# Sepio Technical Documentation

## Welcome to the Sepio Technical Documentation

## Quick Start Guide

### Agent Release Notes

Review the latest Agent updates, including new features, changes, and bug fixes for improved threat mitigation.

### Platform Release Notes

Explore new features, enhancements, and resolved issues introduced in each Sepio Platform version.

### Platform Architecture

Understand the core components of Sepio's architecture that deliver full asset visibility and control.

### Sepio Cloud

Learn how Sepio Cloud leverages the Asset DNA repository to enhance visibility and threat intelligence.

## Sepio Agent, Platform & Knowledge Base – Recent Release Notes

- Sepio Platform v60 (build 17.2604.632) – Release Notes
- Sepio Agent 17.2602.229 Release Notes
- Sepio macOS Agent 17.2604.118 Release Notes
- Sepio Knowledge Base KB 20260506 Release Notes

## Other Recent Updates

- Different Switch Types and the Sepio Platform
- Ensuring Visibility and Compliance for Enforced Authentication (802.1X/MAB)
- Artifact Signature Verification
- Discovery, Classification, and Identification

- Advanced Agent Security Model: Enhanced Host Agent Security
- Deep Dive into Campus and Data Center Switching Architecture
- Auto-Tagging and Tags
- USB Billboard Device
- API Key Management
- Peripheral Policy Introduction
- Sepio and Cisco Identity Services Engine (ISE) NAC Integration
- Enhanced Event and Logging System
- Backup, Redundancy, and High Availability
- Anatomy of a “Duplicated MAC Address” Alert in High-Availability Networks
- Data Extractions
- Licensing
- Platform Monitoring
- Trafficless Network Asset Discovery
- Deep Dive on 802.1X and Some of Its Limitations
- Identity Related Issues
- Improving Network Security with Sepio’s Asset Identity Feature
- Host-only Deployment
- Network-only Deployments
- Asset Identity
- Application Visibility
- About Assets
- Raspberry Pi Deep Dive
- Scopes and Agent Mode in Sepio Platform
- Event Based Scan Engine
- Configuring Aruba Devices Through Aruba Central
- Agent CEF Operations
- Deep Dive on First Hop Redundancy Protocols
- Post Installation and Update Checklist
- Knowledge Base Deep Dive
- Risk Indicator Groups
- Queries and Reports
- Huawei Switches
- CrowdStrike Falcon Integration
- Scan Engine
- Host Agent Best Practices
- Sepio Connector App Configuration
- Switch Scanning Status Explanations
- Deep Dive on Mouse Jigglers
- Supported Operating Systems for Sepio Host Agent
- Deployment of Allowed Peripherals at Scale

- Adding and Deleting User-Defined Attributes
- Blocking Peripherals
- Network HTTP Proxy
- Updating the Knowledge Base
- Known Limitations

# About Sepio

## Hardware Access Control and Asset Risk Management

Sepio is a cybersecurity company that provides solutions for **Hardware Access Control** (HAC) and **Asset Risk Management** (ARM). Its core function is to deliver complete visibility and control over all hardware assets within an organization, addressing the significant security blind spot created by unmanaged and rogue devices.

Sepio's platform operates at the physical layer, using a unique "**Asset DNA**" technology. This allows it to discover and identify *every* device connected to the network, including peripherals (such as USBs, keyboards and mice), OT and IoT devices, and network equipment, without relying on network traffic or network scanning.

By providing this granular visibility, Sepio enables organizations to:

1. **Discover** all known and unknown hardware assets.
2. **Assess** their risk level based on their true identity.
3. **Enforce** granular access control policies, automatically blocking any unauthorized or malicious hardware that violates policy.

This prevents attacks that use hardware-based vectors, such as rogue devices or USB-based malware, ensuring that only trusted and approved assets can operate within the environment.

## Related Topics

- What is Sepio?
- Sepio Cloud
  - Sepio Cloud Structure
  - Sepio Modules
- Sepio Architecture
  - Scan Engine
- Connectivity Diagram
- Redundancy and High Availability

# What is Sepio?

## Asset Risk Management (ARM) at the Physical Layer

Sepio enables you to view all connected Assets on your network, assess your hardware-based risk, and provides risk management for all your hardware Assets. Sepio is a unique software solution for detecting and mitigating the risk of malicious Assets in enterprise environments and infrastructure. Whether by USB and/or network interfaces, Sepio provides total visibility and blocking options.

Using easily configured policies, or choosing our defaults, you can block each USB port, which disables any risky Asset in real-time as soon as it is connected.

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

## Sepio Uses

- Viewing, detecting, and mitigating the risk of malicious Assets in a rapidly expanding, uncontrolled network.
- Generating a detailed risk factor profile for every Asset, at its physical layer source, based on contextual business, location and rules.
- Blocking threats to your organization from connected Assets via USB and/or network interfaces
- Disabling a risky, threatening, or malicious Asset in real-time, as soon as it is connected, according to default and easily configured policies.
- Understanding instantly which Assets need your attention in detail, and improve your overall security posture based on Sepio's Asset risk factor.

## Main Features

### Trafficless Asset Discovery

Sepio is identifying and securing hardware assets without relying on traditional traffic inspection techniques. There is no need to span or collect traffic. There is no need for active probing of assets in order to discover. As the name suggests: there is no need to look inside network packet streams.

### Automatic Asset Profile Generation

Sepio uses its unique technology to automatically discover and show you the inventory of visible and invisible Assets connected to your networks and endpoints (Assets).

### Automatically Takes Action According to Your Policy

Sepio analyzes hardware Assets' behavior, implements their assigned policy, and automatically blocks attacks and allows permitted exception at the device level (for connected USB devices) and at the network level (on network switches).

### Real-time Cloud-based Intelligence

Sepio is augmented by near real-time cloud-based intelligence that provides users with early warning of the latest malicious hardware and threat patterns to keep your Asset Risk Factor constantly updated.

### Hybrid Deployment Model

Sepio's security platform can be deployed as a service from Sepio's cloud (SaaS), and on any physical or virtual environment in any combination of on-premises, private and public cloud infrastructures.

# Different Switch Types and the Sepio Platform

## Overview

Visibility is the foundation of hardware security. In the Sepio ecosystem, we categorize switches based on their management capabilities and how they interact with our Physical Layer visibility tools. Understanding these differences is critical for eliminating “Shadow IT“, enhancing network security, improving asset discovery, and ensuring effective policy enforcement.

## Unmanaged Switches

### The “Blind Spot”

Unmanaged switches are simple “plug-and-play” devices. They do not have an IP address, a management console, or any configurable features.

- **Security Impact:** Because they are invisible to traditional Network Management Systems (NMS) and MAC-based security, they are often used to bypass security controls.
- **Sepio Discovery:** Sepio identifies these devices at the Physical Layer by analyzing the unique electrical “fingerprint” (**AssetDNA™**) of the connection, revealing hidden infrastructure that other tools miss.

## Managed Switches

### The “Configurable Core”

Managed switches are intelligent devices that allow network administrators to control traffic, configure VLANs, and monitor performance. They have their own IP addresses and support protocols like SNMP and SSH.

- **Security Impact:** While they offer features like 802.1X, they can still be bypassed by sophisticated Layer 1 attacks or hardware spoofing.
- **Sepio Discovery:** Sepio monitors managed switches to ensure their configuration remains secure and to verify that the hardware itself has not been tampered with.

## Supervised Switches

### The “Enforcement Point”

A **“Supervised Switch”** is a status within the Sepio platform. It refers to a managed switch that Sepio is actively communicating with to provide real-time security enforcement.

- **Security Impact:** When a switch is supervised, Sepio can automatically mitigate threats. If a rogue device is detected, Sepio can instruct the switch to administratively shut down the specific port or reassign it to a “quarantine” VLAN.
- **Sepio Role:** It transforms a standard piece of networking hardware into an active participant in your hardware security posture.

**Quick Comparison Table**

| Feature | Unmanaged Switch | Managed Switch | Supervised Switch (Sepio) |
|---|---|---|---|
| **Management IP** | No | Yes | Yes |
| **User Configuration** | None | High | High + Sepio Automated Rules |
| **Visibility** | Invisible to NMS | Visible | Visible and Fully Audited |
| **Sepio Interaction** | Detected via AssetDNA™ | Monitored | Used for Port Enforcement |
| **Risk Level** | High (Shadow IT) | Medium | Low (Active Mitigation) |

# Discovery, Classification, and Identification

## Overview

Sepio Discovery, Classification, and Identification of assets is an fully passive, software-only process, part of its solution that utilizes hardware fingerprinting, known as **AssetDNA™**, to manage risk for network and peripheral assets.

For assets that are connected to the network, Sepio uses Trafficless Network Asset Discovery, a method of identifying and securing hardware assets without relying on traditional traffic inspection techniques. Unlike legacy solutions that require intrusive methods such as passive monitoring (using TAPs, SPAN ports, or Network Packet Brokers) or active monitoring (using proxies, traffic steering, or active probing), Sepio's approach decouples asset discovery from data traffic. This method avoids the need to inspect encrypted payloads or install dedicated hardware sensors, offering a streamlined alternative that respects network resilience and privacy.

## How Trafficless Network Asset Discovery Works

The Trafficless asset discovery process operates by leveraging the existing managed network infrastructure rather than analyzing the traffic flowing through it. The mechanism follows a three-step operational flow:

- **Continuous Connection:** As the network operates normally, assets continuously connect and disconnect.
- **Infrastructure Querying:** Sepio's Scan Engine connects directly to the network infrastructure (switches, routers, and Wi-Fi controllers) using standard management interfaces over Out-of-Band (OOB) or Lights Out Management (LOM) channels via SSH or SNMP, using the same methods and commands that network administrators use to validate device operations.
- **Data Extraction & Analysis:** Sepio's Scan Engine uses CLI commands and pulls purely physical and logical metadata, including configuration settings, switching tables, and low-level interface information. Sepio then analyzes this data to generate a unique AssetDNA for every device, which is then used to classify the asset, determine its state, and assess its risk level.

The following sections explain the various solution components in more detail. Differences exist in how the solution operates for wired Ethernet versus wireless Wi-Fi assets.

## 1. Asset Discovery Flow

The discovery process begins the moment a device is physically connected to a switch port.

- **Link Establishment:** When a physical link is established, Sepio immediately determines a **Port Fingerprint.**
- **Dormant Device Creation:** If a link is detected but no MAC address has been learned yet, Sepio creates a placeholder known as a **Dormant Device.**
- **MAC Address Learning:** Once the system learns the MAC address from the port, the Dormant Device is replaced by an identified asset.
- **AssetDNA Generation:** Sepio creates an AssetDNA for the device, which represents the **"first" device physically connected** to the port, even in cascaded scenarios where multiple devices may be seen behind it.

At this stage, Sepio knows that an asset is connected to the network, its exact physical location, its networking behavior and the attributes that internal switch components report.

## 2. Asset Classification

Sepio classifies assets by clustering them based on multiple indicators beyond just the MAC address. These indicators include:

- **Vendor and Product/Model:** Information from the Sepio Knowledge Base (KB) and protocols like CDP/LLDP.
- **Physical Layer Data:** Switch port type (e.g., Fast Ethernet vs. Gigabit), device autonegotiations, and PoE negotiation/consumption.
- **Traffic Behavior:** Distribution and behavior of counters.

This multi-dimensional approach allows Sepio to cluster devices into groups (e.g., "Printers," "IP Phones," "Laptops") based on their shared characteristics.

## 3. Asset Identification

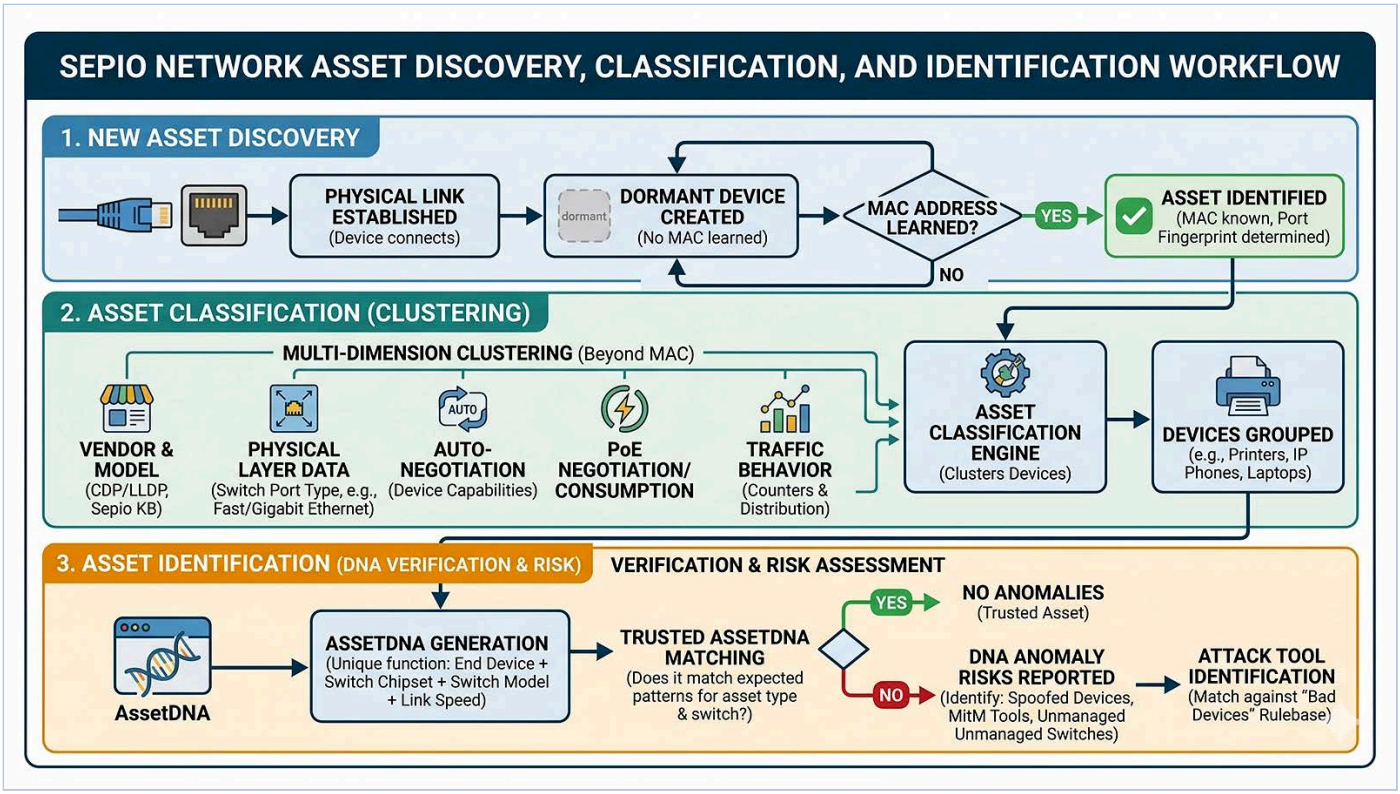
Identification involves matching the discovered AssetDNA against trusted patterns to ensure the device is exactly what it claims to be.

- **Fingerprint Function:** An AssetDNA is a function of the end device, the switch chipset, the switch model, and the negotiated link speed.
- **Trusted DNA Matching:** Sepio maintains a database of **Trusted AssetDNA patterns.** It checks if the observed DNA matches an expected (trusted) pattern for that specific asset type on that specific switch.
- **Anomaly Detection (Spoofing & MitM):**
- If a device (e.g., a laptop) "claims" to be a different device (e.g., an HP printer) via MAC spoofing, its AssetDNA will fall **outside the expected cluster area** for an HP printer.
- Sepio then reports a **DNA Anomaly Risk**, allowing it to identify spoofed devices, Man-in-the-Middle (MitM) tools (like a Raspberry Pi or active tap), and unmanaged "partisan" switches.

- **Attack Tool Identification:** If an anomaly is detected, Sepio can match the observed DNA against a rule base of **“Bad Devices”** to identify the probable attack tool being used.

This process constantly continues using Sepio’s Scan Engine, which collects the relevant information from the network infrastructure elements.

**The diagram below illustrates the process for wired connections:**




Sepio network asset discovery, classification, and identification workflow

# Trafficless Network Asset Discovery

## What is Trafficless Monitoring?

Trafficless Network Asset Discovery is a method of identifying and securing hardware assets without relying on traditional traffic inspection techniques. Unlike legacy solutions that require intrusive methods such as passive monitoring (using TAPs, SPAN ports, or Network Packet Brokers) or active monitoring (using proxies, traffic steering, or active probing), Sepio's approach decouples asset discovery from data traffic. This method avoids the need to inspect encrypted payloads or install dedicated hardware sensors, offering a streamlined alternative that respects network resilience and privacy.

## How It Works

The Trafficless Asset Discovery process operates by leveraging the existing managed network infrastructure rather than analyzing the traffic flowing through it. The mechanism follows a three-step operational flow:

- **Continuous Connection:** As the network operates normally, assets continuously connect and disconnect.
- **Infrastructure Querying:** Sepio's Scan Engine connects directly to the network infrastructure (switches, routers, and controllers) using standard management interfaces over Out-of-Band (OOB) or Lights Out Management (LOM) channels via SSH or SNMP, using the same methods and commands that network administrators use to validate device operations.
- **Data Extraction & Analysis:** The Scan Engine uses CLI commands and pulls purely physical and logical metadata, including configuration settings, switching tables, and low-level interface information. Sepio then analyzes this data to generate a unique "AssetDNA" for every device, which is then used to classify the asset, determine its state, and assess its risk level.

## Key Benefits

Adopting a Trafficless approach offers significant operational and security advantages over traditional methods:

- **Rapid Deployment:** Because it utilizes the customer's existing network infrastructure, the solution can be deployed very quickly without the complex setup associated with hardware installation.
- **Zero Infrastructure Overhead:** There is no need for additional hardware like TAPs or SPAN ports, nor is there a requirement for network changes to support traffic mirroring.
- **Protocol Independence:** The solution is effective regardless of the communication protocols used and does not need to decrypt traffic (SSL/TLS) to identify devices, eliminating privacy concerns and visibility "blind spots" caused by encryption.

- **Non-Intrusive Operation:** By avoiding active probing, the system ensures that sensitive legacy devices or IT/OT equipment are not disrupted or harmed, maintaining full network performance and resilience.

# Sepio Cloud

## Related Topics

- Sepio Cloud
  - Sepio Cloud Structure
  - Sepio Modules

# Sepio Cloud Structure

## Sepio Cloud Component

- **Sepio SaaS Platform** – Enables customers to manage their Sepio deployments from the cloud.
- **Sepio Data Lake** – Sepio's repository of AssetDNA. This repository provides customers with updates based on a collection of anonymized public information gathered from Sepio deployments and the Sepio research team.

## Related Topics

- Sepio Architecture
    - Scan Engine

# Sepio Modules

Sepio is modular and includes the following threat-oriented modules: **USB Device Security** and **Network Device Detection**. You can choose to deploy either module individually or both together.

## USB Device Security Module

The USB Device Security module detects and monitors all USB assets within the organization. It provides full visibility into all connected devices, analyzing their capabilities and behavior in real time to assess risk. This module also supports the enforcement of policies for allowing or blocking specific assets and interfaces based on your requirements.

The USB Device Security module is based on the Sepio agent, which runs as a Windows service on Windows and Linux computers which are referred to as Hosts.

## Network Device Detection Module

The Network Device Detection module continuously monitors the network for rogue LAN assets that are transparent to existing security tools.

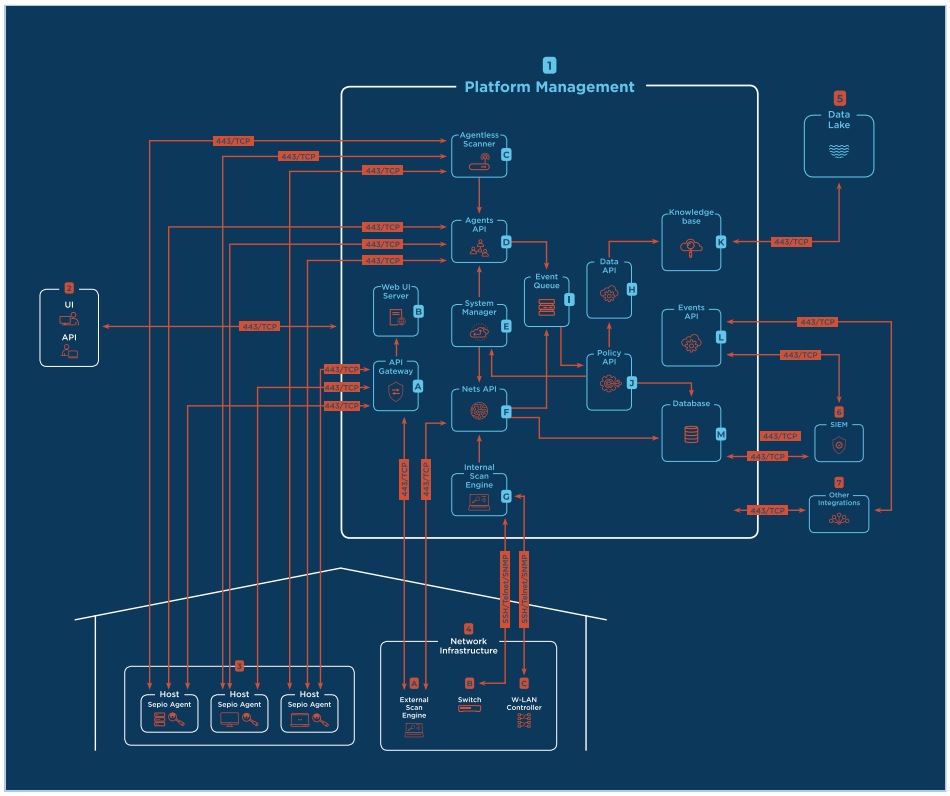
These transparent assets do not possess their own network identity (e.g., no IP or MAC address). Once deployed, they gain an undetectable foothold in the network and facilitate the leaking of sensitive information in an out-of-band manner, all without alarming existing tools.

# Sepio Architecture

## Overview

The detailed platform diagram illustrates the different components of the Sepio Platform, the customer environment, and its ecosystem. Some components are relevant only for specific deployment options. The Sepio Platform is designed to operate from the cloud, on customer premises, or in air-gapped environments.

> **Note:** The arrows in the diagram do not represent connectivity initiation. Please refer to the table below for descriptions of the different elements.




Sepio Platform Architecture: Components of Sepio's Platform

## Components of the Sepio's Platform

The Sepio Management Platform uses a microservices architecture built on a foundation of containers. The components shown in the diagram and listed in the table represent the core internal functions. Each of these components may be implemented using multiple microservices, which are typically transparent to most Sepio administrators.

This architecture provides several key benefits:

- **Independent Scaling:** Each microservice can be scaled independently based on demand, allowing Sepio to efficiently allocate resources and ensure optimal performance.
- **Fault Isolation:** If one microservice fails, it has minimal impact on others. This enhances system stability and reduces the risk of cascading failures that can affect monolithic applications.
- **Resource Optimization:** Containers are lightweight and efficiently utilize resources, reducing overhead while maintaining high performance.

## Description of the Different Elements

| | Component | Sub-component | Description |
|---|---|---|---|
| **1** | Platform Management | – | Manages the Sepio platform. Sepio can be installed on premises, from the cloud (as a service) or air-gapped with no connectivity to the internet at all. |
| **A** | – | API Gateway | Forwards a Host's, or an external network scanner request to the Web UI Server. A Reverse Proxy increases security, performance, and reliability. The Web UI Server is based on NGINX.<br>A Host is any computer running on Windows or Linux, that communicates with the Sepio system. You connect/disconnect Assets, such as USB sticks, mouses, and others to/from a Host with a USB connection. You connect/disconnect assets such as servers, computers (which are also Hosts), switches, IoT Assets and others, to/from your organization network infrastructure with an Ethernet connection. |
| **B** | – | Web UI server | Provides web UI for end users over HTTPs.Receives invocations from the users.Can interface with external/third-party systems using APIs instead of the UI. |
| **C** | – | Agentless Scanner | Optional component (external or internal, depending on deployment mode and routing) that manages the HOST Agentless functionalities, including scanning Agentless targets (Any Host that Sepio can run agentless on) and communicating with them.<br>There are two types of Agentless Hosts:<br>• **Agentless** – Is a Server Manager operation that installs agent code on a Host, not as a service but as a Windows |

| | Component | Sub-component | Description |
|---|---|---|---|
| | | | process. For this Agentless type, Sepio requires the Host's access credentials to authenticate it.<br>• **Session** – A customer installed script that runs the agent code on a Host without taking up CPU. |
| **D** | – | Agents API | Handles Hosts with installed Sepio Agents, including: A Host is any computer running on Windows or Linux, that communicates with the Sepio. You connect/disconnect Assets, such as USB sticks, mouses, and others to/from a Host with a USB connection. You connect/disconnect assets such as servers, computers (which are also Hosts), switches, IoT Assets and others, to/from your organization network infrastructure with an Ethernet connection.<br>• Communication with the agents<br>• periodic updates of Asset statuses<br>• Implements policies and control on Hosts and their associated peripheral Assets (any connected Assets). |
| **E** | – | System Manager | Handles System settings configuration data visualization events and audit log creation report generation monitors system health and other systemic functions. |
| **F** | – | Nets API | Performs the following with managed and unmanaged Network Infrastructure Assets including:<br>Communication to/from the network infrastructure Assetsperiodic updates of connected Asset status implements policy and control on the connected Assets manages the Network Scanner schedule. |
| **G** | – | Internal Scan Engine | Optional component, depending on deployment mode and routing. It handles communication inside a customer's network with Network Elements (Assets) on your network infrastructure. "internal" means that it is installed as part of the management platform itself. |
| **H** | – | Data API | • Handles ML-based analysis of all incoming data streams from NetsAPI and AgentsAPIs.<br>• Detects multiple types of anomalous Assets on your network, based on the system data analytics. |

| | Component | Sub-component | Description |
|---|---|---|---|
| | | | • Analyzes Assets low level data (such as type, location and more) and asses' risks. |
| **I** | – | Event Queue | Repository that holds the Sepio application events prior to being processed by the PolicyAPI. |
| **J** | – | Policy API | • Identifies, characterizes and locates Assets.<br>• Defines Assets Risk Score and Risk Indicators.<br>• Checks assigned rule sets after matching Asset data with rule sets parameters.<br>• Stores and executes defined rules and policies – Sends data for display to the UI.<br>• Builds and maintains Sepio Assets list of all types.<br>• Queues actions per target (Host, email reports and notifications).<br>• Queues new Risk Indicators. |
| **K** | – | Knowledge Base | Sepio's repository of Assets data such as, vulnerabilities. It also includes data used by the Data Analysis API and the Sepio Agent. Sepio's KB is a dynamic integrated data source for the platform that contains information to identify known attack tools and vulnerabilities, maintains device whitelists and blacklists, and provides specific data necessary for Sepio's machine-learning algorithms to provide improved, up-to-date capabilities always. |
| **L** | – | Events API | • Writes system events and audit logs to the database.<br>• Dispatches events to Syslog and other SIEM systems.<br>• Aggregates and dispatches events to:<br>  ◦ the events feed in the UI.<br>  ◦ as email notifications and SMSes. |
| **M** | – | Database | Repository for all system data on events and Assets. Contains the tablets for all system data displayed in the UI. |
| **2** | UI | – | User interface |
| **3** | Host Sepio Agent | – | • The Sepio Agent communicates between a Host and the Management server. |

| | Component | Sub-component | Description |
|---|---|---|---|
| | | | • As soon as the Management server detects that a new Host is connected to the organization network, it installs a Sepio Agent on it, establishes communication and checks its internal components for suspected malicious devices such as adapters, processors and more.<br>• The Sepio Agent automatically runs on the Host when the Sepio Management server starts up, to detect and analyze newly added USB Assets.<br>• The Sepio Agent has three deployment modes:<br>  ◦ **Windows service** – The Sepio Agent runs as a Windows service on the Host.<br>  ◦ **Agentless** – Is a Manager Server operation that installs agent code on a Host, not as a service but as a Windows process. For this agentless type, Sepio requires the Host's access credentials to authenticate it.<br>  ◦ **Session** – A customer installed script that runs the agent code on a Host without taking up CPU. The Sepio Agent will initiate communication with the API gateway. |
| **4** | Network Infrastructure | – | Your (the customer's organization) defined network infrastructure components that Sepio scans. |
| **A** | – | Sepio (external) Engine | Optional component, depending on deployment mode and routing, similar to the internal Scan engine. The Scan Engine comprises two agents that communicate with the networking infrastructure using their supported managed protocols (It can communicate using either SSH, Telnet or SNMP, based on your preferences. The external Scan Engine agent collects low level data from Assets connected to the Switch mangers and W-Lan controllers. "External" means that it is installed outside the Sepio Platform. It is installed on the customer premises. |
| **B** | – | Switch | A network switch connects multiple Assets together in a single or multiple wired LAN networks (Ethernet). Sepio network scanners will connect to the switch using the defined |

| | Component | Sub-component | Description |
|---|---|---|---|
| | | | transport management protocol (SSH, telnet or SNMP) to collect the configuration. |
| **C** | – | W-LAN Controller | On a wireless network, the WLC (Wireless-LAN Controller) makes all frame forwarding decisions in the network, for security reasons. A controlled AP does not allow direct communication between two devices, even if they both are connected with it. The frame forwarding decision is done by the WLC. |
| **5** | Data Lake | – | The Data Lake aggregates authorized, specific exported data upon which technical system health monitoring and other analytics are performed. The Data Lake is compliant with relevant standards for security (data-at-rest and data-in-motion) and privacy standards. |
| **6** | SIEM (Security Information Management and Security Event Management) | – | Exports data (via Syslog or other product specific protocols) to customer's SIEM tools. |
| **7** | Other Integrations | – | Other security solutions that can be integrated directly with the Sepio Platform. For example:<br>• Akamai Guardicore Microsegmentation<br>• Forescout<br>• Cisco ISE<br>• Palo Alto Networks (Demisto) plugin<br>• Splunk plugin<br>• ServiceNow CMDB |

## Communication Direction

| Source | Destination | Initial communication request | Established communication |
|---|---|---|---|
| HOST | Sepio Management, | From HOST to Sepio | The HOST controls communication. It will collect messages and instructions |

| Source | Destination | Initial communication request | Established communication |
|---|---|---|---|
| | using HTTPS://FQDN | | waiting for it on the management and act accordingly. There is no traffic initiation from Sepio Management towards the HOST. |
| External Network Scanner | Sepio Management, using HTTPS://FQDN | From External Network Scanner to Sepio | The scanner controls the communication. It will collect messages and instructions waiting for it on the management and act accordingly. There is no traffic initiation from Sepio Management towards this component. |
| Internal or external Scanners | Network Infrastructure | Scan Engine | The Scan Engine will connect to the network infrastructure over the defined transport protocol via the management IP to collect configuration or perform port actions. |
| Management | SIEM | The management initiates the communication with SIEM | API dependent |
| 3rd party integration | Sepio Management, using HTTPS://FQDN | Typically, the 3rd party integration would initiate the integration request | API dependent |

## Scan Engine

The Sepio Scan Engine, also known as a network Poller, is a key component of the Sepio platform. Designed to discover and identify network infrastructure and connected devices, it gathers data by interacting with the network infrastructure equipment. This distributed component operates independently of the main management system but regularly transmits collected data back to it.  As a distributed component, it can be installed as part of the management Platform and/or any number of separate systems. The Scan Engine that is installed with the management server is known as “Internal” while other Scan Engines are known as “External.”  Using both internal and external Scan Engines allows customers to support complex, distributed, and advanced global networking architectures.

