https://api.recordedfuture.com/gw/misp/feed/vulnerability_malwareActivity	Critical	Malware known to exploit a vulnerability observed in the wild by Recorded Future Malware Hunting [ATT&CK] Tactic: Execution
Recent Verified Proof of Concept Available Using Remote Execution	https://api.recordedfuture.com/gw/misp/feed/vulnerability_recentPocVerifiedRemote	Critical	Verified Proof of Concept exploit code is available using Remote Execution protocols
Historically Exploited in the Wild by Malware	https://api.recordedfuture.com/gw/misp/feed/vulnerability_historicMalwareActivity	High	Malware known to exploit a vulnerability historically observed in the wild by Recorded Future Malware Hunting [ATT&CK] Tactic: Execution
Recently Reported by Insikt Group	https://api.recordedfuture.com/gw/misp/feed/vulnerability_recentAnalystNote	High	Insikt reporting on the severity, threats, or actors leveraging the Vulnerability [Pre-ATT&CK] Technique: Research relevant vulnerabilities/CVEs
NIST Severity: High	https://api.recordedfuture.com/gw/misp/feed/vulnerability_nistHigh	High	Assigned a High CVSS score in the National Vulnerability Database [Pre-ATT&CK] Technique: Research relevant vulnerabilities/CVEs Note: For normalization, Risk Scoring assumed the minimum Temporal Score for CVSSv3 since our other Risk Rules will provide the Temporal component
Recent Verified Proof of Concept Available	https://api.recordedfuture.com/gw/misp/feed/vulnerability_recentPocVerified	High	SCF - Exploits Itw Hashes

APPENDIX G: Supported Threat Lists

List Name	MISP URL	IOC Type	DESCRIPTION AND MITIGATING FACTORS
Log4j Related Scanners	https://api.recordedfuture.com/gw/misp/feed/custom_ip_log4jRelatedScanners	IP	This list includes all servers Recorded Future has observed probing for log4j instances to identify vulnerable systems. This includes legitimate security vendors attempting to identify vulnerable systems as well as malicious activity.
Log4j Malicious Scanners	https://api.recordedfuture.com/gw/misp/feed/custom_ip_log4jMaliciousScanners	IP	This list contains IPs that have been observed scanning for CVE-2021-44228 (Log4Shell) with potential malicious activity. It includes scanners that have been observed attempting to directly load payloads and repetitively send exploit payloads without providing indications of who is conducting the activity. Follow on payloads from these IPs have included coin miners, backdoors, and IOT botnets.