Endpoint Detection & Response
Quick Start Guide

This guide explains how to get started using the SentinelOne® Endpoint Detection & Response (EDR) tool. In particular, it explains how to deploy its agents (small software components) on vessel devices that you want to monitor for threats. These agents will communicate with the SentinelOne Console, which is a cloud-based management portal where you can analyze detected security alerts/threats, set mitigation actions, and investigate incidents.

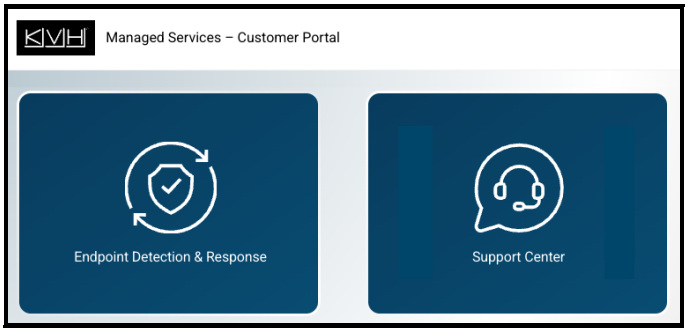
Accessing the SentinelOne Console

The SentinelOne Console is available via the KVH Managed Services Customer Portal. To access the portal, open a web browser and go to **https://ms.kvh.com**. Then log in with the credentials KVH provided during the onboarding process.

Note: *If you are a KVH Airtime customer, use the email address and password you use to log into KVH Manager.*

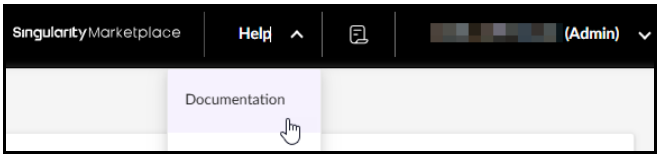
Note: *For initial access, you will first need to follow the verification steps provided in an email from SentinelOne.*

Once you are logged in, select **Endpoint Detection & Response** to launch SentinelOne. From there, you can download its agent installers.



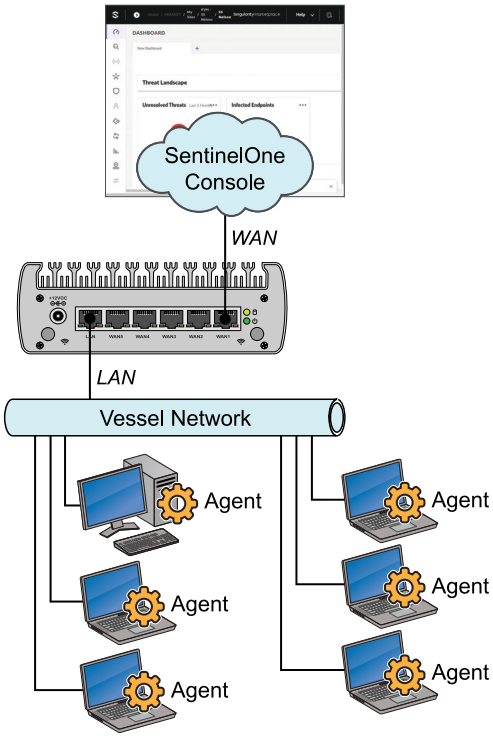
SentinelOne Knowledge Base

These instructions only provide basic information. For complete details and advanced configurations, refer to the comprehensive SentinelOne documentation – select **Documentation** from the Console's Help menu.



Planning Agent Deployment

You need to install a SentinelOne Agent on every endpoint (e.g., computer/server) you want to protect on your network. The agent works continuously in the background to detect suspicious behavior, block attacks, and send reports to the cloud-based SentinelOne platform.



Technical Support

If you have any questions or need technical assistance, please submit a support ticket at the Customer Portal or contact KVH Technical Support 24/7/365:

- Continental USA: 1-866-701-7103
  Worldwide: +1 401-851-3806
- WhatsApp: +1 401-851-3842
- Email: help@kvh.com

System Requirements for Agents

Before installing the SentinelOne agent on a vessel endpoint, be sure it has the following resources that are recommended for optimum operation.

Windows

- 1 GHz dual-core CPU or better
- 2 GB RAM or more
- 3.5 GB free disk space on Windows partition, 10% of disk for VSS snapshots for each drive

Mac

- Intel-based Mac, Apple silicon Mac or MacBook Neo device powered by A18 chip
- 1 GHz dual-core CPU or better
- 2 GB RAM or more
- 2 GB free disk space

Linux

- 1 CPU core/2 threads, dedicated to the agent
- 800 MB RAM minimum, dedicated to the agent
- 3 GB in /opt/sentinelone
- Instruction-supported CPU: SSE4_2

Note: *Older operating systems may require a legacy version of the SentinelOne agent or special considerations. Refer to the Requirements section of the SentinelOne documentation for details.*

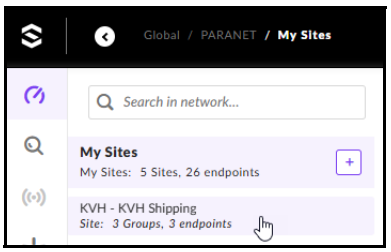
Additions to Firewall Allowlist

If you have ACL (Access Control List) rules protecting your network, be sure to allow traffic to/from ***.sentinelone.net** over TCP port **443** (HTTPS).