Deployable on Windows or Linux systems, the Scan Engine utilizes SSH and other management protocols to connect to network devices. It executes a series of command-line interface (CLI) commands on these devices, collecting data essential for:

- Asset Discovery: Identifying and locating all network assets.
- AssetDNA Collection: Gathering unique identifiers and characteristics of each asset.
- Classification: Categorizing assets based on their role, type, and criticality.
- Asset Information: Collecting additional information about assets that can be available through the network infrastructure.

> **Note:** See the Scan Engine deployment and configuration information here.

The accuracy and timeliness of asset detection and risk alerts heavily rely on the Scan Engine’s data collection frequency. Regular and consistent scans are crucial for maintaining an up-to-date and accurate inventory of network devices and identifying potential security vulnerabilities.

Each scan requires an established connection to the network equipment, which may lead to challenges depending on how the networking device handles Sepio’s Scan Engine connections.

To address these challenges, network switch vendors implement strategies to minimize the impact of operational tasks (management path) on packet switching performance (data path). These strategies ensure a clear separation between the data and management paths, enabling operational tasks to run without significantly affecting packet switching performance. This approach maintains high network availability and responsiveness.

## Common Switch Performance Issues

Several issues can lead to slow network infrastructure response and performance degradation on network switches:

**Authentication, Authorization, and Accounting (AAA) Server Issues**

- **Unreachable or Slow AAA Servers:** If a network switch relies on external servers (such as TACACS+, RADIUS, or other AAA servers) for authentication, authorization, or accounting but cannot reach these servers or experiences slow responses from them, it can cause significant delays:
  - Network connectivity problems between the switch and the AAA server.
  - Server outages or overloads.
  - Slow responses due to network congestion or poor server performance.
- **Incorrect AAA Server Configuration:** Incorrect configuration of the switch's AAA settings can result in communication failures or delays. Examples include:
  - Incorrect server IP addresses, shared secrets, or port numbers.
  - Protocol mismatches between the switch and the AAA server.
  - Misconfiguration on the AAA server itself.
- **Inefficient AAA Server Connection Management:** Performance can degrade due to poor connection management practices, such as:
  - Inefficient reuse of established connections.
  - Frequent connection establishment and teardown cycles.
  - Limitations on the number of concurrent connections.
  - Specific issues like the "single-connection" command in TACACS+ server configuration, which, while intended to optimize TCP connection reuse, caused problems in some Cisco implementations.
- **API Limitations and Licensing for Cloud-Managed Equipment:** Vendors offering cloud-based network management solutions, such as Wireless LAN Controllers (WLC), may impose API restrictions. These include:
  - Limits on the number of API calls to prevent flooding
  - Licensing tiers that restrict API usage, impacting performance or scalability

**Resource Constraints on the Switch**

- **High CPU Utilization:** High CPU usage on the switch, regardless of the cause, can lead to overall performance degradation, including slow SSH responses, delayed command execution, and packet loss. This can be caused by several factors, including excessive network traffic, complex configurations, software bugs, or resource-intensive processes.
- **Memory Exhaustion:** Insufficient memory or memory leaks on the switch can also cause significant performance problems, including slow responses, crashes, and instability.
- **Insufficient Hardware Resources:** The switch's hardware (CPU, memory, processing ASICs) may be inadequate for the current network load or features being used. This is especially relevant in older or lower-end switches.

**Software and Firmware Issues**

- **Software Bugs:** Bugs in the switch's operating system or firmware can lead to various performance issues, including CPU spikes, memory leaks, process hangs, and unexpected behavior. The specific

example of the Cisco “Hulc LED” process consuming excessive CPU is an instance of a software bug.
- **Outdated Firmware:** Running outdated firmware can expose the switch to known vulnerabilities and performance issues that have been addressed in newer releases.

## Impact of Sepio Scan Engine on Switch Performance

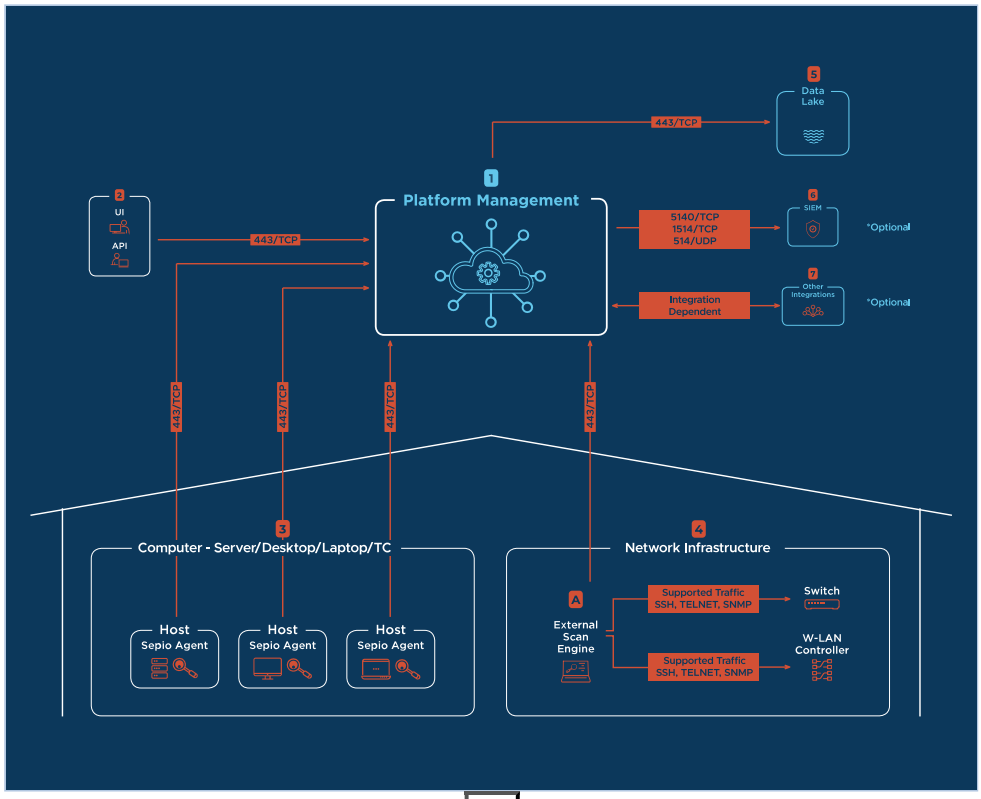
The Sepio Scan Engine can have a limited impact on the performance of network infrastructure elements:

- **Resource Usage:** The scan engine uses SSH to run commands on network equipment, leading to a slight increase in resource utilization.
- **CPU Utilization:** The impact on CPU utilization varies across switch models and switch vendors. Older models, such as the Cisco WS-C2960X-48TS-LL, show a more noticeable increase (13-15%) during scans, but this increase is temporary. Newer models show less than 5% impact during scans. The Juniper switches tend to have high impact on CPU, but overall, it is safe to say that modern network infrastructure elements would show less than 5% CPU increase during scans.
- **Data Throughput:** The scan engine does not significantly impact bandwidth. Data throughput during a scan is around 250-350 KB/s. This minimal traffic is not likely to impact network throughput.

**Note:** See also Installing and Activating a Sepio Scan Engine.

## Connectivity Diagram

The following diagram illustrates the connection initiation direction and the relevant ports that are used to communicate between the different system components and the customer environment. You can review the diagram for host-only deployments and network-only deployments.




Connectivity Diagram

| Source | Destination | Authentication and Networking |
|---|---|---|
| UI (2) | Sepio Management, using HTTPS://FQDN (1) | The UI will initiate the connection request over HTTPS (port 443/TCP). Authentication is required. SAML and Active Directory for passwords and MFA are supported. |
| API calls (2) are mainly used for on-premises automation. | Sepio Management, using HTTPS://FQDN (1) | The application which uses the API will initiate the connection request over HTTPS (port 443/TCP). Authentication is required. Multiple methods and industry standards for Authentication and Authorization are available. |
| HOST (3) | Sepio Management, using HTTPS://FQDN (1) | From HOST to Sepio over port 443/TCP using TLS. |

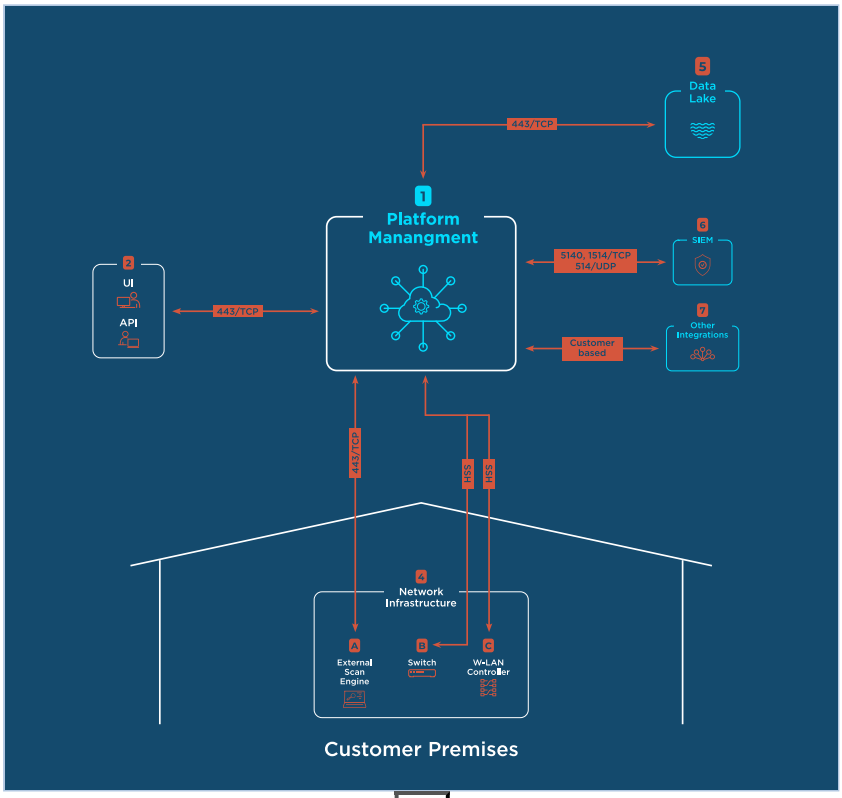
| Source | Destination | Authentication and Networking |
|---|---|---|
| External Network Scanner (4A) | Sepio Management, using HTTPS://FQDN (1) | From External Network Scanner to Sepio over TLS. |
| External Network Scanner (4A) | Customer network infrastructure | From Scan Engine to the network infrastructure over the defined management interface protocol (either SSH, SNMP v2/v3 or Telnet). Credentials are stored secured in the management (1) or customer's RADIUS/TACACS. |
| Management (1) | SIEM (6) | Optional integration: The management initiates the communication with Optional Integration: SIEM uses one of the supported syslog integration protocols. |
| 3rd party (7) integration | Sepio Management, using HTTPS://FQDN | Typically, the 3rd party integration would initiate the integration request. Current integration uses HTTPS (port 443) with TLS for communication. |
| Management (1) | Sepio Data Lake | If enabled, the management can send bleached data and performance KPI to Sepio cloud over use HTTPS (port 443), TLS. |

# Network-only Deployments

## Overview

Customers that are only looking to monitor and manage the use of networked devices, connected using wired Ethernet or Wi-Fi, will likely opt for a Network-only deployment.  In this mode, Sepio Scan Engines connect directly to the Network Infrastructure via the management interface of your equipment. Sepio will not connect to the assets themselves, and all the relevant information is collected from the network infrastructure itself. The diagram below assumes that the Sepio Management is in the cloud and that, a Scan Engine is used on customer premises.

The connectivity diagram and table list the main components and communication protocols.




Network-only Deployments Diagram

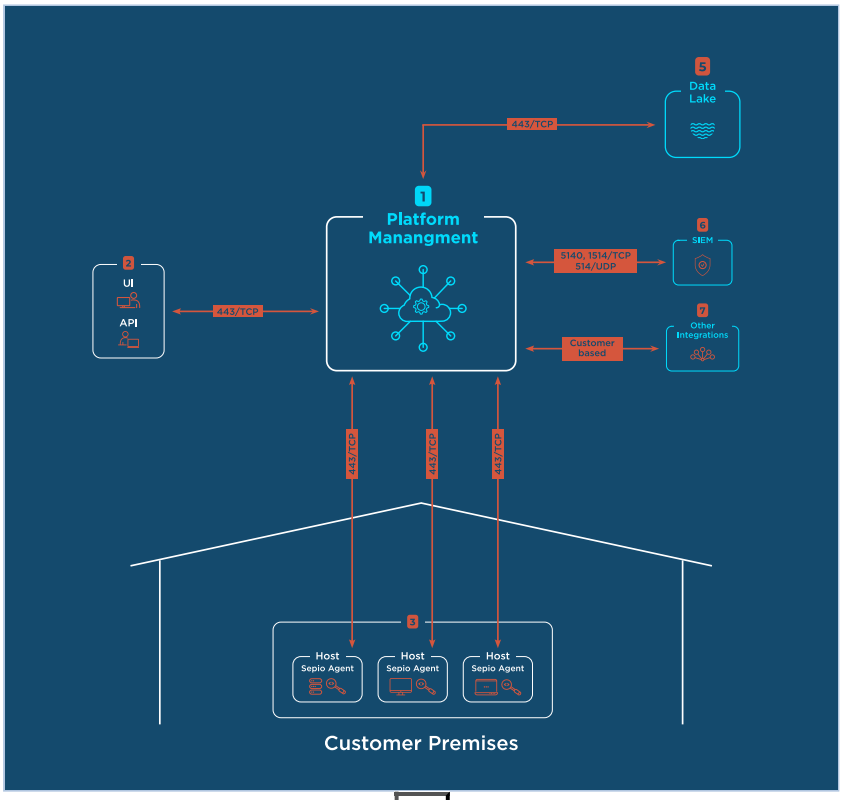
| Source | Destination | Authentication and Networking |
|---|---|---|
| UI (2) | Sepio Management, using HTTPS://FQDN (1) | The UI will initiate the connection request over HTTPS (port 443/TCP). Authentication is required. SAML and Active Directory for passwords and MFA are supported. |
| API calls (2) are mainly used for on-premises automation | Sepio Management, using HTTPS://FQDN (1) | The application which uses the API will initiate the connection request over HTTPS (port 443/TCP). Authentication is required. Multiple methods and |

| Source | Destination | Authentication and Networking |
|---|---|---|
| | | industry standards for authentication and authorization are available. |
| External Network Scanner (4A) | Sepio Management, using HTTPS://FQDN (1) | From External Network Scanner to Sepio over TLS. |
| External Network Scanner (4A) | Customer network infrastructure | From Scan Engine to the network infrastructure over the defined management interface protocol (either SSH, SNMP v2/v3 or Telnet). Credentials are stored securely in the management (1) or customer's RADIUS/TACACS. |
| Management (1) | SIEM (6) | Optional integration: The management initiates the communication. SIEM uses one of the supported syslog integration protocols. |
| 3rd party (7) integration | Sepio Management, using HTTPS://FQDN | Typically, the 3rd party integration initiates the integration request. Current integration uses HTTPS (port 443) with TLS for communication. |
| Management (1) | Sepio Data Lake | If enabled, the management can send bleached data and performance KPIs to the Sepio cloud over HTTPS (port 443) with TLS. |

# Host-only Deployment

## Overview

Customers that are only looking to monitor and manage the use of USB and other peripheral devices on endpoints, preventing data leakage and protecting against threats introduced through these devices will probably opt for a Host-only deployment. In this mode, Sepio Host agents connect directly to the Sepio Management platform over secure communications. The connectivity diagram and table list the main components and communication protocols.




Host-only Deployment Diagram

| Source | Destination | Authentication and Networking |
|---|---|---|
| UI (2) | Sepio Management, using HTTPS://FQDN (1) | The UI will initiate the connection request over HTTPS (port 443/TCP). Authentication is required. SAML and Active Directory for passwords and MFA are supported. |
| API calls (2) | Sepio Management, using HTTPS://FQDN (1) | The application that uses the API will initiate the connection request over HTTPS (port 443/TCP). Authentication is required. Multiple methods and industry standards for authentication and authorization are available. |

| Source | Destination | Authentication and Networking |
| --- | --- | --- |
| HOST (3) | Sepio Management, using HTTPS://FQDN (1) | From HOST to Sepio over port 443/TCP using TLS. |
| Management (1) | SIEM (6) | Optional integration: The management initiates the communication. SIEM uses one of the supported syslog integration protocols. |
| 3rd party (7) integration | Sepio Management, using HTTPS://FQDN | Typically, the 3rd party integration initiates the integration request. Current integration uses HTTPS (port 443) with TLS for communication. |
| Management (1) | Sepio Data Lake | If enabled, the management can send bleached data and performance KPIs to the Sepio cloud over HTTPS (port 443) using TLS. |

# Backup, Redundancy, and High Availability

## Overview

The Sepio Platform can be deployed in the cloud, where Sepio manages the system's availability, or on-premises, where customers can leverage highly available hardware components such as dual power supplies, redundant disks, and other fault-tolerant infrastructure.

> **Note:** Currently, the Sepio Application components do not use an active/active architecture.

## Backup and Restore

Sepio Backup and Restore provides comprehensive capabilities for safeguarding and recovering your Sepio deployment. The system backs up all required components necessary for a complete restoration, including:

- **Service Discovery & Configuration** – Service configuration and metadata
- **Databases** – All system databases (cache, search, relational data)
- **Object Storage** – File storage and artifacts
- **Container Volumes** – Persistent container data
- **System Configurations** – Application and service configuration files

All components are bundled into a single compressed TAR archive, accompanied by detailed logs and component-level summaries.

#### Prerequisites and Requirements

- **Restore Target Server** – An identical server prepared as the restore target, with the same Sepio Platform version already installed.
- **Root Access** – All backup and restore operations must be executed as root (or using sudo).

> **Note:** When using `sudo`, the `-E` flag must be used to preserve environment variables.

- **Environment Variables (Non-Air-Gapped Deployments)** – Ensure the following environment variables are set prior to running backup or restore operations:
  - `SEPIO_REGISTRY_URL`
  - `SEPIO_REGISTRY_USERNAME`
  - `SEPIO_REGISTRY_PASSWORD`

- **Disk Space Requirements**
  - **Backup** – Ensure sufficient free space is available in `/opt/sepio/backup/` to store the compressed TAR archive.
    - Minimum required: **25%** of the total Sepio data size.
    - Recommended space: **50%** of total Sepio data size.
  - **Restore** – At least **2.5x the size of the backup TAR file** is required.

> **Note:** The restore process automatically validates available disk space before execution. If insufficient space is detected, the restore operation will not proceed.

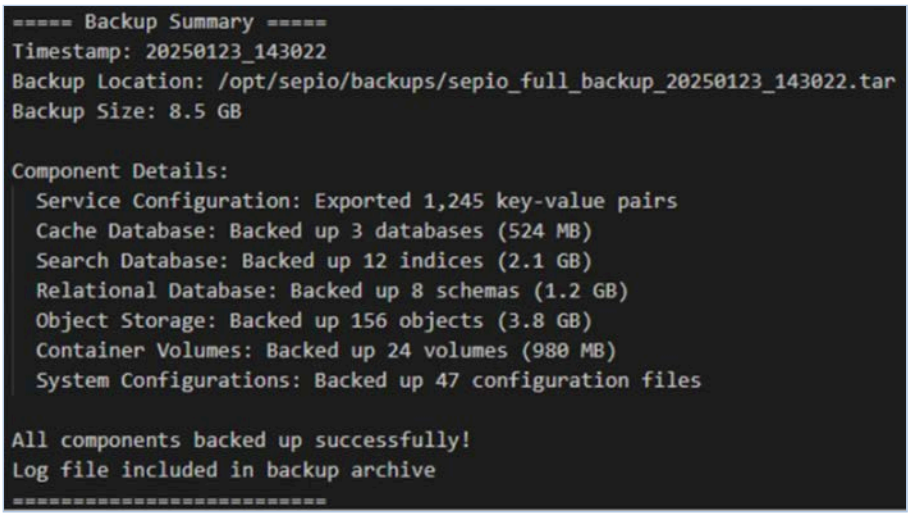
- **Network Access** – Network access to the Sepio container registry is required for non-air-gapped customers only.

### Backup Procedure

- **Prepare the environment**
  - **Set environment variables** (non air-gapped customers only):
    - `export SEPIO_REGISTRY_URL=`
    - `export SEPIO_REGISTRY_USERNAME=`
    - `export SEPIO_REGISTRY_PASSWORD=`
  - **Verify sufficient disk space requirements**
    - `df -h /opt/sepio/backup/`
- **Run backup command using** `sudo -E sepioctl backup`

> **Note:** Air-gapped customers should run `sudo -E sepioctl backup --air-gapped`.

- **Review the backup summary**
  - After the backup completes, a summary will be displayed.
  - In case any component shows a failure, it is recommended to rerun the backup command.
  - If the failure persists, contact Sepio Customer Success.



Backup Summary

### Restore Procedure

- **Prepare the environment on the dedicated restored server**
  - Move the backup file to the dedicated restored server.
    - Default location: `/opt/sepio/backups/`
  - Ensure all environment variables are set (non-air-gapped customers only)
  - Verify sufficient disk space is available:
    - `df -h /tmp`
    - `df -h /opt/`

> **Note:** The restore process will stop and replace the current Sepio deployment on the target server.

- **Run the restore command**
  - Restore from the original location:

    ```
    sudo -E sepioctl restore
    ```
  - Restore from a custom location:

    ```
    sudo -E sepioctl restore --backup-dir /custom/path
    ```
  - Air-gapped customers restore:

    ```
    sudo -E sepioctl restore --air-gapped
    ```

> **Note:** The restore process automatically validates backup integrity and available disk space. Upon completion, it runs `sepioctl` up to bring the system back online.

- **Review restore summary**
  - After the restore completes, a summary of the process is displayed.
  - If any component reports a failure, rerun the restore command.

    - If the failure persists, contact Sepio Customer Success.

- **Verify system status**
    - Run the following commands and verify that all services are running:
    - `sepioctl status`
    - `docker ps # or podman ps`

- **Final validation**
    - Once the system is confirmed to be operating as expected, update the DNS record of the original server to point to the restored server.

### Estimated Backup and Restore Timelines

- **Backup (estimated)**
    - Development server should take ~ 1 hour
    - Production server should take ~ 3 hours

- **Restore (estimated)**
    - Development server should take ~ 1.5 hour
    - Production server should take ~ 4.5 hours

### Troubleshooting

- **Case: A component failed to be backed up**
  **Resolution:**
    - Review the detailed error message in the backup summary output.
    - Inspect the backup log file included in the backup TAR archive (backup file name: `sepio_full_backup_timestamp.tar`).
    - Rerun the backup command.
    - If the failure persists, verify the following:
        - **Component service status:**
          `docker ps # or podman ps`
        - **Component logs:**
          `docker logs <component-container> # or podman logs <component-container>`

- **Case: A component failed to be restored**
  **Resolution:**
    - Rerun the restore command.
    - If the failure persists:
        - Review the restore logs for specific error details
          (logs are printed in the terminal at the end of the restore process).
        - Verify the component container is **not** already running:
          `docker ps # /or podman ps`

- If a database restore failed, ensure all database containers are fully stopped before retrying the restore.

## High Availability

Sepio High Availability (HA) provides automated backup and restore between two Sepio platforms in an Active-Passive configuration:

- **Active Node:** Runs the Scheduler daemon, creates backups, and transfers them to the Passive node.
- **Passive Node:** Runs the Monitor daemon, receives backups, and automatically restores them.

### Prerequisites

- Both servers (Active and Passive) must be operational and meet all prerequisites and requirements of the Sepio Backup and Restore feature.
- Both servers must be running the **same Sepio Platform version**.

### Requirements

- Sufficient disk space as mentioned in Sepio Backup and Restore requirements.
- SSH connectivity (port 22 by default) between Active and Passive nodes.
- Bidirectional network connectivity.
- SCP capability for backup transfer.

### Workflow

- The **Scheduler Daemon** on the Active node creates backups on a configured schedule using `backup-sepio`.
- The backup file is transferred via SCP to the Passive node.
- The **Monitor Daemon** on the Passive node detects the new backup file, verifies its integrity, and restores it using `restore-sepio`.

### Failover Procedure (Active Node Failure)

In the event of an Active node failure, the following manual steps are required:

- Update the **DNS configuration** to point to the Passive node.
- Switch node roles by updating the configuration:
  - Change the **Active node** configuration to **Passive**.
  - Change the **Passive node** configuration to **Active**.

**Note:** Detailed configuration instructions for switching roles are provided in the configuration

section below.

