Threat Grid Integration

Threat Grid Overview

Cisco Threat Grid is a unified threat intelligence and malware analysis platform, which is tightly integrated with Cisco's Advanced Malware Protection (AMP) solution. It performs automated static and dynamic analysis, producing human-readable reports with behavioral indicators for each file submitted. Threat Grid's global scalability drives context-rich information that can be consumed directly or via content rich threat intelligence feeds.

Threat Grid analyzes suspicious files against more than 950 behavioral indicators and a malware knowledge base sourced from around the world to provide industry-leading accuracy and context-rich threat analytics.

Leveraging Threat Grid as a part of a comprehensive network security strategy provides:

- Deeper insights into what malware is doing or attempting to do, how substantial a threat it poses to your organization and how to defend against it
- Accurate identification of threats with context-focused security analytics
- Proactive protection for businesses using threat intelligence from Threat Grid Premium threat feeds
- Defense against threats originating anywhere using the scale and power of a cloud service that analyzes hundreds of thousands of threats every day

ⓘ In firmware **MX 14.56**, **MX 15.43** and **MX 16.7**, important changes required for MX to AMP and Threat Grid communications were implemented. Please upgrade to these firmware versions or higher prior to:

- If **AMP and Threat Grid** are both enabled, please upgrade **prior to Oct 2021**.
- If **only AMP** is enabled, please upgrade **prior to Dec 2021**.

Please note that if AMP enabled MX devices are not upgraded prior to the above mentioned dates, AMP will fail to connect to AMP Cloud and result in a fail closed behavior. This will cause all AMP inspected file downloads to be blocked unless AMP is manually disabled.

Threat Grid and Meraki MX Integration

The AMP integration with Meraki MX Security Appliance provides Meraki users with the capability to leverage AMP's File Reputation and File Retrospection services and benefit from the global intelligence held in the AMP Cloud. The AMP Cloud responds to queries from MX devices on files that are downloaded and returns a file disposition of Clean, Malicious, or Unknown. Malicious files are blocked while Clean and Unknown files are allowed to pass through the MX to the end user. When Threat Grid integration is enabled, the MX will upload qualified, Unknown files to Threat Grid for additional static and dynamic analysis. Once the analysis is completed, a detailed report containing the threat score and behavioral indicators that matched the behaviors observed during analysis will be available in the Meraki Security Center. Depending on the severity of behaviors observed and a threat score, Meraki MX administrator may need to initiate further investigation and response. AMP for Endpoints is a complementary integrated endpoint protection solution which provides robust endpoint level visibility and control capabilities for threats that pass the perimeter defenses.

ⓘ **Note**: AMP for Endpoints is licensed separately.

The supported file types for the File Analysis service are PE executables, DLLs, PDFs, MS Office Documents (RTF, DOC, PPT(x)). If threat trends indicate that new file types are being exploited, support for them will be transparently added.

ⓘ **Note**: The number of daily file submissions which can be made to Threat Grid is determined by the organization's Threat Grid license. Threat Grid Premium license is required to gain access to Threat Grid portal with advanced capabilities for malware research and investigations.

