



ROGUE DEVICE MITIGATION – Protecting against Malicious Hardware Attacks

# SepioPrime

## USER MANUAL

Version 1.4



## Proprietary Information

Copyright © 2020 Cyber Sepio Systems Ltd. All rights reserved.

The Cyber Sepio Systems Ltd. name and Cyber Sepio Systems Ltd. logo are trademarks or registered trademarks of Cyber Sepio Systems Ltd.

Sepio Systems, its logo and certain names, product and Agent names referenced herein may be registered trademarks, trademarks, trade names or Agent marks of Sepio Systems Ltd. in certain jurisdictions.

The material contained herein is proprietary, privileged and confidential and owned by Sepio Systems or its third-party licensors. The information herein is provided only to the person or entity to which it is addressed, for its own use and evaluation; therefore, no disclosure of the content of this document will be made to any third parties without specific written permission from Sepio Systems Ltd. The content herein is subject to change without further notice.

THE INFORMATION SPECIFIED HEREIN IS PROVIDED "AS IS" AND SEPIO SYSTEMS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF ACCURACY, COMPLETENESS, MERCHANTABILITY, TITLE, NON-INFRINGEMENT AND/OR FITNESS FOR A PARTICULAR PURPOSE.

SEPIO SYSTEMS reserves the right to make changes in or to the said information, or any part thereof, in its sole judgment, without the requirement of giving any notice prior to or after making such changes to the information. SEPIO SYSTEMS shall not be expected to update or revise these statements to reflect subsequent occurring events or circumstances, or changes in its actual results, level of activity, performance or achievements.

All other trademarks are the property of their respective owners. Other company and brand products and Agent names are trademarks or registered trademarks of their respective holders.

## Limitation of Liability

Sepio Systems Ltd. shall not be liable.



# Table of Contents

About This User Manual .....	5
Contact Information.....	5
<b>1 INTRODUCING SEPIOPRIME .....</b>	<b>7</b>
1.1 What is SepioPrime? .....	7
1.2 Using SepioPrime.....	10
<b>2 HOW DOES SEPIOPRIME WORK? .....</b>	<b>13</b>
2.1 Overview .....	13
2.2 Solution Architecture – USB Device Security .....	15
2.3 Solution Architecture – Transparent Network Devices Detection .....	18
<b>3 DEVICE VISIBILITY.....</b>	<b>20</b>
3.1 Overview .....	20
3.2 Peripheral Security Dashboard .....	24
3.3 Reviewing the Sepio Agent List .....	27
3.4 Checking Your License Coverage.....	33
3.5 Approving and Setting the Policy of Devices.....	36
<b>4 NETWORK VISIBILITY.....</b>	<b>50</b>
4.1 Overview .....	50
4.2 Defining the Switches .....	53
4.3 Defining Your Scan Policy for Network Switches.....	57
4.4 Network Switches .....	60
4.5 Network Ports.....	62
4.6 Verifying SepioPrime Communication with the Switches.....	63
4.7 Verifying Port License Coverage.....	63







5 RISK INSIGHTS .....64

5.1 Overview ..... 64

5.2 Uncommon Peripherals..... 65

5.3 Vulnerable Peripherals ..... 67

5.4 Switch Vulnerabilities..... 68

5.5 Network Ports ..... 69

5.6 Device Pairs..... 69

6 OTHER SEPIOPRIME OPTIONS.....70

6.1 History ➔ Event Log ..... 70

6.2 Reports ..... 71

6.3 Audit Trail ..... 72

6.4 Users..... 72

6.5 Licensing ..... 73

7 INTEGRATING WITH SEPIOPRIME .....74

**ABOUT SEPIO SYSTEMS.....75**





## About This User Manual

This user manual is intended for security, infrastructure, IT or SOC personnel who will use SepioPrime to protect their organization from malicious hardware attacks. This manual describes both SepioPrime's **Peripheral** (device) visibility/security feature and its **Network** visibility/security feature. According to the license you purchased, you may have access to one or both of these features.

- **Chapter 1, Introducing Sepio Systems**, page 7, introduces the Sepio Systems platform.
- **Chapter 2, How Does Sepio Systems Work**, page 12, describes SepioPrime components, architect and how it works.
- **Chapter 3, Device Visibility**, page 20, describes the workflow for setting up SepioPrime's peripheral visibility/security and the user interface features that are provided to monitor and block attacks.
- **Chapter 4, Network Visibility**, page 50, describes the workflow for setting up SepioPrime's network visibility/security and the user interface features that are provided to monitor and block attacks.
- **Chapter 5, Risk Insights**, page 64, describes the insights provided about the risk from malicious hardware in your organization.
- **Chapter 6, Other SepioPrime Options**, page 70, shows other information and reporting options provided by SepioPrime.
- **Chapter 7, Integrating with SepioPrime**, page 74, describes how to integrate SepioPrime alerts and events with other third-party products.

## Contact Information

Sepio Systems Customer Support Team – [support@sepio.systems](mailto:support@sepio.systems)

Cyber Sepio Systems Ltd.

11810 Grand Park Ave. Suite 500 Rockville, Metadata, 20852, USA

Tel: +1 (240) 660-8690



## User Manual Revision History

1.0	January 2020	Bentsi Ben Atar and Iftah Bratspeiss	Initial release
-----	--------------	--------------------------------------	-----------------

## Terms and Abbreviations

CSV	Comma Separated Values
CCM	Center Configuration Manager
HID	Human Interface Device
SIM	Security Information Management
PID	Product ID
RDM	Rogue Device Mitigation
VID	Vendor ID





# 1

## Introducing SepioPrime

*This chapter introduces the SepioPrime solution.*



### 1.1 What is SepioPrime?

*SepioPrime enables you to Block rogue device attacks and stop the hardware-based data heist.*

*SepioPrime is a unique software solution for detecting and mitigating the risk of rogue hardware devices in enterprise environments and infrastructure. Whether by USB and/or network interfaces, SepioPrime provides total visibility and blocking options.*

#### 1.1.1 The Need – The Problem With Rogue Devices

A data heist can be easy. An attacker plugs a rogue device (such as a Packet Squirrel or a Plunder Bug) into a wired network or connects a Rubber Ducky or USBNinja to a network workstation's USB port. The rogue device then listens, hacks, gains access and siphons critical business information right out of your network.

These vulnerabilities extend to any network where an adversary can gain access long enough to plug in the rogue hardware, such as banks, schools, government offices, businesses or retail establishments. All these can be compromised through an unlocked door, an unsecured jack in a reception area or an Ethernet switch in the data center.

Attacks can also come from within. Nearly any malicious employee, partner, supplier or customer with access to your facility could surreptitiously plug malicious hardware into an unsecured port and launch supply chain attacks cause your IT infrastructure to succumb to inside threats.





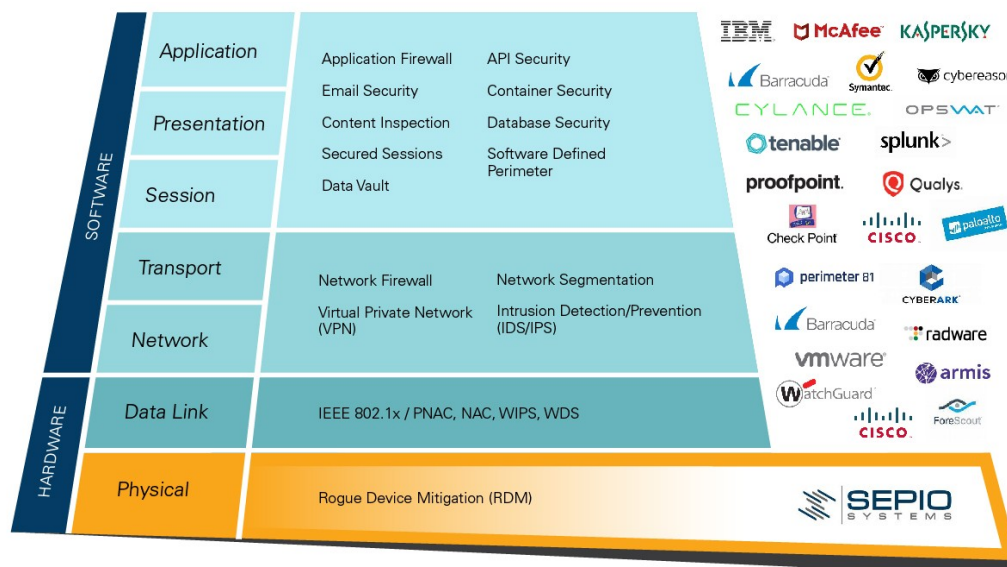


A variety of excellent security solutions do not guard against rogue hardware, which taps into network traffic at Layer 1 – the Physical Layer – thereby flying under the radar of traditional security systems. These include network-protection and intrusion-detection systems, as well as network firewalls (operating at OSI Layers 3 and 4) and application firewalls (operating at Layer 7) with deep packet inspection.

### 1.1.2 The Solution – SepioPrime – Mitigating Rogue Device Attacks

Sepio Systems provides three unique solutions that operate together to stop attacks launched from rogue hardware.

- **SepioPrime Network Security** works at the physical Layer, polling switches to analyze what's happening at that layer and detecting all rogue devices plugged into the Ethernet network switches.
- **SepioPrime Host Protection** guards against rogue devices connected to USB ports through multiple security layers, including real-time behavior analysis of suspicious devices. SepioPrime provides visibility down to the smallest level of each device in your infrastructure, including every keyboard, every headset, every mouse, every USB device and so on. SepioPrime detects rogue devices based on their actual behavior, anomalous behavior and the inherent vulnerabilities of the rich variety of devices known and not yet known by SepioPrime.
- **SepioPrime** orchestrates the Sepio solution, alerts and security threats, enforces policies and delivers risk insights and best-practice recommendations.







The software is augmented by real-time cloud-based intelligence that provides early warning of the latest malicious hardware and threat patterns.

Sepio's SaaS-based security suite can be deployed on any physical or virtual environment in any combination of on-premises, private and public cloud.

### SepioPrime Automatically Takes Action According to Your Policy

SepioPrime uses its unique physical fingerprinting technology to discover and show you the inventory of visible and invisible hardware. It analyzes hardware behavior and automatically blocks attacks on peripheral devices (on host/hosts) and on network level ports (on network switches).

According to default and easily configured policies, Sepio can block each USB port, which disables the rogue device in real time as soon as it is connected.

Policies can be implemented all at once or in stages, such as to first implement inventory visibility, then risk visibility and finally gradual policy implementation.





## 1.2 Using SepioPrime

SepioPrime provides both **Device** visibility/security and **Network** visibility/security functionalities. Installation instructions are provided separately for each functionality. The workflow for using each is different and the user interface provides relevant features accordingly.

- **Device Visibility**, page X
- **Network Visibility**, page X

### 1.2.1 Device Visibility

The use of uncontrolled computer peripheral devices, or products that have been manipulated or tampered with, exposes organizations to huge cyber-risks of data theft and network infections.



To set up SepioPrime for device visibility and security, refer to page X.

For a description of the various options provided by SepioPrime for device visibility and blocking, refer to page X.





## 1.2.2 Network Visibility

The use of transparent network devices that have no logical footprint, provides cyber-criminals with a constant foothold in enterprise networks for stealing and manipulating sensitive information.



### SOC Personnel

Interested in actionable real-time information and alarms with minimal overhead

Network security dashboard



To set up SepioPrime for network visibility and security, refer to page X.

For a description of the various options provided by SepioPrime for network visibility and blocking, refer to page X.









# 2

## How Does SepioPrime Work?



*This chapter describes SepioPrime components, architect and how it works.*

### 2.1 Overview

The following describes the architecture and software components that comprise the SepioPrime solution. Some of these components must be installed locally on the workstations and servers (the USB Device Security software agents), while others may either be deployed locally (on-premise), in a public cloud or in a private cloud. Some of the components are mandatory, while others are optional and provide additional Agents that the administrator can decide whether are needed or not.

The Sepio Security Suite is modular and includes the following threat-oriented modules. You can decide to deploy and start with only some or all of these modules –

- **USB Device Security**, page 13
- **Transparent Network Device Detection**, page x
- **Firmware Validation Module**, page 14

#### 2.1.1 USB Device Security

This USB Device Security module is used to detect and monitor the behavior of all the USB device assets in the organization.

This module provides full visibility of all connected devices, it analyzes their capabilities and behavior in real time and supports policy enforcement – thus allowing or blocking specific devices and interfaces according to the defined policy.





### 2.1.2 Transparent Network Devices Detection

This functional module continuously monitors the network searching for rouge network (LAN) devices that are transparent to existing security tools.

Transparent devices have no network entity of their own (no IP address, no MAC address and so on). They are used to gain an invisible foothold in a target network, and to leaking sensitive information in an out-of-band manner, all the while being invisible to existing tools.

### 2.1.3 Firmware Validation Module

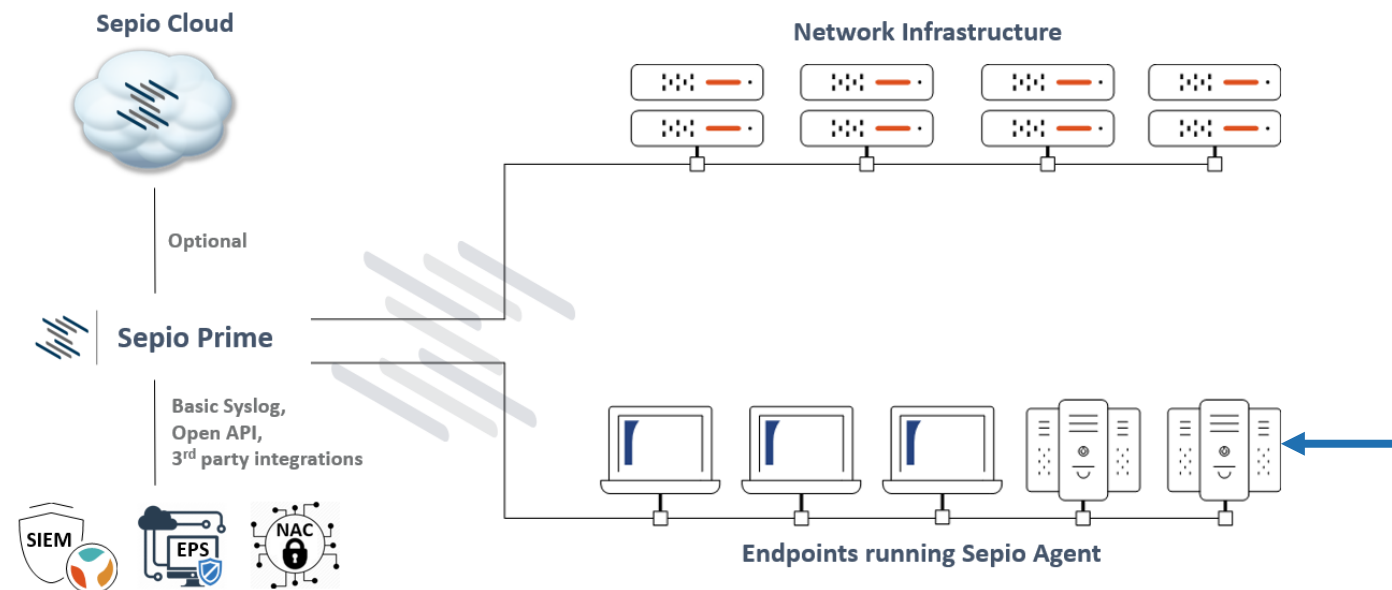
This functional module is responsible for detecting infected or manipulated firmware and software that is running on authentic and authorized devices in the organization.

Such devices can be abused in order to spread malware within the network, and to collect and store sensitive data that will later be exfiltrated from the organization.





## 2.2 Solution Architecture – USB Device Security



The USB Device Security module is based on a small footprint software agent (named the Sepio Agent) that is running on the workstations and servers in the organization.

The agent continuously detects and identifies all attached USB Devices.

The capabilities and realtime behavior of these USB Devices is analyzed and the device is assigned a security grade/rank that is based on the actual and current behavior of this instance. The SepioPrime cloud Agent compares this with the recorded behavior of similar devices.

The system administrator can create a list of approved devices (a white list) based on the list of existing and recognized devices, or based on a list of known devices that were witnessed as not being harmful in other installations.

A visibility report provides the administrator with a list of all the device assets in the organization, including vendor and functional information, and specifies to where each device is connected.

Peripheral devices that are known to be risky or badly-behaving are clearly masked.

The system then recommends the best practice security policy. After the chosen policy has been deployed, each usage breach or attack attempt is immediately reported and blocked.



## 2.2.1 Sepio Agent Components

The Sepio Agent is comprised of the following components –

- **OS Driver**, page 17
- **Sepio Agent**, page 16
- **Sepio UI**, page 16
- **Cloud Agent**, page 17

### Sepio Agent

The SepioPrime Agent (service) is the heart of the host deployed software. It is responsible for the business logic of tracking the peripheral devices, identifying their vendor/product (asset) and profile (interface/class/subclass/protocol) info, tracking the device descriptors and drivers and their plug-and-play behavior, keeping track of their behavior with/against the operating system, and making sure that the approved/defined security policy is enforced.