### Pre-Installation Checklist

1. Verify Sepio Platform installation and version consistency on both nodes:

```
# Check running Sepio containers
docker ps | grep sepioprime | wc -l
# Check Sepio version (should match on both nodes)
cat /opt/sepio/config/*/compose/.env | grep SEPIO_VERSION
```

2. On the Active Node, setup SSH key authentication to the Passive node

```
# Generate SSH key (if not already available)
ssh-keygen -t rsa -b 4096 -f ~/.ssh/sepio-ha-key -N ""
# Copy public key to Passive node (replace PASSIVE_IP with your Passive node's IP address)
ssh-copy-id -i ~/.ssh/sepio-ha-key.pub user@PASSIVE_IP
# Test connectivity (should not prompt for password)
ssh -i ~/.ssh/sepio-ha-key user@PASSIVE_IP "echo 'SSH connection successful'"
```

3. Verify network connectivity between active and passive nodes

```
# From Active node, test SSH to Passive
nc -zv PASSIVE_IP 22
# From Passive node, test SSH to Active (recommended but not mandatory)
nc -zv ACTIVE_IP 22
```

### Configurations

High Availability configurations are stored in:

`/opt/sepio/config/ha-config.yml`

**Initial mandatory configurations:**

**Active Node**

Replace with the actual IP address of your Passive node:

```
sudo /opt/sepio/bin/sepioctl ha init \
--node-id active-node \
--partner-address \
--active
```

**Passive Node**

Replace with the actual IP address of your Active node:

```
sudo /opt/sepio/bin/sepioctl ha init \
--node-id passive-node \
--partner-address
```

### Additional Active Node Configuration

```
# ============================================================================
# SEPIO HA CONFIGURATION - ACTIVE NODE
# ============================================================================
system:
  node_id: active-node                    # Unique identifier for this node
  cluster_id: sepio-ha                    # Cluster name

partner:
  address: 10.0.0.20                      # Passive node IP address
  port: 22                                # SSH port
  ssh_user: root                          # SSH username
  ssh_key_path: ~/.ssh/sepio-ha-key       # SSH private key

role:
  active: true                            # This is the active node

backup:
  # SCP path format: scp://user@host:/path/
  path: scp://root@10.0.0.20:/opt/sepio/backups/
  cron: "0 * * * *"                       # Every hour (minute 0)
  retention_days: 7                       # Keep backups for 7 days
  air_gapped: false                       # Set true if no internet access
  max_retries: 3                          # Retry backup 3 times on failure

monitor:
  auto_restore: false                     # Active node doesn't restore
  poll_interval_seconds: 30

restore:
  source_path: /opt/sepio/backups
  validation_enabled: true
  auto_start_services: true

sepioctl:
  backup_command: /opt/sepio/backup-tool/backup-sepio.sh
  restore_command: /opt/sepio/backup-tool/restore-sepio.sh
  timeout: 7200                           # 2 hour timeout

logging:
  level: info                             # debug, info, warn, error
  path: /opt/sepio/log/ha-system
  max_size_mb: 100
  max_backups: 10
  format: json
```

### Additional Passive Node Configuration

```yaml
# ================================================================================
# SEPIO HA CONFIGURATION - PASSIVE NODE
# ================================================================================
system:
  node_id: passive-node
  cluster_id: sepio-ha

partner:
  address: 10.0.0.10                        # Active node IP address
  port: 22
  ssh_user: root
  ssh_key_path: ~/.ssh/sepio-ha-key

role:
  active: false                             # This is the passive node

backup:
  path: /opt/sepio/backups                  # Local path (receives via SCP)
  cron: "0 * * * *"
  retention_days: 7
  max_retries: 3

monitor:
  auto_restore: true                        # Automatically restore new backups
  poll_interval_seconds: 30                 # Check every 30 seconds
  validation_max_retries: 3                 # Retry validation 3 times
  validation_retry_delay_seconds: 60        # Wait 60s between validation retries
  restore_max_retries: 3                    # Retry restore 3 times
  restore_retry_delay_seconds: 120          # Wait 2 minutes between restore retries

restore:
  source_path: /opt/sepio/backups
  validation_enabled: true
  auto_start_services: true
  air_gapped: true                          # Air-gapped mode for restore

sepioctl:
  backup_command: /opt/sepio/backup-tool/backup-sepio.sh
  restore_command: /opt/sepio/backup-tool/restore-sepio.sh
  timeout: 7200

logging:
  level: info
  path: /opt/sepio/log/ha-system
  max_size_mb: 100
  max_backups: 10
  format: json
```

### Cron Schedule Examples

| Schedule | Cron Expression | Description |
|---|---|---|
| Every hour | 0 * * * * | Minute 0 of every hour |
| Every 2 hours | 0 */2 * * * | Every 2 hours |
| Every 6 hours | 0 */6 * * * | 4 times daily |
| Daily at 2 AM | 0 2 * * * | Once daily |
| Twice daily | 0 2,14 * * * | 2 AM and 2 PM |

### Setup

1. **Copy Service Files**

   Active Node (Scheduler)

   ```
   sudo cp /opt/sepio/backup-tool/systemd/sepio-ha-scheduler.service /etc/systemd/system/
   ```

   Passive Node (Monitor)

   ```
   sudo cp /opt/sepio/backup-tool/systemd/sepio-ha-monitor.service /etc/systemd/system/
   ```

2. **Reload systemd**

   ```
   sudo systemctl daemon-reload
   ```

3. **Enable Auto-Start on Boot**

   Active Node

   ```
   sudo systemctl enable sepio-ha-scheduler
   ```

   Passive Node

   ```
   sudo systemctl enable sepio-ha-monitor
   ```

4. **Start Services**

   Active Node

   ```
   sudo systemctl start sepio-ha-scheduler
   ```

   Passive Node

   ```
   sudo systemctl start sepio-ha-monitor
   ```

5. **Verify Services**

   Check service status

   ```
   sudo systemctl status sepio-ha-scheduler # Active Node
   sudo systemctl status sepio-ha-monitor # Passive Node
   ```

   View service logs

   ```
   sudo journalctl -u sepio-ha-scheduler -f # Active Node
   sudo journalctl -u sepio-ha-monitor -f # Passive Node
   ```

### Service Management Commands

| Action | Active Node (Scheduler) | Passive Node (Monitor) |
|---|---|---|
| Start | systemctl start sepio-ha-scheduler | systemctl start sepio-ha-monitor |
| Stop | systemctl stop sepio-ha-scheduler | systemctl stop sepio-ha-monitor |
| Restart | systemctl restart sepio-ha-scheduler | systemctl restart sepio-ha-monitor |
| Status | systemctl status sepio-ha-scheduler | systemctl status sepio-ha-monitor |
| Enable | systemctl enable sepio-ha-scheduler | systemctl enable sepio-ha-monitor |
| Disable | systemctl disable sepio-ha-scheduler | systemctl disable sepio-ha-monitor |
| Logs | journalctl -u sepio-ha-scheduler -f | journalctl -u sepio-ha-monitor -f |

### Validation

1. Run the following command on **both nodes:**

   ```
   sudo /opt/sepio/bin/sepioctl ha validate-setup
   ```

   Expected output:

   ```
   Validating HA setup…

   Configuration Checks:
   Node ID: active-node
   Role: ACTIVE
   Backup schedule: 0 * * * *
   Retention: 7 days

   Directory Checks:
   Backup directory exists: /opt/sepio/backups
   Log directory exists: /opt/sepio/log/ha-system

   Partner Connectivity:
   Partner address configured: 10.0.0.20
   SSH key configured

   Commands:
   sepioctl binary found
   backup-sepio found
   restore-sepio found
   Setup validation completed successfully.
   ```

2. Test backup (Active node)

   Trigger a test backup:

   ```
   sudo /opt/sepio/bin/sepioctl ha test-backup
   ```

   Verify the backup file was created:

   ```
   ls -lah /opt/sepio/backups/
   ```

   Expected Result:

   A new backup file should appear with a name like:

   ```
   sepio-backup-active-node-YYYYMMDD_HHMMSS.tar
   ```

3. Test restore (Passive node)

   Execute test restore (provide backup file path)

   ```
   sudo /opt/sepio/bin/sepioctl ha test-restore /opt/sepio/backups/sepio-backup-*.tar
   ```

   Check container status

   ```
   docker ps | head -20
   ```

4. Run health check

   Run a comprehensive health check

   ```
   sudo /opt/sepio/bin/sepioctl ha health-check
   ```

   Exit code 0 = healthy, 1 = issues

   ```
   echo "Exit code: $?"
   ```

5. End-to-end test

   Run manual backup on active node:

   ```
   sudo /opt/sepio/bin/sepioctl ha scheduler trigger
   ```

   Watch monitor on Passive node:

   ```
   sudo tail -f /opt/sepio/log/ha-system/passive.log
   ```

   Verify restore completed:

   ```
   sudo /opt/sepio/bin/sepioctl ha show
   ```

### Monitoring and Operating

1. **View System Status**

   Basic status

   ```
   sudo /opt/sepio/bin/sepioctl ha show
   ```

   Detailed status with history

   ```
   sudo /opt/sepio/bin/sepioctl ha show --detailed
   ```

   JSON output (for scripting)

   ```
   sudo /opt/sepio/bin/sepioctl ha show --json
   ```

2. **View Logs**

   HA daemon logs (follow mode)

   ```
   sudo /opt/sepio/bin/sepioctl ha logs -f
   ```

   Backup operation logs

```
sudo /opt/sepio/bin/sepioctl ha logs --backup -f
```

Restore operation logs

```
sudo /opt/sepio/bin/sepioctl ha logs --restore -f
```

Direct log access

```
sudo tail -f /opt/sepio/log/ha-system/active.log # Active Node
sudo tail -f /opt/sepio/log/ha-system/passive.log # Passive Node
sudo tail -f /opt/sepio/log/backup-tool/backup-latest.log
sudo tail -f /opt/sepio/log/backup-tool/restore-latest.log
```

3. **View Backup List**

   List backup files

   ```
   ls -lah /opt/sepio/backups/
   ```

   Show backup details

   ```
   sudo /opt/sepio/bin/sepioctl ha show --detailed
   ```

4. **Live Monitoring Dashboard**

   Live status view (auto-refresh)

   ```
   sudo /opt/sepio/bin/sepioctl ha watch
   ```

5. **Log monitoring dashboard**

   Watch for errors

   ```
   sudo grep -i error /opt/sepio/log/ha-system/*.log
   ```

   Watch for restore failures

   ```
   sudo grep -i "restore failed" /opt/sepio/log/ha-system/passive.log
   ```

   Watch backup transfers

   ```
   sudo grep -i "transfer" /opt/sepio/log/ha-system/active.log
   ```

## Troubleshooting

1. **Issue: Backup not created**

   **Required steps:**

   Check Scheduler Status:

   ```
   sudo /opt/sepio/bin/sepioctl ha scheduler status
   ```

   Check Logs (Active Node):

   ```
   sudo tail -100 /opt/sepio/log/ha-system/active.log
   ```

   Check Disk Space:

   ```
   df -h /opt/sepio/backups
   ```

   **Solutions:**

   Restart the scheduler service:

   ```
   sudo systemctl restart sepio-ha-scheduler
   ```

   Verify the backup schedule in the HA configuration.

   Ensure sufficient disk space is available in `/opt/sepio/backups/`.

2. **Issue: Restore process not starting**

   **Required steps:**

   Check monitor status

   `sudo /opt/sepio/bin/sepioctl ha monitor status`

   Check `auto_restore` setting

   `grep auto_restore /opt/sepio/config/ha-config.yml`

   Check logs

   `sudo tail -100 /opt/sepio/log/ha-system/passive.log`

   **Solutions:**

   Ensure `auto_restore: true` is set in the HA configuration.

   Check logs for any validation errors preventing the restore.

3. **Issue: SCP transfer fails**

   **Required steps:**

   Test SSH connectivity (from Active node)

   `ssh -i ~/.ssh/sepio-ha-key user@PASSIVE_IP "echo OK"`

   Check SSH key permissions

   `ls -la ~/.ssh/sepio-ha-key`

   Permissions should be: -rw——— (600)

   **Solutions:**

   Fix SSH key permissions: `chmod 600 ~/.ssh/sepio-ha-key`.

   Verify the partner address is correctly configured in `/opt/sepio/config/ha-config.yml`.

   Check firewall rules to allow port 22 traffic between nodes.

4. **Issue: Containers not starting after restore**

   **Required steps:**

   Check container status

   `docker ps -a | head -20`

   Check compose logs

   `docker compose logs --tail=50`

   Check restore log

   `sudo cat /opt/sepio/log/backup-tool/restore-latest.log`

   **Solutions:**

   Manually restart containers:

   `/opt/sepio/backup-tool/up-sepio.sh`

   Ensure `docker-compose.yml` exists and is valid.

   Verify the environment file exists at `/opt/sepio/.env`.

## Sepio Platform High Availability – Additional Deployment Options

Several Sepio components can be deployed in **high availability (HA)** mode to improve uptime and scalability.

- **Scan Engines:** Multiple scan engines can be deployed to provide redundancy and backup for each other, either fully or partially. They can also function as load balancers to distribute scanning workloads efficiently.
- **Agent Recovery Servers:** Sepio Agents can operate even when disconnected from the network and do not require online access to the management server during operations. During installation, a backup server can be defined. In cases where the primary Sepio management server is unavailable, Agents can send logs and audit information, receive commands, and process notifications from the backup server.
- **Change Management:** Sepio provides the ability to move Agents between different servers and manage multiple versions of Scan Engines. This allows seamless migration to supported versions when failures or issues are detected in a specific version.
- **Agent Load Balancer / Proxy:** Agents can be redirected using a centralized load balancer, DNS-based load balancing, or proxy servers. This enables traffic distribution and failover between multiple management servers.

## Multiple Version Support

Sepio Scan Engines and Agents do not need to match the version of the Sepio Management server. This allows gradual deployment and upgrade strategies across installations. Multiple operational scenarios are supported, enabling seamless management of heterogeneous environments and staged rollouts of new versions.

# Azure Snapshots to Clone Production Environments

An Azure Virtual Machine (VM) snapshot is a **read-only copy of a disk at a specific point in time**. It captures the state of the managed disk, allowing Sepio customers to recreate the disk and, consequently, a VM in that exact state. This is ideal for creating test environments that are exact replicas of your production setup.

The process generally involves four high-level steps:

## 1. Create Snapshots of Production VM Disks

Sepio's Customer Success team creates snapshots of all the disks attached to your production VM. This includes:

- **Operating System (OS) Disk:** Contains the operating system, installed applications, and system configurations.
- **Data Disks (if any):** Hold your application data, databases, etc.

## 2. Create New Managed Disks from Snapshots

Using the snapshots, it is possible to create **new managed disks**. These disks will be independent copies of the original production disks at the time the snapshot was taken. This step essentially "materializes" the point-in-time copy of the customer's disk data.

## 3. Create a New VM from the New Managed Disks

With the new managed disks (one for the OS and one for each data disk), it is then possible to **create a brand-new Azure Virtual Machine**. When creating the VM, specify the newly created OS disk as the operating system disk.

## 4. Configure the New VM for Testing/Validation

The newly created VM will be an exact clone of the production environment as it existed when the snapshots were taken. Sepio's Customer Success team then configures it appropriately for testing and validation, which might involve:

- Assigning a new IP address.
- Connecting to a separate virtual network for isolation.
- Updating application configurations to use test databases or services.
- Updating hostnames and security configurations.

- Updating SSO and other integrations.

## High-Level Considerations

Cloning Virtual Machines (VM) from snapshots is effective, but several important considerations must be taken into account.

> **Note:** Please consult with Sepio Support team before developing a cloning strategy for your production environment.

### 1. Snapshot Consistency

- **Application-Consistent vs. Crash-Consistent:** If the production VM is running when the snapshot is taken, Azure attempts to create an application-consistent snapshot (which involves quiescing applications). If that fails, it defaults to a crash-consistent snapshot, similar to pulling the plug. For critical applications (e.g., databases), an application-consistent snapshot is ideal.
- **Stopping the VM:** For absolute data consistency, especially with complex applications or databases, the most reliable method is to **gracefully shut down the production VM** before taking snapshots of its disks. This ensures no writes are in progress and that all data is flushed to disk.

### 2. Network Configuration

- **IP Addresses:** The new VM will require a new IP address. You might need to update configurations on the cloned VM or connected systems.
- **Virtual Network Isolation:** For testing and validation, it's critical to deploy the cloned VM into a separate Azure Virtual Network (VNet). This avoids conflicts with other production environments (e.g., duplicate host names or IP addresses) and ensures that testing doesn't impact live services.
- **Network Security Groups (NSGs):** Ensure the NSG applied to the new VM's subnet or network interface (NIC) is configured appropriately for your testing needs, allowing necessary inbound and outbound traffic while maintaining security.

### 3. Resource Group and Location

- **New Resource Group:** Best practice is to deploy the cloned VM and its associated resources (disks, NIC, VNet) into a new, dedicated resource group for the test environment. This facilitates easier management, cost tracking, and eventual deletion.
- **Region:** It is possible to create the new VM in the same Azure region or a different one, depending on customer's testing requirements and latency considerations.

**4. Data Refresh Strategy**

- How often will you refresh the test environment? You'll need a process to regularly take new snapshots from production and repeat the cloning steps to keep the test environment in sync with production.

**5. Security**

- **Access Control:** Ensure that access to the test environment is appropriately restricted using Azure Role-Based Access Control (RBAC).
- **Data Sensitivity:** If your production data contains sensitive information, ensure the cloned environment maintains the same security standards and compliance requirements.

# Upgrading HAC-1 to Sepio

This section provides guidance for upgrading from **HAC-1** to the **Sepio Platform.**

## Related Topics

- Upgrading HAC-1 to Sepio Platform
- HAC-1 to Sepio Platform – Migration Procedure

# Upgrading HAC-1 to Sepio Platform

This topic provides information and planning instructions for upgrading HAC-1 to Sepio Platform. You can use this topic to create a checklist and detailed plan for migrating the existing Hardware Asset Control system to Sepio Platform.

> **Note:** Please, contact Sepio support with any question or request.

## Intended Audience

This topic guides Security Administrators and Architects involved in the migration from Sepio's HAC-1, in your organization, to the latest Sepio Platform. It is also intended for Security and System administrators responsible for operating Sepio Platform and managing the security of their various digital Assets.

## Sepio Platform Overview

Sepio enables you to view all connected Assets on your network, assess your hardware-based risk, and provides risk management for all your hardware Assets.

Sepio is a unique software solution for detecting and mitigating the risk of malicious Assets in enterprise environments and infrastructure. Whether by USB and/or network interfaces, Sepio provides total visibility and blocking options.

Using easily configured policies, or choosing our defaults, you can decide which Asset can be connected and used and thus disables any risky Asset in real-time as soon as it is connected.

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

## Design and Behavior Differences between HAC-1 and Sepio Platform

There are several differences between HAC-1 and the Sepio Platform, some are more visible because of the UI and UX updates. Other, related to Asset DNA and detection algorithms are less visible. See the list of detailed changes in the Sepio Platform documentation. The following list is provided as a high-level reference in order to assist with the verification and acceptance procedures.

## List of detailed changes

- New policy management capabilities
- New universal discovery method that uses standard SNMP in addition to Asset DNA

- More Asset classification options
- Risk scoring and anomaly detection
- Changes in the Asset location algorithm
- Scan engine scheduler scale options, to support larger deployments with more frequent scans
- Better UI/UX, additional integration options and use cases
- New detection capabilities using enhanced Asset DNA, location awareness, anomaly detection and better AI for reduction of false positive
- Asset DNA improvements, supporting additional detection capabilities:
    - Significant reduction in false alarm rate
    - Consistent behavior for all Asset types
    - Setting detection sensitivity for peace time and war time
    - Behavior changes when using Sepio for traffic-less network Asset discovery
        - When a network Asset is connected to a physical port or WIFI, it would be detected and identified
        - Continuous detection and automatic classification of Assets

## Compatibility

- No changes with existing **APIs**, supporting backward compatibility with existing integrations (while new APIs are available).
- **Agents**
    - No changes with endpoint (Hosts) Agents.
    - Current HAC-1 Agents for Windows and Linux (version 16.x.x) are forward compatible with Sepio Platform (version 17.2022.x and beyond).
    - Older HAC-1 (version 16.x.x) is backward compatible with the new Sepio Platform Agents (version 17.x.x).
- HAC-1 **Scan Engine (netpoller)** functionality is backward compatible

# HAC-1 to Sepio Platform – Migration Procedure

The migration process uses a gradual method to simplify each necessary step. It was designed to support migration from previously installed HAC-1 on different components and operating systems on customer premises and public clouds and create a single support option.

## Migration Options

**The following migrations paths are possible**

## Connectivity Requirements

**This diagram shows Sepio Platform architecture and connectivity requirements.**

## Data that will not be Migrated

HAC-1 historic events will not be migrated to the new Platform. If you are using HAC-1 as a compensating control for a compliance requirement, or if it is used to meet a regulation mandate, the HAC-1 server should not be decommissioned.

## Before Migration

**These steps should be performed before starting the migration**

## Migration Process

The migration process itself should be straightforward. First verify that the newly installed Sepio Platform is functioning properly and compare. Then add Agents and network elements to the new system, integrate any 3rd party solutions. After initial migration is complete import labels to all Assets.

### DNS

You can change the DNS record to point at the new system at any time during the process, however it is recommended to do it after the initial verification. Agents events and logs are kept locally and will not be lost during the transition. In addition, it is possible to define an Agent Recovery server during the migration process.

### Verification

To verify the different system attribute and its behavior it is recommended to take the following steps:

1. Migrate several Agents from the current system to the new Platform.
2. Perform parallel network scanning to create the network inventory.
3. Compare alerts on both systems.

### Agent Migration

A specific Agent or multiple Agents can be automatically migrated from HAC-1 to Sepio Platform.

Before starting the procedure contact support@sepiocyber.com to enable the '**update HAC-1 address**' action in HAC-1.

**To migrate an Agent/s from HAC-1 to Sepio Platform:**

### Scan Engine Migration

Since multiple Scan Engines can be used in parallel, it is recommended to create a new Scan Engine, use the existing credentials list and verify the results.

### Network Infrastructure Migration

The list of network devices can be exported, however due to security considerations, network infrastructure credentials can not be exported directly from Sepio. If you do not have a copy of current credentials and you are not using a centralized AAA solution such as Radius or Tacacs, please contact Sepio support to create a solution that will allow you to pull the credentials directly from the HAC-1 database.

### Migration Process Timeline Summary



# Platform Installation and Update

## Overview

This section of the user guide provides detailed instructions for installing and updating the Sepio platform. You will find several installation methods tailored to different environments, including cloud-based deployments and on-premise solutions for both online and air-gapped systems. The documentation outlines the necessary prerequisites and provides step-by-step procedures. Please choose the method that best fits your technical requirements and operational environment. Additionally, refer to the best practices section to ensure a smooth and successful installation or update process.

## Related Topics

- Platform Requirements
- Installation
  - SepioCTL
  - Artifact Signature Verification
  - Before Installing Sepio
  - Installing Sepio on a Virtual Appliance
  - Installing Sepio on Customer Owned Hardware and Software
  - Reinstalling and Reimaging a host with Sepio Agent
  - Installing and Uninstalling a Sepio Agent
  - Installing Sepio Agent for VDI
  - Installing for Session Based and Agentless Modes
  - Audit Mode
  - Installing and Activating a Sepio Scan Engine
  - High Performance Deployment
- Update
  - Platform Update
  - Updating a Sepio Agent
  - Updating a Scan Engine
  - Updating the Knowledge Base
  - Platform Configuration
    - Setting Agents Connection Intervals
    - Managing Integrations
    - Setting Host/s (Agent) Mode
- Post Installation and Update Checklist
- Sepio Platform SaaS
- Platform Decommission

# Platform Decommission

This guide is intended for system administrators, security engineers, and IT operations teams responsible for managing Sepio deployments. It applies to on-premises, virtual appliance, and customer-owned hardware installations.

## Executive Summary

This document provides a structured procedure for safely decommissioning the Sepio platform while preserving data integrity and meeting compliance requirements.

Before decommissioning, organizations must review regulatory obligations, obtain compliance approval, and document all deployed components, integrations, and network dependencies. Required access includes administrative privileges and network permissions.

The decommissioning process includes data preservation and full system backup, removal of Sepio Agents and Scan Engines, cleanup of network configurations and external integrations, and decommissioning of the Sepio Platform Management Server.

Final validation ensures that all components have been fully removed, backups are securely stored, integrations are disconnected, and licensing matters are addressed. All activities must be documented and coordinated with relevant technical, security, and compliance teams.

## Prerequisites and Planning

### Compliance Considerations

**Important:**

- If Sepio is used as a compensating control for compliance requirements or to meet regulatory mandates, historical event data must be retained. Do not fully decommission the platform until all regulatory retention periods have been satisfied.
- Consult with your compliance team before proceeding with decommissioning.

### Required Access and Permissions

- Root or Administrator access to all Sepio components
- Access to the Sepio Platform Management GUI
- SSH access to servers hosting Sepio Platform, Scan Engines, and managed hosts
- Network access to all deployed components

#### Documentation Requirements

Before decommissioning, document the following:

- Current Sepio Platform version
- List of all hosts with Sepio Agents installed
- List of all deployed Scan Engines
- Network infrastructure elements configured for Sepio scanning
- Integration configurations (SIEM, CMDB, etc.)
- DNS records pointing to Sepio management servers

## Phase 1: Data Preservation and Backup

#### Step 1.1: Extract Non-Identifiable Data (Optional)

For analytics and future reference, extract anonymized data from the platform:

- Log in to the Sepio Platform Management GUI
- Navigate to **Settings** -> **Server**
- Scroll to the **Data Lake** section
- Click **Download Information**
- Select:
  - “Non-identifiable Agent and Peripheral Information”
  - “Non-identifiable Network Switch and Device Information”
- Click **Download File** and save it securely

**Reference:** Data Extractions

#### Step 1.2: Create Full Platform Backup

Before any decommissioning activities, create a comprehensive backup of the entire Sepio deployment:

**Prerequisites:**

- Ensure sufficient disk space: a minimum of 25% of the total Sepio data size in /opt/sepio/backup/
- Root access or sudo privileges
- For non-air-gapped deployments, set environment variables:
  bash
  ```
  export SEPIO_REGISTRY_URL=<value>
  export SEPIO_REGISTRY_USERNAME=<value>
  export SEPIO_REGISTRY_PASSWORD=<value>
  ```

**Backup Procedure:**

1. Verify disk space:
   bash
   ```
   df -h /opt/sepio/backup/
   ```
2. Execute backup command:
   bash
   ```
   sudo -E sepioctl backup
   ```

- For air-gapped customers:
  bash
  ```
  sudo -E sepioctl backup --air-gapped
  ```

3. Review the backup summary for any component failures or warnings
4. Store the backup file securely in an offsite location
5. Document the backup file timestamp and location

**Backup Contents Include:**

- Service configuration and metadata
- All system databases (cache, search, relational data)
- File storage and artifacts
- Persistent container data
- Application and service configuration files

**Reference:** Backup, Redundancy, and High Availability

#### Step 1.3: Export Reports and Queries (If Required)

- Export any custom queries and reports that may be needed for future reference
- Document any configured policies and risk management rules
- Export asset inventory lists, if needed, for handover to replacement solutions

## Phase 2: Component Decommissioning

#### Step 2.1: Uninstall Sepio Agents

Decommission agents from all managed hosts using the appropriate method for each operating system:

**Windows Hosts:**

- Navigate to **Control Panel** -> **Programs and Features**
- Select **Uninstall a program**
- Locate **SepioAgent**
- Click **Uninstall**
- Follow the uninstallation wizard

Note: Navigation paths may vary by Windows version

**Linux Hosts (Debian/Ubuntu):**

bash

```
sudo ./LinuxUninstallDeb.sh
```

Script located in: SepioFiles/Logs directory under the agent installation path.

**Linux Hosts (Red Hat/CentOS):**

bash

```
sudo ./LinuxUninstallRH.sh
```

Script located in: SepioFiles/Logs directory under the agent installation path.

**macOS Hosts:**

bash

```
sudo ./clean.sh
```

The clean.sh script is provided separately from the .pkg installation file

**Verification:**

- Confirm the Sepio Agent service is no longer running
- Verify agent files have been removed from installation directories
- Check that the host no longer appears in the Sepio Platform GUI

**Reference:** Installing and Uninstalling a Sepio Agent

**Step 2.2: Uninstall Scan Engines (External)**

Remove all external Scan Engines deployed in your environment:

**Windows Scan Engines:**

- Open **Control Panel** -> **Programs and Features**
- Select **Uninstall a program**
- Locate **NetpollerService**
- Select **Uninstall**
- Complete the uninstallation process

Note: Navigation paths may vary by Windows version

**Linux Scan Engines (Debian/Ubuntu):**

bash

```
sudo ./LinuxUninstallDeb.sh
```

**Linux Scan Engines (Red Hat/CentOS):**

bash

```
sudo ./LinuxUninstallRH.sh
```

Scripts located in: SepioFiles/Logs directory under the agent installation path.

**Verification:**

- Confirm NetpollerService is no longer running
- Verify the Scan Engine no longer appears in the Sepio GUI under **Settings** -> **Network Infrastructure** -> **Scan Engines**

**Reference:** Installing and Activating a Sepio Scan Engine

**Step 2.3: Remove Network Infrastructure Configurations**

Clean up network device configurations that were established for Sepio integration:

- **SNMP Access:** Remove SNMP community strings or SNMPv3 credentials configured for Sepio
- **SSH/Telnet Access:** Remove dedicated Sepio user accounts from network switches and devices
- **802.1X Integration:** Remove Sepio-specific RADIUS configurations if applicable
- **Firewall Rules:** Remove firewall rules allowing Sepio platform and Scan Engine communications:
  - Port 443 (HTTPS) from Agents to Platform Management
  - Port 22 (SSH), 161 (SNMP), 23 (Telnet) from Scan Engines to network devices

**Step 2.4: Decommission Sepio Platform Management Server**

**For Virtual Appliance Deployments:**

1. Stop all Sepio services:
   bash
   ```
   /opt/sepio/bin/sepioctl down
   ```
2. Verify all containers/services are stopped:
   bash
   ```
   docker ps
   #or for Podman deployments
   podman ps
   ```
3. For complete removal of the platform:
   - Power down the virtual appliance
   - Remove the VM from your virtualization platform
   - Delete associated storage volumes
   - Remove DNS entries pointing to the Sepio management server

**For Customer-Owned Hardware Deployments:**

1. Stop all Sepio services:
   bash
   ```
   /opt/sepio/bin/sepioctl down
   ```
2. Remove Sepio installation directories (after confirming backups are secure):
   bash
   ```
   # Backup location verification
   ls -lah /opt/sepio/backup/
   # Remove Sepio installation (exercise caution)
   sudo rm -rf /opt/sepio/
   ```
3. Remove Docker/Podman containers and images:
   bash
   ```
   docker system prune -a
   #or
   podman system prune -a
   ```
4. Clean up systemd services if configured for High Availability:
   bash
   ```
   sudo systemctl stop sepio-ha-scheduler
   sudo systemctl stop sepio-ha-monitor
   sudo systemctl disable sepio-ha-scheduler
   sudo systemctl disable sepio-ha-monitor
   sudo rm /etc/systemd/system/sepio-ha-*.service
   sudo systemctl daemon-reload
   ```

**Note:** The Sepio documentation does not provide a formal "sepioctl uninstall" command. The platform is designed to be removed by stopping services and deleting installation directories after proper backup.