Configuration

Prerequisites

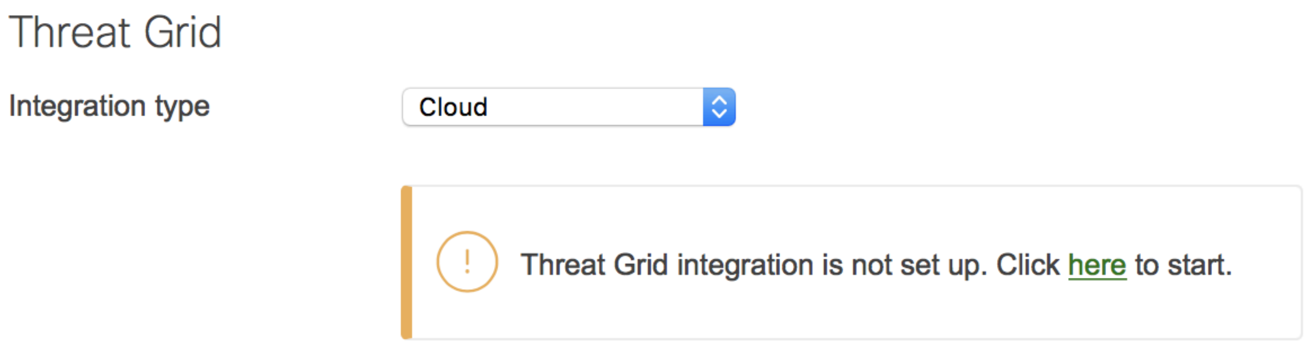
1. Ensure that you have a valid Advanced Security license for your MX appliances
2. Ensure that you have a valid Threat Grid license for MX or a Threat Grid Premium license
3. Ensure that you have enabled AMP services on your MX appliances

Linking Threat Grid and Dashboard

Navigate to the **Organization > Configure > Settings** menu.

Under the Threat Grid heading, select the **Integration type** from the drop-down and select **Cloud** or **On-Premise Appliance**.

ⓘ **Note**: Integration with Threat Grid Appliance is currently not supported. Once support is declared, this article will be updated.

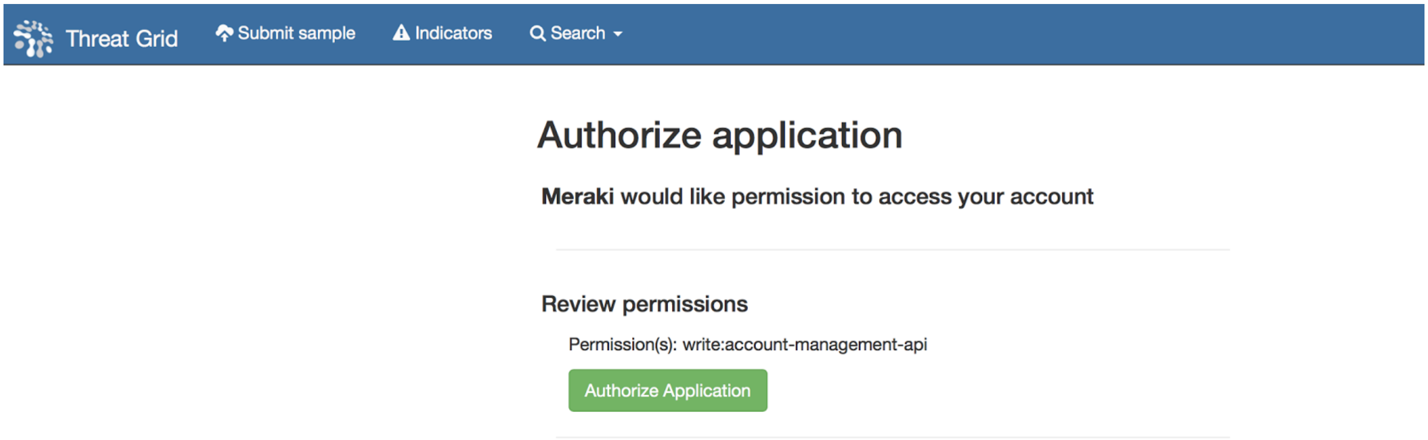


Threat Grid

Integration type: Cloud

Threat Grid integration is not set up. Click here to start.

Next, click the "here" link to access the Threat Grid portal. When prompted, click 'Authorize application' to provide MX devices within your organization with permission to access your Threat Grid account.



