Sensor Guide

The Invary Sensor measures your operating system's behavior at runtime. Designed for performance and convenience, the Sensor is compatible with most Linux distributions.

Installing the Invary Sensor

Invary determines the Runtime Integrity of operating systems, finding hidden malware that other threat detection solutions can't. Invary strengthens an organization's Zero Trust Architecture by removing assumptions about the OS at runtime. A vital first step in validating the Runtime Integrity of an operating system is measuring the current running state of a system. The Invary sensor performs this measurement process to examine a system, which is then sent to the Invary platform for appraisal.

Installation is supported via the invary_install.sh shell script provided in the installation package. You can either run this script without any options and be prompted for all configuration, or provide the necessary configuration via command line arguments to the script or a configuration file.

You must run this installation script as root or via sudo. You will need to know your provisioning token and organization ID as parameters to this script. These values are available once a user has signed up for an account. Please refer to the Account > Organization section of the UI where this information can be copied. User specified tags can be used for identification purposes. This must be a quoted, comma-separated list of tags such as: __"tag1, tag2, tag3"__. The tags should be concise and meaningful to the user.

This information can be provided by command line options to the installation script, or via a configuration file in this format:

> tags = ["tag1", "tag2", "tag3"]

>

> [provisioning]

> token="db9f9hp3135ya40am5820dqyy"

> organization="ckqa9hnwt94ebw6ctrxh25ahy"

The following additional installation options are currently available:

> ./invary_install.sh -h

>

> USAGE:

> ./invary_install.sh [OPTIONS] provisioning_token organization_id tag_data

>

> OPTIONS:

> -c, --config-file <FILE> Daemon configuration file

> -g, --group <GROUP> Run installed daemon as the given group

> -u, --user <USER> Run installed daemon as the given user

> -e, --stderr <FILE> Write stderr to the given file

> -o, --stdout <FILE> Write stdout to the given file

> -p, --pid-file <FILE> Write the process ID to the given file

> -h, --help Print this help information

The default user/group is root/root. This daemon must be run with root access, so if another user is chosen you will need to make sure that user has **sudo** access on your system.

The pid and stdout/stderr output files for the daemon are normally stored in the directories /var/opt/invary/ and /run/ respectively. If you select another location, the installer will create the desired directories if they do not exist.

Once the required configuration is provided, the installer will add the Invary sensor daemon binary and configuration file to your system and create the needed initialization script based on your environment. For SystemD environments, the new configuration will be added to /etc/systemd/system/ and for older SysV environments, the configuration will be updated in /etc/init.d/ along with updates to the run-level data to start/stop the daemon correctly.

Removing the Invary Sensor: If you no longer wish to run the Invary Sensor on your system, please use the invary_uninstall.sh script to remove the daemon and its associated configuration.> ./invary_uninstall.sh This script does not require any arguments and will determine what needs to be removed from the system based on the installed configuration. If you did add a new user/group for the daemon to use, you will need to remove that user/group if it is no longer needed on your system after the removal.

Validating the Invary Sensor is deployed: The Invary Sensor measures your system every 15 minutes by default, and takes an initial measurement shortly after starting. Each measurement is then appraised by the Invary platform. A list of registered endpoints and their appraisals can be found on the Invary console (https://console.invary.com). If you do not see your endpoints or appraisals shortly after starting the Sensor please ensure your configuration is correct or contact Invary at support@invary.com.

Testing a failed appraisal: Invary provides a method to safely trigger a failed appraisal. It can be used to validate your IR workflows and integrations using Invary's webhook and API. Utilize Invary's Test Probe project located on GitHub to generate a failed appraisal. https://github.com/Invary-Runtime-Integrity/invary-test-probe

The Invary Test Probe is a simple Linux kernel module which only inserts a symbol into the kernel symbol table for discovery by the Invary sensor software. It does not modify the running system in any other way.