## Phase 3: Integration and External System Cleanup

#### Step 3.1: Remove Third-Party Integrations

Disconnect and remove configurations for integrated systems:

1. **SIEM Integrations** (Splunk, QRadar, ArcSight, etc.)
   - Remove Sepio data source configurations
   - Disable CEF/Syslog forwarding rules

    - Archive or delete Sepio-related logs as per retention policy
2. **CMDB Integrations** (ServiceNow, etc.)
    - Disable Sepio integration application
    - Decide on handling of asset data previously synchronized from Sepio
    - Remove scheduled import jobs
3. **Network Access Control** (Cisco ISE, Forescout, etc.)
    - Remove Sepio connector applications
    - Disable policy enforcement rules dependent on Sepio data
4. **Cloud Security Platforms** (Palo Alto Cortex, Check Point, etc.)
    - Remove API integrations
    - Disable data sharing configurations
5. **Ticketing Systems** (Jira, ServiceNow, etc.)
    - Remove Sepio webhook configurations
    - Archive Sepio-generated tickets as needed

**Reference:** Integrations

#### Step 3.2: DNS and Network Cleanup

1. Remove or update DNS records pointing to Sepio management servers
2. Release any dedicated IP addresses
3. Update network documentation to reflect removal of Sepio infrastructure
4. Remove firewall rules specific to Sepio communications

## Phase 4: Verification and Final Steps

#### Step 4.1: Verification Checklist

Confirm complete decommissioning by verifying:

- All Sepio Agents have been uninstalled from managed hosts
- All Scan Engines have been removed
- Sepio Platform Management Server has been stopped/removed
- Backup files are securely stored and accessible
- Network device configurations have been cleaned up
- Third-party integrations have been disconnected
- DNS records have been updated or removed
- Firewall rules have been cleaned up
- No Sepio processes are running on any system
- Licensing information has been communicated to Sepio (if applicable)

#### Step 4.2: Documentation

Create decommissioning completion documentation including:

- Date of decommissioning completion
- Final backup file locations and timestamps
- List of all systems where components were removed
- Confirmation of data retention compliance
- Any issues encountered and their resolutions
- Archival location of exported data and reports

#### Step 4.3: License and Support

Contact Sepio support (support@sepiocyber.com or +1 240-660-8690) to:

- Notify them of the decommissioning
- Discuss license termination or transfer
- Close any open support cases
- Discuss options for retaining access to historical backup data if needed

## Important Notes and Best Practices

- **Data Retention:** Ensure backup files are retained according to your organization's data retention policies and compliance requirements. The backup TAR archive contains all necessary data for future restoration if needed.
- **Staged Approach:** Consider decommissioning in stages (e.g., pilot group of hosts first) to identify and resolve any issues before full-scale removal.
- **Rollback Capability:** Maintain the ability to restore from backup until you are certain the decommissioning is complete and no issues have been identified.
- **Coordination:** Coordinate decommissioning activities with:
  - Security operations team
  - Network operations team
  - Compliance team
  - IT asset management
  - Any teams using Sepio data for security monitoring
- **Timing:** Schedule decommissioning during a maintenance window to minimize impact on security monitoring capabilities.
- **Alternative Solutions:** Ensure replacement asset visibility and hardware security solutions are operational before fully decommissioning Sepio to avoid security monitoring gaps.

## Support and Additional Resources

For additional assistance during decommissioning:

- Sepio Support: support@sepiocyber.com
- Phone: +1 240-660-8690
- Docs: https://docs.sepiocyber.com
- Website: https://sepiocyber.com

**Key Documentation References:**

- Installing and Uninstalling a Sepio Agent
- Installing and Activating a Sepio Scan Engine
- Backup, Redundancy, and High Availability
- Data Extractions
- SepioCTL Command Reference

# Platform Requirements

The preferred deployment mode for the Sepio Platform is SaaS. Customers that are required by internal regulations or compliance mandates to run from their own premises (on-premise) can install and manage Sepio.

> **Note:** Please contact support@sepiocyber.com for additional information.

## Permissions

The installation script requires administrator permissions. You should have the ability to install as root / use sudo for Linux platforms and have Administrator permissions for Windows.

## Connectivity and Firewall

The Architecture section lists the different components and connectivity. In general, all communication uses Transport Layer Security (TLS) and unless specifically mentioned, uses port 443.

## Platform Management

The following are the minimum platform requirements.

**Platform Management Hardware**

| Item | Minimum Requirement | Comments |
|---|---|---|
| CPU | Intel® Xeon® Silver 4214R Processor or higher, 12 Cores, 2.6GHz | More cores or more advanced models are supported |
| Memory | 32GB RAM | – |
| Minimum System Disk | 256 GB | SSD |
| Storage | 1 TB | SSD RAID 1 configuration (2 disks) |
| Network | 2 x Gigabit Ethernet NICs | – |

### For Large-Scale Network Environments

For very large network environments with thousands of switches and hundreds of thousands of connected ports the following hardware guidelines should be used:

| Item | Minimum Requirement | Comments |
|---|---|---|
| CPU | Intel® Xeon® Silver 4214R Processor or higher, 16 Cores, 2.6GHz | More cores or more advanced models are supported |
| Memory | 64 GB RAM | – |
| Minimum System Disk | 512 GB | SSD |
| Storage | 2 TB | SSD RAID 1 configuration (2x1TB disks) |
| Network | 2 x Gigabit Ethernet NICs | – |

### Platform Management Software

| OS | Minimum Requirement | Comments |
|---|---|---|
| Red Hat Linux | Enterprise 7, 8, 9 | – |
| Ubuntu | 22.04 LTS, 20.04 LTS | – |
| Amazon Linux | 2 | AWS deployments. Recommended instance: t3.2xlarge |

### Docker Ecosystem Components

| Component | Version |
|---|---|
| Docker Engine – Server | 28.1.1 |
| Docker Engine – Client | 28.1.1 |
| Docker Compose | 2.35.1 |

## Cloud Environments

You can install and run the Sepio Platform from any cloud environment that allows you to run and manage the supported operating systems. Such cloud environments include AWS, Azure, GCP and OCI.

## User Interface (UI)

For monitoring purposes (view-only access) of the Sepio Platform.
There are no hardware requirements for this functionality. The system can be monitored from any device, including smartphones, tablets, and more, using a standard web browser.

| Item | Minimum Requirement | Comments |
|---|---|---|
| Browser | Latest versions of Chromium based browsers | – |

## Host with a Sepio Agent

> **Note:** Please see the list of Supported Operating Systems for Sepio Host Agent.

The following requirements apply to all Sepio Agent deployment modes:

- **Windows service** – Sepio Agent runs as a Windows service on a Host.
- **Agentless** – This is a Management Server operation that installs agent code on a Host, not as a service, but as a Windows process.
- **Session** – A customer-installed script that runs the agent code on a Host without utilizing CPU resources.

### Host with a Sepio Agent Hardware

| Item | Minimum Requirement | Comments |
|---|---|---|
| CPU | Dual core CPU / Core i3 and above or similar AMD | – |
| Memory | 4GB RAM | – |
| Free Disk Space | 200 MB | – |

### Host with a Sepio Agent Software

#### Linux Agent Dependencies

The following dependencies are also listed in the **Dependencies.txt** file included in the agent installation package:

- **cpuid** – It is required to detect the processor id (Download link).
- **dmidecode** – Required to detect the motherboard serial and PC model fields.
- **hhdparm** – Required to detect the disk ID.
- **lshw** – Required to detect the Network Interface Cards.
- **yum-utils** – Required for Red Hat 7.9.
- **lttng-ust** – Required for Red Hat 7.9.

#### Windows

| Item | Minimum Requirement | Comments |
|---|---|---|
| Microsoft .NET framework | Version 4.7 | – |

## Scan Engine (External)

#### Scan Engine Hardware

| Item | Minimum Requirement | Comments |
|---|---|---|
| CPU | 4 CPU or vCPU | – |
| Memory | 16GB RAM | – |
| Free Disk Space | 50GB | – |

**Note:** For scanning 5,000 or more switches, ensure your disk has a minimum capacity of 128 GB.

#### Scan Engine Software

| OS | Supported version | Comments |
|---|---|---|
| Windows | • Windows 10, 11<br>• Windows Server 2019, 2022 | .NET 8 is required starting from Sepio Platform version 17.2503.508 and Scan Engine version 17.2503.20. |
| Red Hat Linux | Enterprise 8 | – |
| Ubuntu | 20.04, 22.04 | – |

| OS | Supported version | Comments |
| --- | --- | --- |
| Amazon Linux | 2 | AWS deployments. Recommended instance: t3.xlarge |

**Note:** If .NET 8 is missing or not installed, the Windows installation process may fail with permission-related error messages.

# Installation

## Overview

There are several methods to install the Sepio platform, depending on the desired architecture and customer's requirements. While the preferred and easiest method is to use the Sepio cloud, there are additional options for customers that are required to run inside their own data center or in a completely isolated, air-gapped environment.

Sepio supports the following deployment methods in addition to Sepio cloud SaaS.

| Installation method | Operating system | Installation & deployment flexibility |
|---|---|---|
| Virtual appliance – OVF | Sepio virtual appliance based on Ubuntu | N/A |
| Online, requires connectivity to the internet | Ubuntu | Yes |
| Online, requires connectivity to the internet | Redhat Enterprise Linux | Yes. Using Podman. Requires RHEL subscription |
| Offline or air-gapped. There is limited or even no connectivity to external networks | Ubuntu | Yes |
| Offline or air-gapped. There is limited or even no connectivity to external networks | Redhat Enterprise Linux | Yes. Using Podman. Requires RHEL subscription |

**Note:** Installations are performed using the SepioCTL.

## Related Topics

- SepioCTL
- Before Installing Sepio
- Installing Sepio on a Virtual Appliance
- Installing Sepio on Customer Owned Hardware and Software
- Installing and Uninstalling a Sepio Agent
- Installing Sepio Agent for VDI
- Installing for Session Based and Agentless Modes
- Audit Mode

- Installing and Activating a Sepio Scan Engine
- High Performance Deployment

# Artifact Signature Verification

## Overview

To ensure the integrity and authenticity of Sepio artifacts, we utilize Cosign (part of the Sigstore project) for digital signatures. This process allows you to verify that the SepioCTL binary has not been tampered with and was indeed produced by Sepio.

## Prerequisites

Before beginning the verification process, ensure the following requirements are met:

- **Cosign Installed:** You must have Cosign installed on your local machine. You can find installation instructions via the Sigstore Documentation or download specific binaries from the Cosign Releases page.
- **Verification Bundle:** Download the appropriate bundle for your system from the Sepio Download Center:
  - sepioctl-ubuntu.bundle (for Ubuntu/Debian-based systems)
  - sepioctl-rhel.bundle (for RHEL/CentOS-based systems)
- **Binary File:** Ensure that the corresponding SepioCTL binary is in the same working directory as the bundle.

## Verification Procedures

The following commands use **online verification**, which requires an active internet connection to reach the Sigstore transparency log.

### Linux Systems

Execute the following commands in your terminal based on your distribution:

#### Ubuntu (Default)

Bash

```
cosign verify-blob sepioctl-ubuntu \
 --bundle sepioctl-ubuntu.bundle \
 --certificate-identity-regexp 'https://github\.com/SepioCyber/' \
 --certificate-oidc-issuer 'https://token.actions.githubusercontent.com'
```

#### Red Hat (RHEL)

Bash

```
cosign verify-blob sepioctl-rhel \
 --bundle sepioctl-rhel.bundle \
 --certificate-identity-regexp 'https://github\.com/SepioCyber/' \
 --certificate-oidc-issuer 'https://token.actions.githubusercontent.com'
```

#### Windows Systems

Using Command Prompt (CMD) or PowerShell, run the following (ensure the cosign executable name matches your downloaded version):

#### Ubuntu Artifacts

PowerShell

```
.\cosign-windows-amd64.exe verify-blob sepioctl-ubuntu --bundle sepioctl-ubuntu.bundle --
certificate-identity-regexp "https://github\.com/SepioCyber/.*" --certificate-oidc-
issuer "https://token.actions.githubusercontent.com"
```

#### Red Hat Artifacts

PowerShell

```
.\cosign-windows-amd64.exe verify-blob sepioctl-rhel --bundle sepioctl-rhel.bundle --
certificate-identity-regexp "https://github\.com/SepioCyber/.*" --certificate-oidc-
issuer "https://token.actions.githubusercontent.com"
```

## Troubleshooting

If the verification is successful, the output will confirm **Verified OK**. If you receive any other message, please perform the following checks:

1. **Connectivity:** Confirm you have an active internet connection to reach the Sigstore infrastructure.
2. **File Location:** Ensure both the binary and the .bundle file are located in your current working directory.
3. **Filenames:** Verify that the filenames used in your command string exactly match the files saved on your disk.

# SepioCTL

## Overview

Sepio command line interface, SepioCTL, is a tool that installs Sepio's platform on a server. It is designed to support all the deployment methods and is generated for each version of Sepio Platform. It is important to verify that you are using the same version of SepioCTL for a target release.

## Usage

$ sepioctl COMMAND ...

## Options

- `--install-completion`: Install completion for the current shell.
- `--show-completion`: Show completion for the current shell, to copy it or customize the installation.
- `--help`: Show this message and exit.

## Commands

- `airgapped`
- `compose`
- `download`
- `generate`
- `install`
- `update`
- `upload`
- `version`: Print version.

Please refer to the online help for specific explanations and arguments.

## Prerequisites for Customers Using RHEL

1. Test if `/tmp` allows executables

   ```
   echo -e '#!/bin/bash\necho OK' > /tmp/test.sh
   chmod +x /tmp/test.sh
   /tmp/test.sh
   ```

   - If you see `OK` `/tmp` works fine, no further action is needed.
   - If you see `Permission denied`, your system blocks executables in `/tmp`. **Continue with the next steps.**

2. Create an alternative temp folder

   ```
   sudo mkdir -p /opt/tmp
   sudo chmod 1777 /opt/tmp
   ```

   This makes `/opt/tmp` safe for temporary files and executables.
3. Run `sepioctl` with the alternative temp folder:

   Before running `sepioctl`, export the temp directory:

   ```
   export TMPDIR=/opt/tmp
   sepioctl version
   ```

   This ensures sepioctl uses /opt/tmp instead of /tmp.
4. (Recommended but not mandatory) Make the TMPDIR path permanent for future installations:

   **For a regular user**

   Add the export command to your shell config:

   ```
   echo 'export TMPDIR=/opt/tmp' >> ~/.bashrc
   ```

   If you use Zsh instead of Bash:

   ```
   echo 'export TMPDIR=/opt/tmp' >> ~/.zshrc
   ```

   Then reload your shell or log in again.

   **For sudo use cases**

   Add the same line to root's profile:

   ```
   sudo sh -c 'echo "export TMPDIR=/opt/tmp" >> /root/.bashrc'
   ```

**Note:** For both installation modes contact Sepio support for assistance.

## Before Installing Sepio

You can install the Sepio Platform using different deployment options using a variety of operating systems to support your business requirements. Before starting, you should verify the following:

- You have the relevant installation files according to your target deployment model.
- You have the necessary credentials and permissions.
- Network configuration is completed.

See the complete list of prerequisites in the “Platform Requirements” section.

# Installing Sepio on a Virtual Appliance

This topic provides a step-by-step procedure on how to install and deploy Sepio on a virtual appliance. An Open Virtualization Format (OVF) file is provided for use as a virtual appliance in VMware environments. You can use a pre-installed hardened virtual appliance and import it to any VMware virtual environment.

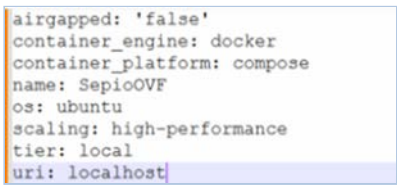
## Step 1: Import a Virtual Machine

1. Import the OVF and VMDK files provided by Sepio into the virtual environment. The default credentials for the virtual machine are:
   **Username**: hac1admin
   **Password**: Sep!oSyst5ms
2. Change the default account credentials after installation is complete.

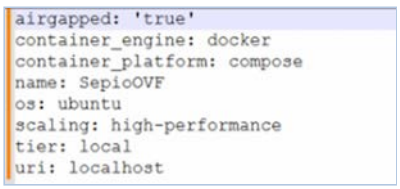
## Step 2: Setting the System for Air-Gapped Environment

To use Sepio in an on-prem environment, you must modify the system's basic configuration file.

1. Using your preferred text editor, open the 'config.yml' file for editing.




2. Change the parameter 'airgapped' from 'false' to 'true'.



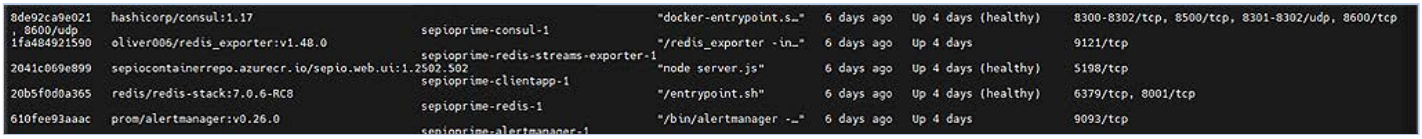

## Step 3: Using sepioctl

Actions like shutting down, starting up, or upgrading the system are performed using the sepioctl executable.

1. The sepioctl executable is located in '/opt/sepio/bin'.
2. To stop the system, use the command '`./sepioctl down`'.
3. To start the system, use the command '`./sepioctl up`'.

## Step 4: Checking System Health

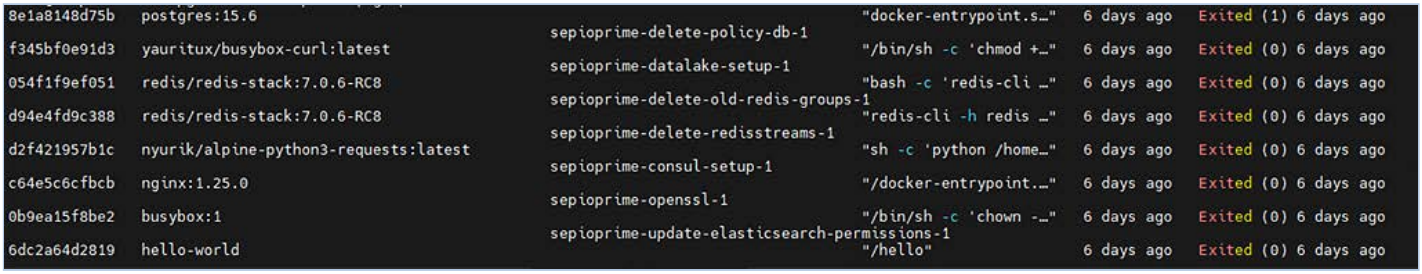
1. After successfully deploying the VM, you can check the system health by running the command ‘`docker ps -a`’.
2. All listed containers should be in ‘up’ or ‘healthy’ state.



| | | | | | | |
|---|---|---|---|---|---|---|
| 8de92ca9e021 | hashicorp/consul:1.17 | sepioprime-consul-1 | "docker-entrypoint.s…" | 6 days ago | Up 4 days (healthy) | 8300-8302/tcp, 8500/tcp, 8301-8302/udp, 8600/tcp, 8600/udp |
| 1fa484921590 | oliver006/redis_exporter:v1.48.0 | sepioprime-redis-streams-exporter-1 | "/redis_exporter -in…" | 6 days ago | Up 4 days | 9121/tcp |
| 2041c069e899 | sepiocontainerrepo.azurecr.io/sepio.web.ui:1.2502.502 | sepioprime-clientapp-1 | "node server.js" | 6 days ago | Up 4 days (healthy) | 5198/tcp |
| 20b5f0d0a365 | redis/redis-stack:7.0.6-RC8 | sepioprime-redis-1 | "/entrypoint.sh" | 6 days ago | Up 4 days (healthy) | 6379/tcp, 8001/tcp |
| 610fee93aaac | prom/alertmanager:v0.26.0 | sepioprime-alertmanager-1 | "/bin/alertmanager -…" | 6 days ago | Up 4 days | 9093/tcp |

Healthy state

3. Some containers are used only during system setup or startup; they may appear as ‘Exited’ with an exit code of 0 or 1.



| | | | | | |
|---|---|---|---|---|---|
| 8e1a8148d75b | postgres:15.6 | sepioprime-delete-policy-db-1 | "docker-entrypoint.s…" | 6 days ago | Exited (1) 6 days ago |
| f345bf0e91d3 | yauritux/busybox-curl:latest | sepioprime-datalake-setup-1 | "/bin/sh -c 'chmod +…" | 6 days ago | Exited (0) 6 days ago |
| 054f1f9ef051 | redis/redis-stack:7.0.6-RC8 | sepioprime-delete-old-redis-groups-1 | "bash -c 'redis-cli …" | 6 days ago | Exited (0) 6 days ago |
| d94e4fd9c388 | redis/redis-stack:7.0.6-RC8 | sepioprime-delete-redisstreams-1 | "redis-cli -h redis …" | 6 days ago | Exited (0) 6 days ago |
| d2f421957b1c | nyurik/alpine-python3-requests:latest | sepioprime-consul-setup-1 | "sh -c 'python /home…" | 6 days ago | Exited (0) 6 days ago |
| c64e5c6cfbcb | nginx:1.25.0 | sepioprime-openssl-1 | "/docker-entrypoint.…" | 6 days ago | Exited (0) 6 days ago |
| 0b9ea15f8be2 | busybox:1 | sepioprime-update-elasticsearch-permissions-1 | "/bin/sh -c 'chown -…" | 6 days ago | Exited (0) 6 days ago |
| 6dc2a64d2819 | hello-world | | "/hello" | 6 days ago | Exited (0) 6 days ago |

Exited containers

# Installing Sepio on Customer-Owned Hardware

When required by regulatory or compliance mandates, the Sepio Platform can be installed on customer-owned, on-premises hardware with or without internet connectivity, including air-gapped environments.

There are two primary installation modes suitable for on-premises deployments:

- Online Installation
- Offline Installation

## Online Installation

- Suitable when the Platform Management has an active internet connection.
- All installation files can be downloaded and installed automatically.

#### Prerequisites for Docker-Based Installations (Ubuntu)

Before proceeding with online or offline installation using Docker, ensure Docker Engine and Docker Compose are installed on your Ubuntu system.

- **Docker Engine:** Follow the official Docker documentation to install Docker Engine on Ubuntu. After installation, start the Docker service:
  `sudo systemctl start docker`
- **Docker Compose:** Follow the official Docker Compose installation guide for Linux to install the standalone binary.
  Download the binary with:
  `sudo curl -L "https://github.com/docker/compose/releases/latest/download/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose`
  Make it executable with:
  `sudo chmod +x /usr/local/bin/docker-compose`
  Verify the installation with:
  `docker-compose version`
  Verify Docker is running:
  `docker version`
  To allow your user to run Docker commands without `sudo`, add the user to the Docker group:
  `sudo usermod -aG docker $USER`

## Offline Installation

- Suitable when the Platform Management has an no active internet connection.
- Installation requirements:

    - All required installation files are provided by Sepio and uploaded manually to the Platform Management server.
    - Installation is performed using SepioCTL.
- Infrastructure dependencies:
    - **Ubuntu**: Docker Engine and Docker Compose
    - **Red Hat Enterprise Linux (RHEL)**: Podman and Podman Compose

## Offline Installation Using Docker for Ubuntu

#### Docker – Step 1: Import Installation Files

Copy the files provided by Sepio to your server using a secure transfer method. Typically, Sepio will provide:

- Installation file: `offline_installation_17.2502.613.tar.gz`
- Installer application: `sepioctl`

#### Docker – Step 2: Create Installation Folders

For a new installation, create the following folders inside /opt:

- /opt
    - /sepio
    - /sepio/bin
    - /sepio/offline
    - /sepio/offline/(version to be installed)

For example:

```
root@sepio-test:/home/hac1admin# cd /opt/
root@sepio-test:/opt# ls -l
total 0
root@sepio-test:/opt# mkdir sepio
root@sepio-test:/opt# cd sepio/
root@sepio-test:/opt/sepio# mkdir bin
root@sepio-test:/opt/sepio# mkdir offline
```

When upgrading an existing installation, create a new subfolder with the version number.

For example:

```
root@sepio-test:/opt/sepio# cd offline/
root@sepio-test:/opt/sepio/offline# mkdir 17.2502.613
```

### Docker – Step 3: Place the Installation Files

Moving **sepioctl** to its location.

```
root@sepio-test:/home/hac1admin#mv sepioctl /opt/sepio/bin/sepioctl
```

Move **offline_installation_17.2502.613.tar.gz** to its location:

```
root@sepio-test:/home/hac1admin#mv offline_installation_17.2502.613.tar.gz
/opt/sepio/offline/17.2502.613/
```

### Docker – Step 4: Installing/Upgrading Sepio Platform

> **Note:** Assuming Docker and Docker Compose are installed per the prerequisites section above, proceed with the following steps.

**Set executable permissions for sepioctl:**

```
root@hac1admin:/opt/sepio/bin#chmod +x sepioctl
```

**Extract the installation files:**

```
root@hac1admin:/opt/sepio/bin#./sepioctl airgapped extract-tar --force
```

**Load Docker images:**

```
root@hac1admin:/opt/sepio/bin# ./sepioctl airgapped load-images
```

**Stop the system before activating the new version:**

```
root@hac1admin:/opt/sepio/bin# ./sepioctl down
```

**Verifying airgapped is configured to True**

To use the system in an on-premises environment, we need to modify the system's basic configuration file. Open the config file using your preferred editor:

```
/opt/sepio/config/17.2502.613/config.yml
```

```
airgapped: 'false'
container_engine: docker
container_platform: compose
name: SepioOVF
os: ubuntu
scaling: high-performance
tier: prod
uri: localhost
```

config.yml

Change the parameter 'airgapped' from 'false' to 'true'.

```
airgapped: 'true'
container_engine: docker
container_platform: compose
name: SepioOVF
os: ubuntu
scaling: high-performance
tier: prod
uri: localhost
```

config.yml

**Start the system with the new version:**

```
root@hac1admin:/opt/sepio/bin# ./sepioctl up
```

### Docker – Step 5: Checking System Health

Check the status of Docker containers:

```
docker ps -a
```

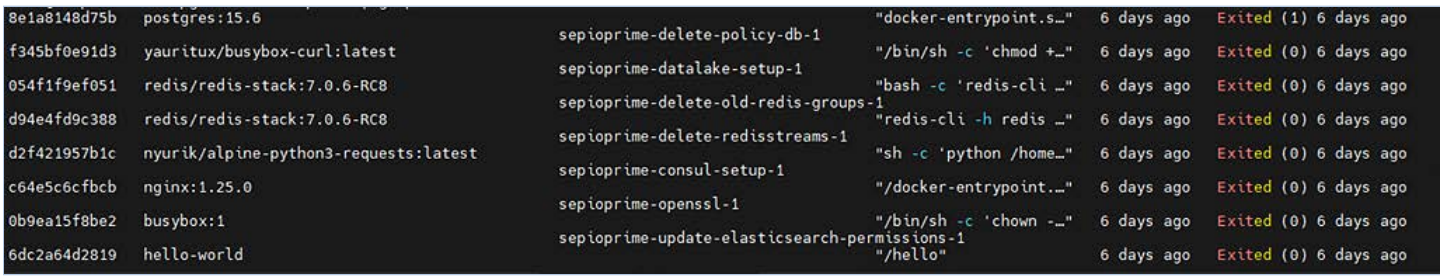
All listed containers should be in ‘up’ or ‘healthy’ state.



| | | | | | | |
|---|---|---|---|---|---|---|
| 8de92ca9e021 | hashicorp/consul:1.17 | sepioprime-consul-1 | "docker-entrypoint.s…" | 6 days ago | Up 4 days (healthy) | 8300-8302/tcp, 8500/tcp, 8301-8302/udp, 8600/tcp, 8600/udp |
| 1fa484921590 | oliver006/redis_exporter:v1.48.0 | sepioprime-redis-streams-exporter-1 | "/redis_exporter -in…" | 6 days ago | Up 4 days | 9121/tcp |
| 2041c069e899 | sepiocontainerrepo.azurecr.io/sepio.web.ui:1.2502.502 | sepioprime-clientapp-1 | "node server.js" | 6 days ago | Up 4 days (healthy) | 5198/tcp |
| 20b5f0d0a365 | redis/redis-stack:7.0.6-RC8 | sepioprime-redis-1 | "/entrypoint.sh" | 6 days ago | Up 4 days (healthy) | 6379/tcp, 8001/tcp |
| 610fee93aaac | prom/alertmanager:v0.26.0 | sepioprime-alertmanager-1 | "/bin/alertmanager -…" | 6 days ago | Up 4 days | 9093/tcp |

Healthy state

Some containers are used only during system setup or startup; they may appear as ‘Exited’ with an exit code of 0 or 1. This is normal.



| | | | | | |
|---|---|---|---|---|---|
| 8e1a8148d75b | postgres:15.6 | sepioprime-delete-policy-db-1 | "docker-entrypoint.s…" | 6 days ago | Exited (1) 6 days ago |
| f345bf0e91d3 | yauritux/busybox-curl:latest | sepioprime-datalake-setup-1 | "/bin/sh -c 'chmod +…" | 6 days ago | Exited (0) 6 days ago |
| 054f1f9ef051 | redis/redis-stack:7.0.6-RC8 | sepioprime-delete-old-redis-groups-1 | "bash -c 'redis-cli …" | 6 days ago | Exited (0) 6 days ago |
| d94e4fd9c388 | redis/redis-stack:7.0.6-RC8 | sepioprime-delete-redisstreams-1 | "redis-cli -h redis …" | 6 days ago | Exited (0) 6 days ago |
| d2f421957b1c | nyurik/alpine-python3-requests:latest | sepioprime-consul-setup-1 | "sh -c 'python /home…" | 6 days ago | Exited (0) 6 days ago |
| c64e5c6cfbcb | nginx:1.25.0 | sepioprime-openssl-1 | "/docker-entrypoint.…" | 6 days ago | Exited (0) 6 days ago |
| 0b9ea15f8be2 | busybox:1 | sepioprime-update-elasticsearch-permissions-1 | "/bin/sh -c 'chown -…" | 6 days ago | Exited (0) 6 days ago |
| 6dc2a64d2819 | hello-world | | "/hello" | 6 days ago | Exited (0) 6 days ago |

Exited containers

### Docker – Step 6: Import Root Certificate

Copy root certificate to Sepio instance in the user home folder.