This Agent has no user interface and runs automatically when the system starts. It has three interfaces with user or management related entities, as follows –

- Socket interface with a local UI application (that is optional, and in some cases administrators prefer not to install it at all).
- Periodic reporting towards Sepio Console (the centralized management systems).
- Listener for remote administrator connections – usually coming from Sepio Console, but can also act as an API for external systems.

### Sepio UI

A local SepioPrime graphic user interface application is used for monitoring (for user roles) and configuring the SepioPrime Agent (for administrator roles).

Only a system tray icon is displayed while the application is running icon represents the overall SepioPrime security status.

When an event takes place, a small popup appears in the right-hand corner of the screen, as shown below –





Clicking on this icon displays the following window which shows complete information regarding the workstation and Devices, as shown below –

Device	Manufacturer	VID	PID	Serial Number	
USB Root Hub (xHCI)	(Standard USB HUBs)	\ROO	\ROO		✓
USB Input Device	(Standard system devices)	04B3	3025		✓
SCR35xx USB Smart Card Reader	SCM Microsystems Inc.	04E6	5410		✓
Microsoft Usbccid Smartcard Reader..	Microsoft	0529	0630		✗
USB Input Device	(Standard system devices)	17EF	6019		✓
Intel(R) Wireless Bluetooth(R)	Intel Corporation	8087	0A2B		✗

## OS Driver

The signed driver can run at the highest possible privilege level and is therefore required for all low-level interactions within the operating system.

The driver level is required whenever the system must block or interfere with the operation of a device that is not approved as part of the policy, or when the system must handle an approved device that starts acting dangerously.

The driver is controlled by the Agent layer that runs the actual business logic.

## Cloud Service

The Sepio Cloud Agent provides an additional layer of deeper device behavior analysis that is combined with threat intelligence regarding known to be vulnerable devices.

The use of the SepioCloud Agent is optional – if you configure your SepioPrime to connect with SepioCloud, you improve the overall level of security and the readiness of your organization.

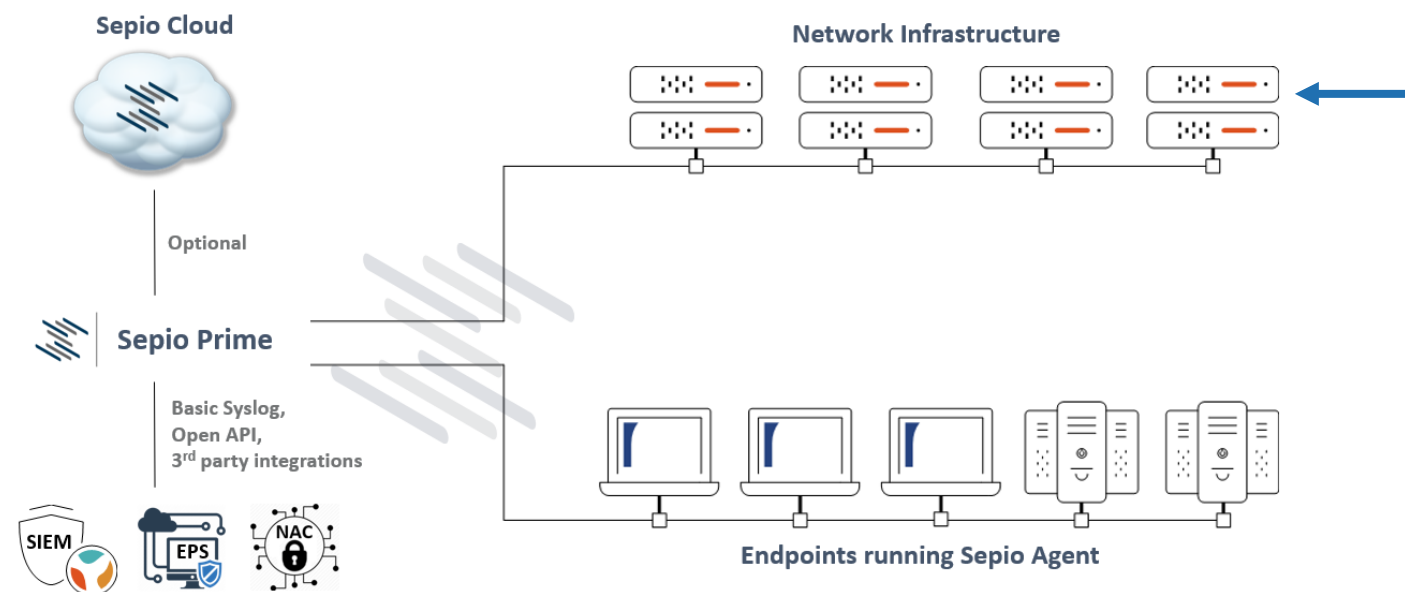
The major benefit from using SepioCloud, is the wide and global visibility of high quantity of peripheral devices and with many instances of each type. This large and growing physical and behavioral fingerprinting of many USB Devices provides the administrator with a much broader insights and early warning regarding attacks and vulnerabilities before they have effect on the organization.

The Cloud Agent is deployed based on Microsoft Azure infrastructure and can be deployed in any of Microsoft supported regions (currently 38) and includes automatic high availability and hitless performance.





## 2.3 Solution Architecture – Transparent Network Devices Detection



The Network visibility/Security module runs as part of the SepioPrime management server and communicates with the existing Cisco network infrastructure in order to collect and analyze low level device information regarding the elements that are connected to the switch ports.

The software calculates the realtime fingerprints of the devices that are connected to the switch ports and compares them with a known set of malicious devices together with specific network topology related information.

As a result, it can detect and report on the existence of transparent and ghost devices, that otherwise are completely invisible to existing security tools.

The system administrator can define the scanning and monitoring profile and its parameters and can configure the interfaces in order to report the discovery of malicious devices.

A visibility report provides the administrator with a list of suspected devices, and specifies to where each device is physically connected.



## Cloud Service

The Sepio Cloud Agent provides an additional layer of deeper device fingerprinting analysis that is combined with threat intelligence regarding malicious devices that are detected in real environments.

The use of the SepioCloud Agent is optional – if you configure your SepioPrime to connect with SepioCloud, you improve the overall level of security and the probability of detecting transparent network devices in your organization



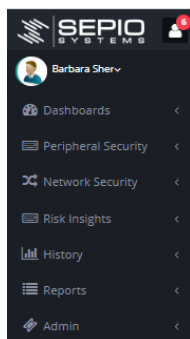
# 3

## Device Visibility

*This chapter describes the workflow for setting up SepioPrime peripheral visibility/security and the user interface features that are provided to monitor and block attacks.*

### 3.1 Overview

The following menu options are provided for setting up, monitoring and implementing the policies of device visibility/security.

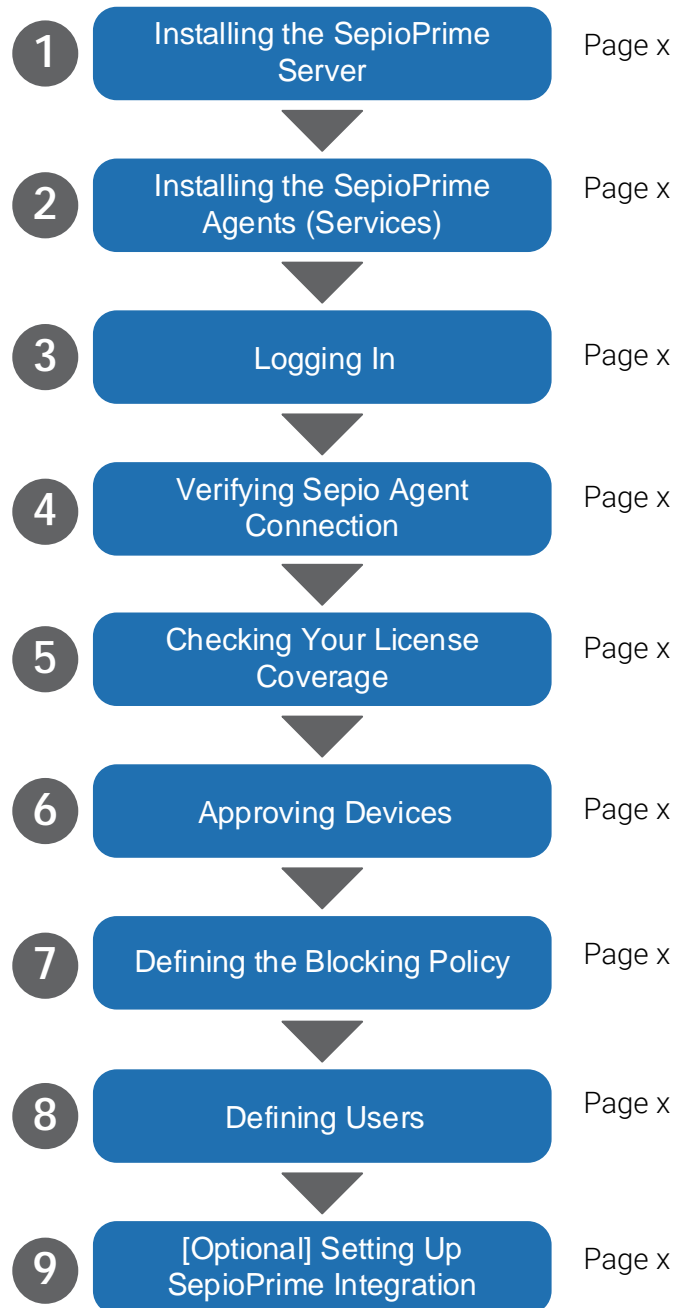


- Dashboards → Peripheral Security, as described on page X
- Peripheral Security → Sepio Agent, as described on page X
- Peripheral Security → USB Peripherals, as described on page X
- Risk Insights → Uncommon Peripherals, as described on page X
- Risk Insights → Vulnerable Peripherals, as described on page X
- Reports → Self-Generated Reports, as described on page X



### 3.1.1 Setting Up SepioPrime for Device Visibility/Security – Workflow

The following is recommended workflow for setting up SepioPrime –







The following provides more information about the workflow depicted above and a page reference to the place in this user manual that describes it in detail.

- **Step 1, Installing the SepioPrime Server** – Install the SepioPrime server according to the instructions in the *SepioPrime Installation Manual*.
- **Step 2, Installing the SepioPrime Agents (Services)** – Install a SepioPrime Agent on each host to be covered according to the instructions in the *SepioPrime Agent Installation Manual*.
- **Step 3, Logging In** – Log into the SepioPrime user interface, as described on page X.
- **Step 4, Verifying Sepio Agent Connection** – Verify that all the SepioPrime agents are communicating with the SepioPrime server, as described on page X.
- **Step 5, Checking Your License Coverage** – Export a list of the SepioPrime agents and send it to Sepio in order to receive and upload licenses to each agent, as described on page X.
- **Step 6, Approving Devices** – Review risk indications and approve (or not) each device on each host. Various options are provided for reviewing and approving multiple devices at once across the entire organization, as described on page X.
- **Step 7, Defining the Blocking Policy** – By default SepioPrime monitors and alerts you regarding each device. In addition, you can define a policy that automatically blocks malicious devices in real time. You can assign this policy per device, per device type, per host or per user, as described on page X.
- **Step 8, [Optional] Defining Users** – Define additional SepioPrime users as needed, as described on page X.
- **Step 9, [Optional] Setting Up SepioPrime Integration** with Syslog and CEF according to the instructions in the *SepioPrime Northbound Interfaces Manual*.

### 3.1.2 Using SepioPrime for Device Visibility and Blocking

SepioPrime provides various options in the user interface for detecting the overall security and risk situation, as well as enabling you to drill down into the exact details of each peripheral in your organization.

- **Peripheral Security Dashboard** – Shows a variety of risk and status features regarding the peripherals in your organization, as described on page X.
- **Risk Insights** – Provides insights into your uncommon and vulnerable peripherals, as described in page X.



- **Sepio Agent** – Provides a detailed list of each covered host, its risk and its status.
- **USB Peripherals** – Provides a detailed list of each peripheral connected to each covered host, its risk and its status.
- **Viewing and Generating Reports** – Provides various ready-made reports and enables you to generate your own customized reports to be distributed by email.
- **History – Event Log** – Provides a detailed log of all system events.

## Free Mode and Armed Mode

Each Sepio Agent installed on a host runs the policy that you define for it. Two primary modes are provided – Free Mode and Armed Mode.

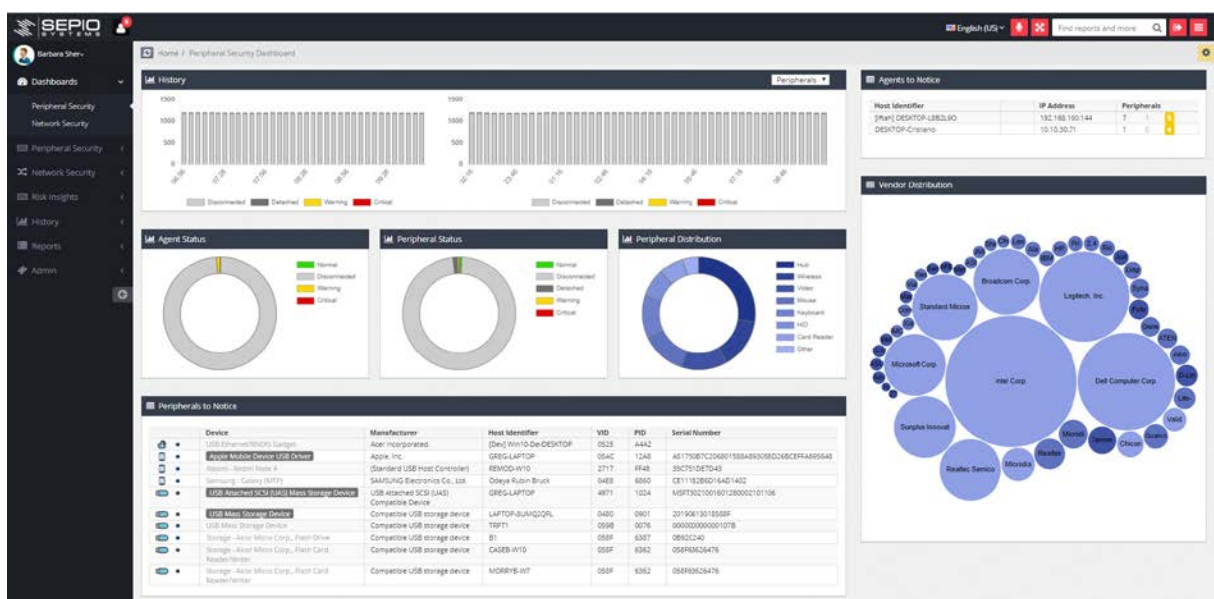
- **Free Mode** – SepioPrime provides total visibility regarding the rouge devices in your organization it collects information, shows you this information, warns you about risk indications, but does not take any action.
- **Armed Mode** – This mode provides total visibility (as described above), and in addition it blocks the USB port in real time, which disables rogue device.

## 3.2 Peripheral Security Dashboard

The **Peripheral Security** dashboard is displayed by default when you launch the SepioPrime user interface. It provides a variety of types of information about the risk and status of the devices in your organization.

► To review the Peripheral Security dashboard –

1 In the left pane, select **Dashboards** ➔ **Peripheral Security**. The following displays –

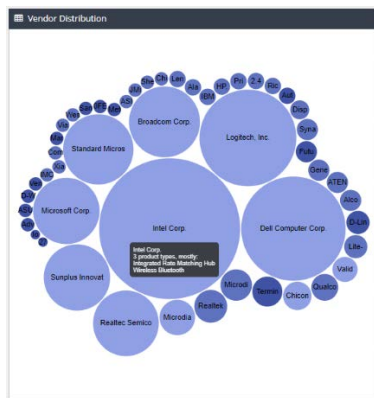




## Reviewing Dashboard Information

The Peripheral Security dashboard provides various sections presenting textual and graphical information.

