Privacy and Sample Visibility

This chapter provides information about the privacy and sample visibility model for sample submissions to Threat Grid. It includes the following topics:

About Privacy and Sample Visibility

When submitting samples to a Threat Grid appliance for analysis, an important consideration is the privacy of their contents. Privacy is a particularly important consideration if sensitive documents or archive types are submitted for analysis, because locating sensitive material could be relatively easy for those with access to the Threat Grid Appliance, especially with the search API.

The privacy and sample visibility model for sample submissions to Threat Grid is as follows:

- Unless samples are designated as Private, they are visible to users who are outside the submitter's organization.
- Private samples can only be seen by Threat Grid users within the same organization as the user who submitted the sample.

Privacy and Visibility for Integrations

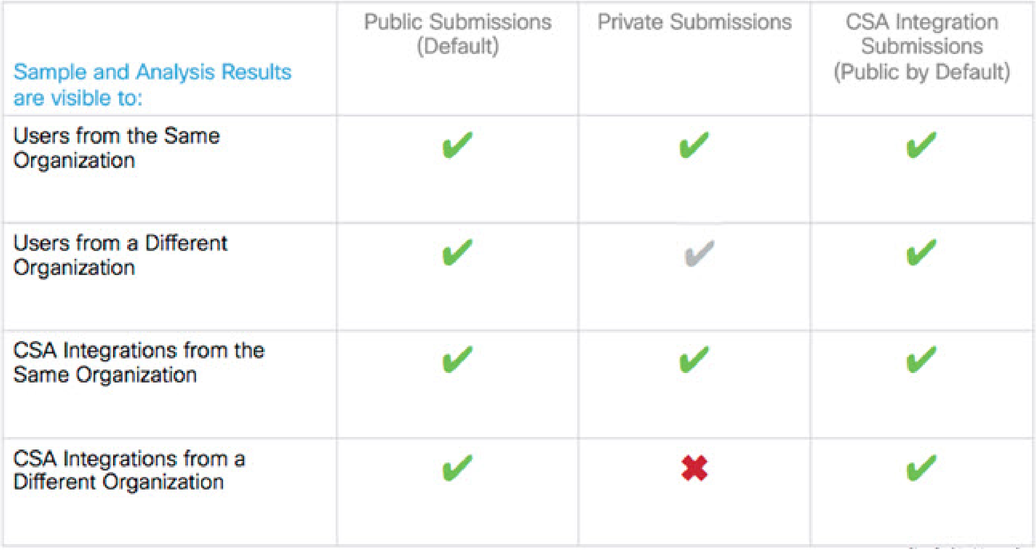
The privacy and sample visibility model is modified on Threat Grid Appliances for samples that are submitted by integrations. Integrations are Cisco products such as Email Security Appliance (ESA), Web Security Appliance (WSA), and other devices or third-party services (you may see the term CSA Integrations, which refers to ESA/WSA and other Cisco appliances, devices, and services that are integrated; for example, registered, with Threat Grid Appliance via the Cisco Sandbox API.)

All sample submissions on Threat Grid Appliances are Public by default, and can be viewed by any other appliance user, including integrations, regardless of the organization to which they belong. All appliance users can see all details of samples submitted by all other users.

Threat Grid users may also submit Private samples to the Threat Grid Appliance, which are only visible to other Threat Grid Appliance users, including integrations, from the same organization as the sample submitter.

Privacy and sample visibility model on Threat Grid Appliances are illustrated in the table.

Figure 1: Privacy and Visibility on a Threat Grid Appliance



Sample and Analysis Results are visible to:	Public Submissions (Default)	Private Submissions	CSA Integration Submissions (Public by Default)
Users from the Same Organization	✔	✔	✔
Users from a Different Organization	✔	✓	✔
CSA Integrations from the Same Organization	✔	✔	✔
CSA Integrations from a Different Organization	✔	✖	✔

- **Full Access** - The green check mark indicates that users have full access to the sample and the analysis results.
- **Scrubbed Reports** - The grey check mark indicates that the Private submission results are scrubbed. Users have partial access to the sample and analysis results, but all potentially sensitive information about the sample is removed. There are no filenames, process names, screenshots, or even specifics about its activity in the glovebox.

  We omit details from the Metadata section, such as the sample submitter's login information. If you encounter a hash from a private sample in the course of doing business, this will let alert you to known threats, and if you need more details, submit your own copy of the sample for full analysis.

  Private samples may not be downloaded. Scrubbed reports include Artifacts (with filename removed), Behavioral Indicators, Domains, and IPs.
- **No Access** - The red X indicates that users have no access to the sample or the analysis results.

The same basic privacy rules apply to Threat Grid appliance integrations with AMP for Endpoints Private Cloud.