Copy the certificates into the Sepio docker containers:

```
sudo docker cp server.key sepioprime-rproxy-1:/etc/nginx/cert/server.key
```

```
sudo docker cp server.pem sepioprime-rproxy-1:/etc/nginx/cert/server.pem
```

Update the permissions of the certificate files:

```
sudo docker exec --user root sepioprime-rproxy-1 chmod 644 /etc/nginx/cert/server.key
```

```
sudo docker exec --user root sepioprime-rproxy-1 chmod 644 /etc/nginx/cert/server.pem
```

Update the owner of the certificate files:

```
sudo docker exec --user root sepioprime-rproxy-1 chown root:root /etc/nginx/cert/server.key
```

```
sudo docker exec --user root sepioprime-rproxy-1 chown root:root /etc/nginx/cert/server.pem
```

Update the folder permissions:

```
sudo docker exec --user root sepioprime-rproxy-1 chmod 755 /etc/nginx/cert
```

Reload the docker container for the new certificates to take effect:

```
sudo docker exec sepioprime-rproxy-1 nginx -s reload
```

## Offline Installation Using Podman for RedHat Enterprise Linux (RHEL)

#### Podman – Step 1: Import Installation Files

Copy the files provided by Sepio to your server using a secure transfer method of your choice. Sepio will provide the installation file and the installer application. For example: `offline_installation_17.2506.603.tar.gz, install_rpms.sh` and `offline-dependencies-repo.tgz`.

#### Podman – Step 2: Create Installation Folders

For a new installation, create the following folders inside /opt:

- /opt
  - /sepio
  - /sepio/config

For example:

```
root@sepio-test:/home/hac1admin# cd /opt/
root@sepio-test:/opt# ls -l
total 0
root@sepio-test:/opt# mkdir sepio
root@sepio-test:/opt# cd sepio/
root@sepio-test:/opt/sepio# mkdir config
```

### Podman – Step 3: Place the Installation Files

The files that were transferred to the server in Step 1 should be moved to the `/opt/sepio/config` folder.

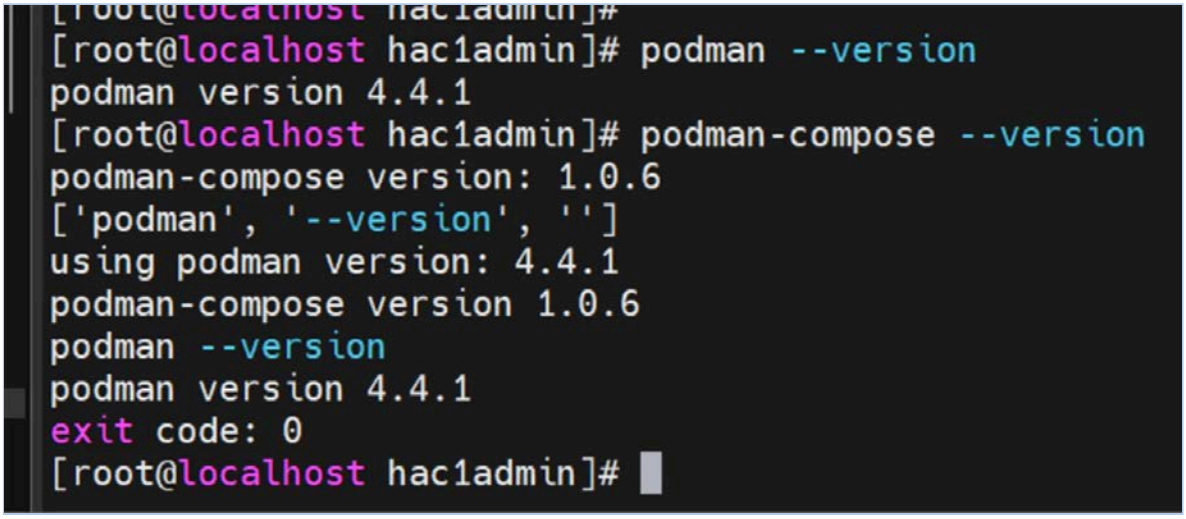
### Podman – Step 4: Installing Podman and Podman Compose

The provided `install_rpms.sh` script will install Podman and Podman Compose with all the necessary dependencies.

**Run the script:**

```
install_rpms.sh
```

Upon successful installation, you should see that Podman and Podman Compose are installed.




Podman and Podman Compose installation

Alternatively, if the provided `install_rpms.sh` script fails or for manual setup, install Podman and Podman Compose directly on RHEL:

• **For Podman:** Use the official Red Hat guide: Installing Podman

Enable the container-tools module:

```
sudo dnf module enable container-tools
```

Install Podman:

```
sudo dnf install podman
```

• **For Podman Compose:** Follow the Podman Compose GitHub guide. You can install via pip:

```
sudo pip3 install podman-compose
```

Or install from source if preferred. Ensure Podman is configured as a **rootless user** for security.

**Verify the installation:**

```
podman --version
```

```
podman-compose --version
```

Proceed with the script if provided, or use these manual steps for custom environments.

### Podman – Step 5: Installing Sepio Platform

- While in `opt/sepio/bin` extract the installation package. For example:
  `tar -zxvf offline_installation_17.2506.603.tar.gz`
- Load container images:
  `podman load –input images_tar`
- Start the platform:
  `cd 17.2506.603/compose/`
  `vi restart_podman.sh`

> **Note:** SepioCTL can be used depending on previous installations or upgrades. Consult with Sepio Customer Success if SepioCTL should be used.

Comment out (with `#`) the two lines that use `sepioctl`.

```
# If using sepioctl
/opt/sepio/bin/sepioctl compose down
/opt/sepio/bin/sepioctl compose up --airgapped
```

Comment the two lines used by sepioctl

Uncomment the last three lines if SepioCTL is not used.

```
# If not using sepioctl
# cd /opt/sepio/config/17.2501.609 || exit 1
# /usr/bin/podman-compose -p sepioprime down -t 0
# /usr/bin/podman-compose --in-pod 1 -p sepioprime up -d
~
```

Uncomment the last three lines if SepioCTL is not used

Rename `docker-compose.yml` to prevent Podman from executing it automatically.

```
-rw-r--r--. 1 1001 root 28849 May 13 05:23 config.json
-rw-r--r--. 1 root root   420 May 13 05:23 consul.json
drwxr-xr-x. 2 root root  4096 May 13 05:23 dashboards
-rw-r--r--. 1 root root   208 May 13 05:23 dashboard.yml
-rw-r--r--. 1 root root  1085 May 13 05:23 datasource_prom.yml
-rw-r--r--. 1 root root 49353 May 13 05:23 docker-compose.old
-rw-r--r--. 1 root root  3580 May 13 05:23 elastic-certificates.p12
-rw-r--r--. 1 root root  1494 May 13 05:23 fluent_bit.docker.conf
-rw-r--r--. 1 root root  2041 May 13 05:23 fluent_bit.podman.conf
```

Rename the docker-compose.yml file

**Run Podman Compose:**

```
podman-compose --in-pod 1 -p sepioprime up -d
```

Once the process is complete, verify that the containers are up and healthy:

```
podman ps -a
```

```
[root@localhost hac1admin]# podman ps -a
CONTAINER ID  IMAGE                                                                                COMMAND               CREATED
 STATUS                   PORTS                                                                       NAMES
acc37bdbe22c  localhost/prom/alertmanager:v0.26.0                                                   --config.file=/et...  4 days ago
 Up 4 days                                                                                           sepioprime_alertmanager_1
85f7a6a0c4a8  localhost/willfarrell/autoheal:1.2.0                                                 autoheal              4 days ago
 Up 4 minutes (healthy)                                                                              sepioprime_autoheal_1
dd6c46f142d2  gcr.io/cadvisor/cadvisor:v0.47.2                                                     --housekeeping_in...  4 days ago
 Up 4 days (healthy)      0.0.0.0:8080->8080/tcp                                                     sepioprime_cadvisor_1
f5a8b6731bad  sepiocontainerrepo.azurecr.io/sepio.web.ui:1.2504.8                                                      4 days ago
 Up 4 days (healthy)      0.0.0.0:5198->5198/tcp                                                     sepioprime_clientapp_1
2059ac6e21fa  localhost/hashicorp/consul:1.17                                                       consul agent -con...  4 days ago
 Up 4 days (healthy)      0.0.0.0:8500->8500/tcp                                                     sepioprime_consul_1
8b2ea610e0ed  quay.io/minio/minio:RELEASE.2023-08-31T15-31-16Z.fips                                server /data --co...  4 days ago
 Up 4 days (healthy)      0.0.0.0:9000-9001->9000-9001/tcp                                           sepioprime_datalake_1
58ada526e609  localhost/fluent/fluent-bit:3.1.3                                                    /fluent-bit/bin/f...  4 days ago
```

Verify that the containers are up and healthy

Some containers are only used during system setup or startup. These may appear as `Exited` with an exit code of `0` or `1`.

```
[root@localhost hac1admin]# podman ps -a | grep Exit
30350da80503  localhost/nginx:1.25.0                                                                bash -c if [ -e /...  4 days ago  Exited (0) 4 days ago
              sepioprime_openssl_1
07675e57c9a5  localhost/busybox:1                                                                   /bin/sh -c chown ...  4 days ago  Exited (0) 4 days ago
              sepioprime_update-elasticsearch-permissions_1
f01af7ac4760  localhost/nyurik/alpine-python3-requests:latest                                       sh -c python /hom...  4 days ago  Exited (0) 4 days ago
              sepioprime_consul-setup_1
151934ef7478  localhost/yauritux/busybox-curl:latest                                                /bin/sh -c chmod ...  4 days ago  Exited (0) 4 days ago
              sepioprime_datalake-setup_1
0183c5de28a6  localhost/redis/redis-stack:7.0.6-RC8                                                 bash -c redis-cli...  4 days ago  Exited (0) 4 days ago
              sepioprime_delete-old-redis-groups_1
81695f22006e  localhost/postgres:15.6                                                               dropdb SepioPolic...  4 days ago  Exited (1) 4 days ago
              sepioprime_delete-policy-db_1
c31d031c92aa  localhost/redis/redis-stack:7.0.6-RC8                                                 redis-cli -h redi...  4 days ago  Exited (0) 4 days ago
              sepioprime_delete-redisstreams_1
[root@localhost hac1admin]#
```

Some containers are used only during system setup or startup

**Podman – Step 6: Adding Startup Command**

To ensure the platform starts automatically after a power down or reboot, add a cron job to the system.

Run the command:

```
crontab -e
```

Then add the following line:

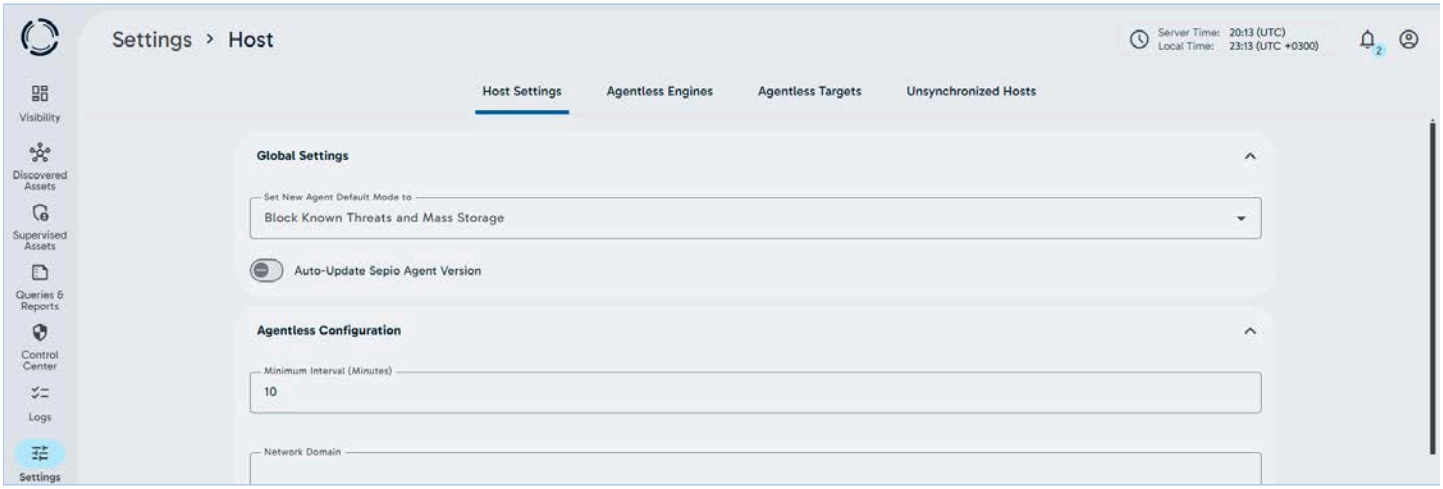
```
@reboot /opt/sepio/config/17.2506.603/compose/restart_podman.sh
```

**Note:** For both installation modes contact Customer support for assistance.

## Reinstalling and Reimaging a Host with Sepio Agent

Reimaging or reinstalling employee computers is a common practice in enterprise environments to maintain data security, compliance, and overall system integrity. Main reasons and use cases include transfer of ownership, improving security posture by creating a new baseline and cleanup of files that might have been copied or left locally.

When reimaging or reinstalling the Agent, one should remember that the default mode is set for new Agents (see Settings -> Host).




The Host Settings screen for configuring the new Agent default mode.

Hosts with previously installed Agents, either those that were reimaged or have a new agent installed are not considered “new” and as such will have the default installation mode which is “free”. This behavior is since the Agent’s identity is determined by the UUID.

> **Note:** changing the hostname will not change the host’s UUID

To ensure the Sepio Management Platform treats reimaged or reinstalled employee computers as new hosts, the Sepio Administrator should delete the Host from the Sepio Management Platform before connecting the new host to the Sepio Management Platform.

The following table describes the different options when reimaging or reinstalling a host.

| Current state | Desired state | Steps to be taken | Outcome |
|---|---|---|---|
| Sepio Agent was never installed. (New host) | Install a new agent and have the default installation mode set. | 1. Set the default installation mode.<br>2. Install the Sepio Agent, configure management FQDN. | A new agent will be associated with the Sepio Management Platform. Default mode for new hosts will be used. The Agent's UUID is created based on the host's hardware. |
| Host with Sepio Agent installed | Upgrade to a new Sepio Agent version and maintain the current Agent mode. | Upgrade the Sepio Agent using any of the supported methods. | The Agent will be upgraded. The previously defined mode that can be defined for every agent separately will be preserved. |
| Host with Sepio Agent installed | Reimage the host or reinstall the agent and set it to the default Agent mode. | 1. Uninstall the Sepio Agent from the host.<br>2. When the agent becomes offline, delete it from the Sepio Management UI.<br>3. Reimage the host or reinstall the Agent. | A new agent will be associated with the Sepio Management Platform. Since the Agent's UUID is created based on the host's hardware, this new Agent will have the same UUID as the previously used agent. "The new agent default mode" will be used. |
| Host with Sepio Agent installed | Reimage the host or reinstall the agent and set it to FREE Agent mode. | Reimage the host or reinstall the Agent. | An agent will be associated with the Sepio Management Platform. It will have the same hardware based UUID but will not be considered "new" and thus the default mode for new Agents will not apply. |

# Installing and Uninstalling a Sepio Agent

This topic explains how to install and uninstall a Sepio Agent on a host. A Sepio Agent serves as the security component that offers comprehensive visibility and enables policy enforcement for assets integrated into a host and connected to it. The Platform Management remotely manages the Sepio Agent.

## Preparing for Installation

You can install Sepio Agent in one of two ways:

- Locally on each user's computer as a standalone installation.
- Using a network deployment tool compatible with MSI installation packages (e.g., Microsoft Endpoint Configuration Manager).

Typically, the local installation is simpler and easier to deploy for a single computer or a small network. However, larger-scale networks that use centralized management and administration tools usually use network installation to pre-configure some setup parameters.

> **Note:** For a list of Agent system requirements, go to Platform Requirements.

## Firewall Configuration

Sepio Agent uses HTTPS for communication between Sepio Agent and the Platform Management. We recommend using the standard port 443. Ensure port 443 is allowed on Windows by adding it to Windows Firewall, and on Linux by configuring your firewall (e.g., iptables, firewalld, or ufw).

> **Note:** If using any port other than 443, contact Sepio Support.

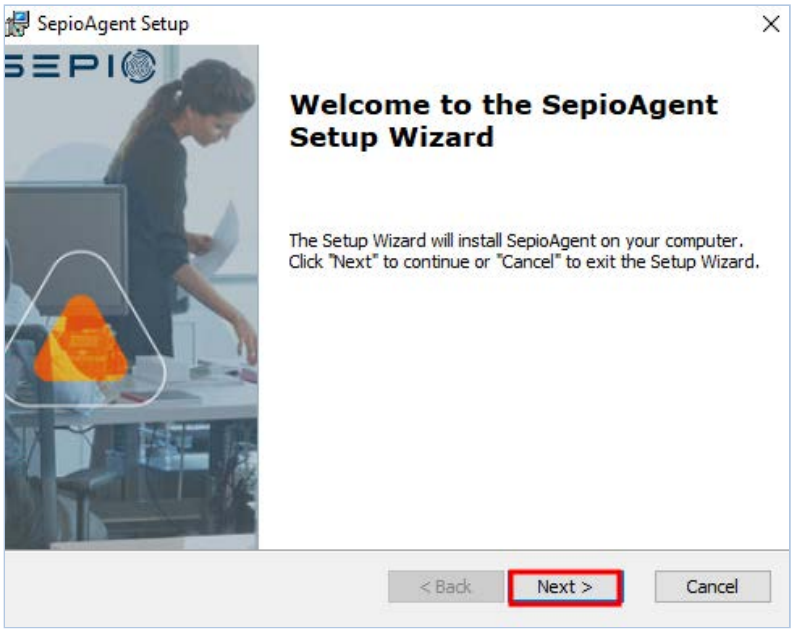
## Windows Installation

> **Note:** If you are modifying or disabling the Recovery Override mechanism, run the required command in the CLI. See Modifying or Disabling the Recovery Override Mechanism.

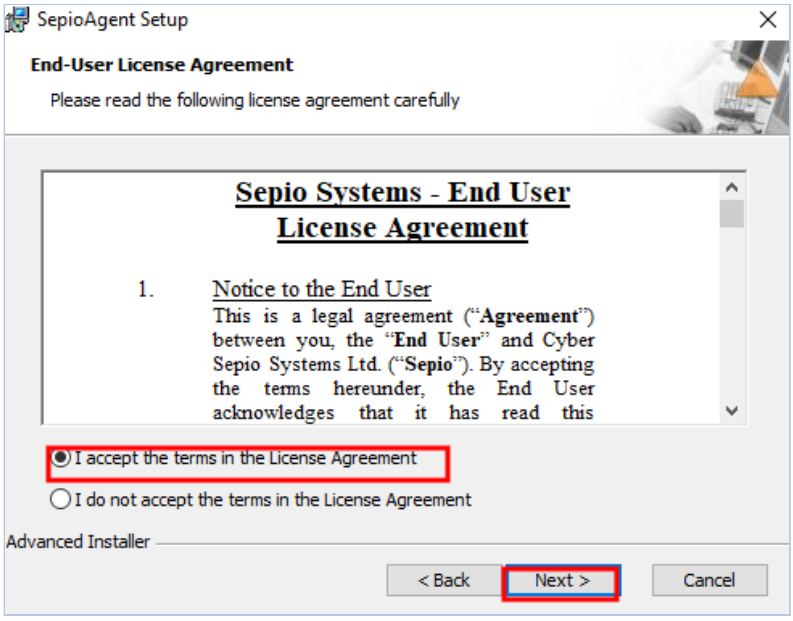
### Windows GUI Installation

1. Download the current version of the Sepio Agent for Windows from download.sepiofiles.com.

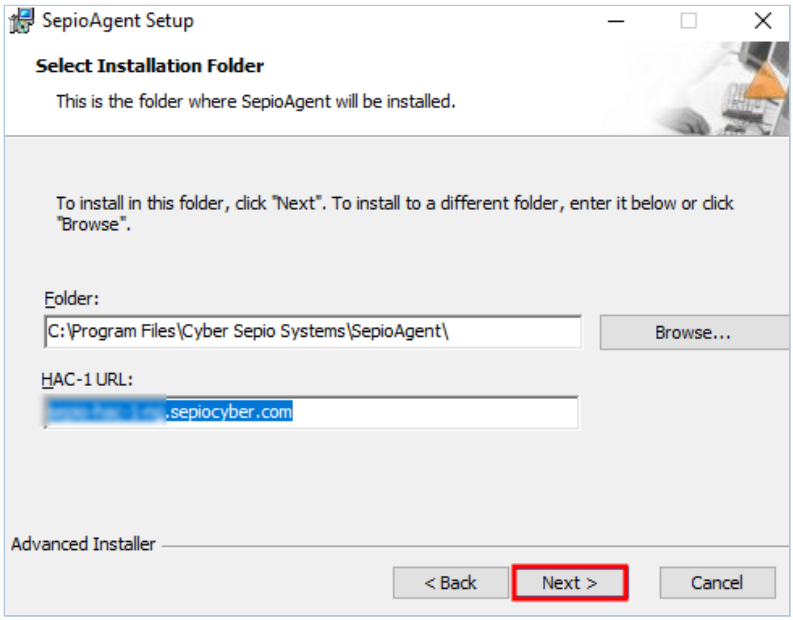
2. Double-click the downloaded file to start the installation.




3. Click **Next.**

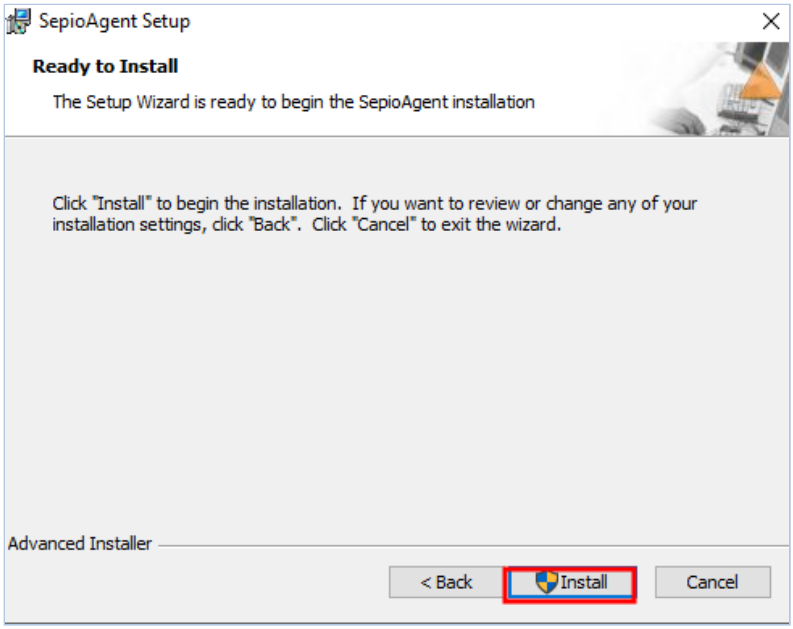



4. Select "I accept the terms in the License Agreement," then click **Next.**

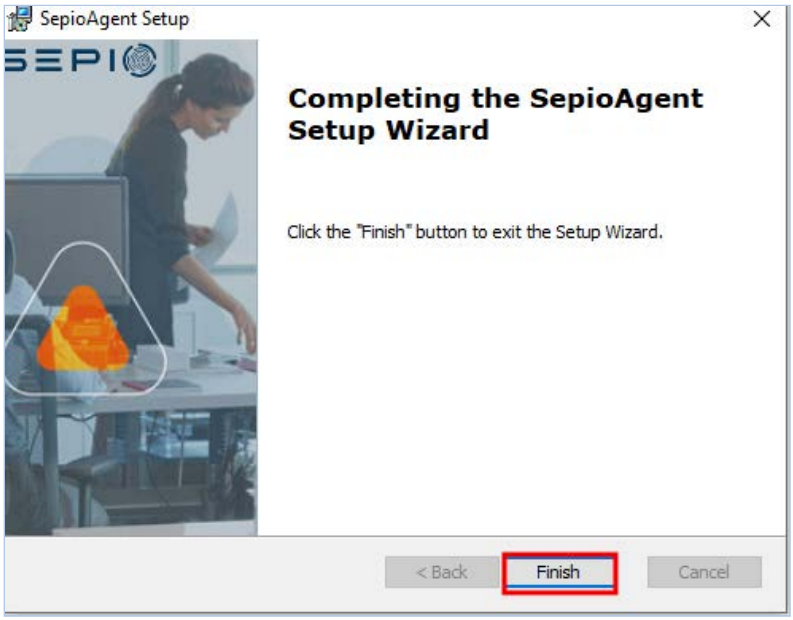



5. (Optional) Click **Browse** to change the installation location.
6. Enter the Sepio Platform Management fully qualified domain name (FQDN) in one of the following formats:
   - `server.domain.com`
   - `server.subdomain.domain.com`

**Note:** Entering an incorrect FQDN format may disrupt connectivity and cause high CPU usage.



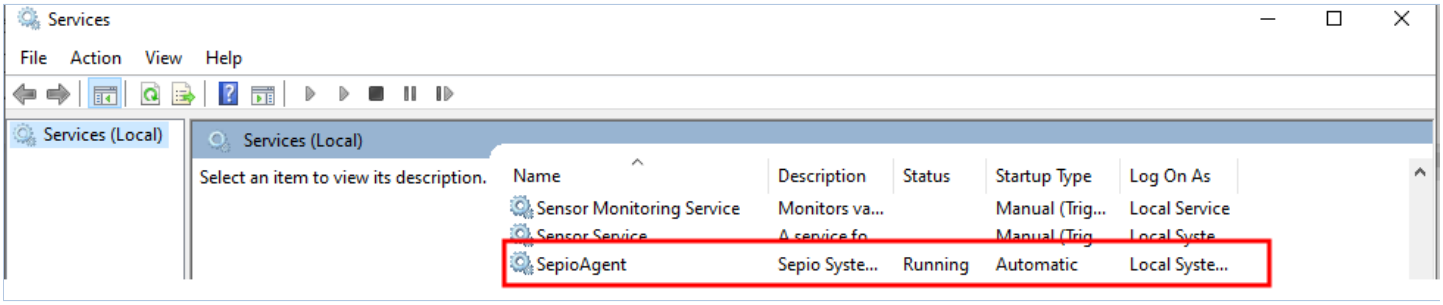

7. Click **Install.**




8. Click **Finish**. The agent is now installed and ready to log in to Sepio.

### Windows CLI Installation

1. Run the installation using:
    - `SepioAgent_Win_64_<sepio agent version>.msi /q CENTRALIZEDIP=<Platform Management FQDN>`
2. Valid FQDN formats:
    - `server.domain.com`
    - `server.subdomain.domain.com`
3. Verify Sepio Agent Service.
    - Open Windows **Services** and ensure the SepioAgent status is **Running**.




### Verify .NET Runtime Installation

Before proceeding with additional components or installing a Sepio Scan Engine, ensure that at least the following **.NET 8.x components** are installed on the Windows host:

1. Open a Command Prompt and run:
    - `C:> dotnet --list-runtimes`
2. Verify that the output includes:
    - `Microsoft.AspNetCore.App 8.0.21`

- `Microsoft.NETCore.App 8.0.21`

**Note:** Versions may vary slightly, but both **Microsoft.AspNetCore.App** and **Microsoft.NETCore.App** for **8.x** must be present.

3. If either runtime is missing, download and install the **x64 versions** from: https://dotnet.microsoft.com/en-us/download/dotnet/8.0

## Linux Installation

The Sepio Linux Agent is currently provided for Debian, Ubuntu, and Red Hat–based systems. The installation file consists of a compressed package that contains the following:

- Dependencies.txt
- LinuxInstallation.sh
- LinuxUninstall.sh
- Scripts.sh
- `sepio.agent<version>.`
- `sepio.agent..service`

### Installation Path

- **Ubuntu / Debian:** /debian/netcoreapp/opt/sepio.agent/Sepio.Agent
- **Red Hat:** /usr/local/bin/sepio.agent

### Dependencies

The `Dependencies.txt` file lists all required dependencies. On systems with Internet access, the scripts automatically download them from online repositories.

> **Note:** Red Hat Enterprise Linux (RHEL) customers must ensure their organization has a valid RHEL subscription configured.

Dependencies can also be reordered manually, which is useful for offline installations.

### Before installing the Agent

1. Download the current version of the Sepio Agent for Linux from download.sepiofiles.com.
2. Ensure you have the correct package for your Linux distribution.
3. Extract all files into the same directory:
   - `tar -xzvf <agent_package_filename>.tar.gz`
4. If required, modify or disable the Recovery Override mechanism (as explained in this topic).