Hovering over a graphical element displays a tooltip of additional information. For example, as shown below –



Clicking on a row in a table drills down to show more detailed information. For example, clicking on the first row below –

	Device	Manufacturer	Host Identifier	VID	PID	Serial Number
	USB Ethernet/RNDIS Gadget	Acer Incorporated.	[Dev] Win10-DevDESKTOP	0525	A4A2	
	Apple Mobile Device USB Driver	Apple, Inc.	GREG-LAPTOP	05AC	12A8	A51750B7C206801588A893058D26BCEFFA695648
	Xiaomi - Redmi Note 4	(Standard USB Host Controller)	REM0D-W10	2717	FF48	35C751DE7D43
	Samsung - Galaxy (MTP)	SAMSUNG Electronics Co., Ltd.	Odeya Rubin Bruck	04E8	6860	CE11182B6D16AD1402
	USB Attached SCSI (UAS) Mass Storage Device	USB Attached SCSI (UAS) Compatible Device	GREG-LAPTOP	4971	1024	MSFT3021001601280002101106
	USB Mass Storage Device	Compatible USB storage device	LAPTOP-8UMQ2QFL	0480	0901	20190613018588F
	USB Mass Storage Device	Compatible USB storage device	TRPT1	059B	0076	000000000000107B
	Storage - Alcor Micro Corp., Flash Drive	Compatible USB storage device	B1	058F	6387	0B92C240
	Storage - Alcor Micro Corp., Flash Card Reader/Writer	Compatible USB storage device	CASEB-W10	058F	6362	058F63626476
	Storage - Alcor Micro Corp., Flash Card Reader/Writer	Compatible USB storage device	MORRYB-W7	058F	6362	058F63626476

Displays the following detailed table –

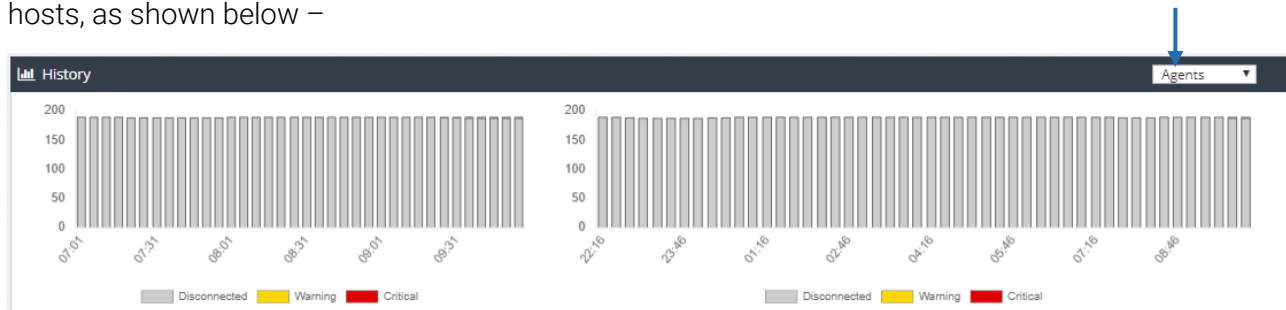
Device	Manufacturer	VID	Vendor	PID	Product Info	Serial Number	
Intel(R) Wireless Bluetooth(R)	Intel Corporation	8087	Intel Corp.	0A2B	Wireless Bluetooth		
USB Ethernet/RNDIS Gadget	Acer Incorporated.	0525	Nanchip Technology, Inc.	A4A2	Linux-USB Ethernet/RNDIS Gadget		
USB Composite Device	(Standard USB Host Controller)	046D	Logitech, Inc.	C31C	Keyboard K120		
USB Input Device	(Standard system devices)	046D	Logitech, Inc.	C31C	Keyboard K120		
USB Input Device	(Standard system devices)	046D	Logitech, Inc.	C31C	Keyboard K120		
USB Root Hub (USB 3.0)	(Standard USB Hubs)	VID0	VID0	VID0	VID0		

Showing 1 of 6 entries





The **History** section provides a dropdown menu in which you can select whether to display information about the devices covered by SepioPrime or about the Sepio Agents that are installed on hosts, as shown below –





### 3.3 Reviewing the Sepio Agent List

The instructions in this chapter assume that you have already installed the SepioPrime server according to the instructions in the *SepioPrime Installation Manual* and have installed the Sepio Agent on each host to be covered by SepioPrime according to the instructions in the *SepioPrime Agent Installation Manual*. Verify installation and operation of the Sepio Agents using an external tool of your choosing.

Part of the installation process of each Sepio Agent on a host, is to specify the SepioPrime server with which it communicates. During this installation, keep a list of the hosts on which a Sepio Agent was installed.

The following describes how to review the list of Sepio Agents detected by the server and verify that all those that were installed are listed there, meaning that they are actually communicating with the SepioPrime server.

#### ► To review the Sepio Agents (agents) list –

In the left pane, select **Peripheral Security** ➔ **Sepio Agent**. The following displays –

Host Identifier	IP Address	OS Version	UUID	Status	Peripherals	Last Configuration	Version	License
LAPTOP-BUMQ2QFL	10.10.30.122	Windows 10 Pro 64-bit	BFEBBF000806ECL1HF99B01...	Free	8 0 1	2020-01-14 12:15:36	2.4.7.0	
YOSL_SURFACE_L	10.125.143.183	Windows 10 Pro	BFEBBF000406E3203717539A	Disconnected	5 0 0	2019-06-19 07:45:43	2.2.6.0	
A-Broder	10.100.6.30	Windows 10 Pro 64-bit	BFEBBF000806EAK0093U1AA...	Disconnected	5 2 0	2019-12-11 08:42:01	2.4.7.0	
DONK-W10			BFEBBF00030604963564017...	Disconnected	2 0 13	2019-12-27 09:58:33	1.95.5.0	
DAVE-LAP	192.168.1.6		BFEBBF000906E996378V005...	Disconnected	1 0 6	2019-01-27 10:57:30	1.95.5.0	
RONRW-W7	10.100.102.13		BFEBBF000806EAK0085R002...	Disconnected	1 0 10	2019-02-25 15:25:51	1.98.4.0	
LEONB-W10	192.168.1.16		BFEBBF000806E996373030...	Disconnected	1 0 6	2019-02-18 09:51:35	1.95.5.0	
SIMONM-DESK	192.168.22.100		BFEBBF000406E3963725054...	Disconnected	0 0 0	2019-01-20 10:46:49	1.95.5.0	
TRPT1	192.168.6.93		178BF0F00800F8242127100444	Disconnected	4 0 7	2019-02-21 14:02:08	1.95.5.0	

The following information is provided for each Agent –

- **Host Identifier/IP Address** – Specifies the name/IP address of the host on which the Sepio Agent is installed.



- **OSVersion/UUID** – Specifies the version and unique identifier of the host on which the Sepio Agent is installed.
- **Status** – Specifies the status of the Sepio Agent, as described below.
- **Peripherals** – Specifies the quantity of devices on this host according to their **Status** (as shown in the **Status** column) and approval state (approved/not approved).

3 present and approved 0 disconnected and approved 10 not approved		
3	0	10

From left to right these numbers represent the following –

- **Present and Approved** – Specifies the quantity of devices that are currently connected to the host and have been approved by a Sepio Prime user, as described on page X.
- **Disconnected and Approved** – Specifies the quantity of devices that are not currently connected to the host and have been approved by a SepioPrime user, as described on page X. These devices were connected at some point and were approved, but are currently not connected to the host.
- **Not Approved (Orange)** – Specifies the quantity of devices that are not approved. This is the default state of Sepio Agents after they have been installed.
- **Risk Indication** – This is an extremely important column. It specifies the inherent risk of this device, as follows –




- **Danger! Red Mask** – **An attack tool masquerading as a legitimate device has been detected.** It is impersonating a legitimate device by duplicating the value of the Vendor ID (VID) and Product ID (PID).




- **Anonymous** – Specifies that this device is known to be vulnerable by design. It has a built-in vulnerability that enables it to be exploited by hackers. This vulnerability is listed in the Sepio threat intelligence database and is recognized by hackers. Hovering over this icon displays a description. For example, as shown below –






If this device is actually being used as an attack tool, then the rubber ducky  icon appears on its left. For example, as shown below –

PoisonTap									
	1/188	1 	USB Ethernet/RNDIS Gadget	Acer Incorporated.		0525	Netchip Technology, Inc.	A4A2	Linux-USB Ethernet/RNDIS Gadget

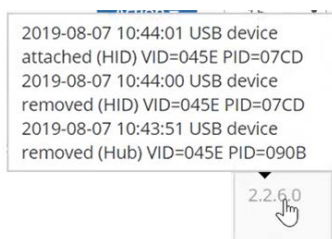
If no rubber ducky  icon appears on its left then the device is not currently being used as an attack tool, but still has the potential to be used as one because it is vulnerable by design.



-  **Black Mask** – This icon is only displayed for SepioPrime users that have administrative privileges. This indication does not mean that it is an attack tool. However, although SepioPrime recognizes this device, SepioPrime has never encountered this version of the device. For example, a new version of a known mouse.



Please contact Sepio support if you see this icon so that we can update our threat information database.

- **Last Configuration** – Specifies the timestamp of the most recent configuration or policy change sent to that host from the SepioPrime server.
- **Version** – Specifies the version of the Sepio Agent installed on the host. Hovering over this column displays a tooltip showing the last three events such as inserting or removing a USB device. For example, as shown below –



- **License** – Specifies whether the Sepio license that was imported for this host.
    - **Valid** – A green checkmark  indicates that a license was imported
    - **Pending** – Indicates that a license was not imported yet.
    - **Expired** – A red flag  indicates that the license has expired.
- 2 Verify that a row appears for each host on which you installed a Sepio Agent by comparing this displayed list with the list of hosts on which you installed each Sepio Agent (such as using Microsoft Center Configuration Manager (CCM)).





An easy way to get started is to do a sanity check by comparing the quantity of SepioPrime Agents that were installed with the quantity of rows that appears at the bottom of the list, as shown below –

ZAKT-LAP	192.168.6.90	BFEBFBFF000906EA20087300N...	Disconnected	0	0	0	2019-01-24 16:23:19	1.5
Showing 1 to 188 of 188 entries								Previous 1 Next

- **Connected (Free or Armed)** – All the hosts whose Sepio Agents is communicating with the SepioPrime server, appear in this list with the word **Free** or **Armed** in the **Status** column. **Free** is the default status that is automatically assigned. A Sepio Agent can be set to **Armed** status (to block), as described on page X.
- **Missing** – If a host on which the Sepio Agent was installed does not appear in the list, then check this on the host itself. For example, check whether the SepioAgent was actually installed.
- **Disconnected** – If a host appears in this list with **Disconnected** in the **Status** column, the row appears grayed out. This means that the host successfully connected with the SepioPrime server at some point and is currently not connected. In this case, use the usual network connectivity methods to check why these Agents no longer running or connected.





## Reviewing the Devices on a Host

The following describes how to drill down into a specific host in order to review the devices that are connected to it.

### ► To review the devices on a specific host –

- 1 Double-click on the row of a Sepio Agent to display all the peripherals (devices) connected to it.

Double-click  
on a Sepio  
Agent

Host Identity	IP Address	OS Version	UUID	Status	Peripherals	Last Configuration	Version	License
AARONS-SEPIO-LA	192.168.1.21	Windows 10 Home	BFEBFBFF00806EAC007B0000...	Disconnected	6 1 0	2019-07-16 10:53:03	2.2.8.0	✓
ABE-W10	192.168.20.195		BFEBFBFF00406E396372G007...	Disconnected	1 0 10	2018-12-26 16:34:20	1.95.5.0	✓
A-Broder	10.100.6.30	Windows 10 Pro 64-bit	BFEBFBFF00806EAK0093U14A...	Disconnected	5 2 0	2019-12-11 08:42:01	2.4.7.0	✓
ACCESS-CONTROL	192.168.6.96		178EBFBFF00800F8242127100155	Disconnected	4 0 6	2019-02-21 18:22:55	1.95.5.0	✓

A list of the devices connected to this host is displayed, as shown below –

Device Icon	Device Name	Device Type	Device ID	Manufacturer	Model	Serial Number	Approval State	Enabled
USB Input Device	(Standard system devices)	0557	ATEN International Co., Ltd	2261	2261		1	<input type="checkbox"/>
USB Input Device	(Standard system devices)	0557	ATEN International Co., Ltd	2261	2261		1	<input type="checkbox"/>
USB Input Device	(Standard system devices)	0557	ATEN International Co., Ltd	2261	2261		1	<input type="checkbox"/>
Generic USB Hub	(Standard USB HUBs)	0557	ATEN International Co., Ltd	8021	Hub		1	<input type="checkbox"/>
USB Root Hub (USB 3.0)	(Standard USB HUBs)	\ROO	\ROO	\ROO	\ROO		0	<input type="checkbox"/>

Showing 1 to 7 of 7 entries

- 2 A row appears for each device connected to the host. The following columns appear for each device –


- **Approval State** – Specifies whether the device has been approved by a SepioPrime user and is enabled.



-  – Indicates that this device is enabled and approved.

**Note** – Some devices have been soldered into the motherboard and therefore cannot be blocked by a SepioPrime policy. Therefore, these devices automatically appear enabled and pre-approved. Their manufacturer is specified as **(Standard USB Hubs)** and their vendor, the ID and product info columns show \ROO. For example, as shown below –


	USB Root Hub (USB 3.0)	(Standard USB Hubs)	\ROO	\ROO	\ROO	\ROO	
---	------------------------	---------------------	------	------	------	------	---

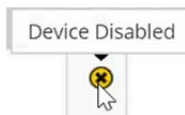
-  – Each device after it has been installed is not approved and is enabled. It appears with a red icon, as shown below –



**Note** – Some devices have been soldered into the motherboard and therefore cannot be blocked by a SepioPrime policy. Therefore, these devices automatically appear enabled and pre-approved. Their manufacturer is specified as **(Standard USB Hubs)** and their vendor, the ID and product info columns show \ROO. For example, as shown below –

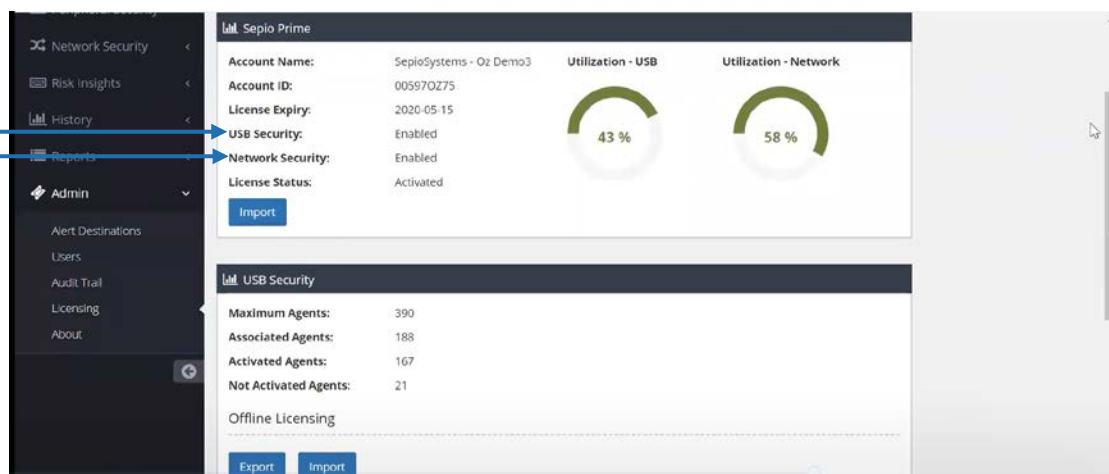
	USB Root Hub (USB 3.0)	(Standard USB Hubs)	\ROO	\ROO	\ROO	\ROO	
---	------------------------	---------------------	------	------	------	------	---

-  – Each device must be both approved and enabled in order to be covered. SepioPrime disables a device while blocking it. This yellow icon appears after you have approved a disabled device, but have not yet enabled it.



## 3.4 Checking Your License Coverage

The SepioPrime server has a license that is handled during installation. It can be displayed by selecting the **Administrator** ➔ **Licensing** option in the left pane. It is shown below in the **SepioPrime** section. The **USB Security** option should be enabled if you purchased device visibility and the **Network Security** option should be enabled if you purchased network visibility.



### Sepio Agent Licenses

The following describes how to generate a license for each host on which the Sepio Agent is installed.

#### ► To generate licenses for each host –

- 1 Verify that all the hosts on which you installed a Sepio Agent are listed in the Sepio Agents list, as described on page X.
- 2 Select the **Administrator** ➔ **Licensing** option in the left pane.







- 3 In the **USB Security** section (shown above), click the **Export** button to generate a CSV file to be sent to Sepio support at [licensing@sepio.systems](mailto:licensing@sepio.systems). For example, as shown below –

The screenshot shows the Microsoft Excel interface with the following details:

- Title Bar:** AutoSave | Benti Ben Atar | Excel
- Ribbon:** File, Home, Insert, Page Layout, Formulas, Data, Review, View, Help, Search.
- Home Tab Groups:** Clipboard, Font, Paragraph, Alignment, Number, Styles, Cells, Editing, Ideas.
- Status Bar:** POSSIBLE DATA LOSS. Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format. [Don't show again] [Save As...]
- Name Box:** A1
- Worksheet Grid:** Columns A-S, Rows 1-20.
  - Row 1: # Sepio Systems Agent List Export
  - Row 2: # Export Time: 01/06/2020 16:07:10
  - Row 3: #
  - Row 4: # The order of fields (per agent) are:
  - Row 5: # Uuid Host name Status Date Version
  - Row 6: BFEBF3FFIRONRW-V Pending ##### 1.98.4.0
  - Row 7: BFEBF3FFIDESKTOP-Pending ##### 2.4.7.0
  - Row 8: BFEBF3FFWIN10 Pending ##### 2.4.7.0
  - Row 9: BFEBF3FFMAWLWA Pending ##### 2.4.7.0
  - Row 10: BFEBF3FFYOSSI\_SUI Activated ##### 2.2.6.0
  - Row 11: BFEBF3FFFOR\_DESC Activated ##### 2.2.3.0
  - Row 12: BFEBF3FFIDESKTOP-Activated ##### 2.2.6.0
  - Row 13: BFEBF3FFIERAN-DES Activated ##### 2.2.6.0
  - Row 14: BFEBF3FFIGREG-LAP Activated ##### 1.91.06
  - Row 15: BFEBF3FFIGREG-SE Activated ##### 2.2.8.0
  - Row 16: BFEBF3FFIAARONS-S Activated ##### 2.2.8.0
  - Row 17: BFEBF3FFILenovo@ Activated ##### 2.2.8.0
  - Row 18: RFEBF3FFIA-Broder Activated ##### 2.4.7.0
  - Row 19: BFEBF3FFICr-DESKT Activated ##### 2.0.6.0
  - Row 20: BFEBF3FFIrdema-Rui Activated ##### 1.98.4.0

- 4 Sepio will generate a licensing file and send it to you.
- 5 After you receive this licensing file, import it using the **Import** button (shown on the previous page).