Authorize application

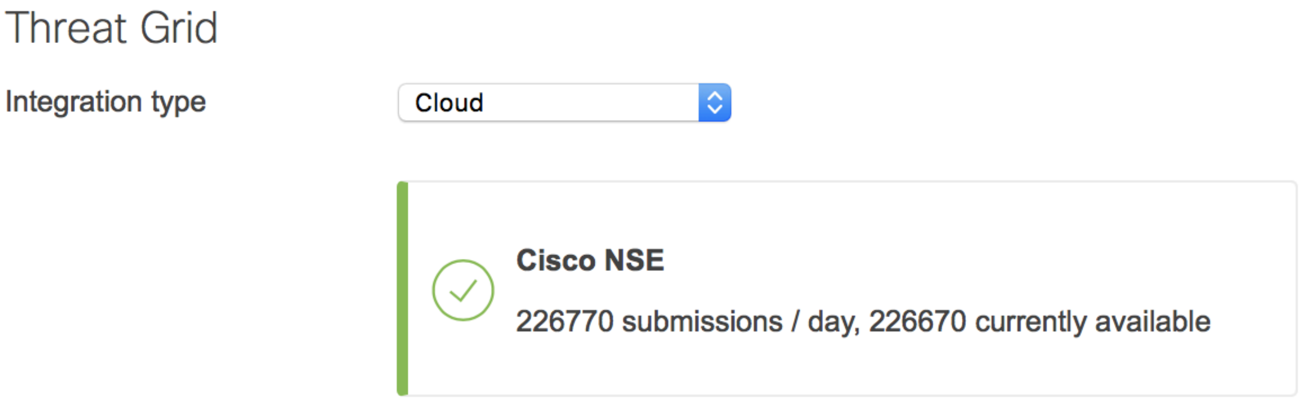
Meraki would like permission to access your account

Review permissions

Permission(s): write:account-management-api

ⓘ **Note**: You must be the Threat Grid organizational admin in order to allow Meraki MXs to access your Threat Grid account.

When Threat Grid and the Meraki Dashboard are successfully linked, you will be able to see the daily file submission limit for your organization and how many are currently available.



Threat Grid

Integration type: Cloud

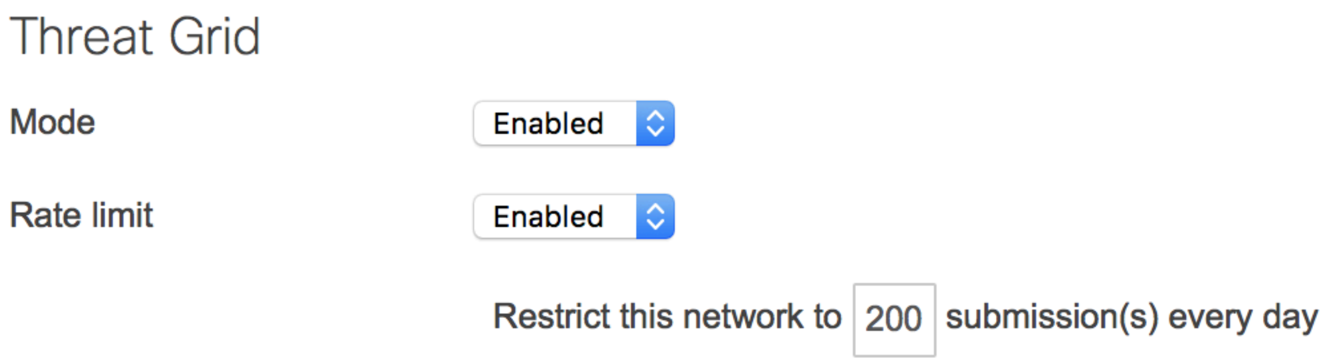
✓ **Cisco NSE**

226770 submissions / day, 226670 currently available

Enable Threat Grid Submissions

Navigate to the **Security & SD-WAN > Configure > Threat protection** page.

Under the Threat Grid heading, set the mode to Enabled. If desired the rate limit can also be configured to limit the number of file submissions that the network can submit to Threat Grid for analysis in a 24-hour period. The rate limit cannot exceed the maximum allowed daily submissions.