**Note:** The RHEL 9 package supplying /usr/lib64/libssl.so.1.1 and /usr/lib/libcrypto.so.1.1 library binaries is compat-openssl11

### Install a Sepio Agent

4. **Ubuntu / Debian:**
   `sudo ./LinuxInstallationDeb.sh CENTRALIZEDIP=<Platform_Management_FQDN>`
5. **Red Hat:**
   `sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=<Platform_Management_FQDN>`
6. Use one of the following FQDN formats:
   - `server.domain.com`
   - `server.subdomain.domain.com`

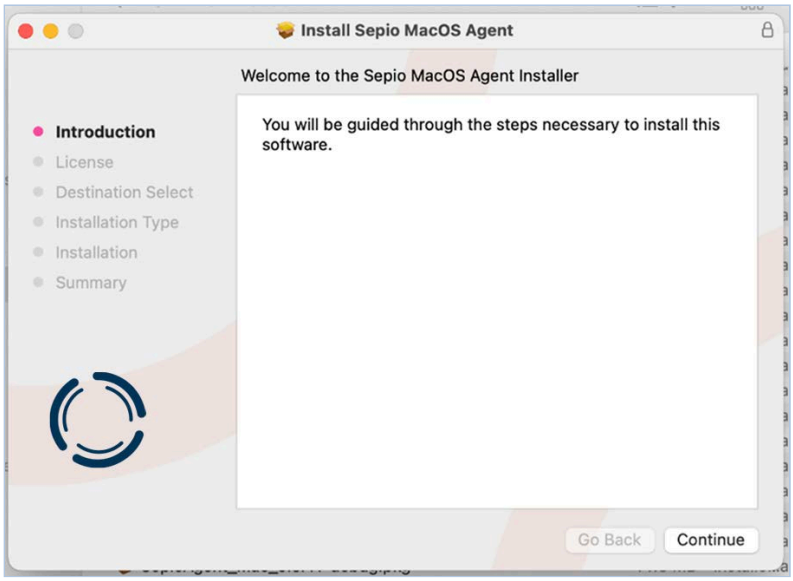
The script logs its actions in the terminal. If it completes with a green line, the installation was successful. Log files are always saved in the `SepioFiles/Logs` directory within the installation folder.

## MacOS Installation

### Install Sepio Agent Using the Agent Installer

1. **Download the Installer**
   Obtain the .pkg installer file named in the format: SepioAgent_MAC_<Version>_prod.pkg from download.sepiofiles.com

2. **Run the Installer**
   Double-click the installation file to open the installation wizard.



Install Sepio MacOS Agent

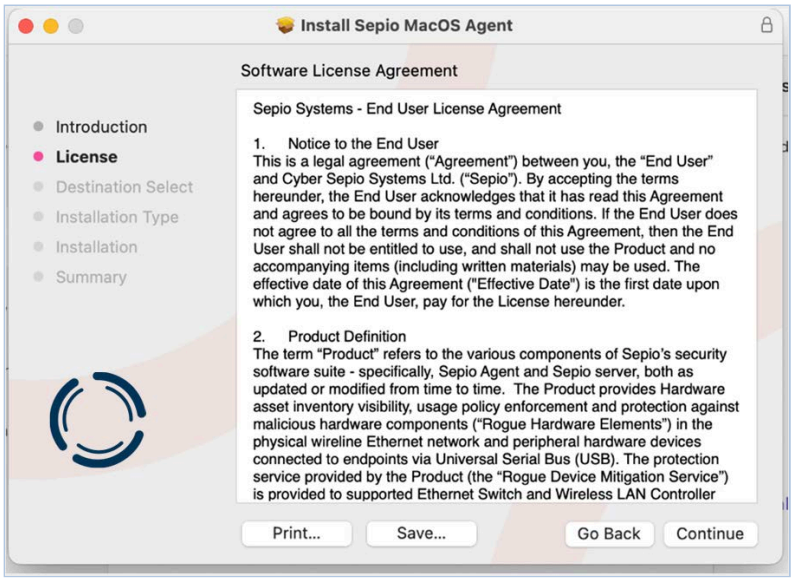
3. **Follow the Installation Instructions**

- **License Agreement**

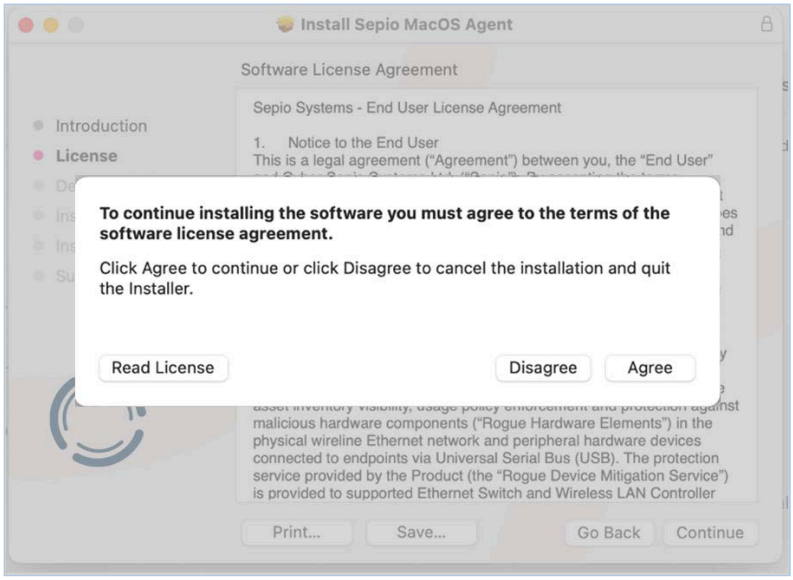
  On the License screen, click Continue, then select Agree to accept the license terms.
- **Installation** Type

  On the Installation Type screen, click Install.
- **Authentication**

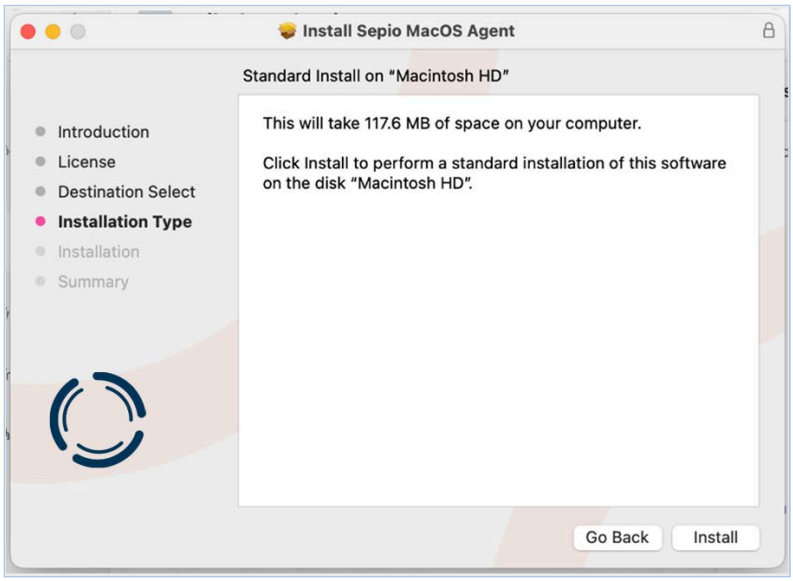
  Click Use Password… and enter your Mac user password. This step is required to ensure the Agent functions properly.



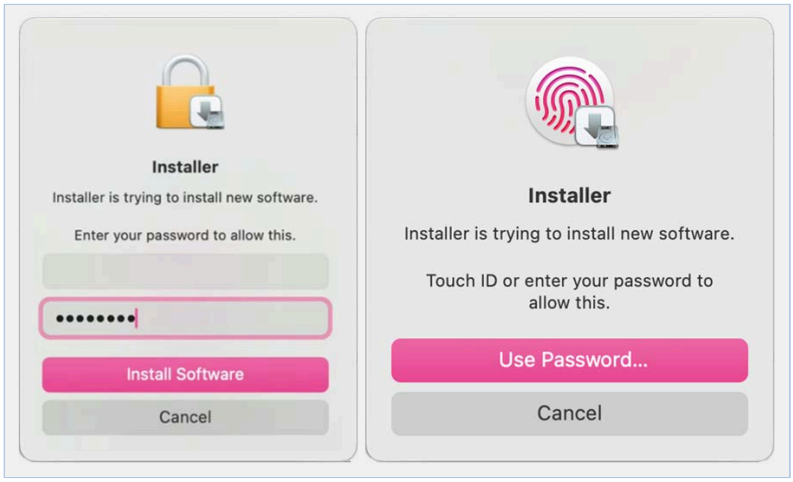
Software License Agreement



License Agreement



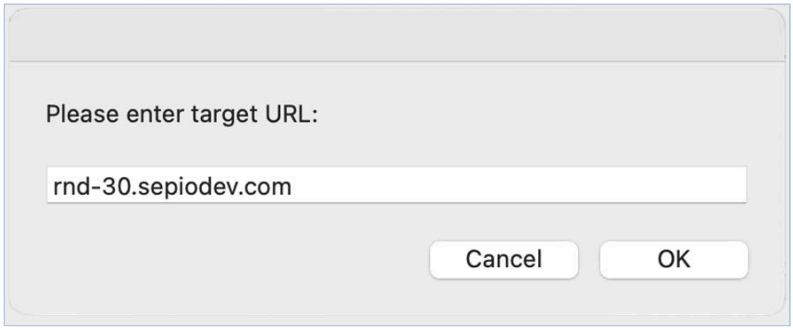

Installation Type




Authentication

4. **Install the Software**

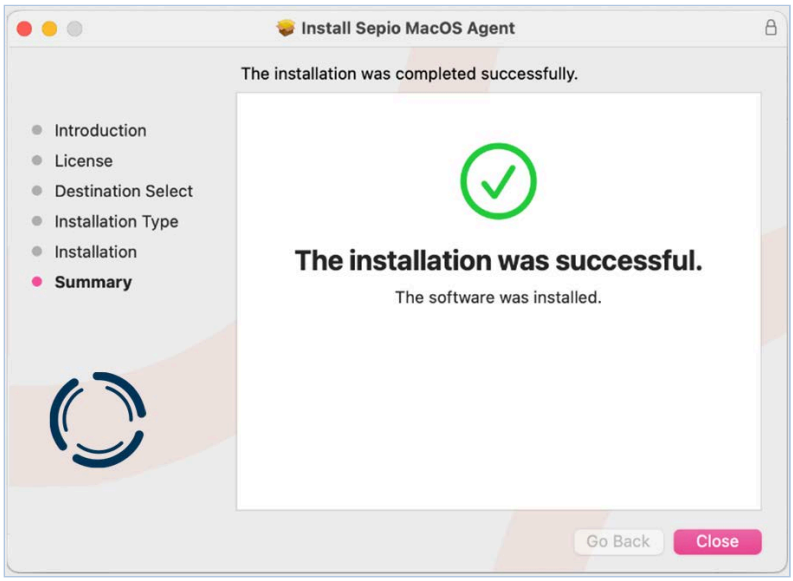
   Click **Install Software.** Once the installation is complete, the window will close, and a new screen will appear, prompting you to configure the Sepio Management Platform URL.




Please enter the Sepio Management Platform URL

5. **Finish Installation**

   After entering the server URL, click Close to complete the installation.



Finish Installation

6. **Post-Installation Option**
   A prompt will appear allowing you to either keep the installer file or delete it. Choose your preferred option.

### Silent Installation of Sepio Agent Using the Agent Installation Script

> **Note:** Installing the Sepio agent using the installation script requires Administrator privileges (sudo access).

1. **Download the Installer**
   Obtain the `.pkg` installer file named in the format: `SepioAgent_MAC__prod.pkg` from download.sepiofiles.com.
2. **Fresh Installation**
   Use this method for first-time installation or when reinstalling from scratch:
   ```
   chmod a+x install_agent.sh
   sudo ./install_agent.sh --url "your-server.sepio.com" --pkg "SepioAgent_Mac_xx.pkg"
   ```
3. **Upgrade Sepio agent version**
   Use this method to upgrade an existing installation. The server URL is preserved from the existing configuration:
   ```
   sudo ./install_agent.sh --pkg "SepioAgent_Mac_xx.pkg"
   ```
4. **Complete Uninstallation**
   Removes all agent files, configuration, and logs
   ```
   sudo ./clean.sh
   ```

**Note:** When upgrading an agent running a version earlier than 17.2511.160 using the installation script, you must first perform a full uninstall of the existing agent before proceeding with the upgrade.

5. **Verification**
   Check if the agent service is running:
   ```
   sudo launchctl list | grep sepio
   ```

After successful installation, the machine and connected USB devices should appear in the Sepio platform, where the agent is associated.

**Command Summary**

| Scenario | Command |
|---|---|
| Fresh install | `chmod a+x install_agent.sh`<br>`sudo ./install_agent.sh --url "server.sepio.com" --pkg "SepioAgent_Mac_xx.pkg"` |
| Upgrade | `sudo ./install_agent.sh --pkg "SepioAgent_Mac_xx.pkg"` |
| Uninstall | `sudo ./clean.sh` |
| Check status | `sudo launchctl list \| grep sepio` |

## Modifying or Disabling the Recovery Mechanism (Optional)

If a Sepio Agent cannot connect to the Sepio Platform Management, it can attempt to connect to a Backup Sepio Platform Management. Customers have the option to use the Backup Sepio Platform Management deployed in the cloud. Older versions of Sepio Agents, released prior to Version 17 (build 17.2306.275), could automatically connect to the backup server.

Sepio understands that some customers may prefer not to use the default Backup Sepio Platform Management. Therefore, an option to disable the Agent Recovery mechanism has been introduced. If you choose this option, please note that while the Sepio Agent can be updated after installation, the Recovery Mechanism must be configured or disabled during the initial installation through the command line.

**Note:** In recent versions, the Sepio Agent no longer automatically attempts to connect to the default backup server.

**WINDOWS**

Before installing the Agent, if required, in the CLI enter one of the following:

The below can be set with a fully-qualified domain name or address.

**To disable the Recovery Mechanism:**

```
%SepioAgent_Win_64_<sepio agent version>.msi RECOVERY_OVERRIDE=0.0.0.0
```

**To enter an alternate FQDN:**

```
%SepioAgent_Win_64_<sepio agent version>.msi RECOVERY_OVERRIDE=<Alternate FQDN>
```

**LINUX**

Before installing the Agent, if required, enter one of the following:

You can set this with either a fully qualified domain name or an address.

**To disable the Recovery Mechanism:**

```
%./LinuxInstallationDeb.sh RECOVERY_OVERRIDE=<0.0.0.0>
```

**To enter an alternate FQDN:**

```
%./LinuxInstallationDeb.sh RECOVERY_OVERRIDE=<Alternate FQDN>
```

## Uninstalling a Sepio Agent

**On Windows:**

- Go to Windows **Control Panel** ->**Programs and Features** ->**Uninstall a program** ->**SepioAgent**->**Uninstall**
- Navigation paths may vary depending on your version of Windows.

**On Linux:**

- Run the LinuxUninstall.sh script in the SepioFiles/Logs directory installation folder.

**On macOS:**

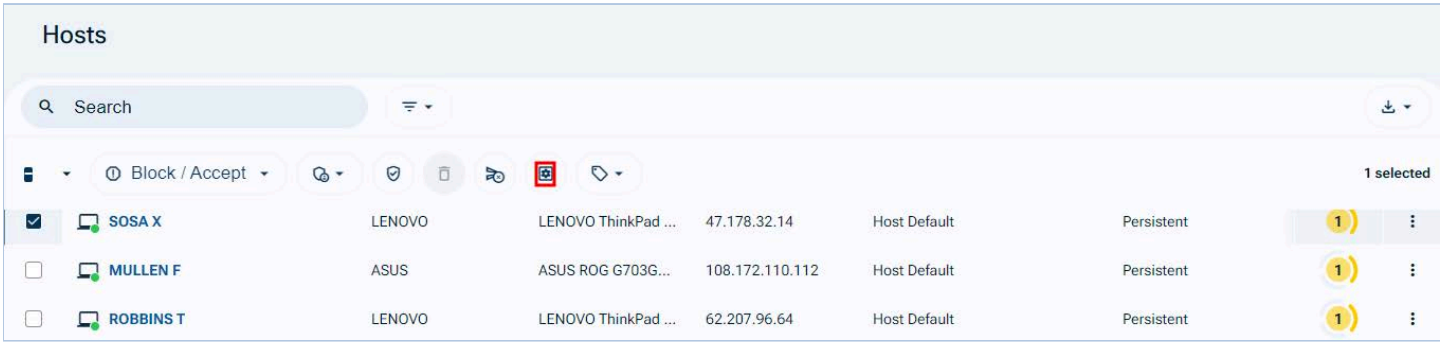
- To uninstall the Mac Agent, run the clean.sh script, which is provided separately from the .pkg file. Use the following command in the terminal: `sudo ./clean.sh`

# Redirecting Sepio Traffic and Changing the Platform Management

If you need to redirect Sepio traffic to a Management Platform with a Fully Qualified Domain Name (FQDN) different from the one set during installation (e.g., to switch Platform Management), follow these steps:

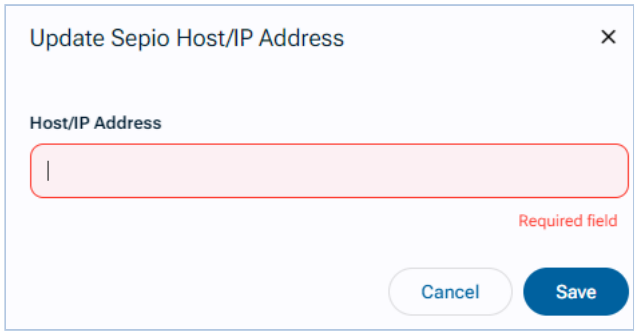
**To redirect Sepio traffic to an FQDN different from the one set during installation:**

1. From the Sepio menu select **Assets Visibility** -> **Hosts.**
2. Select the host whose traffic you want to redirect, then click Update Sepio Host/IP Address.




Assets Visibility -> Hosts

3. Enter the Fully Qualified Domain Name (FQDN) of the host to which you are redirecting the traffic using one of the following formats:
   - Host=server.domain.com
   - Host=server.subdomain.domain.com




Update Sepio Host/IP Address

4. Click **Save.**

# Installing Sepio Agent for VDI

## IGEL

Sepio Agents are built into IGEL which is a transformative secure endpoint OS designed for SaaS, DaaS, VDI and secure browser environments.

**Availability**
IGEL OS 12.4.2 Patch 1

**Files**
IGEL OS 12.4.2+1 6.6.22 x86_64 https://app.igel.com/base_system/12.4.2+1
The Sepio Agent is installed on a custom partition.

- Custom Partition: https://kb.igel.com/en/igel-os-base-system/12.4/custom-partition-in-igel-os-12
- Configuration: https://kb.igel.com/en/igel-os-base-system/12.4/partition-configuring-custom-partition-in-igel-os-

## Stratodesk

Sepio Agents are built into Stratodesk NoTouch which is a proven endpoint software for Citrix, Microsoft Azure Virtual Desktop (AVD) and Windows 365, Nutanix Frame deployments and VMware Horizon, as well as many others – on-premises or within the Cloud. It is capable of running on the most cutting-edge Thin Client, Laptop, PC and Raspberry Pi devices.

**Availability**
Stratodesk 3.5.1

**Files**
**All-In-One-Installer**

- Stratodesk-NoTouchOS-3.5.1-EEs-k519-x64-230809.zip, NoTouch OS – Standard Edition k519 (Normal PCs, Laptops, Thin Clients)
- Size: 3156693931 SHA1: 7c54b0fd15578eb77424a5da146940bea526d38f
- More information: https://kb.stratodesk.com/Install_NoTouch_OS

**Update package**

- lnx-3.5.1-EEs-k519-x64-230809.lfi, NoTouch OS – Standard Edition k519 (Normal PCs, Laptops, Thin Clients)
- https://www.stratodesk.com/dlfile/DfM1gt1lOHQwT2b2vhDK/lnx-3.5.1-EEs-k519-x64-230809.lfi
- Size: 3062198316 SHA1: 34dfdb42dd6de66edc2c1c5b2393d2bfc5057714
- More information: https://kb.stratodesk.com/Firmware_Update

**Note:** Please contact support@sepiocyber.com for additional VDI related questions.

## Citrix

Sepio is a Citrix Ready Partner approved with following Citrix Products:

- Citrix Virtual Apps and Desktops service
- Citrix Gateway service
- Citrix Workspace App for Windows

# Installing for Session Based and Agentless Modes

**Deployment methods**

In addition to a permanent Agent deployment, Sepio provides additional methods that are designed to support different use cases:
The Session-based (previously known as “Zero Trust Agent” or in short, Zero Trust) and Agentless deployment modes allow organizations to gain visibility and control of their endpoint assets without the need to install the Sepio Agent and run it as a service on endpoint devices.
The Audit deployment mode was designed for cases in which an Agent must run for a short period of time, collecting Asset and BOM information and then exiting.

## Why different deployment modes are required

Sepio Agent is the security solution for providing in-depth visibility and policy enforcement for devices connected to endpoint machines. There are various use cases that cannot provide an option to install the Sepio Agent software on endpoint machines. The additional modes provide device visibility and policy enforcement across the organization without the need to install the Sepio Agent.

- Installation: No manual installation or software update (to the endpoint) is required.
- Operations: It is possible to activate the solution using standard IT operational tools.
- Running options: Periodic sampling and one-time running options are available.

**It is important to understand the differences between the Sepio agent, and other deployment modes:**

- The Sepio agent runs continuously and thus it detects changes, sends alerts, and enforces policy in real time.
- In Agentless and Session-based modes the Sepio solution might run periodically and thus while changes are detected, it is less suitable for policy enforcement.
- In Audit mode, the Sepio Administrator can control the duration in which the Agent will be active.

**Detection:**

Only USB devices connected to the endpoint machine during the sampling cycle are detected and relevant policy can be enforced.
The table below explains the four deployment options and how they are different. Please verify the supported operating systems for each deployment mode.
The table below explains the 4 deployment options and how they are different.

| | **Agent** | **Agentless** | **Session based** | **Audit** |
|---|---|---|---|---|
| Main use case | Asset discovery and control, endpoint | Asset discovery and control, endpoint | Continuous Asset | Collect asset information once. |

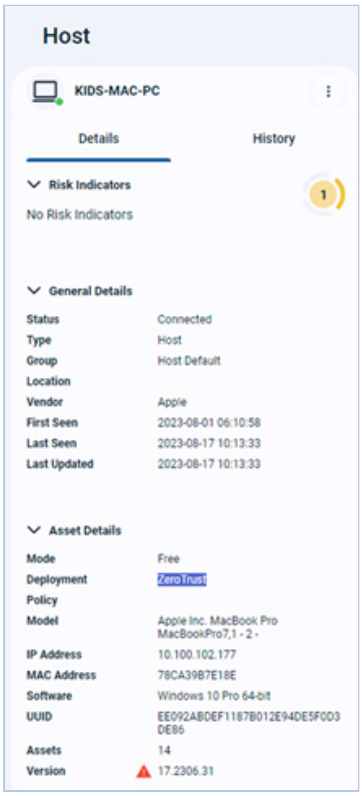
| | Agent | Agentless | Session based | Audit |
|---|---|---|---|---|
| | protection, rogue device mitigation. | protection, rogue device mitigation. | discovery and audit. | |
| Supported deployment modes | Free (visibility only), ARM (white list), Block known Threats (Black list). Block Known Threats and Mass Storage Devices. | Free (visibility only), ARM (white list), Block known Threats (Black list). | Free (visibility only). | Free (visibility only). |
| Operational mode | Installing files and running as a service with continuous operation. | Sepio files copied to the HOST using a deployment tool and can be invoked by it. | Sepio files copied to the HOST. | Sepio files copied to the HOST or downloaded from the Sepio Platform. One time operation. |
| Known limitations | N/A | Windows-based Deployments only. Requires domain-level access. | N/A | Red Hat Enterprise Linux deployments only. Automatic Agent update method not supported. |

## Agent, Agentless and Session-based Deployment and Execution

1. Copy the agent files to the deployment folder.
2. Run the agent binary (Sepio.Agent) using the following parameters:

- -al: Agentless mode
- -zt: Session Based mode
- -url: Sepio Platform URL (https://sepio.example.com)

```
Sepio.Agent.exe -al -url https://FQDN.of.Sepio.Platform
```



Example of host connected in session-based (Zero Trust) mode

**Note:** To install Sepio Agentless deployment server please contact support (support@sepiocyber.com). US Government and Federal customers should contact fedsupport@sepiocyber.com.

# Audit Mode

The Audit deployment mode was designed for cases in which an Agent must run for a short period of time, collecting Asset and BOM information and then exit. The main use case is collecting asset information occasionally with an Agent Free policy.
The Sepio installation files are copied to the HOST or downloaded from the Sepio Platform.

> **Note:** As of July 2024, only Windows and Red Hat platforms are supported for Audit mode.

## Audit Mode Agent Deployment

The Audit mode agent is the same as the regular agent, however it is running with additional parameters to enable the one-time operation.

The deployment of Sepio agent in audit mode involves a three steps process:

1. Download the installation scripts from Sepio.
2. Copy the deployment scripts to the machines that you'd like to audit:
    - **SepioAuditLinuxRedhat.sh** for RHEL
    - **SepioAuditWindows.ps1** for Windows
    - You can copy the file manually or use any robotic process automation (RPA) platform.
3. Execute the scripts and review the audit results in the Sepio Platform UI.

Deployment scripts will connect to the Sepio Platform, pull the required agent and in the case of RedHat can also pull the required dependencies. Then it will copy or install files as required by the operating system, Run the audit and then clean up after.

### Audit Mode for Windows

The deployment script will download the latest Sepio Agent .msi from the Sepio Platform you point it to, into a specific directory. It will extract the Agent's files from the .msi and will run the SepioAgent executables.

> **Note:** Run this script as Administrator

```
##############################
#### SepioAuditWindows.ps1 ####
##############################

Run this script as Administrator to download and run the Sepio agent in a specific directory

-URL / -ut              : Sepio server base URL to download the agent from

-InstallDirectory / -f  : Absolute path to directory to download and extract the agent to

-SessionDuration / -sd  : (optional) if present, run for this amount of seconds

-SkipMSIDownload        : (optional) Assume MSI is already downloaded (useful for reruns)

-KeepAgentFiles         : (optional) Don't delete the extracted agent files after running

-KeepAgentMSI           : (optional) Don't delete the downloaded Agent MSI after running

Example: .\SepioAuditWindows.ps1 -ut 'https://my-sepio-server/ -f C:\path\to\agent\dir'
```

Run this script as Administrator

**Flags:**

| | |
|---|---|
| -URL / -ut | Mandatory: Sepio server base URL to download the agent from |
| -InstallDirectory / -f | Mandatory: Absolute path to directory to download and extract the agent to |
| -SessionDuration / -sd | (optional) if present, run for this amount of seconds |
| -SkipMSIDownload | (optional) Assume MSI is already downloaded (useful for reruns) |
| -KeepAgentFiles | (optional) Don't delete the extracted agent files after running |
| -KeepAgentMSI | (optional) Don't delete the downloaded Agent MSI after running |

**Example:**

```
.\SepioAuditWindows.ps1 -ut 'https://my-sepio-server/ -f C:\path\to\agent\dir'
```

## Common Issues with Audit Mode for Windows

**"Execution of scripts is disabled on this system"**

1. if you get an error like "cannot be loaded because the execution of scripts is disabled on this system.", you can either:
    - Modify the script execution policy systemwide
        - Set-ExecutionPolicy -ExecutionPolicy Bypass
    - Run powershell.exe once with modified execution policy
        - powershell -ExecutionPolicy Bypass -File c:\path-to\SepioAuditWindows.ps1

**“Failed to resolve full path of the current executable ”**

- happens when trying to download to some paths (like system32), resolved by downloading to a different path that is writable.

## Audit Mode for RedHat Enterprise Linux (RHEL)

For air gapped deployments, Audit mode installation script for RHEL can bring the necessary package dependencies from the Sepio Platform’s management server. The script will download the sepio agent install package, will extract the contents of the agent install package + the agent install .rpm inside it to a local directory then. (optionally) will install dependencies necessary to run the agent from an archive. Then, after running the sepio agent one time it will clean up.

> **Note:** Run this script as root

```
# bash SepioAuditLinuxRedhat.sh --help
```

Downloads Sepio Agent files, extracts them, and runs the agent a single time.

```
usage: SepioAuditLinuxRedhat.sh --url https://my.sepio.server --install-directory /home/user/he
```

| | |
|---|---|
| -URL / -ut | Mandatory: Sepio server base URL to download the agent from |
| –install-directory | /path/to/directory Mandatory: Absolute path to directory to download and extract the agent to |
| –dependency-rpms-tar | /path/to/tar (optional) absolute path to local tar archive to install dependencies from |
| –dependendcies-from-server | (optional) if present, download dependencies tar archive from server |
| –session-duration | (optional) Integer value. if present, run for this amount of seconds |
| –skip-agent-download | (optional) Assume agent is already downloaded (useful for reruns) |
| –keep-agent-files | (optional) Don’t delete the extracted agent files after running |
| –keep-agent-archive | (optional) Don’t delete the downloaded Agent .rpm after running |

**Example with all arguments:**

```
sudo bash SepioAuditLinuxRedhat.sh --url https://fqdn-of-sepio-platform/ --install-directory /h
```

**Note:** The dependencies package is provided by Sepio as part of the platform. Please contact Sepio Support with questions related to the dependencies files.

## Supported Versions Audit Mode Deployment

As of July 2024, Audit mode deployment method is supported for Windows, RHEL 8 and RHEL 9. For other RHEL distributions please contact us.

## Installing and Activating a Sepio Scan Engine

A **Scan Engine** (previously known as a Netpoller) collects data from a **Network Element (NE)**. The Sepio installation includes an internal Scan Engine, which requires activation. Additional Scan Engines are typically added to the Platform in the following cases:

- The Platform Management is installed **on-premises** or in the cloud, and does not have SNMP, SSH, or Telnet access to your network.
- You have a **large network** (for example 20,000 or more switch ports) and want to enable the Platform Management to distribute Network Element traffic across multiple Scan Engines for **load balancing**, resulting in faster and more efficient processing.

After installing a Scan Engine, you can assign a Domain to it if needed. If no Domain is assigned, it will remain in the **default Domain**. Once assigned, activate the Scan Engine. You can also adjust its scan interval priorities, if necessary.