- 6 Select the **Peripheral Security** → **Sepio Agents** option in left pane to display the Agents list. Verify that each agent has a green checkmark ✓ in the license column. It should not be **Pending** (awaiting a license) or have a red flag 🚩 (license expired). Hosts that do not have a valid license ✓ are not covered. We recommend that you immediately import a proper license.

Host Identifier	IP Address	OS Version	UUID	Status	Peripherals	Last Configuration	Version	License
AARON-SEPIO-LA	192.168.1.21	Windows 10 Home	BF8BF0000000AC007000...	Disconnected	0 1 0	2019-07-16 15:55:03	2.7.8.0	✓
ABE-W10	192.168.20.195		BF8BF0000000000072007...	Disconnected	1 0 10	2019-12-26 16:54:20	1.95.5.0	✓
A-Binder	10.100.5.30	Windows 10 Pro 64-bit	BF8BF0000000A0000000...	Disconnected	5 2 9	2019-12-11 08:42:01	2.4.7.0	✓
ACCESS-CONTROL-W17	192.168.6.96		1700BF000000000020100105	Disconnected	8 0 8	2019-02-21 18:23:55	1.95.5.0	✓
ALBERTA-PC	192.168.5.37		BF8BF00000000000000000...	Disconnected	2 0 4	2019-12-24 08:46:47	1.98.2.0	✓
ALEXIS-W7	192.168.1.149		BF8BF00000000000000000...	Disconnected	1 0 9	2019-01-06 16:16:23	1.95.5.0	✓
ALEXIS-W10	192.168.20.243		BF8BF00000000000000000...	Disconnected	1 0 2	2019-01-03 09:50:56	1.95.5.0	✓
AMRS-W7	192.168.20.212		BF8BF00000000000000000...	Disconnected	1 0 8	2019-12-31 17:34:19	1.95.5.0	✓
ANDREAS-W10	10.132.196.140		BF8BF00000000000000000...	Disconnected	1 0 8	2019-02-18 17:13:34	1.98.5.0	✓
ANTHONY-LAP	192.168.65.187		BF8BF00000000000000000...	Disconnected	2 0 5	2019-01-06 14:21:57	1.95.5.0	✓
ATM-LB-PC	192.168.22.176		BF8BF00000000000000000...	Disconnected	0 0 8	2019-02-11 18:11:21	1.95.5.0	🚩
ATM-NEW01	192.168.6.40		BF8BF00000000000000000...	Disconnected	3 0 10	2019-01-15 12:07:05	1.95.5.0	✓
ATM-NEW02	192.168.6.46		BF8BF00000000000000000...	Disconnected	1 0 2	2019-02-09 08:54:57	1.98.5.0	✓
AVAP-PC	192.168.5.71		BF8BF00000000000000000...	Disconnected	3 0 7	2019-01-01 14:15:15	1.95.5.0	✓
AWEL-W10	192.168.81.35		BF8BF00000000000000000...	Disconnected	1 0 9	2019-01-28 11:11:21	1.98.5.0	✓





## 3.5 Approving and Setting the Policy of Devices

In this step you must review each device in order to decide which to approve (allow) and which not to approve. The decision whether to approve a device should be taken according to the **Risk Indication** shown by SepioPrime (as described on page X) and your organization's policies. For example, if an employee brought in a gaming keyboard and connected it to the corporate network, you may decide to approve its usage or not.

► Multiple options are provided for approving and setting the policies of devices –

- Per Host in the Sepio Agent List, page 38
- Per Device of a Specific Host in the USB Peripherals List, page 42
- Per Device in Your Organization, page 42
- Per Device per User, page x

### 3.5.1 Understanding Device Approval

This step should be performed after installation on all devices and then from time to time as needed.

In order for a device to be covered, it must be –

- **Approved** – Set to **Approved**, as described in this section. By default, all devices are **Not Approved** and must be approved by a SepioPrime user in order to be covered (in Free Mode). More importantly, if the device falls under an Armed policy, it will be automatically blocked by SepioPrime, unless it has been **Approved**.
- **Enabled** – Set to **Enabled** (not **Disabled**), as described on page x. By default, each device is **Enabled**. SepioPrime disables a device when it blocks it.  
**Note** – Disabling is performed automatically by SepioPrime when it blocks a device. The SepioPrime user does not need to disable devices.
- **Status – Free or Armed** – The status of the SepioPrime Agent on the host of this device must be sent to either **Free** or **Armed**; and not be **Disconnected** (as described on page X).

### Approving Devices in Order to Start Coverage

When new devices are introduced to SepioPrime (as described on page X), by default they are set to **Enabled** and **Not Approved**. This means that in order for a device to be covered by SepioPrime, you must approve each device. A variety of options are provided for approving multiple devices at once.



## Armed Mode – Blocking USB Ports

By default, all devices that are both **Enabled** and **Approved** are set to **Free** mode, which means that SepioPrime provides total visibility regarding the rouge devices in your organization, it collects information, shows you this information, warns you about risk indications, *but does not take any blocking action*.

You may refer to page X for a description of how to set a device to Armed Mode.

Setting devices to **Armed** mode before approving them will result in all these devices being blocked. We recommend that you be careful not to arm devices before approving them so as not to mistakenly block their usage. The quantity of such devices that are both not approved and armed is displayed in **red** in the peripherals column of the Sepio Agents list. For example, 1 device is shown below as **not approved** –



Host Identifier	IP Address	OS Version	UUID	Status	Summary
[OZ]-Desktop	192.168.100.116	Windows 10 Pro 64-bit	BFBFBFF000806ECL14F98CD1...	Armed	8 present and approved 3 disconnected and approved 1 not approved

## Allowing Device Usage after Blocking

After a device has been blocked by the **Armed** policy, it is automatically set to **Disabled**. As a double failsafe, in order to allow a blocked device to be used again, you must both **Enable** it and **Approve** it.

Both **Free** mode and **Armed** mode show events in the dashboard (as described on page x), in the History Event Log (as described on page x) and will be sent to an external SOC if it has been integrated with SepioPrime (as described on page x).





### 3.5.2 Approving and Setting Policies for all Host Devices at Once

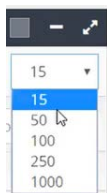
The Sepio Agent list shows a row for each agent that is deployed in your organization, as described on page X. The following describes how to approve or set a policy for all the devices connected to a specific host.

► To approve or set a policy for all devices of a host –

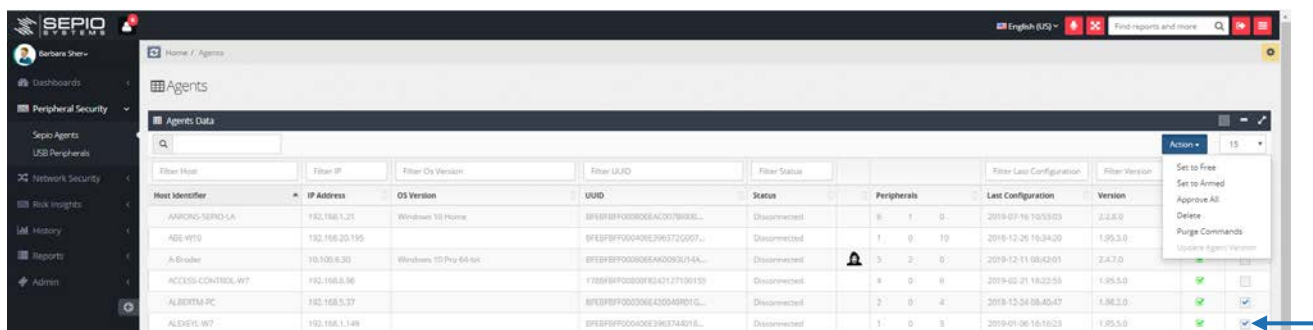
- 1 Select **Peripheral Security** ➔ **Sepio Agent** in the left pane.
- 2 Check the checkboxes on the right side of each relevant Sepio Agent's row.

In order easily find the hosts in which you are interested, you can filter the list of displayed Sepio Agents using the options at the top of the list.

The top right corner provides a drop down which enables you to select how many rows are displayed in each page.



- 3 Click the **Action** button to display a dropdown menu of options, as shown below –



- 4 Select the relevant action to be applied to ALL the devices of this host, as follows –
  - **Set to Free / Set to Armed** – To apply this policy. You may refer to page X for more information the **Free** and **Armed** policy.
  - **Approve All** – To approve all the devices on this host. We do not recommend using this option. It is better to review and approve each device separately, as described on page x.



- **Delete** – To remove a host from SepioPrime. Use this when a host is no longer relevant after it has been defined in SepioPrime.
- **Purge Commands** – To clear all the pending policy changes and approvals to be sent to a host(s), so that they are not sent, as described on page x.
- **Update Agent Version** – To update the SepioPrime Agent software on the selected host. From time to time Sepio may provide you with a new SepioPrime Agent, which should be placed on the SepioPrime server. You can then use this option to determine which hosts to update. We recommend that you update all the hosts.

After you select one of these dropdown menu options the action is performed by sending the relevant commands (policy changes and approvals) to the SepioPrime Agent.

### 3.5.3 Approving and Setting Policies for Specific Host Devices

The following describes how to review the devices of the specific host and to approve, not approve or set the policy for each device separately.

The screenshot shows the Sepio Systems web interface. The left sidebar contains navigation links: Dashboards, Peripheral Security (selected), Sepio Agents, USB Peripherals, Network Security, Risk Insights, History, Reports, and Admin. The main content area displays the 'Peripherals Data' table for the host 'ARONS-SEPIO-LA'. The table has columns for Device, Manufacturer, VID, Vendor, PID, Product Info, and Serial Number. There are three rows of data, each with a green checkmark in the 'Action' column, indicating approval.

Device	Manufacturer	VID	Vendor	PID	Product Info	Serial Number	Action
USB Composite Device	(Standard USB Host Controller)	F000	F000	FFF0	FFF0	C-H000001	<input checked="" type="checkbox"/>
USB Input Device	(Standard system devices)	0EEF	D-WAV Scientific Co., Ltd	C0AA	C0AA		<input checked="" type="checkbox"/>
Qualcomm QCA61x4A Bluetooth	Qualcomm	0CF3	Qualcomm Atheros Communications	E007	QCA61x4A Bluetooth 4.1		<input checked="" type="checkbox"/>

► To approve or set a policy for each device of a host –

- 1 Select **Peripheral Security** ➔ **Sepio Agent** in the left pane.



- 2 Double-click on the row of a Sepio Agent to display all the peripherals (devices) connected to it.

Double-click  
on a Sepio  
Agent

Host Identity	IP Address	OS Version	UUID	Status	Peripherals	Last Configuration	Version	License
AARON-SEPIO-LA	192.168.1.21	Windows 10 Home	BFE8FBF00806AC0C7B003...	Disconnected	6 1 0	2019-07-16 18:53:03	2.2.8.0	✓
AARON-SEPIO-LA	192.168.20.195		BFE8FBF00806AC0C7B003...	Disconnected	1 0 10	2018-12-26 19:34:20	1.95.5.0	✓
A-Broder	10.103.6.30	Windows 10 Pro 64-bit	BFE8FBF00806AC0C7B003...	Disconnected	5 2 0	2019-12-11 08:42:01	2.4.7.0	✓
ACCESS-CONTROL	192.168.6.96		17889BF400806AC0C7B003...	Disconnected	4 0 6	2019-07-21 18:22:55	1.95.5.0	✓

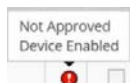
A list of the devices connected to this host is displayed, as shown below –

Device Icon	Device Name	Device Type	ID	Vendor	Product ID	Approval State
USB Input Device	(Standard system devices)	0557	ATEN International Co., Ltd	2261	2261	Not Approved (Red icon)
USB Input Device	(Standard system devices)	0557	ATEN International Co., Ltd	2261	2261	Not Approved (Red icon)
USB Input Device	(Standard system devices)	0557	ATEN International Co., Ltd	2261	2261	Not Approved (Red icon)
Generic USB Hub	(Standard USB Hubs)	0557	ATEN International Co., Ltd	8021	Hub	Not Approved (Red icon)
USB Root Hub (USB 3.0)	(Standard USB Hubs)	VROO	VROO	VROO	VROO	Approved (Green icon)

Showing 1 to 7 of 7 entries

- 3 A row appears for each device connected to the host. You may refer to page X for a description of each of these columns. Particularly interesting is the **Approval State** column on the right, which specifies whether the device has been approved by a SepioPrime user.

- – Each device that is already **Approved** (and **Enabled**) appears with a green icon on the right side of the row.
- – After each device has been installed, it is **Not Approved** and is **Enabled**. It appears with a red icon, as shown below –




**Note** – Some devices have been soldered into the motherboard and therefore cannot be blocked by a SepioPrime policy. Therefore, these devices automatically appear enabled and pre-approved. Their manufacturer is specified as **(Standard USB Hubs)** and their vendor, the ID and product info columns show **VROO**. For example, as shown below –

USB Root Hub (USB 3.0)	(Standard USB Hubs)	VROO	VROO	VROO	VROO	
------------------------	---------------------	------	------	------	------	--





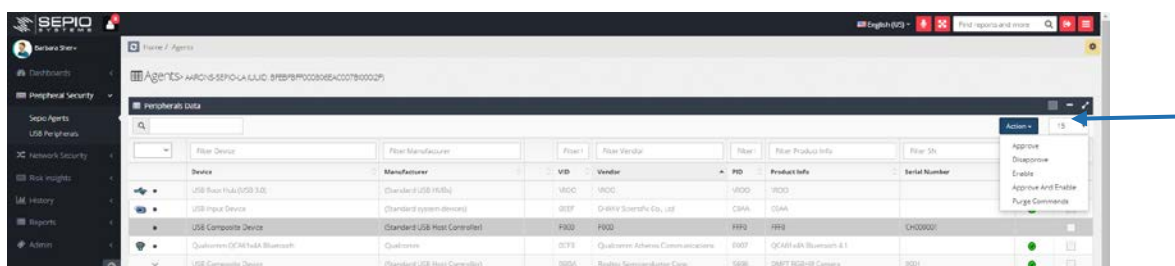
-  – Each device must be both **Approved** and **Enabled** in order to be covered. SepioPrime **disables** a device when it blocks it. This yellow icon appears after you have **Approved** a disabled device, but have not yet **Enabled** it.



- Check the checkboxes on the right side of each relevant device's row.

In order easily find the devices in which you are interested you can filter the list using the options at the top of the list.

- Click the **Action** button to display a dropdown menu of options, as shown below –



- Select the relevant action to be applied to the selected device(s), as follows –
  - Approve** – To approve all the selected device(s) on this host.
  - Disapprove** – To set the selected device(s) to **Not Approved** on this host.
  - Enable** – By default, each device is **Enabled**. SepioPrime disables a device when it blocks it. This option enables you to reenables the device. The device must then also be **Approved** in order to be covered.
  - Approve and Enable** – SepioPrime disables a device when it blocks it. As a double failsafe measure after a device has been blocked by SepioPrime, you must both **Enable** it and **Approve** it. This option does both at the same time.
  - Purge Commands** – To clear all the pending policy changes and approval commands to be sent to a host(s), so that they are not sent, as described on page x.

After you select one of these dropdown menu options the action is performed by sending the relevant commands (policy changes and approvals) to the SepioPrime Agent. The text in this row is displayed in blue font until after the command has been implemented on the relevant host. This may happen for example, when a person with a laptop is traveling and therefore is offline.



### 3.5.4 Approving and Setting Policies for a Device Types across your entire Organization

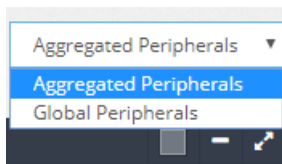
The **Peripheral Security** ➔ **USB Peripherals** option enables you to view –

- **Aggregated Peripherals** – You can review, approve/disapprove or enable **all the devices of a specific type** in your entire organization, as described on page X.
- **Global Peripherals** – You can review, approve/disapprove or enable all the devices of a specific user in your organization, as described on page X.