Threat Grid

Mode: Enabled

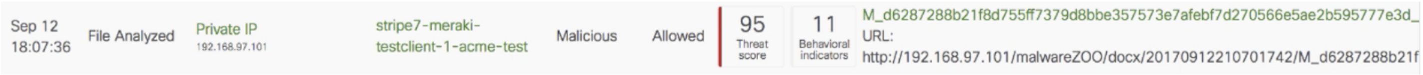
Rate limit: Enabled

Restrict this network to 200 submission(s) every day

Reporting

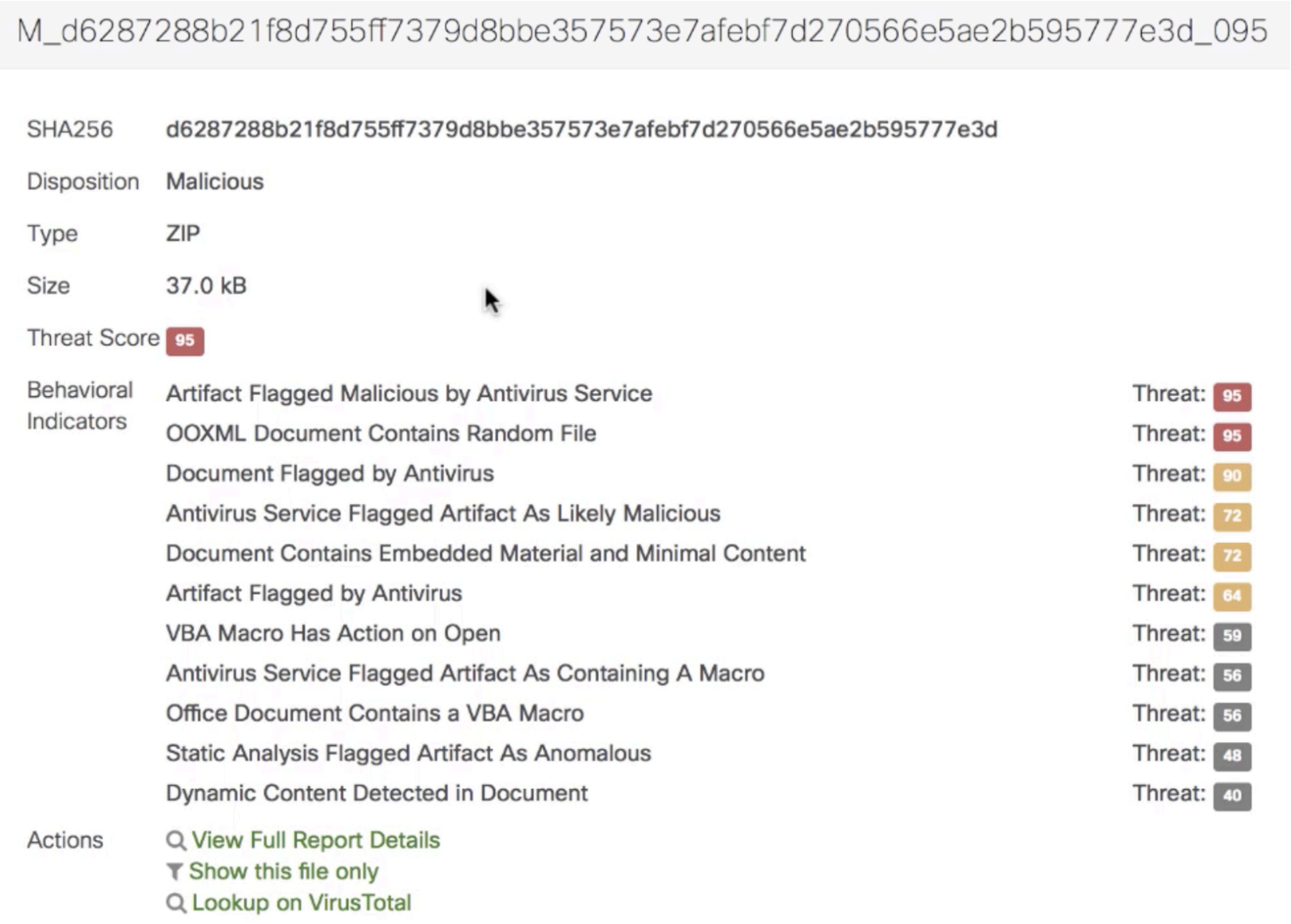
To view the results of Threat Grid analysis, navigate to the **Security & SD-WAN > Monitor > Security center** page. Within the Security Center, select the Events view.