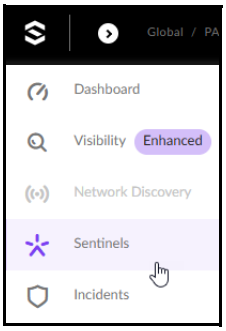
IMPORTANT!
If you are unable to install an agent following the instructions in the next section, please contact KVH Technical Support. With your help, KVH may install it for you over a secure remote desktop connection.

Installing Agents on Endpoint Devices

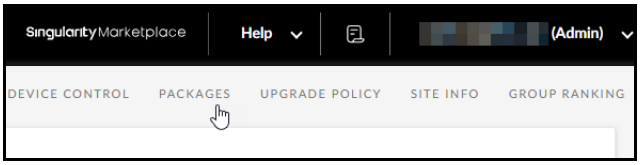
1. If you manage multiple sites (i.e., companies or fleets), select the site associated with the desired vessel(s). *If you do not see My Sites in the sidebar, click the arrow button in the upper-left corner.*



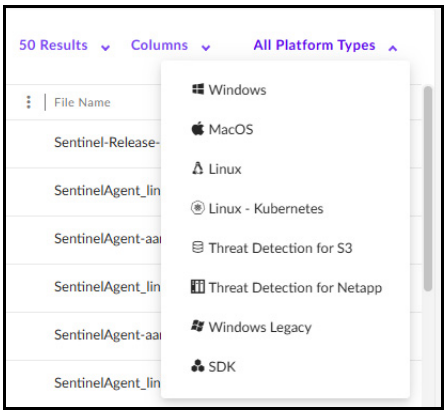
2. Select **Sentinels** from the main menu.



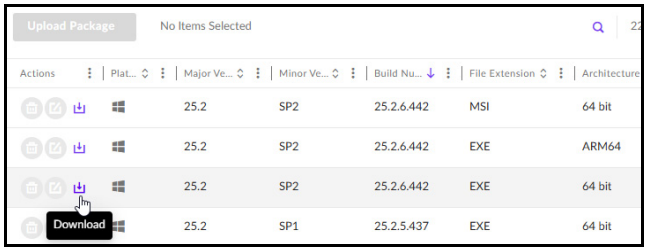
3. Select **Packages** from the Sentinels menu.



4. Select the endpoint's operating system from the drop-down menu of platform types. This will filter the list of available agent installation packages.



5. Choose the latest version agent installation package that matches your endpoint's operating system, architecture (e.g., 64 bit), and deployment method (e.g., EXE or MSI extension). Select the **Download** button to download the package to your computer.

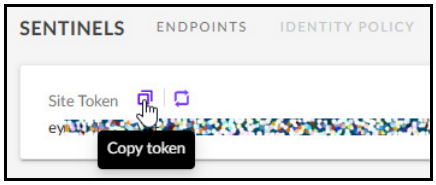


Note: *If an RMM (Remote Monitoring and Management) tool is deployed on your network, you may push the agent installer to multiple endpoints using a deployment script.*

6. Retrieve the applicable site token or group token. You will need it during the agent installation process.

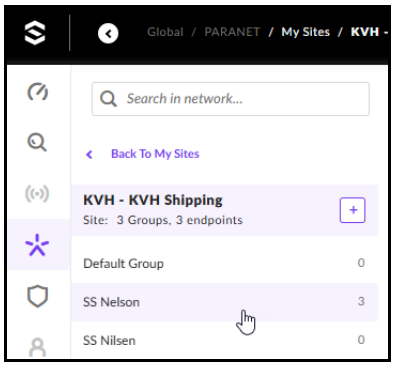
IMPORTANT!
Protect your token like any other security credential.

If your site does not have any groups, copy the site token and save it to a text file.

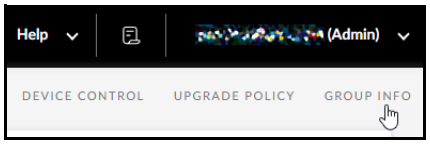


If your site contains groups (a group was created for each vessel), follow these steps:

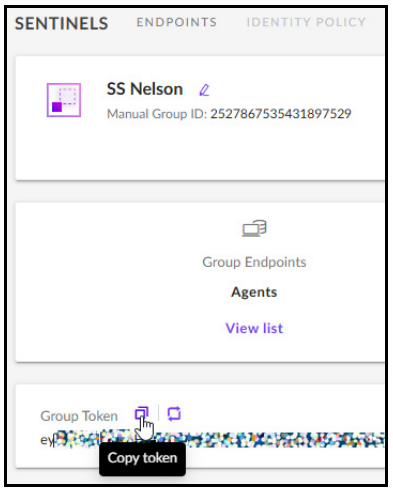
a. Select the group associated with the desired vessel. *If you do not see My Sites in the sidebar, click the arrow button in the upper-left corner.*



b. Select **Group Info** from the Sentinels menu.