#### Aggregated Peripherals

► To approve or set a policy for a device type to be applied across your entire organization –

- 1 Select **Peripheral Security** ➔ **USB Peripherals** in the left pane. By default, the **Aggregated Peripherals** option is selected in a dropdown menu and the top right corner, as shown below –





The following displays showing an aggregated view of all the devices and all the hosts on which a Sepio Agent has been installed. Each row represents a device type and shows the quantity of hosts on which it is deployed, as shown below –




A screenshot of a web application interface titled 'Peripherals'. It shows a table with columns for Quantity, Device, Manufacturer, VID, Vendor, PID, and Product Info. The table lists various USB devices like USB Root Hubs, USB Input Devices, and USB Composite Devices. On the left, there is a sidebar with navigation options like 'Dashboards', 'Peripheral Security', 'Sepio Agents', 'USB Peripherals', 'Network Security', 'Risk Insights', 'History', 'Reports', and 'Admin'. The top right corner shows 'Aggregated Peripherals' and a count of 15 items.



Quantity	Device	Manufacturer	VID	Vendor	PID	Product Info
161/190	USB Root Hub (USB 3.0)	(Standard USB HUBs)	1800	1800	1800	1800
117/190	USB Root Hub	(Standard USB Host Controller)	1800	1800	1800	1800
70/190	Intel(R) Wireless Bluetooth(R)	Intel Corporation	8087	Intel Corp.	0A2B	Wireless Bluetooth
40/190	USB Input Device	(Standard system devices)	048D	Logitech, Inc.	C077	M105 Optical Mouse
38/190	Generic USB Hub	(Standard USB HUBs)	413C	Dell Computer Corp.	2513	Internal USB Hub of E-Port Replicator
38/190	Generic USB Hub	(Generic USB Hub)	8087	Intel Corp.	0024	Integrated Rate Matching Hub
36/190	USB Composite Device	(Standard USB Host Controller)	045C	Broadcom Corp.	5832	BCM5880 Smartcard Reader
36/190	Dell ControlVault w/o Fingerprint Sensor	Dell	045C	Broadcom Corp.	5832	BCM5880 Smartcard Reader
36/190	Microsoft Uniboot Smartcard Reader (WUDF)	Microsoft	045C	Broadcom Corp.	5832	BCM5880 Smartcard Reader
33/190	USB Composite Device	(Standard USB Host Controller)	048D	Logitech, Inc.	C31C	Keyboard K120
32/190	USB Input Device	(Standard system devices)	048D	Logitech, Inc.	C31C	Keyboard K120
32/190	USB Input Device	(Standard system devices)	048D	Logitech, Inc.	C31C	Keyboard K120
30/190	Generic USB Hub	(Generic USB Hub)	8087	Intel Corp.	8000	USB Hub
25/190	Generic SuperSpeed USB Hub	(Standard USB HUBs)	413C	Dell Computer Corp.	5534	USB Hub
24/190	Intel(R) Wireless Bluetooth(R)	Intel Corporation	8087	Intel Corp.	0A2A	Wireless Bluetooth
















Each row in this page represents a device type. The following describes columns of information provided for each device –

- **Device Type Icon** – The leftmost column provides an icon representing the type of device. For example,  represents a keyboard and  represents a mouse. A description of this type of device is provided in the **Device** column.

Pay special attention to the rubber ducky  device icon that represents a malicious HID (Human Interface Device). These devices show a **Red Mask**  icon or an **Anonymous**  icon in the risk indication column. You may refer to page X for more information about the meaning of these icons.

- **Composite Devices** – Some devices are a composition of other devices. These are indicated by a down arrow . The down arrow represents the composite device. The subject devices that are composite device contains are represented by a right facing arrow . Another way to understand which rows represent composite devices and which are the sub-devices that belong to it is to look in the **VID**, **Vendor** and **PID** column. All those with the same value in these columns belong to the same composite device.

For example, the following shows three rows for a USB Composite Device from **Broadcom Corp.** and another three rows for a USB Composite Device from **Logitech Inc.**.

	Quantity ▾		Device ▾	Manufacturer ▾	VID ▾	Vendor ▾	PID ▾
	38/190	38 	Generic USB Hub	(Generic USB Hub)	8087	Intel Corp.	0024
▾	36/190	35 	USB Composite Device	(Standard USB Host Controller)	0A5C	Broadcom Corp.	5832
>	36/190	35 	Dell ControlVault w/o Fingerprint Sensor	Dell	0A5C	Broadcom Corp.	5832
	36/190	35 	Microsoft Usbccid Smartcard Reader (WUDF)	Microsoft	0A5C	Broadcom Corp.	5832
▾	33/190	29 	USB Composite Device	(Standard USB Host Controller)	046D	Logitech, Inc.	C31C
	32/190	29 	USB Input Device	(Standard system devices)	046D	Logitech, Inc.	C31C
	32/190	29 	USB Input Device	(Standard system devices)	046D	Logitech, Inc.	C31C
	30/190	29 	Generic USB Hub	(Generic USB Hub)	8087	Intel Corp.	8000

Broadcom  
Composite Device

Logitech Composite  
Device

**Note** – The indication of the composite device and its sub-devices is represented by the arrows regardless of the icons on their left.


- **Quantity** – Specifies the distribution of this device type in your organization, meaning the number of hosts that have this type of device out of all the hosts in the organization. For example, **40/188** means that this device type is deployed on 40 hosts out of the 188 hosts in your organization.

	Quantity ▾
	40/188






37

- **Quantity of Not Approved Devices**  – Specifies the number of hosts that have this device type on which it has not been approved. For example, 40 hosts in your organization may

37

have this device type, but this icon  means that on 37 of those hosts that this device type has not been approved.

- **Risk Indication** – This is an extremely important column. It specifies the inherent risk of this device, as follows –




- **Danger! Red Mask** – **An attack tool masquerading as a legitimate device has been detected.** It is impersonating a legitimate device by duplicating the value of the Vendor ID (VID) and Product ID (PID).




- **Anonymous** – Specifies that this device is known to be vulnerable by design. It has a built-in vulnerability that enables it to be exploited by hackers. This vulnerability is listed in the Sepio threat intelligence database and is recognized by hackers. Hovering over this icon displays a description. For example, as shown below –



If this device is actually being used as an attack tool, then the rubber ducky  icon appears on its left. For example, as shown below –

PoisonTap									
	1/188	1 	USB Ethernet/RNDIS Gadget	Acer Incorporated.		0525	Netchip Technology, Inc.	A4A2	Linux-USB Ethernet/RNDIS Gadget

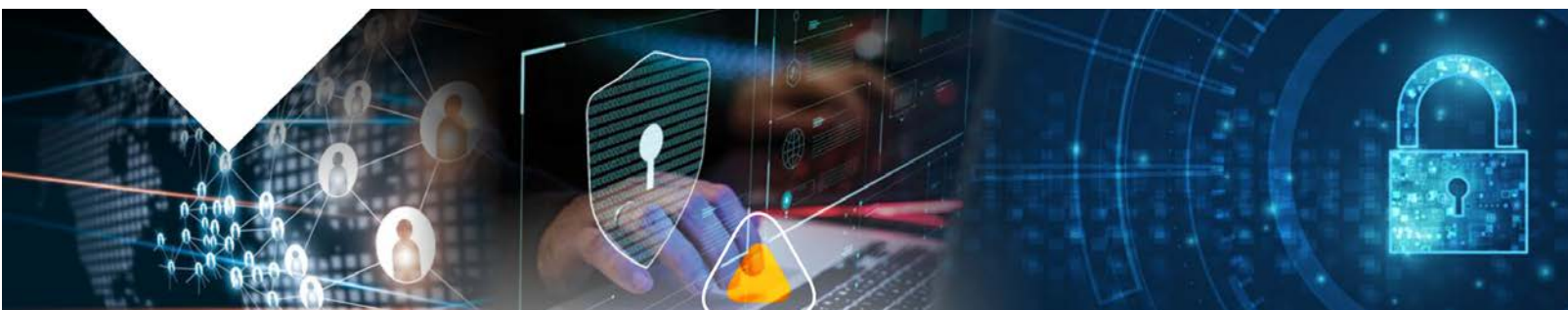
If no rubber ducky  icon appears on its left then the device is not currently being used as an attack tool, but still has the potential to be used as one because it is vulnerable by design.



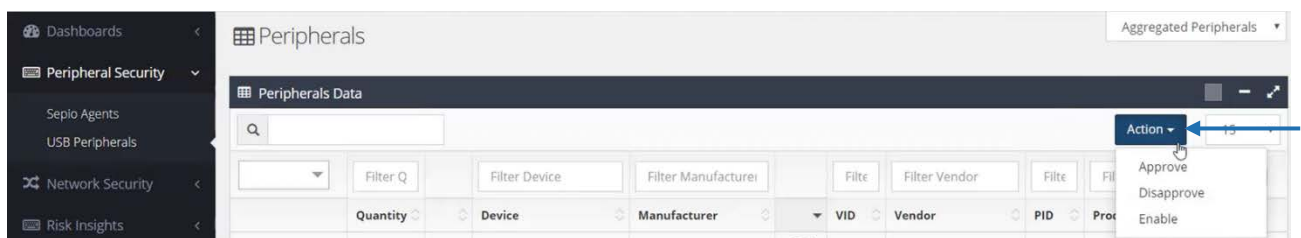
- **Black Mask** – This icon is only displayed for SepioPrime users that have administrative privileges. This indication does not mean that it is an attack tool. However, although SepioPrime recognizes this device, SepioPrime has never encountered this version of the device. For example, a new version of a known mouse.



Please contact Sepio support if you see this icon so that we can update our threat information database.



- **Manufacturer/VID/Vendor/PID/Product Info** – Provides various types of information about this device.
- 2 Check the checkboxes on the right side of each relevant device's row.  
In order easily find the devices in which you are interested you can filter the list using the options at the top of the list. For example, by PID (Product ID).
  - 3 Click the **Action** button to display a dropdown menu of options, as shown below –



- 4 Select the relevant action to be applied to each device, as follows –
  - **Approve** – To approve all the selected device(s) on this host.
  - **Disapprove** – To set the selected device to Unapproved on this host.
  - **Enable** – By default, each device is **Enabled**. SepioPrime disables a device when it blocks it. This option enables you to reenables the device. It must then also be approved in order to be covered.

After you select one of these dropdown menu options the action is performed by sending the relevant commands (policy changes and approvals) to the SepioPrime Agent. The text in this row is displayed in blue font until after the command has been implemented on the relevant host. This may happen for example, when a person with a laptop is traveling and therefore is offline.

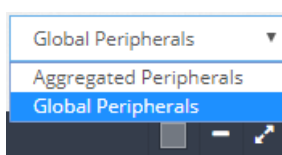




### 3.5.5 Approving and Setting Policies for Devices per User – Global Peripherals

► To approve or set a policy for a specific device for a specific user –

- 1 Select **Peripheral Security** ➔ **USB Peripherals** in the left pane.
- 2 In a dropdown menu and the top right corner, select **Global Peripherals**, as shown below –





The following displays showing a global view of all the devices and all the specific devices in your organization. Each row represents a specific device deployed on a specific host, as shown below –




The screenshot shows the SEPIO Systems 'Peripherals' dashboard. The left sidebar contains navigation links: Dashboards, Peripheral Security (selected), Sepio Agents, USB Peripherals, Network Security, Risk Insights, History, Reports, and Admin. The main content area is titled 'Peripherals' and includes a 'Global Peripherals' dropdown. Below this is a 'Peripherals Data' table with columns for Device, Manufacturer, Host Identifier, Host UUID, VID, PID, and Serial Number. The table contains several rows of data, including USB Composite Devices and USB Input Devices, each associated with a specific host and UUID.



Device	Manufacturer	Host Identifier	Host UUID	VID	PID	Serial Number
USB Composite Device	(Standard USB Host Controller)	REM00-W10	BFEBFBFF000806E996375U01A62F	FFFF	0035	08FF20150112
USB Input Device	(Standard system devices)	REM00-W10	BFEBFBFF000806E996375U01A62F	FFFF	0035	
USB Input Device	(Standard system devices)	REM00-W10	BFEBFBFF000806E996375U01A62F	FFFF	0035	
USB Composite Device	(Standard USB Host Controller)	TAMIR-W10	BFEBFBFF000806E996375U019A2F	FFFF	0035	08FF20150112
USB Input Device	(Standard system devices)	TAMIR-W10	BFEBFBFF000806E996375U019A2F	FFFF	0035	









Each row in this page represents a specific device. The columns in this page are the same as the **Aggregated Peripherals** view, as described on page X, except that additional columns are provided to describe the specific host on which each specific device is deployed, such as **Host Identifier** and **Host UUID**.

- **Device Type Icon** – The leftmost column provides an icon representing the type of device. For example,  represents a keyboard and  represents a mouse. A description of this type of device is provided in the **Device** column.



Pay special attention to the rubber ducky  device icon that represents a malicious HID (Human Interface Device). These devices will show a **Red Mask**  icon or an **Anonymous**  icon in the risk indication column. You may refer to page X for more information about the meaning of these icons.



- **Composite Devices** – Some devices are a composition of other devices. These are indicated by a down arrow . The down arrow represents the composition device and then each row that follows it has a right facing arrow  that represents the sub-devices that comprise it. Another way to understand which rows represent opposite devices and which are the sub-devices that belong to it is to look in the **VID**, **Vendor** and **PID** column. All those with the same value in these columns belong to the same composite device. For example, the following shows three rows for a USB Composite Device from Broadcom Corp. and another three rows for a USB Composite Device from Logitech Inc.

	Quantity		Device	Manufacturer	VID	Vendor	PID
Broadcom Composite Device	38/190	38 	Generic USB Hub	(Generic USB Hub)	8087	Intel Corp.	0024
	36/190	35 	USB Composite Device	(Standard USB Host Controller)	0A5C	Broadcom Corp.	5832
	36/190	35 	Dell ControlVault w/o Fingerprint Sensor	Dell	0A5C	Broadcom Corp.	5832
	36/190	35 	Microsoft Usbccid Smartcard Reader (WUDF)	Microsoft	0A5C	Broadcom Corp.	5832
Logitech Composite Device	33/190	29 	USB Composite Device	(Standard USB Host Controller)	046D	Logitech, Inc.	C31C
	32/190	29 	USB Input Device	(Standard system devices)	046D	Logitech, Inc.	C31C
	32/190	29 	USB Input Device	(Standard system devices)	046D	Logitech, Inc.	C31C
	30/190	29 	Generic USB Hub	(Generic USB Hub)	8087	Intel Corp.	8000

**Note** – The indication of the compass and divides and it some devices is represented by the arrows regardless of the icons on their left.



- **Quantity** – Specifies the distribution of this device type in your organization, meaning the number of hosts that have this type of device out of all the hosts in the organization. For example, **40/188** means that this the device type is deployed on 40 hosts out of the 188 hosts in your organization.

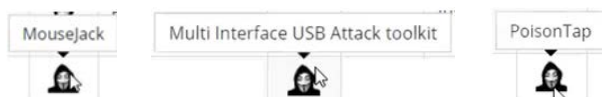
	Quantity
	40/188


- **Quantity of Not Approved Devices**  – Specifies the number of hosts that have this device type on which it has not been approved. For example, if 40 hosts in your organization have this device type, then this icon  indicates that this device type has not been approved on 37 hosts.







- **Risk Indication** – This is an extremely important column. It specifies the inherent risk of this device, as follows –


-  – **Danger! Red Mask** – **An attack tool masquerading as a legitimate device has been detected.** It is impersonating a legitimate device by duplicating the value of the Vendor ID (VID) and Product ID (PID).
-  **Anonymous** – Specifies that this device is known to be vulnerable by design. It has a built-in vulnerability that enables it to be exploited by hackers. This vulnerability is listed in the Sepio threat intelligence database and is recognized by hackers. Hovering over this icon displays a description. For example, as shown below –




If this device is actually being used as an attack tool, then the rubber ducky  icon appears on its left. For example, as shown below –

PoisonTap									
	1/188	1 	USB Ethernet/RNDIS Gadget	Acer Incorporated.		0525	Netchip Technology, Inc.	A4A2	Linux-USB Ethernet/RNDIS Gadget

If no rubber ducky  icon appears on its left then the device is not currently being used as an attack tool, but still has the potential to be used as one because it is vulnerable by design.

-  **Black Mask** – This icon is only displayed for SepioPrime users that have administrative privileges. This indication does not mean that it is an attack tool. However, although SepioPrime recognizes this device, SepioPrime has never encountered this version of the device. For example, a new version of a known mouse.



Please contact Sepio support if you see this icon so that we can update our threat information database.

- **Manufacturer/VID/Vendor/PID/Product Info** – Provides various types of information about this device.

### 3 Check the checkboxes on the right side of each relevant device's row.

In order to easily find the devices in which you are interested, you can filter the list using the options at the top of the list. For example, by VID (Vendor ID).