> **Note:** For more information about Scan Engines go to About Scan Engines.

## Preparing for Installation

### Network Access

Ensure your Scan Engine has SSH and SNMP access (Telnet optional) and can reach the Sepio Platform Fully Qualified Domain Name (FQDN), `monitoring.Sepiocyber.com`, and your DNS servers.

Also, verify that your **firewall** does not block the required connections.

### Firewall Configuration

The Scan Engine uses several TCP ports to communicate with the Management Platform and other platform components. For proper operation, ensure that the firewall allows traffic through the ports listed below:

| Source IP | Destination IP | Protocol | Destination Port | Comment |
|---|---|---|---|---|
| Scan Engine | Sepio Platform | TCP | 443 | Can be any port configured on the External Scan Engine |
| Scan Engine (external) | Monitored enterprise switches (NEs) | SSH, SNMP or Telnet | 161/UDP for SNMP<br>22/ TCP for | – |

| Source IP | Destination IP | Protocol | Destination Port | Comment |
|---|---|---|---|---|
| | | | SSH<br>23/ TCP for<br>Telnet | |

#### Network Bandwidth Consumption

Sepio's Scan Engine uses approximately 500 bytes of data each time it retrieves information from a network port, regardless of port type or configuration (e.g., 10G or 100G interfaces). For example, a switch with 24 ports results in roughly 12KB of data per polling interval. Communication from the **Scan Engine** to the **Management Platform** adds approximately 25% more data to the total transfer.

> **Note:** Verify that your system meets the required software and hardware Platform Requirements.

## Windows Installation

This process includes the following two procedures. Please complete them both.

#### Verify .NET Runtime Installation

Before proceeding with additional components or installing a Sepio Scan Engine, ensure that at least the following **.NET 8.x components** are installed on the Windows host:

1. Open a Command Prompt and run:
    - `C:> dotnet --list-runtimes`
2. Verify that the output includes:
    - `Microsoft.AspNetCore.App 8.0.21`
    - `Microsoft.NETCore.App 8.0.21`
3. If either runtime is missing, download and install the **x64 versions** from dotnet.microsoft.com/en-us/download/dotnet/8.0.

> **Note:** Versions may vary slightly, but both **Microsoft.AspNetCore.App** and **Microsoft.NETCore.App** for **8.x** must be present.

#### Install a Sepio Scan Engine

1. Download the latest version of the External Scan Engine for Windows from download.sepiofiles.com.

2. Navigate to: **Current Version -> Sepio Platform -> External Scan Engine -> Windows**
   Select one of the following files:
   - **NetpollerService_xx.xxxx.xx_Installer.exe**
3. Double click the downloaded installer file.



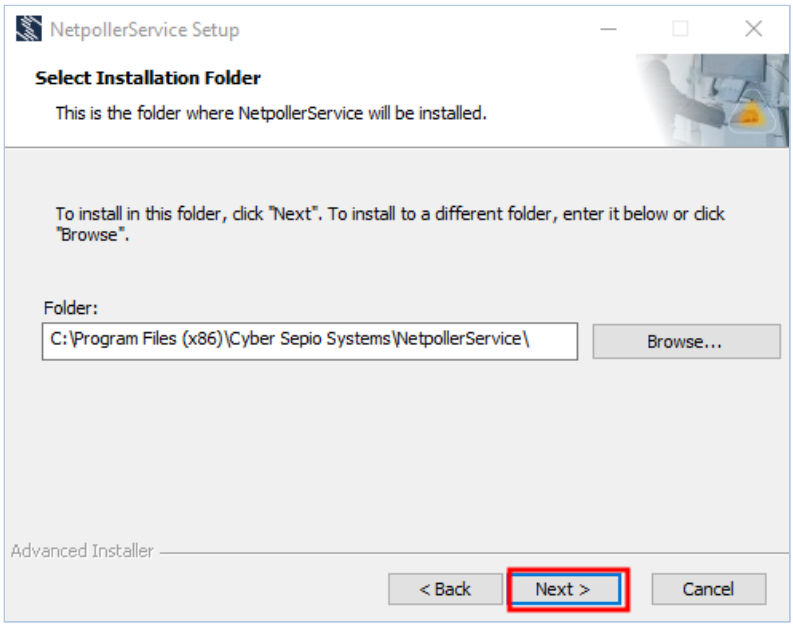

NetpollerService Setup

4. Click **Next.**



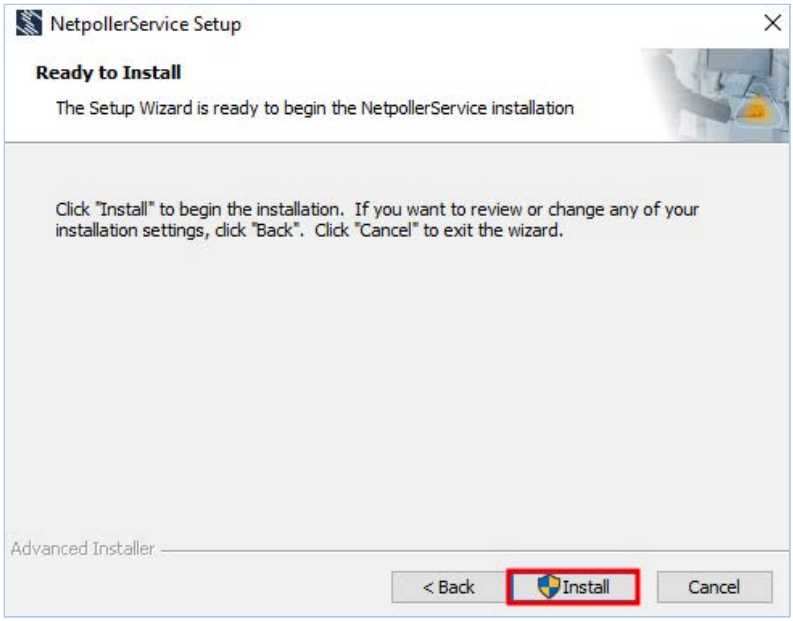

NetpollerService Setup – End-User License Agreement

5. Select 'I accept the terms in the License Agreement' then click **Next.**



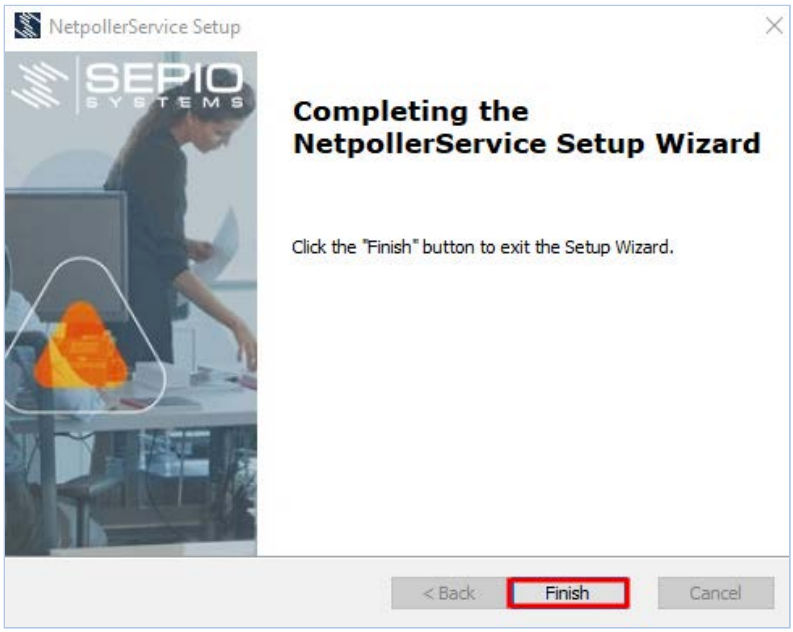

NetpollerService Setup – Select Installation Folder

6. Click **Next**, or if needed, click **Browse** to change the file location, then click **Next.**




NetpollerService Setup – Install

7. Click **Install.**



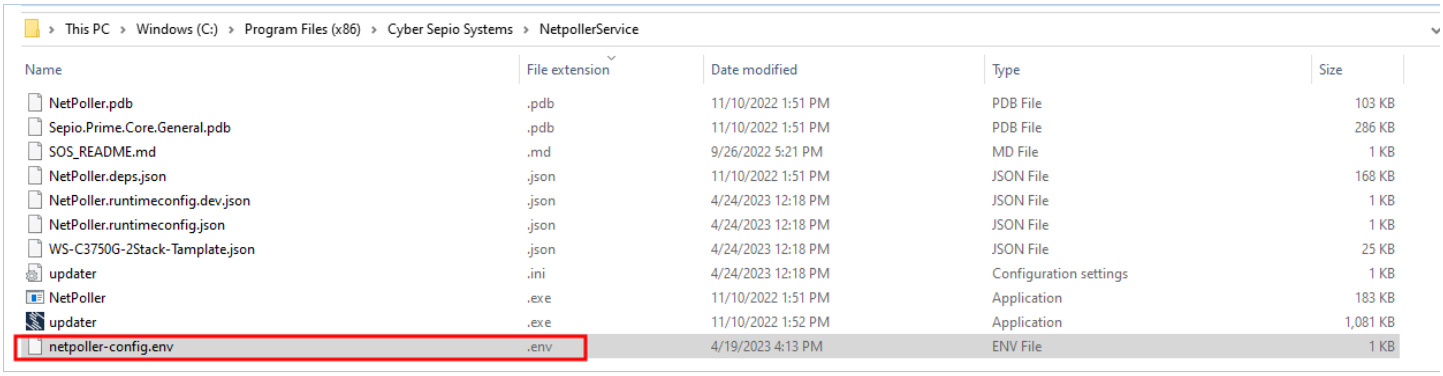

NetpollerService Setup – Finish

8. When the installation is complete, click **Finish**. Sepio's Scan Engine is now installed.

### Modify the Scan Engine Configuration File and Activate It

1. Navigate to the Installation Directory.

   `C:\Program Files (x86)\Cyber Sepio Systems\NetpollerService`




netpoller-config.env

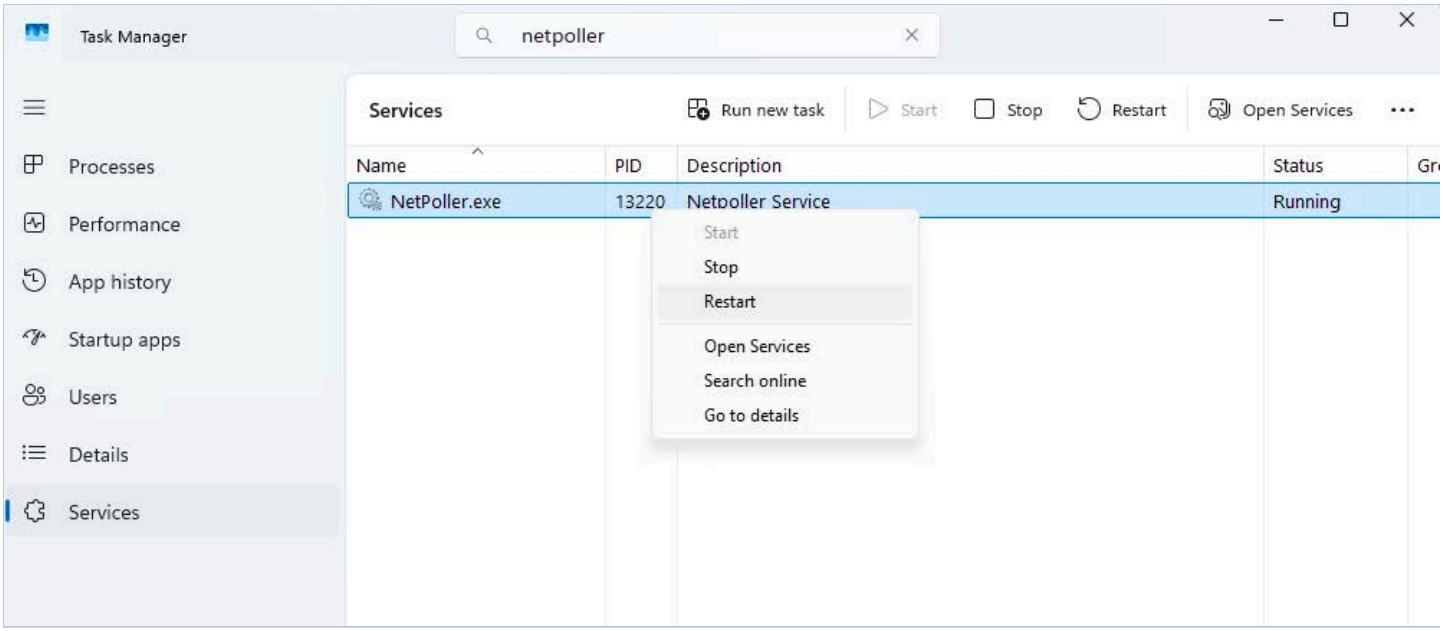
2. Open the Scan `netpoller-config.env` file with an editor.
3. Update the following parameters:
   - `SCAN ENGINE_BASE_URL` – Set this to the Sepio Platform Management FQDN.

     For example: `https://<server.domain.com>/prime/netsapi`.
   - `SCAN ENGINE_NAME` – Set the display name for the Scan Engine in the Sepio GUI.
4. If necessary, modify the optional parameters listed in the Scan Engine Optional Parameters section.

```
NETPOLLER_BASE_URL="https://sepiodemo.sepiocyber.com/prime/netsapi"
NETPOLLER_NAME = "External Netpoller"
NETPOLLER_NUM_OF_POLLERS = 10
NETPOLLER_LIFETIME_THRESHOLD = 8000
NETPOLLER_POLLING_TIMEOUT = 7200
NETPOLLER_RESTART_THRESHOLD = 0.3
NETPOLLER_STAND_ALONE = false
NETPOLLER_SIMULATE = false
NETPOLLER_USE_ENABLE_PASSWORD = true
NETPOLLER_WIFI_BUFFER_SIZE = 512000
NETPOLLER_WIFI_DISABLE_PAGING = true
```

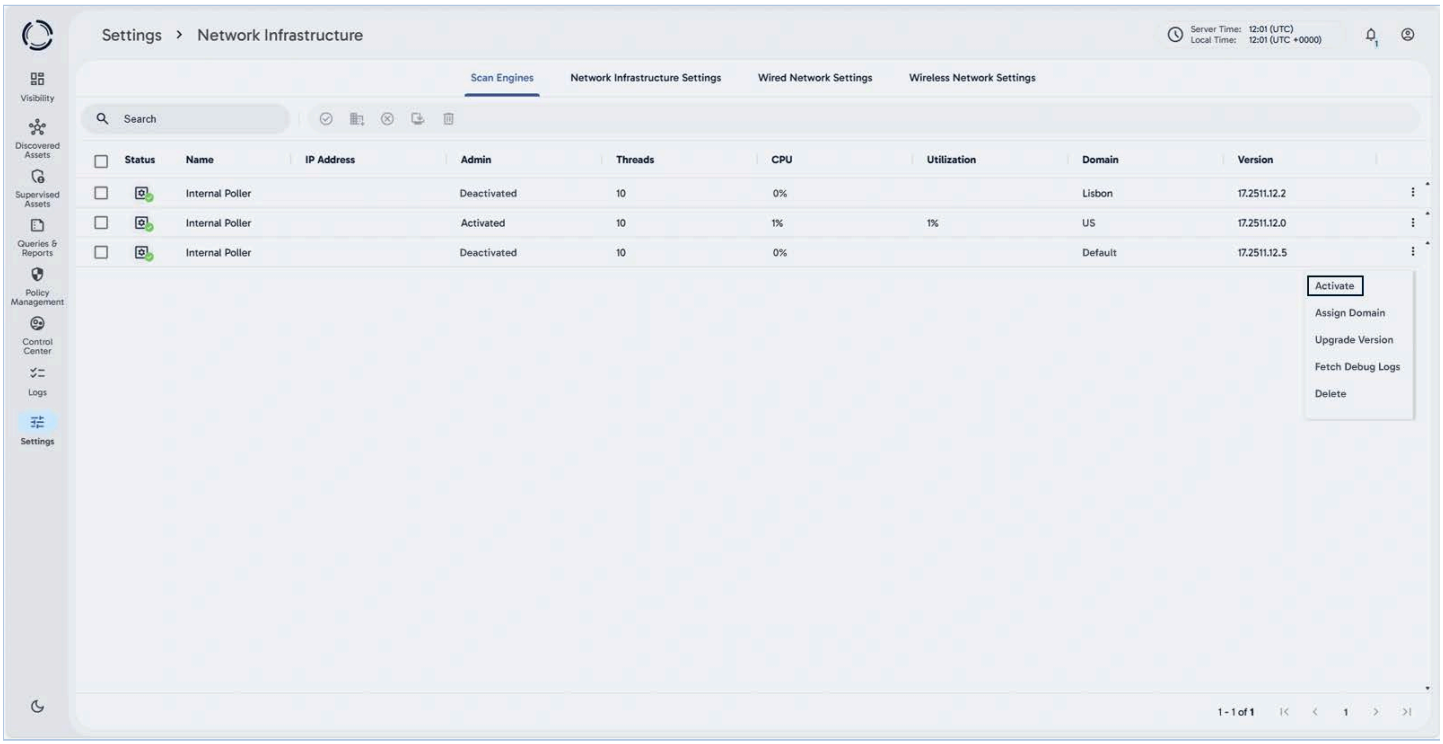
Parameters

5. Save and close the configuration file.
6. Restart the Netpoller Service using **Windows Services** interface.




Restart the Netpoller

7. Activate the Scan Engine: On the Sepio Platform menu select **Settings** -> **Network Infrastructure** -> **Scan Engines.**
    - Select the Scan Engine and click **Activate.**




Select the Scan Engine and click Activate.

**Note:** Please contact support@sepiocyber.com for additional support.

## Linux Installation

This section covers installation on **Red Hat** and **Ubuntu/Debian** distributions, including configuration and activation of the Scan Engine. Before installation, you must edit the configuration file to define the **mandatory parameters** required for proper operation.

### Mandatory Parameters:

| Parameter | Description |
|---|---|
| `NETPOLLER_BASE_URL` | `/prime/netsapi` – Sepio Platform Management FQDN. Formats supported: `server.domain.com` or `server.subdomain.domain.com` |
| `NETPOLLER_NAME` | – The Scan Engine name displayed in Sepio GUI |

```
NETPOLLER_BASE_URL="https://sepiodemo.sepiocyber.com/prime/netsapi"
NETPOLLER_NAME = "External Netpoller"
NETPOLLER_NUM_OF_POLLERS = 10
NETPOLLER_LIFETIME_THRESHOLD = 8000
NETPOLLER_POLLING_TIMEOUT = 7200
NETPOLLER_RESTART_THRESHOLD = 0.3
NETPOLLER_STAND_ALONE = false
NETPOLLER_SIMULATE = false
NETPOLLER_USE_ENABLE_PASSWORD = true
NETPOLLER_WIFI_BUFFER_SIZE = 512000
NETPOLLER_WIFI_DISABLE_PAGING = true
```

Parameters

**Example Command:**

```
./LinuxInstallationDeb.sh NETPOLLER_NAME= NETPOLLER_BASE_URL=/prime/netsapi
```

## Install a Scan Engine on Ubuntu/Debian

**Installation Path:**

`/debian/netcoreapp/opt/netpoller/`

**Log Files Path:**

`/Logs`

**Check Installation Status:**

`dpkg -s netpoller`

**Ubuntu Server 22.04 Requirement:**

Please note that the 22.04 version of Ubuntu Server needs an additional library, **libssl**, which can be downloaded and installed using the following commands:

`wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl1.0/libssl1.0.0_1.0.2n-1ubuntu5.10_amd64.deb sudo dkpg -i libssl1.0.0_1.0.2n-1ubuntu5.10_amd64.deb`

**Installation Steps**

1. Download the latest External Scan Engine for Ubuntu/Debian from Sepio Download Page.
   - **Current Version** -> **Sepio Platform External** -> **External Scan Engine** -> **Linux** -> **netpoller#debian#xx.xxxx.xx#.tar.gz**
2. Copy the downloaded file to your Linux server and unpack it:
   - `tar -xzvf netpoller#debian#xx.xxxx.xxx#.tar.gz`
3. Run the installation script:

   `sudo ./LinuxInstallationDeb.sh NETPOLLER_NAME=Demo NETPOLLER_BASE_URL=https://demo.sepio.systems/prime/netsapi`

The script will log actions to the terminal console. Successful steps will be displayed in **green**, while errors will appear in **red**. If the script completes with a green line, the operation was successful.

4. Verify installation: The Scan Engine should appear in the Sepio GUI within a few minutes.

## Install a Scan Engine on Red Hat

**Installation Path:**

`/usr/local/bin/netpoller`

**Log Files Path:**

`/Logs`

**Check Installation Status:**

`rpm -q netpoller`

**Installation Steps**

1. Download the latest External Scan Engine for Red Hat from the Sepio Download Page.
    - **Current Version** -> **Sepio Platform External** -> **External Scan Engine** -> **Linux** -> **netpoller#redhat#xx.xxxx.xxx#.tar.gz**
2. Copy the downloaded file to your Linux server and unpack it:
    - `tar -xzvf netpoller#redhat#xx.xxxx.xxx#.tar.gz`
3. Run the installation script:

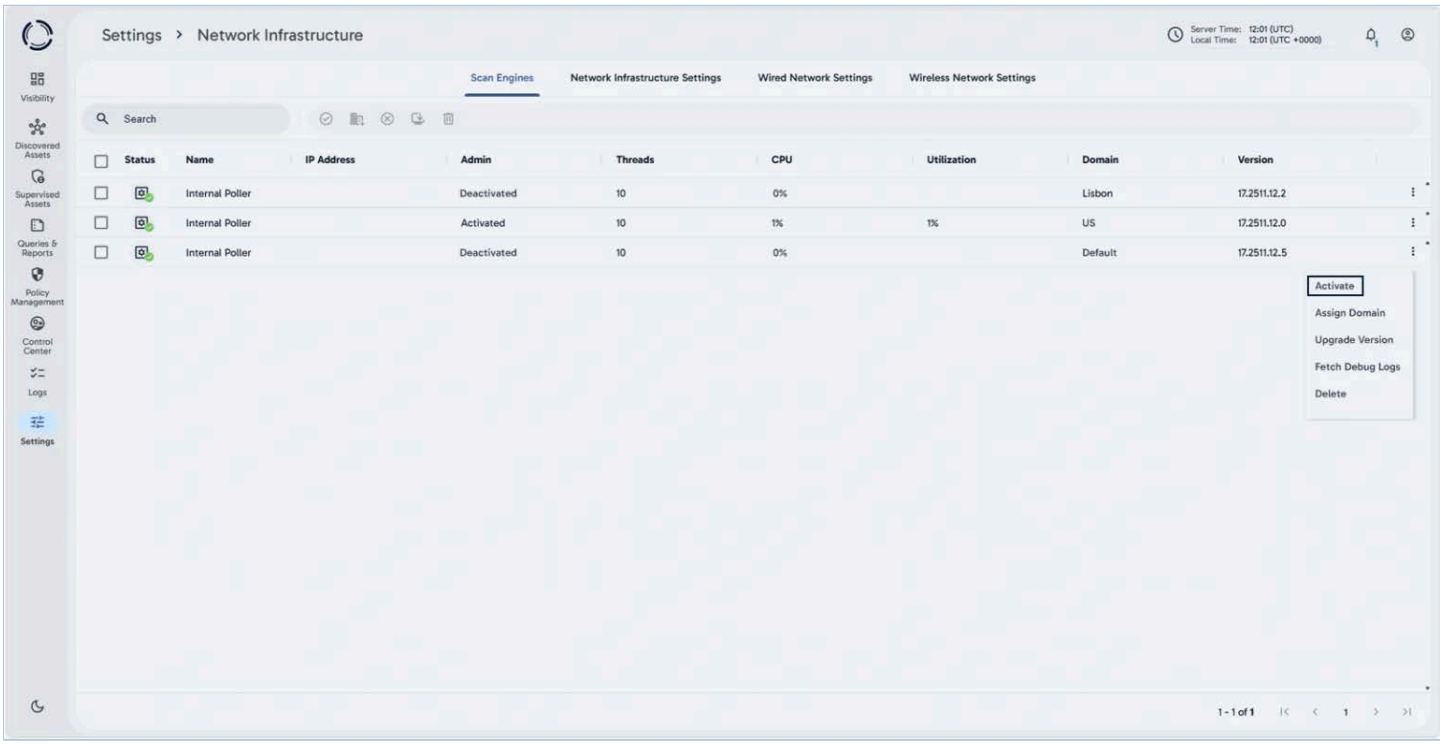
    ```
    sudo ./LinuxInstallationDeb.sh NETPOLLER_NAME=Demo
    NETPOLLER_BASE_URL=https://demo.sepio.systems/prime/netsapi
    ```

The script will log actions to the terminal console. Successful steps will be displayed in **green**, while errors will appear in **red**. If the script completes with a green line, the operation was successful.

4. Verify installation: After a few minutes, the Scan Engine (Netpoller) should appear in the Sepio GUI.

## Activate the Scan Engine

On the Sepio menu select **Settings** -> **Network Infrastructure** -> **Scan Engines**. Select the Scan Engine and click **Activate**.




Select the Scan Engine and click Activate.

## Scan Engine Optional Parameters

Optional parameters can be edited in the `netpoller-config.env` file.

| Parameter | Description | Default Value |
|---|---|---|
| `NETPOLLER_NUM_OF_POLLERS` | Number of simultaneous threads (services) that collect data | 10 |
| `NETPOLLER_USE_ENABLE_PASSWORD` | Enable/disable password when connecting to a network switch | true |
| `NETPOLLER_WIFI_BUFFER_SIZE` | SSH Wi-Fi bandwidth buffer size | 512000 |
| `NETPOLLER_WIFI_DISABLE_PAGING` | Enable/disable SSH paging | true |

**Editing the Configuration File:**

**Windows:**

- File name: `netpoller-config.env`
- File location: `C:\Program Files (x86)\Cyber Sepio Systems\NetpollerService`
- After editing the file, restart the `Netpoller.exe` service for the changes to take effect.

**Linux:**

- File name: `netpoller.service`
- File location: `/etc/systemd/system/`
- After editing the file, use the following command to restart the service:
  `systemctl restart netpoller.service`

## Uninstalling a Scan Engine

**Windows:**

- Open **Control Panel** -> **Programs and Features** -> **Uninstall a program**.
- Locate **NetpollerService** and select **Uninstall.**
- Note: Navigation paths may vary depending on your Windows version.

**Linux:**

- Run the uninstall script located in the `SepioFiles/Logs` directory within the installation folder:
  - `LinuxUninstall.sh`

> **Note:** Please contact support@sepiocyber.com for additional support.

## Downgrade a Scan Engine Version

1. Close the scan engine service on the scan engine instance.
2. Deactivate it from Sepio Platform.
3. Wait until it appears as disconnected in Sepio Platform (should take few minutes).
4. Delete it from the UI.
5. Install the Scan Engine.

## High Performance Deployment

Starting with Sepio Platform v32 (build 17.2306.732) the default Sepio installation supports high performance deployment by separating the Asset Producer into two different components:

1. Asset Producer worker that is processing data retrieved from Scan Engines
2. Asset Producer worker that is processing data retrieved from Agents

To support deployments that requires higher performance, it is possible to scale out the following Sepio services:

- riskenricher
- transformerdataworker
- eventproducerworker

> **Note:** Please contact Sepio Customer Success with questions regarding high performance deployment configuration

# Update

## Related Topics

- Platform Update
- Updating a Sepio Agent
- Updating a Scan Engine
- Updating the Knowledge Base
- Platform Configuration
    - Setting Agents Connection Intervals
    - Managing Integrations
    - Setting Host/s (Agent) Mode

# Platform Update

> **Warning:** This page is obsolete and no longer maintained.
> Please refer to the updated documentation here: Installing Sepio on Customer-Owned Hardware.

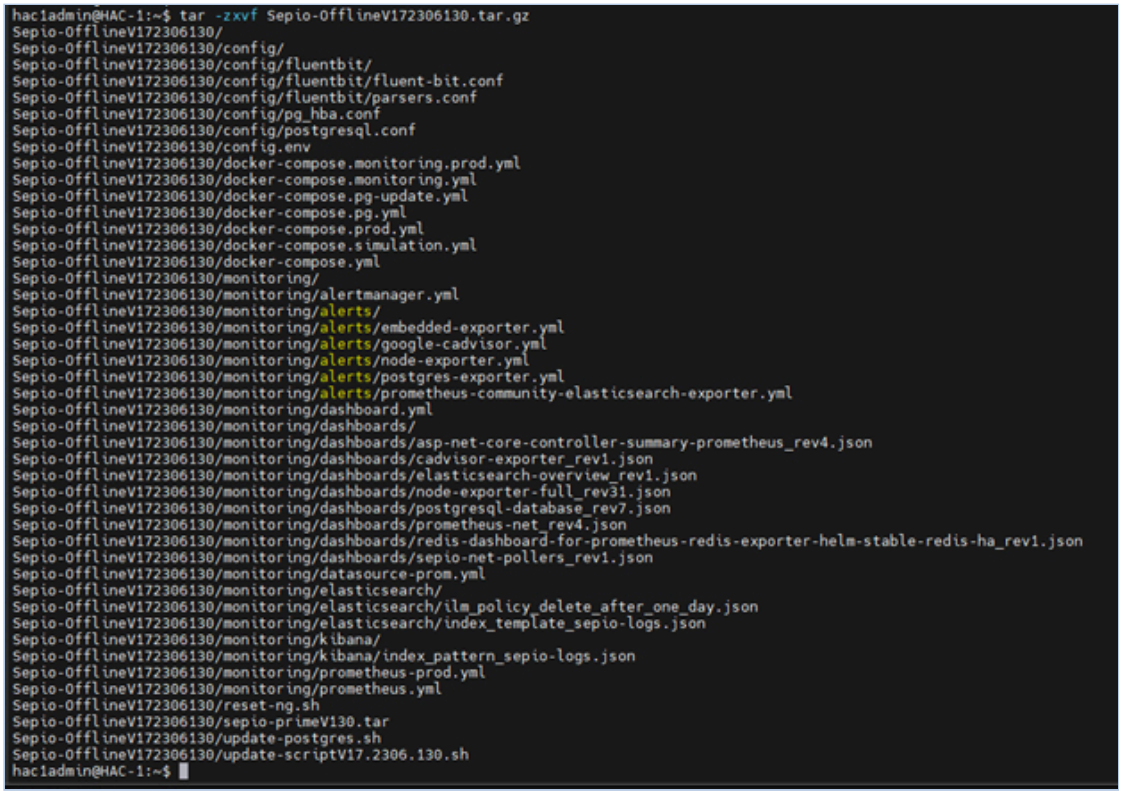
## Sepio Platform Update Using Offline Package

### Download and Prepare the Package

- Download the package from the Sepio file repository.
- Copy the .tar.gz file to the installation folder.
- Perform the following actions as a **root user**.