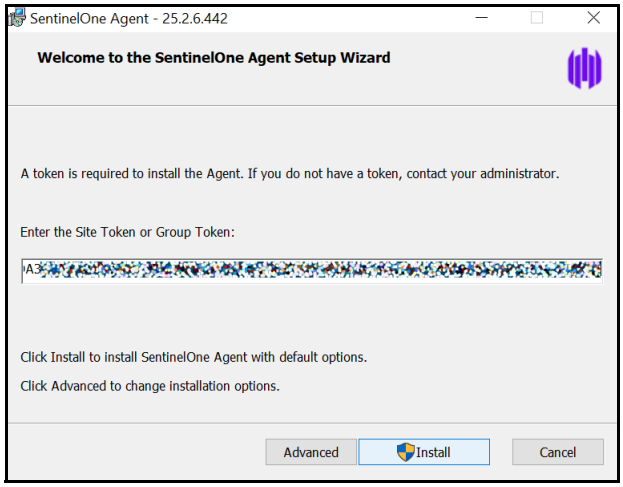
c. Copy the group token and save it to a text file.



7. Find the agent installation package in your Downloads folder. The filename starts with "Sentinel."

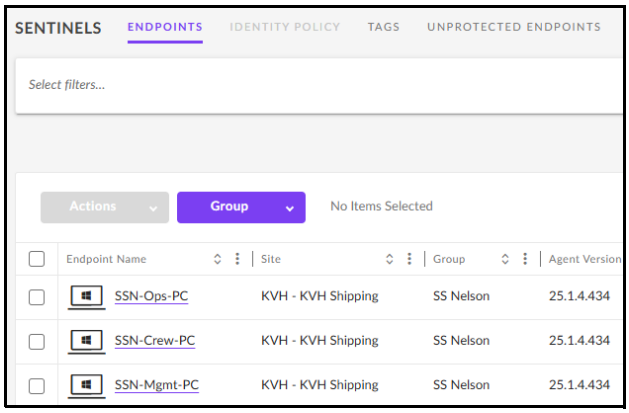
8. Copy and run the installer on every endpoint device you want to protect, assuming they share the same operating system and architecture. *For any endpoints that differ, simply download and install the appropriate agent for that device.*

9. During the installation process, enter the site token or group token when prompted. Then select **Install**.



10. When the installation is done, select **Finish** to exit.

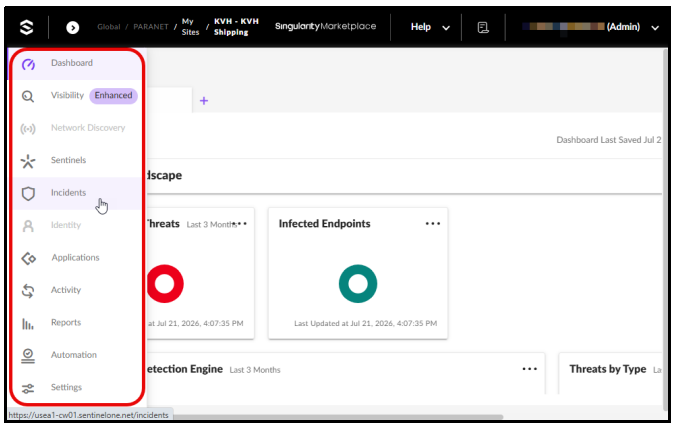
11. When you are done installing agents, your endpoints should appear in the SentinelOne Console, assuming they all have access to the Internet.



Exploring the SentinelOne Console

Once you have installed your agents, you can view their reported threat data in a variety of ways by selecting the desired option from the main menu.

Note: *Some options might be unavailable based on your user permissions.*



- **Dashboard**: Create your own custom dashboard, consisting of different widgets, to quickly see the information that is most relevant to you
- **Visibility**: Open the Singularity™ Data Lake to find all endpoint telemetry, including benign events, for deep investigation, analysis, and threat hunting
- **Network Discovery**: Not available
- **Sentinels**: Monitor and manage all endpoint devices that have a SentinelOne agent installed; check status, block bad software, and implement actions
- **Incidents**: See all detected threats, analyze their forensic details, and take mitigation actions
- **Identity**: Not available
- **Applications**: See an inventory of all software discovered on endpoints and identify potentially risky applications
- **Activity**: See and filter the full log of SentinelOne activities, including configuration changes and administrative actions
- **Reports**: Generate and download one-time and scheduled reports for insights into your site's trends, threats, mitigations, and applications
- **Automation**: Run scripts to remotely perform actions on one or more endpoint devices
- **Settings**: Configure the Console, create users, set notification preferences, and more

Note: *Refer to the SentinelOne documentation, accessible via the Help Link, for complete details.*