- 4 Click the **Action** button to display a dropdown menu of options, as shown below –



- 5 Select the relevant action to be applied to each device, as follows –
  - **Approve** – To **Approve** all the selected device(s) on this host.
  - **Disapprove** – To set the selected device to **Not Approved** on this host.
  - **Enable** – By default, each device is **Enabled**. SepioPrime disables a device when it blocks it. This option reenables the device. However, it must then also be **Approved** in order to be covered.

After you select one of these dropdown menu options, the action is performed by sending the relevant commands (policy changes and approvals) to the SepioPrime Agent. The text in this row is displayed in blue font until after the command has been implemented on the relevant host. This may happen for example, when a person with a laptop is traveling and therefore is offline.

## 3.5.6 Mitigating Vulnerable Devices

### Device Supply Chain Vulnerabilities

Some devices are vulnerable by manufacturer design, meaning that hackers have found a way to exploit organizations' networks through a vulnerability that is inherent to the actual device. You may decide to replace these devices (such as a mouse or keyboard) with other devices that do not have vulnerabilities (such as a mouse from different manufacturer or a different version of the same mouse). Alternatively, you might exile these devices to be used in a less important and separate part of your organization.

### Devices That Are or Contain Attack Tools

Devices that contain attack tools should be handled more aggressively as you see fit.



We recommend that you immediately run over to this device and grab it, since someone may quickly pull it out and disappear.





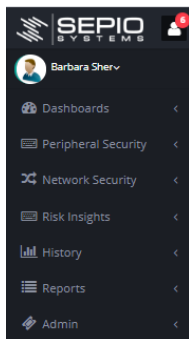
# 4

## Network Visibility

*This chapter describes the workflow for setting up SepioPrime network visibility/security and the user interface features that are provided to monitor and block attacks.*

### 4.1 Overview

The following menu options are provided for setting up, monitoring and implementing the policies of network visibility/security.

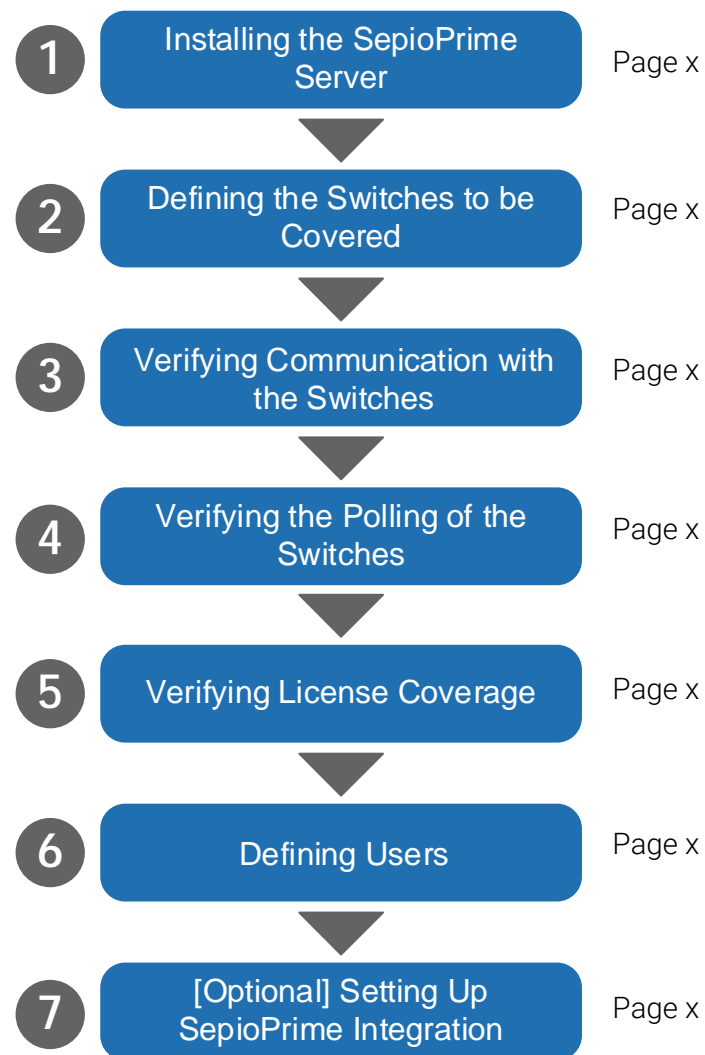


- Dashboards ➔ Network Security, as described on page X
- Network Security ➔ Network Switches, as described on page X
- Network Security ➔ Network Ports, as described on page X
- Network Security ➔ Configuration, as described on page X
- Risk Insights ➔ Switch Vulnerabilities, as described on page X
- Risk Insights ➔ Network Ports, as described on page X
- Reports ➔ Alarmed Ports, as described on page X
- Reports ➔ Zero MAC Ports, as described on page X
- Reports ➔ Port Administration, as described on page X



### 4.1.1 Setting up SepioPrime for Network Visibility/Security

The following is recommended workflow for setting up SepioPrime for network visibility/security –



The following provides more information about the workflow depicted above and a page reference to the place in this user manual that describes it in detail.

- **Step 1, Installing the SepioPrime Server** – According to the instructions in the *SepioPrime Installation Manual*.
- **Step 2, Defining the Switches to be Covered** – SepioPrime provides three methods for importing the list of switches to be covered by SepioPrime, as follows –
  - **Importing a CSV file**, as described on page x.



- **Manually adding switches in the user interface**, as described on page x.
- **API**, as described on page x.
- **Step 3, Verifying Communication with the Switches**, as described on page x
- **Step 4, Verifying the Polling of the Switches**, as described on page x.
- **Step 5, Verifying License Coverage**, as described on page x.
- **Step 6, [Optional] Defining Users** – Define additional SepioPrime users as needed, as described on page X.
- **Step 7, [Optional] Setting Up SepioPrime Integration** with Syslog and CEF according to the instructions in the *SepioPrime Northbound Interfaces Manual*.

### 4.1.2 Using SepioPrime for Network Visibility and Blocking

The following options can be used for ongoing monitoring of network security.

- **Network Security Dashboard** – SepioPrime shows a variety of risk and status features regarding the switches in your organization, as described on page X.
- **Risk Insights** – SepioPrime provides insights into your switch vulnerabilities and network ports, as described in page X.
- **Network Switches** – Sepio provides a detailed list of each covered switch, its risk and its status, as described on page X.
- **Network Ports** – Sepio provides a detailed list of each hurtful connected to each covered host, its risk and its status, as described on page X.
- **History – Event Log** – SepioPrime provides a detailed log of all system events, as described on page X.
- **Viewing and Generating Reports** – SepioPrime provides various ready-made reports and enables you to generate your own customized reports to be distributed by email, as described on page X.

**Important Note** – Before investigating risk insights (as described on page x) or generating reports (as described on page X), you must allow the system to operate for at least three times the time period that you defined in the scan policy parameter (as described in page x).

## 4.2 Defining the Switches

Three methods are provided for importing the list of switches to be covered by SepioPrime, as follows –

- Importing a CSV File, page 53
- Manually Adding Each Switch in the User Interface, page 55
- API, page 56

### 4.2.1 Importing a CSV File

The following describes how to add multiple switches to SepioPrime from a Comma Separated Values (CSV) file. This is the most popular and the most efficient method.

► To import a CSV file of switches –

- 1 Select **Network Security** ➔ **Configuration** and then scroll down to the **Switch List Operations** section, as shown below –

The screenshot displays the SepioPrime web interface. On the left, a dark sidebar contains a menu with 'Peripheral Security' and 'Network Security' (expanded). Under 'Network Security', 'Network Switches', 'Network Ports', and 'Configuration' are listed. The 'Configuration' option is selected. The main content area is divided into three sections. The top section, 'Scan Policy', contains a table with columns: Priority, Interval, Number of Switches, Number of Ports, Utilization, and an Action column. The middle section, 'Scan Engines', contains a table with columns: Name, IP Address, Admin, Status, Threads, Utilization, Version, and an Action column. The bottom section, 'Switch List Operations', contains 'Export' and 'Import' buttons.

Priority	Interval	Number of Switches	Number of Ports	Utilization	
Critical	1 min	61	7302	N/A	<input type="checkbox"/>
High	30 min	1	112	N/A	<input type="checkbox"/>
Normal	1 hour	1	50	N/A	<input type="checkbox"/>
Low	8 hours	0	0	N/A	<input type="checkbox"/>
Occasional	24 hours	0	0	N/A	<input type="checkbox"/>

Name	IP Address	Admin	Status	Threads	Utilization	Version	
Eran's Simulate Poller	192.168.100.112	Deactivated	Not Connected	40		3.27	<input type="checkbox"/>
Internal demoseet Poller	192.168.100.126	Deactivated	Not Connected	40		3.36	<input type="checkbox"/>
Internal Poller	192.168.100.126	Activated	Not Connected	40		3.36	<input type="checkbox"/>
Internal Poller		Deactivated	Connected	10		3.39	<input type="checkbox"/>
Internal demo Poller	192.168.100.126	Deactivated	Not Connected	40		3.36	<input type="checkbox"/>

Switch List Operations

Export Import





- 2 Create a CSV file in which each row represents a switch and each column represents the parameters of the switch to be added to SepioPrime. The format of the file to be imported is shown below –

```
# Any comment here
# Or here.
# As long as they start with the '#' character
#
# The order of fields (per switch) are:
# IP Address, Priority, Transport, Username, Password, EnablePass
# - Priority from 1 (Critical) through 3 (Normal) to 5 (Occasional)
# - Username, Password, and EnablePass can be set or omitted
#
# In the below example:
# .24 does not need a Password but does need an EnablePass
# .39 does need a user Password but does not need an EnablePass
# .72 does not need a Username but does need Password and EnablePass
#
192.168.100.23,1,Telnet,User1,Password1,EnablePassword
192.168.100.24,1,Telnet,User1,,EnablePass
192.168.100.39,3,SSH,User2,Password2,EnablePW2
# Comments are also possible throughout the file
#192.168.100.23,SSH,User3
192.168.100.51,1,Telnet,User3,Pass3,
192.168.100.72,4,Telnet,,Password,EnablePass
```

**Note** – It is important to note that when importing a switch list from a file, the administrator should define whether the imported entries will replace the existing list of switches, or will be added to the existing list (meaning that switches that are defined in the system and do not appear in the list will remain after the import is completed). When importing an entry with IP address of an existing switch, the entry from the list will replace the existing one.

## Exporting the Switch List

For security purposes, access credentials (such as passwords), are not exported.

**Note** – However, you must specify these credentials when importing switch lists in order to enable access.

You can export the switch list file for your own records, as follows –

- Click the **Export** button to export a list of the switches are defined in SepioPrime. For example, as shown below –

```
# Sepio Systems Switch List Export
# Export Time: YYYY/MM/DD HH:MM:SS
# User: Matthew Bailey
#
# The order of fields (per switch) are:
# IP Address, Priority, Transport, Username, Password, EnablePass
# - Priority from 1 (Critical) through 3 (Normal) to 5 (Occasional)
#
192.168.100.23,1,Telnet,User1,X67FR@,
192.168.100.24,1,Telnet,User1,X67FR@,K4^7bG
192.168.100.39,3,SSH,User2,Pass75,myEnableSecret
192.168.100.51,1,Telnet,User3,,
```



## 4.2.2 Manually Adding Each Switch in the User Interface

The following describes how to manually define each switch in the user interface.

► To manually add a switch to be covered by SepioPrime –

- 1 Select the **Network Security** ➔ **Network Switches** options.
- 2 Click the **Action** button in the top right of the page to display the dropdown menu of options and select the **Add Switch** option.

Filter IP Address	Filter Model	Filter Name	Filter IOS	Filter Status	Filter Scan Prio	Filter Last Updated	Action
IP Address	Model	Name	IOS	Status	Scan Priority	Last Updated	
10.9.91.1	WS-C3850-48P	HQ-Distribution	3.6.5E	Normal	High	2019-09-01 11:38:59	
10.20.84.5	WS-C3960-24TC-L	BASE-4432-RACK	15.0(2)SE11	Normal	Critical	2019-09-01 11:40:01	
10.20.86.5	WS-C3960-24TC-L	SW65-SOUTH-END	15.0(2)SE11	Normal	Critical	2019-09-01 11:40:01	SSH

The following displays –

Protocol

SSH

Host

Username

Password

Enable Password

Scan Priority

Normal

Cancel

Save

**Note** – SepioPrime does not disclose usernames and passwords.

- 3 Define the switch to be added and assign a scanning priority. You may refer to page X for more information about scanning priority.
- 4 Click the **Save** button.





## 4.2.3 API

Sepio provides an open format to enable integrators to provide switch lists via API command. Vendor and product specific interfaces can be enabled upon request.

### Open Format – Get Switch List

Request	GET https://192.168.75.12/prime/api/switchlist/
Response	<pre>{ [   "IpAddress": "192.168.100.23",   "Priority": "1",   "Transport": "Telnet",   "Username": "User1",   "Password": "Password1",   "Enable": "EnablePassword" ], [   "IpAddress": "192.168.100.24",   "Priority": "1",   "Transport": "Telnet",   "Username": "User1",   "Password": null,   "Enable": "EnablePass" ], [   "IpAddress": "192.168.100.39",   "Priority": "3",   "Transport": "SSH",   "Username": "User2",   "Password": "Password2",   "Enable": "EnablePW2" ], [   "IpAddress": "192.168.100.51",   "Priority": "1",   "Transport": "Telnet",   "Username": "User3",   "Password": "Pass3",   "Enable": null ], [   "IpAddress": "192.168.100.72",   "Priority": "4",   "Transport": "Telnet",   "Username": null,   "Password": "Password",   "Enable": "EnablePass" ] ] }</pre>



## 4.3 Defining Your Scan Policy for Network Switches

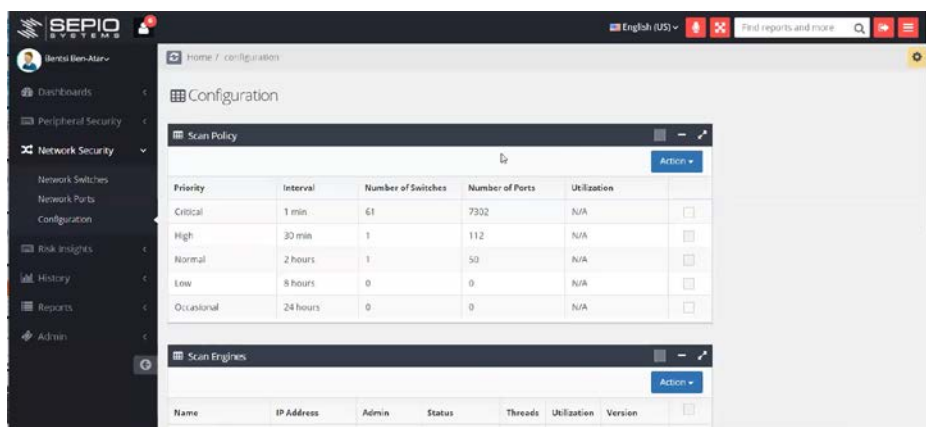
The following describes how to define the SepioPrime scanning policy of your network switches, including the frequency (interval) .



It's up to you how frequently to define to poll the ports of a switch. The network load is not significant, but you may decide to poll some switches every few minutes and some others switches every few hours.

► To define your scan policy of network switches –

1 The Networks Security ➔ Configuration. The following displays –



The **Scan Policy** section shows a list of scan policies according to the priority assigned to each switch, as follows –

- **Priority** – Specifies the priority that to be assigned to each switch – **Critical, High, Normal, Low** and **Occasional**, which determines the interval (frequency) at which it is scanned, as described below. The priority of each switch is assigned when it is created in SepioPrime, as described on page X.

Priority	Interval	Number of Switches	Number of Ports	Utilization	
Critical	1 min	61	7302	N/A	<input type="checkbox"/>
High	30 min	1	112	N/A	<input type="checkbox"/>
Normal	2 hours	1	50	N/A	<input type="checkbox"/>
Low	8 hours	0	0	N/A	<input type="checkbox"/>
Occasional	24 hours	0	0	N/A	<input type="checkbox"/>





- **Interval** – Specifies how often SepioPrime scans the switches in your organization according to the priority that has been assigned to each switch. A default interval is assigned to each priority, as shown above. For example, **Critical** switches are scanned every minute (**1 min**) by default and switches with **Low** priority are scanned every **8 hours**.
  - **Number of Switches** – Specifies how many switches in your organization have been assigned this priority.
  - **Number of Ports** – Specifies the total quantity of ports that belong to the switches in your organization that have been assigned this priority.
- 2 Select the checkbox of one of the rows in the **Scan Policy** section, such as the **Critical Priority** row. Only a single checkbox can be selected at a time.
  - 3 Click the **Action** button and select the **Edit** option, as shown below –



The following displays –

Update Scan Policy Interval

Name

High

Interval

30 min

Cancel

Save

- 4 In the **Name** dropdown menu, select the priority to be changed.
- 5 In the **Interval** dropdown menu, select how often SepioPrime will scan.
- 6 Click the **Save** button.





