

## Rule Importer Instrument

Rule Importer Instrument is a tool for importing and generating Suricata rules from .tar.gz packages and blacklisted addresses.

### General usage

Pre-created rules can be obtained from rule packages such as Emerging Threats. Blacklist rule generation supports IP addresses and DNS names with optional comment listed in semicolon-separated CSV file.

These files are configured for download using Fleet Management, and Rule Importer does the rest. It keeps track of Suricata instruments and delivers rules to them when downloaded files are changed.

Suricata group ID (gid) is added or changed from rules so Rule Importer won't conflict with other rule sources such as Rule Manager Instrument.

## Rule Importer properties

---

Instrument developer	SensorFleet Oy
Network access type	None
Required interfaces	None
Instrument dependencies	Suricata IDS
Data retention	Stores latest generated rule set to application RAM and a list of current Suricata Instruments to persistent data. Does not store user specific data.
Management UI	No
Performance	Handles easily rule packages and blacklists with tens of thousands of entries

---

## Example use cases

Rule importer can be used when ready-to-use rule set and/or set of blacklisted addresses is already available.

Otherwise Rule Manager can be used as it supports enabling and disabling individual rules etc.