Files that have been submitted for analysis to Threat Grid will have the threat score and a list of associated behavioral indicators available in the Event view.



Sep 12 18:07:36	File Analyzed	Private IP 192.168.97.101	stripe7-meraki-testclient-1-acme-test	Malicious	Allowed	95 Threat score	11 Behavioral indicators	M_d6287288b21f8d755ff7379d8bbe357573e7afebf7d270566e5ae2b595777e3d_ URL: http://192.168.97.101/malwareZOO/docx/20170912210701742/M_d6287288b21f

Clicking the file name link will pull up an info-card that will provide additional information about the file. This will include more specific information about any of the behavioral indicators that matched to behaviors observed during Threat Grid analysis.



M_d6287288b21f8d755ff7379d8bbe357573e7afebf7d270566e5ae2b595777e3d_095

SHA256	d6287288b21f8d755ff7379d8bbe357573e7afebf7d270566e5ae2b595777e3d
Disposition	Malicious
Type	ZIP
Size	37.0 kB
Threat Score	95

Behavioral Indicators	
Artifact Flagged Malicious by Antivirus Service	Threat: 95
OOXML Document Contains Random File	Threat: 95
Document Flagged by Antivirus	Threat: 90
Antivirus Service Flagged Artifact As Likely Malicious	Threat: 72
Document Contains Embedded Material and Minimal Content	Threat: 72
Artifact Flagged by Antivirus	Threat: 64
VBA Macro Has Action on Open	Threat: 59
Antivirus Service Flagged Artifact As Containing A Macro	Threat: 56
Office Document Contains a VBA Macro	Threat: 56
Static Analysis Flagged Artifact As Anomalous	Threat: 48
Dynamic Content Detected in Document	Threat: 40