## Scan Engines

The **Scan Engines** section describes the SepioPrime network pollers that handle the scanning of your networks switches. One or more scan engine were created during the installation of the SepioPrime server. Each scan engine handles a specific site and multiple scan engines may be installed in order to extend your network to a remote site. The primary scan engine is created and activated to run on your entire organization's network on a specific site and is called the *internal scan engine*.

All the information collected from all scan engines is aggregated and shown in the SepioPrime user interface described in this user manual. This section provides an **Action** button that enables you to **Activate** or **Delete** a scan engine. Only a single scan engine can be activated at a time.

Scan Engines							Action
Name	IP Address	Admin	Status	Threads	Utilization	Version	
Eran's Simulate Poller	192.168.100.112	Deactivated	Not Connected	40		3.27	<input type="checkbox"/>
Internal demoseet Poller	192.168.100.126	Deactivated	Not Connected	40		3.36	<input checked="" type="checkbox"/>
Internal Poller	192.168.100.126	Activated	Not Connected	40		3.36	<input type="checkbox"/>
Internal demo Poller	192.168.100.126	Deactivated	Not Connected	40		3.36	<input type="checkbox"/>
Internal Poller		Deactivated	Connected	10		3.39	<input type="checkbox"/>

If you delete a scan engine, its information is still shown in the user interface, but is no longer updated of course.





## 4.4 Network Switches

The following describes how to display a list of the network switches covered by SepioPrime. A row appears for each switch that was added to SepioPrime, as described on page X. The following displays –

IP Address	Model	Name	IOS	Status	Scan Priority	Last Updated	Transport
10.9.91.1	WS-C3850-48P	HQ-Distribution	3.6.5E	Normal	High	2019-09-01 11:38:59	Telnet
10.20.84.5	WS-C2960-24TC-L	BASE-432-RACK	15.02SE11	Normal	Critical	2019-09-01 11:40:01	SSH
10.20.86.5	WS-C2960-24TC-L	SWMS-SOUTH-BND	15.02SE11	Normal	Critical	2019-09-01 11:40:01	SSH
10.20.88.4	WS-C2960-24TC-L	ACCT-C296	15.02SE11	Normal	Critical	2019-09-01 11:40:01	SSH
10.22.31.5	WS-C2960X-8PPD-L	JFFF-TEST-SW	15.20E	Normal	Critical	2019-09-01 11:40:01	SSH
10.28.146.4	WS-C3850-48P	Q1165-SW-B1	3.6.5E	Normal	Critical	2019-09-01 11:39:01	SSH
10.28.147.4	WS-C3850-48P	HQ_3FL	3.6.5E	Normal	Critical	2019-09-01 11:39:01	SSH
10.29.32.16	WS-C3750G-48PS-S	T208_BFL	12.2(33)SE10	Normal	Critical	2019-09-01 11:40:01	SSH
10.29.32.18	WS-C3850-48P	MEZZU-ELEVATE	3.6.5E	Normal	Critical	2019-09-01 11:39:01	SSH
10.29.32.20	WS-C3850-48P	D5199	3.6.6E	Normal	Critical	2019-09-01 11:39:01	SSH
10.29.32.21	WS-C3850-48P	D514J76	3.6.5E	Normal	Critical	2019-09-01 11:39:01	SSH
10.29.32.22	WS-C3850-48P	D-KINGS_C01	3.6.5E	Normal	Critical	2019-09-01 11:39:01	SSH
10.34.0.3	WS-C3850-48P	AG35_BC72	3.6.5E	Normal	Critical	2019-09-01 11:39:02	SSH
10.34.2.2	WS-C3850-48P	GAINSBURG_BFL	3.6.5E	Normal	Critical	2019-09-01 11:39:00	SSH
10.51.2.17	WS-C3850-48P	TOPFLOOR_CUG	3.6.5E	Normal	Critical	2019-09-01 11:39:01	SSH

Each row in this list represents a switch that was added to SepioPrime, as described in page X.

The following describes the columns that appear for each switch –

### Switch Icon



### Model / Name / IOS

Describes the switch.

### Status

Specifies the status of this switch, as follows –

- **Unable To Connect** – Specifies that there is no network connectivity to the switch. For example, when the access credentials are not correct.





## Scan Priority

Specifies the priority assigned to the switch – **Critical, High, Normal, Low** and **Occasional**. This priority which determines the interval (frequency) at which it is scanned. You may refer to page X for more information about defining the scanning interval.

## Last Updated

Specifies with the timestamp of when the most recent scan was performed of this switch.

## Transport

Telnet or SSH.

### 4.4.1 Network Switches Actions

The following actions can be performed by clicking the **Action** button in the top right of this page –

IP Address	Model	Name	IOS	Status	Scan Priority	Last Updated
10.9.91.1	WS-C3850-48P	HQ-Distribution	3.6.5E	Normal	High	2019-09-01 11:38:59
10.20.84.3	WS-C2960-24TC-L	BASE-4432-RACK	15.0(2)SE11	Normal	Critical	2019-09-01 11:40:01
10.20.86.5	WS-C2960-24TC-L	SW55-SOUTH-END	15.0(2)SE11	Normal	Critical	2019-09-01 11:40:01

- **Add Switch** – Enables you to manually add a switch to be covered by SepioPrime, as described on page X.
- **Edit Switch** – Enables you to manually edit a previously added switch to be covered by SepioPrime.
- **Delete Switch** – Enables you to delete a previously added switch.
- **Poll Now** – Initiates an immediate SepioPrime scan of the selected switch(es). This does not affect the currently defined scanning policy. This option may be useful when you need to create a snapshot of the current status.
- **Scan Policy** – Enables you to change the SepioPrime scanning priority assigned to the selected switch(es). The following displays. You may refer to page X for more information.

Update Scan Policy

Scan Priority

Normal

Cancel Save





## 4.5 Network Ports

The following describes how to display an aggregated list of the network ports covered by SepioPrime. A row appears for each physical port of each switch, as shown below –

IP Address	Switch Name	Port	Port Name	# Addresses	Link Partner	Fingerprint	Port Status	CDP Info
10.104.17.2	HQ_DR3FL	Gi1/0/1		2	10CDAE6908DF,90B11C63ADC3	1140796D01410EE101E1C1E1000D4F96-----	connected	
10.104.17.2	HQ_DR3FL	Gi1/0/30		1	7446A09D879D	1140796D01410EE103712DE1000D4006-----	connected	
10.104.17.2	HQ_DR3FL	Gi1/0/31		1	50CD22B37A4D	1140796D01410EE101E1C1E1000D4BE5-----	connected	
10.104.17.2	HQ_DR3FL	Gi1/0/32		1	50CD22B1E28A	1140796D01410EE101E1C1E1000D4F59-----	connected	
10.104.17.2	HQ_DR3FL	Gi1/0/33		1	7446A09D87C0	1140796D01410EE103712DE1000D4006-----	connected	
10.104.17.2	HQ_DR3FL	Gi1/0/34		1	10CDAE690292	1140796D01410EE101E1C1E1000D49FC-----	connected	
10.104.17.2	HQ_DR3FL	Gi1/0/35		0			notconnect	
10.104.17.2	HQ_DR3FL	Gi1/0/36		0			notconnect	
10.104.17.2	HQ_DR3FL	Gi1/0/37		0			notconnect	
10.104.17.2	HQ_DR3FL	Gi1/0/38		2	10CDAE69133F,5065F346B400	1140796D01410EE101E1C1E1000D4E59-----	connected	
10.104.17.2	HQ_DR3FL	Gi1/0/39		1	7446A09A9B4E	1140796D01410EE103712DE1000D4006-----	connected	

This list shows the switch name, its IP address, quantity of unique MAC addresses connected to each physical port and so on. You can hover over the information in this table to display more detail.

### # Addresses Column

For example, hovering over the **# Addresses** column displays a tooltip listing details about each network device connected to this physical port. This means that if the number **2** appears in this column, that two network devices are connected to that physical port, as shown below –

IP Address	Switch	# Addresses	Link Partner	Fingerprint
192.168.1.7	Floor1	1054	0000C9FF005,000B001038A8,000...	
192.168.13.25	Calgary	1025	0022BES24031,00351AFF4282,FCS...	
192.168.13.16	Toronto	961	0000C9FF01E,000B00102ASE,000...	1140796D01410C970001C1E1000D4E187C...
192.168.1.15	SW-Calg	920	0000C9FF005,000B001038A8,000...	
192.168.13.10	DR-Swit	610	0022BES24031,FC5B398D5PCD,00...	1140796D600D85310001C001006D4E24...
192.168.13.17	Toronto	597	0000C9FF022,000B00101A86,000...	3000782D0143BC0103E143E100050000...
192.168.1.8	Floor1_Main	191	000000000100,000000000101,000...	



The top right corner provides a drop down which enables you to select how many rows are displayed in each page.



The bottom of this list indicates how many ports are covered by SepioPrime.

### Link Partner Column

Shows the MAC address of the port's link partner.

### Fingerprint Column

Shows the unique fingerprint generated by SepioPrime for this port.

### Port Status Column

Indicates whether the port is **Connected** or not (**Disconnected**) to another network.

### CDP Info

Shows Cisco Discovery Protocol (CDP) information.

## 4.6 Verifying SepioPrime Communication with the Switches

The following describes how to verify that SepioPrime is properly polling each of the switches.

- To verify communication with each of the switches –

## 4.7 Verifying Port License Coverage

the following describes how to verify that the license you purchased from Sepio is sufficient for the quantity of ports that you defined to be covered.

- To verify your port license coverage –

# 5

## Risk Insights

*This chapter describes the insights provided about the risk from malicious hardware in your organization.*

### 5.1 Overview

The Risk Insights page provides the following sections –

- Uncommon Peripherals, page x
- Vulnerable Peripherals, page x
- Switch Vulnerabilities, page x
- Network Ports, page x

The screenshot displays the SEPIO Systems Risk Insights dashboard. The left sidebar shows the navigation menu with 'Risk Insights' selected. The main content area is divided into three sections:

- Rogue Peripherals:** A table listing a 'HAK5 Rubber Ducky' with a risk of 'Keystroke injection', 'Malicious macro programming', and 'Remote shell invocation'. It is attached to 'LAPTOP-SUMQ2QFL' and there is 1 device.
- Vulnerable Peripherals:** A table listing a 'Logitech, Inc. Unifying Receiver' with a risk of 'Force pairing', 'Keystroke injection', 'Fake mouse', 'HID packet injection', 'Unencrypted keystroke injection', 'Unencrypted keystroke injection fix bypass', 'Encrypted keystroke injection', and 'Malicious macro programming'. It is attached to 'EUGENIA-W10', 'NAG-SBC-SAMPLE', and 'RONRW-W7' (more devices). There are 5 devices in total.
- Odd Compositions:** A table listing 'ATEN International Co., Ltd (0557), 2261' with a total quantity of 2 devices. It shows a 'Quantity: 2' of 'Attached to: WIN10 MAWLWARE'. The devices are listed as 'USB Input Device' with 'Class/Sub/Proto: 03/01/01' and 'Functionality: Keyboard'.





## 5.2 Uncommon Peripherals

The screenshot displays the SEPIO Vulnerable Peripherals interface. The main table lists detected devices with columns for Vendor, Product Info, Vulnerability, Risk, Quantity, and Attached to. The table shows four entries for Logitech, Logitech, Logitech, and Microsoft Corp. devices. A detailed view on the right shows the 'Odd Compositions' for a specific device, listing its attached components and their vulnerabilities.

Vendor	Product Info	Vulnerability	Risk	Quantity	Attached to
Logitech, Inc.	Unifying Receiver	Keyjack + Mousejack	Force parking Keylogger injection Fake mouse HID packet injection Unauthorized keylogger injection Unauthorized keylogger injection to system Encrypted keylogger injection Malicious macro programming	2 Devices	USB-HUB-010 HID-SEC-CAMPSH BONNIE-010 ...
Logitech, Inc.	Unifying Receiver	Keyjack + Mousejack	Force parking Keylogger injection Fake mouse HID packet injection Unauthorized keylogger injection Unauthorized keylogger injection to system Encrypted keylogger injection Malicious macro programming	5 Devices	AVD-010 DAVID-LAP COMING-010 ...
Logitech, Inc.	Unifying Receiver	Keyjack + Mousejack	Force parking Keylogger injection Fake mouse HID packet injection Unauthorized keylogger injection Unauthorized keylogger injection to system Encrypted keylogger injection Malicious macro programming	2 Devices	BONNIE-010 CAROLINE-010
Microsoft Corp.	Integrated Keyboard/Mouse	Keyjack + Mousejack	Force parking Keylogger injection Fake mouse HID packet injection Unauthorized keylogger injection Unauthorized keylogger injection to system Encrypted keylogger injection Malicious macro programming	2 Devices	VARO-010 GDS-010









- **Uncommon Peripherals** – Includes a table of rarely used devices that were detected. The following may be specified next to each device –
  - **One of** – Only a single device like this was detected in the entire the monitored IT infrastructure.
  - **Two of** – Only two devices like this were detected in the entire the monitored IT infrastructure.
  - **Few of** – Multiple devices (more than two) like this were detected in the entire the monitored IT infrastructure.

This display is particularly interesting because it shows uncommon devices. These devices are considered uncommon because enterprises typically purchase equipment in batches and therefore it is quite unusual to find singularities in an enterprise's infrastructure. In addition, a Rogue Device-based campaign typically starts by deploying only one or two devices.





- **Uncommon Composition** – Provides a highlighted view of specific device interface setups that are different from other identical devices found on the same infrastructure. For example, as shown below –

Uncommon Compositions			
Broadcom Corp. (0A5C) , BCM5880 Smartcard Reader (5832)			
VID: 0A5C	PID: 5832	Total Quantity:	194 Devices
<div>    </div>			
Quantity: 192		Attached to:	Dell ControlVault w/o Fi... SHARPCARD ...more
		Device:	Dell ControlVault w/o Fi...
		Class/Sub/Proto:	FE/00/00
		Functionality:	Unknown
		Device:	Microsoft Usbccid Smartc...
		Class/Sub/Proto:	0B/00/00
		Functionality:	Card Reader
<div>      </div>			
Quantity: 2		Attached to:	Dell ControlVault w/o Fi... Dell ControlVault w/o Fi...
		Device:	Dell ControlVault w/o Fi...
		Class/Sub/Proto:	FE/00/00
		Functionality:	Unknown
		Device:	Microsoft Usbccid Smartc...
		Class/Sub/Proto:	0B/00/00
		Functionality:	Card Reader
		Device:	Microsoft Usbccid Smartc...
		Class/Sub/Proto:	0B/00/00
		Functionality:	Card Reader
		Device:	NFC USB Bus Driver
		Class/Sub/Proto:	FF/00/00
		Functionality:	Wireless
+ Broadcom Corp. (0A5C) , BCM5880 Secure Applications Processor with fingerprint swipe sensor (5801)			
+ Samsung Electronics Co., Ltd (04E8) , Galaxy (MTP) (6860)			



## 5.3 Vulnerable Peripherals

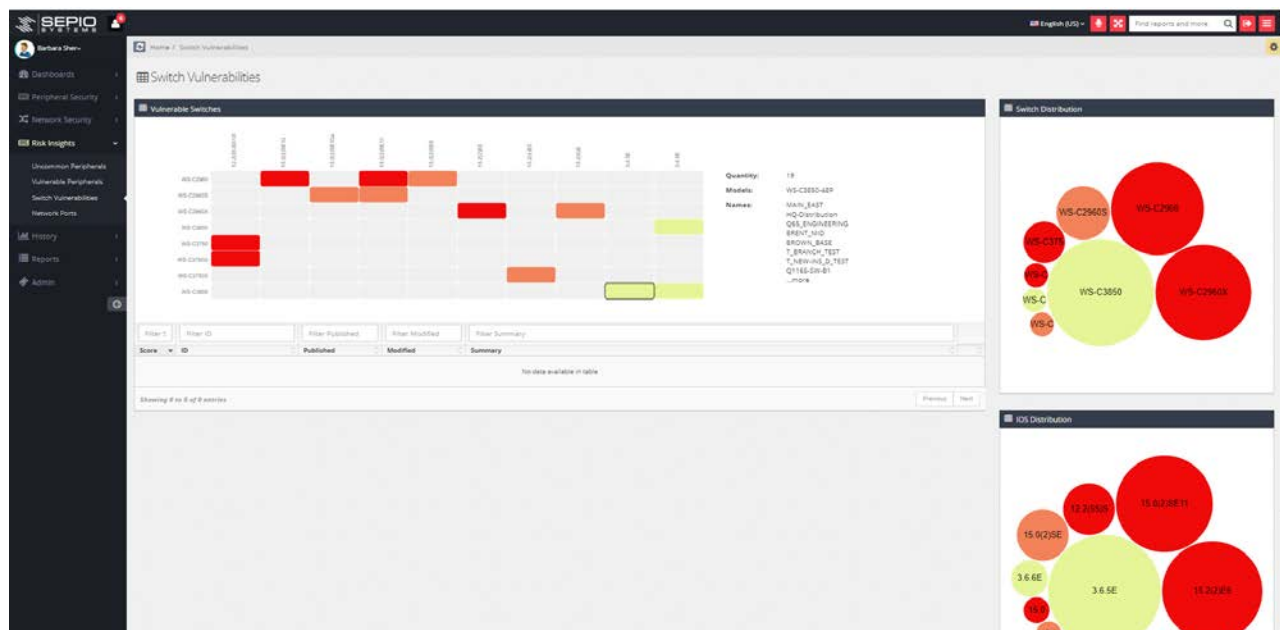
The screenshot displays the SEPIO Prime web interface. The left sidebar contains navigation links: Dashboard, Peripheral Security, Network Security, Risk Insights, Unknown Peripherals, Vulnerable Peripherals (selected), Switch Vulnerability, Network Run, History, Reports, and Admin. The main content area is titled 'Vulnerable Peripherals' and shows a table of detected devices. The table has columns for Vendor, Product Info, Vulnerability, Risk, Quantity, and Attached to. The data is organized into four rows, each representing a different vendor's products. To the right of the table is a panel titled 'Odd Compositions' which shows details for a specific device, including its VID, PID, Total Quantity, and a list of attached devices with their respective functionalities.

Vendor	Product Info	Vulnerability	Risk	Quantity	Attached to
Logitech Inc.	Unifying Receiver	Keyjack + Mousejack	Some pairing Keystroke injection Fake mouse HID packet injection Unencrypted keystroke injection Unencrypted keystroke injection fix bypass Emulated keystroke injection Malicious macro programming	3 Devices	8UGEN-W10 H4D-BE-CARDIO BD4RW-W10 ...more
Logitech Inc.	Unifying Receiver	Keyjack + Mousejack	Some pairing Keystroke injection Fake mouse HID packet injection Unencrypted keystroke injection Unencrypted keystroke injection fix bypass Emulated keystroke injection Malicious macro programming	3 Devices	8UGEN-W10 DAVED-LAP CONHD-W10 ...more
Logitech Inc.	Unifying Receiver	Keyjack + Mousejack	Some pairing Keystroke injection Fake mouse HID packet injection Unencrypted keystroke injection Unencrypted keystroke injection fix bypass Emulated keystroke injection Malicious macro programming	3 Devices	8UGEN-W10 DAVED-LAP CONHD-W10 ...more
Logitech Inc.	Unifying Receiver	Keyjack + Mousejack	Some pairing Keystroke injection Fake mouse HID packet injection Unencrypted keystroke injection Unencrypted keystroke injection fix bypass Emulated keystroke injection Malicious macro programming	3 Devices	8UGEN-W10 DAVED-LAP CONHD-W10 ...more

- **Rogue Peripherals** – Provides a list of detected USB rogue devices.
- **Vulnerable Peripherals** – Provides a list of devices that are known to be vulnerable. This device list was extracted according to SepioPrime's threat intelligence database. These devices are vulnerable by manufacturer design. These are considered to be *Supply Chain Vulnerabilities* because they originate from the vendor itself and leave the device open to attack by hackers who are aware of this vulnerability.
- **Odd Composition** – Provides a list of devices with an unusual composition setup, as defined by Sepio. For example, a mass storage device with an HID interface is unusual. The same applies for a device with two mice/keyboards in it (meaning on the same device, not as two separate keyboard connected to the host).



## 5.4 Switch Vulnerabilities



- **Switch Distribution** – Provides the distribution of switches in the enterprise's network infrastructure.
- **IOS Distribution** – Provides the distribution of the operating systems of the switches in the enterprise's network infrastructure.
- **Vulnerable Switches** – Provides a dynamically built heat map that includes a graphical representation of the vulnerabilities associated with the existing network infrastructure. A brick is colored red when the following conditions are all met –
  - High grade vulnerability.
  - The vulnerability is relevant to the specified switch's P/N and OS version.
  - The vulnerable functionality is actually enabled in that specific switch.

Upon clicking a brick, a detailed table of its CVE is displayed with direct links to it. A list of the switches shown in the heatmap appears on its right and specifies switch names and the total quantity of switches.





## 5.5 Network Ports

Attached To	Combination
102.10.10.10, 10.10.10.10	10.10.10.10, 10.10.10.10
102.10.10.10, 10.10.10.10	10.10.10.10, 10.10.10.10
102.10.10.10, 10.10.10.10	10.10.10.10, 10.10.10.10
102.10.10.10, 10.10.10.10	10.10.10.10, 10.10.10.10

Device Name	Port	MAC Address	Vendor
102.10.10.10, 10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10
102.10.10.10, 10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10
102.10.10.10, 10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10
102.10.10.10, 10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10
102.10.10.10, 10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10

- **Precarious Devices** – Provides a table listing all the network devices that have dual usage and are extremely popular within the hacking community. These devices are visible and show their authentic MAC.
- **Port Violations** – Provides a list of all ports in which a loop has been detected.
- **Uncommon Device** – Includes a table of rarely used network devices that were detected. The following may be specified next to each network device –
  - **One of** – Only a single device like this was detected in the entire monitored IT infrastructure.
  - **Two of** – Only two devices like this were detected in the entire the monitored IT infrastructure.
  - **Few of** – Multiple devices (more than two) like this were detected in the entire the monitored IT infrastructure.

This display is particularly interesting because it shows uncommon devices. They are considered uncommon because enterprises typically purchase equipment in batches and therefore it is quite unusual to find singularities in their infrastructure. In addition, it is typical for a Rogue Device-based campaign to start by deploying only one or two device.

## 5.6 Device Pairs

Provides a list of visible devices (meaning devices with visible MAC address) that are connected to the same physical port in the switch. This may result from an internal unmanaged switch up, an internal implant or from an optional daisy-chain network connection. These are categorized according to the pair's members (PC+PC/Camera+Communication and so on).



# 6

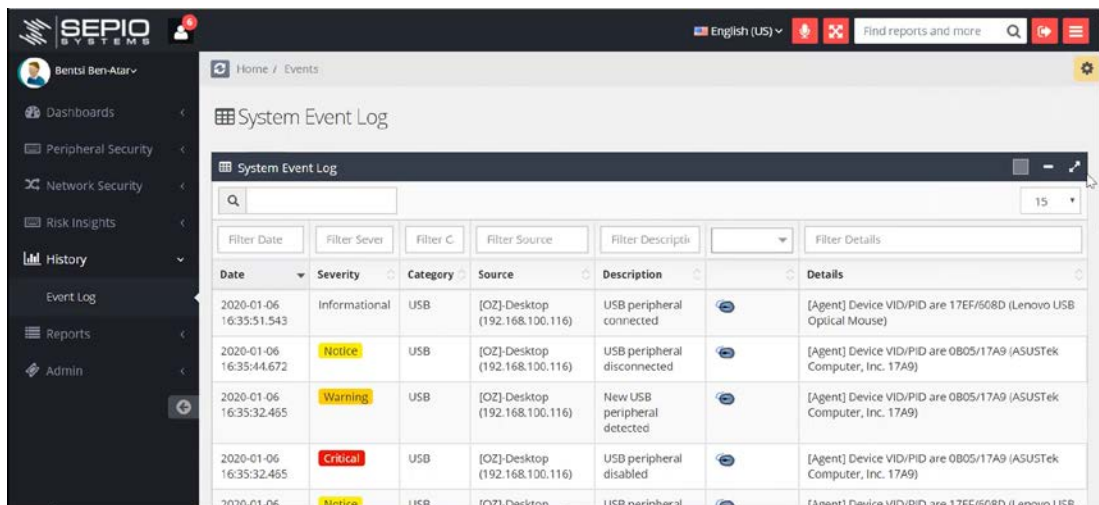
## Other SepioPrime Options

*This chapter shows other information and reporting options provided by SepioPrime.*

### 6.1 History → Event Log

► To display the SepioPrime event log –

1 Select **History** and then **Event Log** from the left pane.



Date	Severity	Category	Source	Description	Details
2020-01-06 16:35:51.543	Informational	USB	[OZ]-Desktop (192.168.100.116)	USB peripheral connected	[Agent] Device VID/PID are 17EF/508D (Lenovo USB Optical Mouse)
2020-01-06 16:35:44.672	Notice	USB	[OZ]-Desktop (192.168.100.116)	USB peripheral disconnected	[Agent] Device VID/PID are 0B05/17A9 (ASUSTek Computer, Inc. 17A9)
2020-01-06 16:35:32.455	Warning	USB	[OZ]-Desktop (192.168.100.116)	New USB peripheral detected	[Agent] Device VID/PID are 0B05/17A9 (ASUSTek Computer, Inc. 17A9)
2020-01-06 16:35:32.455	Critical	USB	[OZ]-Desktop (192.168.100.116)	USB peripheral disabled	[Agent] Device VID/PID are 0B05/17A9 (ASUSTek Computer, Inc. 17A9)
2020-01-06	Notice	USB	[OZ]-Desktop	USB peripheral	[Agent] Device VID/PID are 17EF/508D (Lenovo USB

## 6.2 Reports

The **Reports** option in the left pane provides a variety of precompiled reports showing the latest information.

The screenshot shows the SEPIO Systems web interface. The left sidebar contains a menu with options: Dashboards, Peripheral Security, Network Security, Risk Insights, History, Reports, Alarmed Ports, Zero MAC Ports, Port Administration, Self Generated Report, and Admin. The main content area is titled 'Zero MAC Ports' and displays a table of network data. The table has columns for IP Address, Name, Port ID, Name, and Alarmed. The data is filtered by IP Address and Name.

IP Address	Name	Port ID	Name	Alarmed
10.104.17.2	HQ_DR3FL	Gi1/1/1	T1-WHITE	
10.104.17.2	HQ_DR3FL	Gi1/1/2	T1-WHITE	
10.20.86.5	SW65-SOUTH-END	Gi0/2	T1-AS21	
10.20.88.4	ACCNT-C296	Fa0/20	Lobby Signage	True
10.20.88.4	ACCNT-C296	Fa0/6		
10.22.31.5	JEFF-TEST-SW	Te1/0/1	T1-CS1_108YORK_1FL	
10.22.31.5	JEFF-TEST-SW	Te1/0/2	T1-CS1_108YORK_1FL	

### 6.2.1 Self Generated Reports

This option enables you to configure the report that you would like to generate and to have it automatically sent to the recipients of your choice through the SMTP email server that is configured in SepioPrime.

#### ► To define a new report –

- 1 Select **Reports** and then the **Self-Generated Report** option. The following displays –

The screenshot shows the SEPIO Systems web interface for the 'Self Generated Report' section. The left sidebar contains a menu with options: Dashboards, Peripheral Security, Network Security, Risk Insights, History, Reports, Alarmed Ports, Zero MAC Ports, Port Administration, Self Generated Report, and Admin. The main content area is titled 'Self Generated Report' and displays a table of report configurations. The table has columns for Report Name, Active, Days, Time, Report Type, and Recipients. The data is filtered by Report Name and Active. An 'Action' dropdown menu is visible, showing options: Add Report, Edit Report, Delete Report, Activate Report, Deactivate Report, and Send Report Now. Below the table, there is a section for 'SMTP Configuration' with fields for SMTP Server, Port, Use SSL, and Mail User.

Report Name	Active	Days	Time	Report Type	Recipients
No data available in table					

Showing 0 to 0 of 0 entries

**SMTP Configuration**

SMTP Server: \_\_\_\_\_  
Port: \_\_\_\_\_  
Use SSL: \_\_\_\_\_  
Mail User: \_\_\_\_\_



- 2 Click the **Action** button to display a dropdown menu and select the **Add Report** option.

## 6.3 Audit Trail

SepioPrime provides a detailed audit trail of all user actions, as shown below –

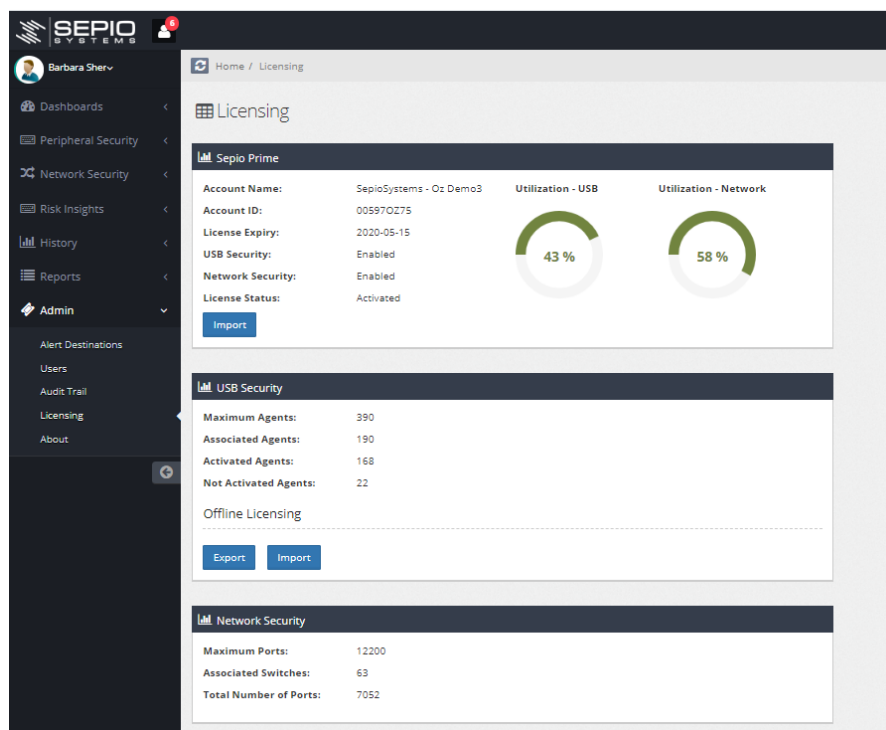
SEPIO SYSTEMS					
Home / Audit Trail					
System Audit Trail					
Date	Severity	User	Description	Details	
2020-01-09 16:10:42.216	Error	benb (Bentsi Ben-Atar)	Port Audit Proof	Switch is TOPFLOOR_C_UG (10.51.2.17), Port is Gi1/0/20	
2020-01-09 16:08:37.843	Error	benb (Bentsi Ben-Atar)	Port Zeroized	Switch is TOPFLOOR_C_UG (10.51.2.17), Port is Gi1/0/20	
2020-01-09 16:08:25.796	Error	benb (Bentsi Ben-Atar)	Port Zeroized	Switch is TOPFLOOR_C_UG (10.51.2.17), Port is Gi3/0/3	
2020-01-09 16:08:19.729	Error	benb (Bentsi Ben-Atar)	Port Zeroized	Switch is TOPFLOOR_C_UG (10.51.2.17), Port is Gi3/0/25	
2020-01-09 16:08:12.660	Error	benb (Bentsi Ben-Atar)	Port Zeroized	Switch is TOPFLOOR_C_UG (10.51.2.17), Port is Gi3/0/12	
2020-01-09	Error	benb (Bentsi Ben-Atar)	Port Zeroized	Switch is TOPFLOOR_C_UG (10.51.2.17), Port is Gi2/0/21	

## 6.4 Users

The **Administrator** ➔ **Users** option enables you to define/add SepioPrime users as needed.

## 6.5 Licensing

The **Administrator** ➔ **Licensing** option enables you to handle various aspects of SepioPrime Licensing, as follows –



- **SepioPrime Section** – Licensing of the SepioPrime server is handled during installation. The **USB Security** option should be enabled if you purchased device visibility and the **Network Security** option should be enabled if you purchased network visibility. You may refer the *SepioPrime Installation Manual* for more information.
- **USB Security Section** – This section enables you to verify the SepioPrime licenses deployed on the hosts of enterprise's network. It enables you to export a list of the SepioPrime Agents and to send it to Sepio in order to receive and upload licenses to each Agent, as described on page X.





# 7

## Integrating with SepioPrime

*This chapter describes how to integrate SepioPrime alerts and events with other third-party products.*





## About SEPIO SYSTEMS

The Latin word "Sepio" means "defend" and "guard."

Bad actors are gaining access by implanting rogue hardware –  
Sepio's Rogue Device Mitigation (RDM) stops them.

Sepio is disrupting the cyber-security industry by uncovering hidden hardware attacks. Sepio Prime provides security teams with full visibility into their hardware assets and their behavior in real time. A comprehensive policy enforcement module allows administrators to easily define granular device usage rules and continuously monitor and protect their infrastructure. Leveraging a combination of physical fingerprinting technology together with device behavior analytics, Sepio's software-only solution offers instant detection and response to any threat or breach attempt coming from a manipulated or infected element.

Sepio Systems was founded by cyber security experts from private industry and government agencies. Our team has earned global recognition and decoration in fighting attacks through malicious hardware devices.

[www.sepio.systems](http://www.sepio.systems)

[support@sepio.systems](mailto:support@sepio.systems)





access denied



**SEPIO**  
SYSTEMS