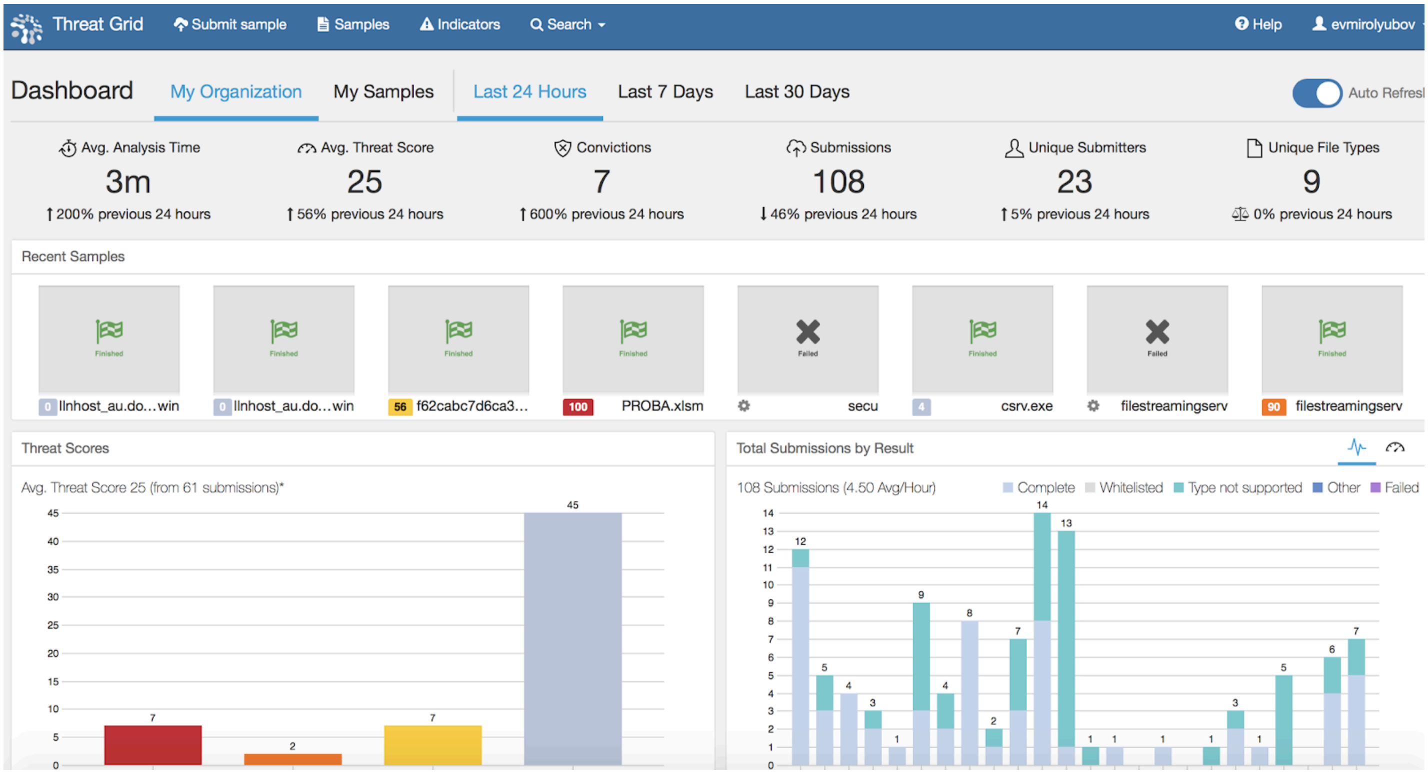
Actions

Threat Grid Portal

Threat Grid Premium customers can also access the Threat Grid Premium Cloud portal, which allows users to perform detailed analysis and threat intelligence searches on samples analyzed by Threat Grid. Users can access the portal through a web interface or via a set of robust APIs, which Threat Grid provides. Threat Grid also provides curated feeds which can be used to augment existing customer threat intelligence platforms.

The Threat Grid Premium portal allows users to interact directly with live malware using the “Glove Box” feature and to view recordings of malware being executed in the virtual environment. Playbooks, process maps, JSON reports, sample runtime adjustments and many other features are available to Threat Grid Premium users.

Finally, the Threat Grid Premium portal offers users an organizational view of Threat Grid cloud submissions across AMP and Threat Grid-enabled devices in your organization.



Avg. Analysis Time 3m ↑ 200% previous 24 hours

Avg. Threat Score 25 ↑ 56% previous 24 hours

Convictions 7 ↑ 600% previous 24 hours

Submissions 108 ↓ 46% previous 24 hours

Unique Submitters 23 ↑ 5% previous 24 hours

Unique File Types 9 0% previous 24 hours

Recent Samples

Status	Score	Sample
Finished	0	llnhost_au.do…win
Finished	0	llnhost_au.do…win
Finished	56	f62cabc7d6ca3…
Finished	100	PROBA.xlsm
Failed	⚙	secu
Finished	4	csrv.exe
Failed	⚙	filestreamingserv
Finished	90	filestreamingserv

Threat Scores

Avg. Threat Score 25 (from 61 submissions)*

Total Submissions by Result

108 Submissions (4.50 Avg/Hour)