### Extract the Installation Package

```
tar -zxvf Sepio-offline-package.tar.gz
```




Extract the installation package

### Run the Update Script

- The file name update-script-VVVV.sh (VVVV represents that the version number. For example V17.2306.130).
- Use one or more of the following parameters by listing it in command line interface:
  - formatted: The current date and time in a formatted string.
  - air-gapped: A boolean value indicating whether the installation is air-gapped.

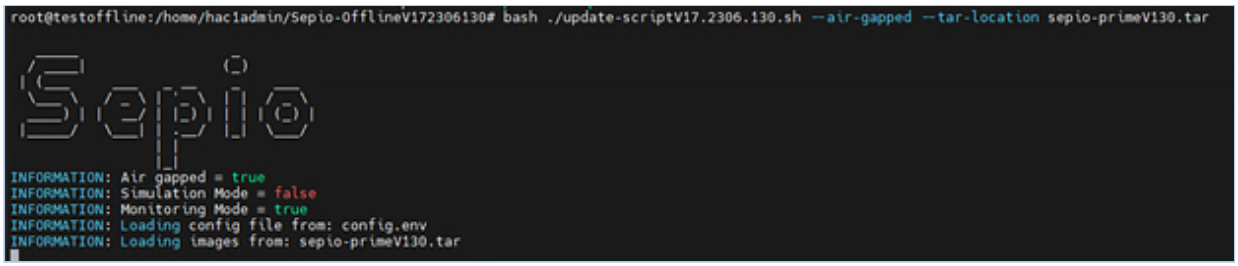
- simulation: A boolean value indicating whether the simulation mode is enabled.
- Monitoring: A boolean value indicating whether the monitoring mode is enabled.
- tar-location: The path to the configuration file.

> **Note:** The `NOW_FORMATTED` parameter is used to update the version of the container images.

**Example:**

```
./update-scriptV17.2306.130.sh --air-gapped --tar-location sepio-primeV130.tar
```

The script will display the configuration flags used.

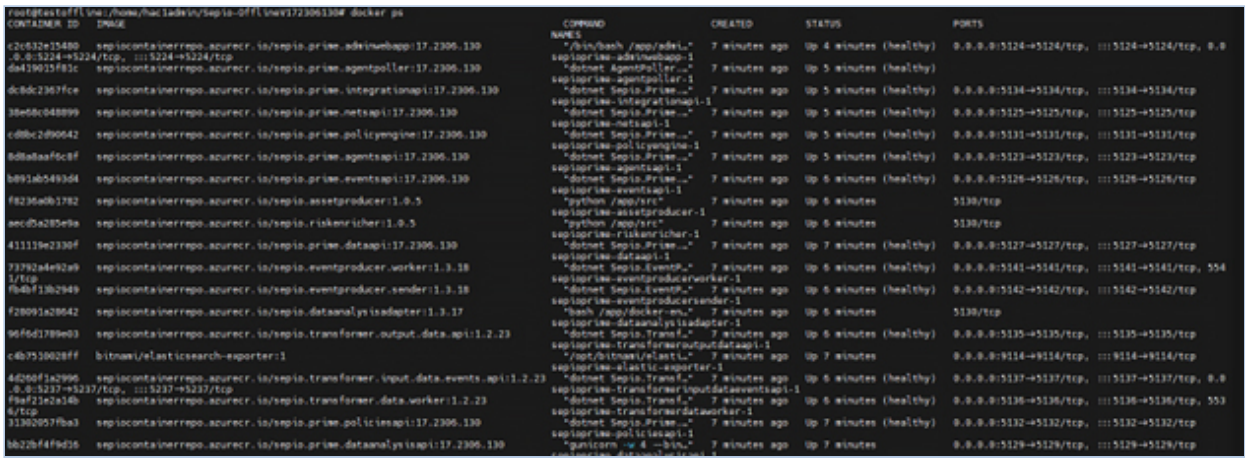



Configuration flags used

> **Note:** Loading the images from the tar file can take few minutes due to its size.

### Verify Upgrade Completion

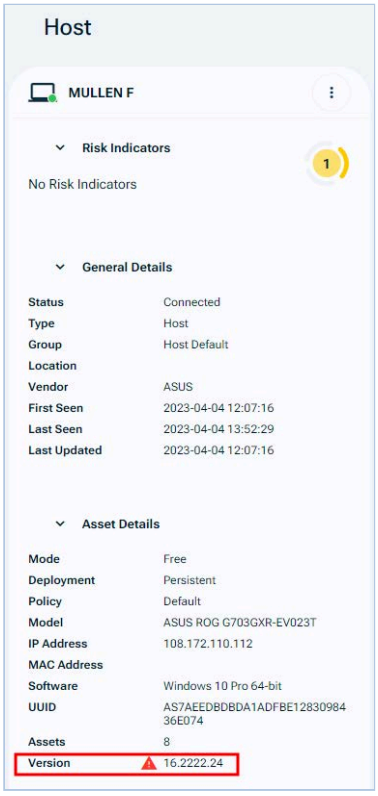
- When the upgrade ends, a prompt will be displayed.
  Verify the health of the upgrade using the **docker ps** command:
  `root@testoffline:/home/hac1admin/Sepio-OfflineV172306130# docker ps`



Verifying the health of the upgrade

# Updating a Sepio Agent

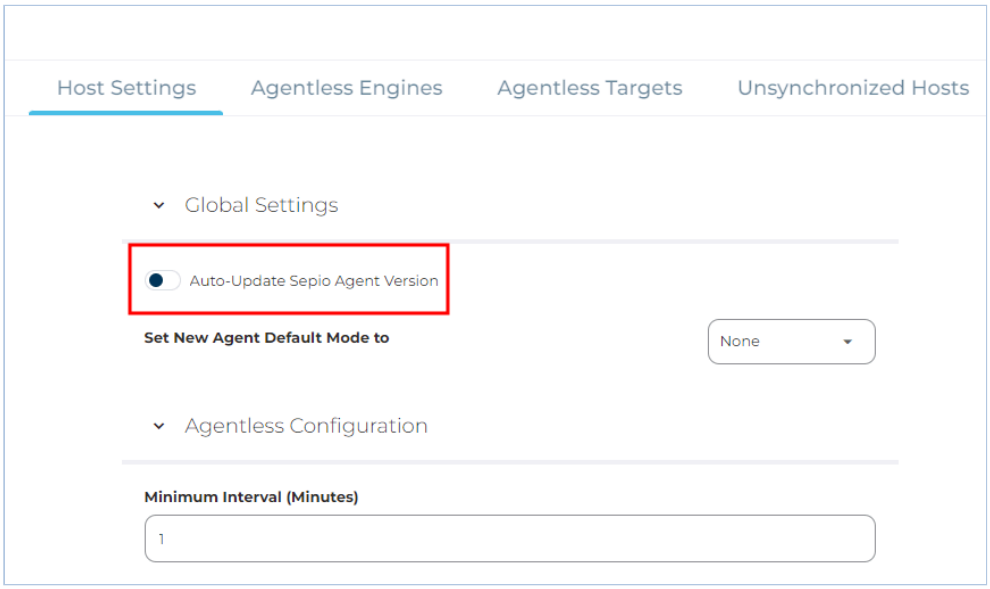
This page explains how to update the Sepio Agent using the Sepio Management Platform, which supports both automatic and manual updates. By default, the platform automatically performs Sepio Agent upgrades. However, you can manually update an agent when needed.
Manual updates are typically performed when the latest version is not yet installed. This status is shown in the **Host view** -> **Asset Details** area (as shown below).



Asset Details

## To Automatically Update a Sepio Agent

1. In the Sepio main menu, go to:
    - **Settings** -> **Host** -> **Host Settings** -> **Global Settings.**
2. If the **Auto-Update Sepio Agent Version** option is disabled, enable it, as shown below.

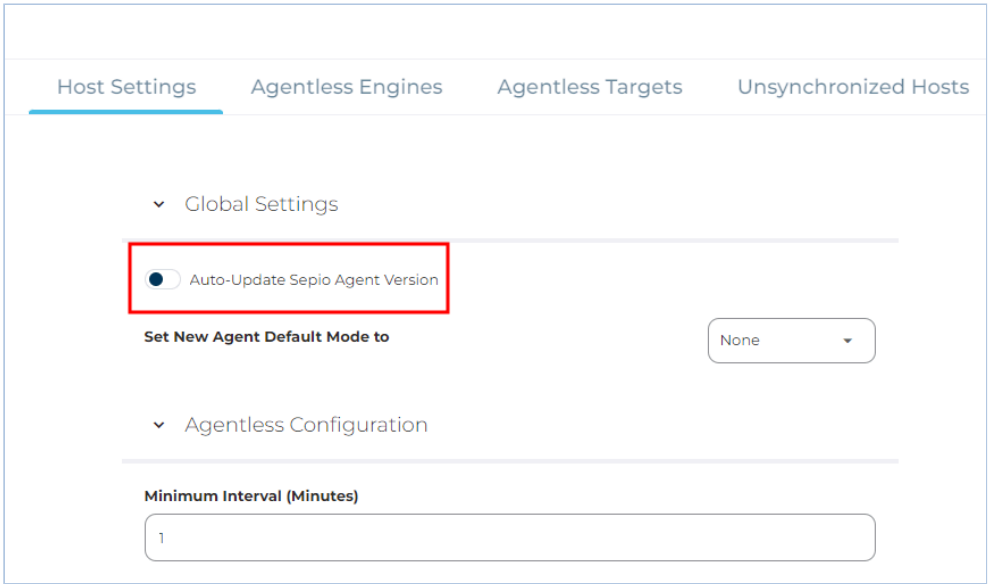


Auto-Update Sepio Agent Version

**Note:** Updating a Sepio Agent to a version lower than the one currently installed will fail. Additionally, if you use software-distribution tools such as Microsoft Intune, it is recommended to disable the Auto-Update feature to avoid potential version-management conflicts.

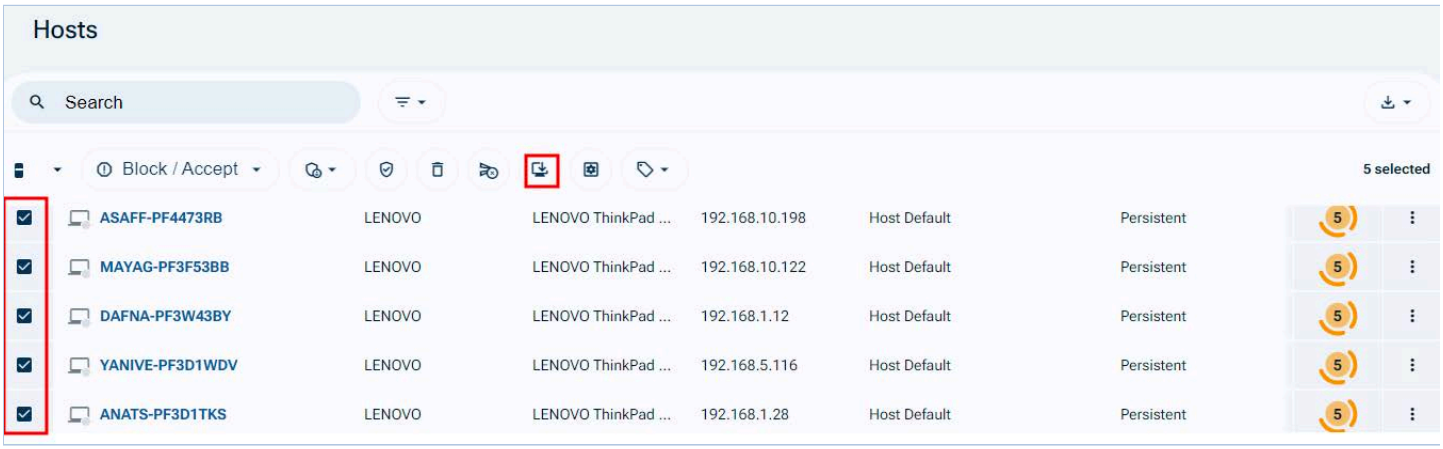
## To Manually Update a Sepio Agent

1. On Sepio main menu go to:
    - **Settings** -> **Host** -> **Host Settings** -> **Global Settings.**
2. Disable the **Auto-Update Sepio Agent Version** option.



Disable the Auto-Update Sepio Agent Version

3. Open the **Hosts** view:
    - In the Sepio main menu go to **Assets Visibility** -> **Hosts.**



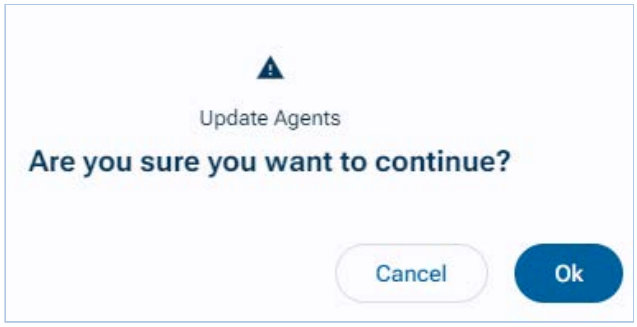

Go to Assets Visibility -> Hosts

4. Select the Host(s) whose agents you want to upgrade.
    - To select all Hosts on a page, check the box at the top of the list.




Select all Hosts on a page

5. On the toolbar, click **Update Agents.**
    - A confirmation message will appear.

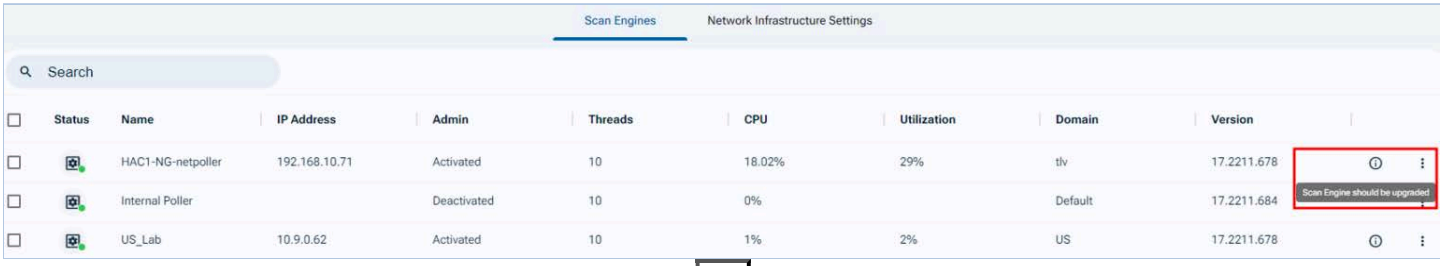



Update Agents

6. Click **OK** to start the update.

# Updating a Scan Engine

Update a Scan Engine when the message 'Scan Engine should be upgraded' is displayed when hovering over the ⓘ next to the Scan Engine version number.



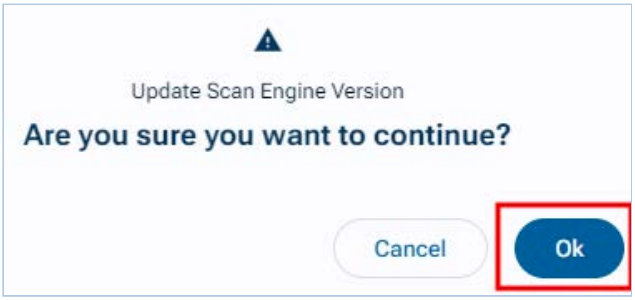

Update a Scan Engine

## Update a Scan Engine

1. On Sepio main menu go to **Settings** -> **Network Infrastructure** -> **Scan Engines**
2. Click ⋮ then select **Upgrade Version**, the following message appears, click **OK**




Go to Settings -> Network Infrastructure -> Scan Engines




Following message appears, click OK

# Updating the Knowledge Base

## About Sepio Knowledge Base

The Sepio Knowledge Base (KB) package is a collection of files used to provide the most up-to-date information about assets, peripherals, and known attack tools. The package is enriched with information collected from Sepio installations, customers, and manufacturers, that is then processed by our research team at Sepio.

To ensure compatibility with Sepio Agent, the Sepio Knowledge Base package also includes the necessary deployment files for Sepio Windows Agent. The Sepio Knowledge Base package is updated on a weekly basis to continuously provide our customers improvements on assets' visibility and risks. It is recommended to update it frequently in your Sepio Platform to leverage these improvements effectively.

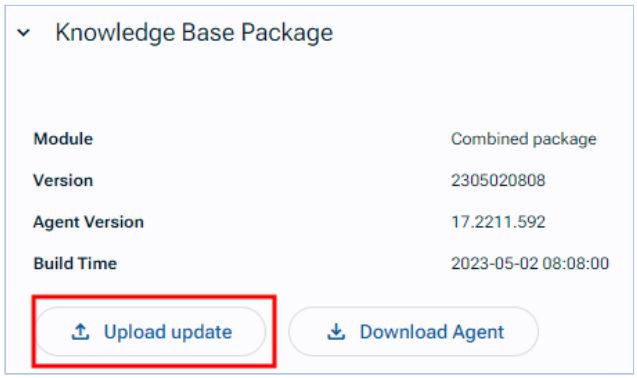
**Note:** To stay informed about new Knowledge Base package releases, we offer a notification list that keeps you updated. Please contact support@sepiocyber.com to be added to the list.

**Note:** The Sepio Knowledge Base file is signed and encrypted.

Updating the Knowledge Base is possible using the Web UI, or via an API which is the preferred method for automation, tests, and when customer security controls prevent transfer of encrypted files.

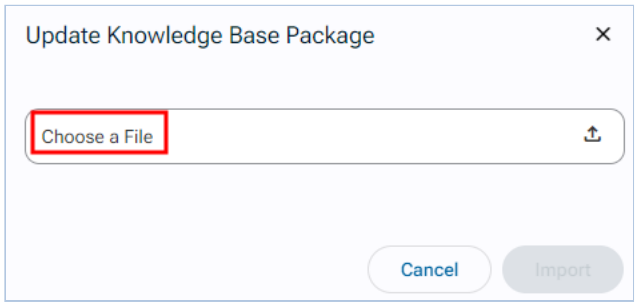
## Update the Knowledge Base using the Web UI

1. Download the current version of the Sepio Knowledge Base from download.sepiofiles.com
    - **Current Version** -> **Sepio Platform (NG)** -> **Knowledge Base Package** -> **KB WIN** or **KB Linux** -> **ng-data-windowsxx.xxxx.xxxxxx- signed.zip** or **ng-data- linuxxx.xxxx.xxxxxx- signed.zip**
2. On the Sepio menu select **Settings** -> **About** -> **Knowledge Base Package.**
3. Click **Upload update.**

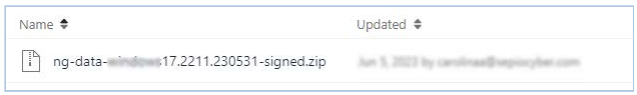


Knowledge Base Package

4. Click to **Choose a File.**

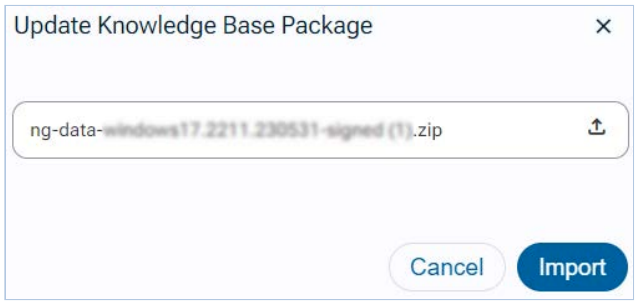


Update Knowledge Base Package



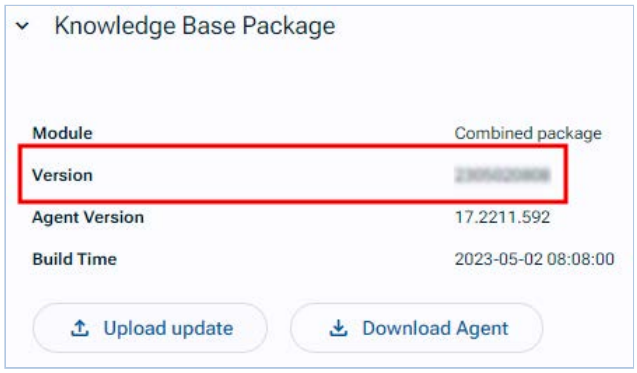
Choose a File

5. Click **Import.**



Import

6. The updated Knowledge Base version number is displayed below:
    - A Knowledge Base update may take up to ~10 minutes to propagate across the Sepio platform after the new version number appears in the web interface.
    - The risk assessment for existing and newly connected USB peripherals and network devices will use the updated Knowledge Base data.



Updated knowledge base version number

**Note:** Knowledge Base updates may take up to ~10 minutes to fully propagate across the Sepio platform.

## Update the Knowledge Base using API

To use the API for Knowledge Base update, you should complete the following steps:

1. Get API token
2. Verify the API token
3. Upload Knowledge Base file

### Get API Token

- please update username and password if needed

```
TOKEN=$(curl --location --insecure --request POST 'https://localhost/prime/webui/Auth/LocalLog
  --header 'Content-Type: application/json' \
  --data-raw '{ "username": "Administrator", "password": "SepioSystems" }' | \
  jq -Rr 'fromjson? // {"token": ""}' | \
  jq -r '.token')
```

### Verify Token

- This command checks if the token is working.
- You should see a response indicating the version and other parameters.

```
curl --location 'https://localhost/prime/webui/admin/PrimeVersion' \
  -H 'Authorization: Bearer '"$TOKEN" \
  --insecure
```

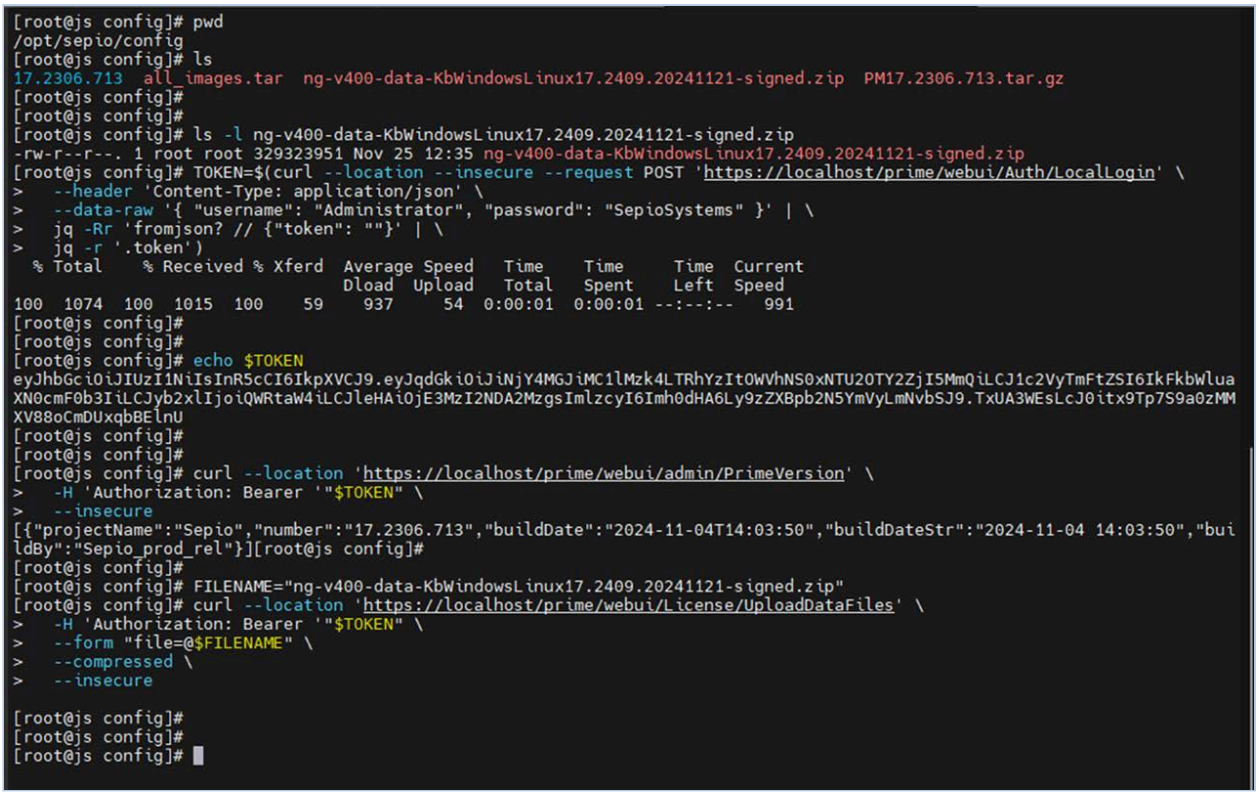
### Upload Knowledge Base File

- Run this command in the directory where the file is located.

- Please update the filename with the correct Knowledge Base file name.

```
FILENAME="ng-v400-data-KbWindowsLinux17.2409.20241121-signed.zip"
curl --location 'https://localhost/prime/webui/License/UploadDataFiles' \
  -H 'Authorization: Bearer '"$TOKEN" \
  --form "file=@$FILENAME" \
  --compressed \
  --insecure
```

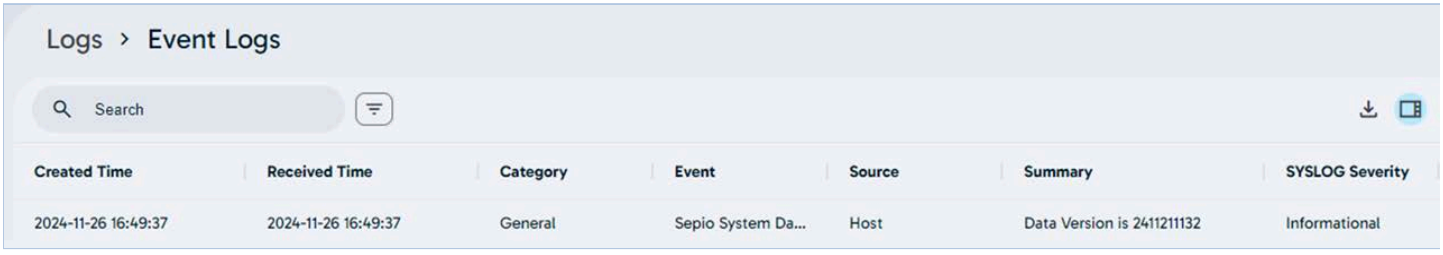
### Linux Console Session Log




Linux console session

### Result of the Procedure in the Sepio Web UI

- **Event Logs:** Timestamped update will be shown.
- **Audit Trail:** Timestamped update will be shown.




Event logs – Timestamped update




Audit trail – Timestamped update

# Platform Configuration

## Related Topics

- Platform Configuration
  - Setting Agents Connection Intervals
  - Managing Integrations
  - Setting Host/s (Agent) Mode

## Setting Agents Connection Intervals

The Agents require connectivity to the Sepio Platform Management to provide security alerts, system updates, inventory, and notifications. As part of the communication protocol between the Agent and the Platform Management, updates are sent to the Agent. The Agent initiates communication with the Platform Management.

The Agent sends the following data (and more) to the Platform Management:

- Immediate notification – Data that requires immediate action by the Platform Management , such as a security alert: For example, when connecting a peripheral device the Agent immediately identifies it and sends the Management Platform a message, as this device may harm the platform.
- Data that does not require immediate action by the Management Platform, such as Assets status updates, logs and keep alive information.

Data that does not require immediate action by the Platform Management is sent using a changing interval load balancing algorithm to automatically support scaling up and down. A calculated connection interval is used for this data.

The connection interval determines how often the Platform Management waits for a connection request from the Agent. The Management Platform makes three consecutive requests, and if the Agent does not respond after the third request, it is marked as disconnected. To ensure that non-response is not a result of Platform Management load, the connection interval is changed. It is calculated according to the connection duration and the number of Agents connected to the Platform Management.

The more Agents connected, the longer the interval duration is. By default, the connection duration is 5 seconds for every 400 Agents.

You can modify the default by setting a connection interval in the Platform Management config.env file (as described in the procedure below).

For example, if 1000 Agents are connected to the Platform Management and the connection detection interval is 5 seconds (default), the Platform Management will expect a communication update from the Agent every 15 (3×5) seconds {400(5 seconds)+ 400(5 seconds)+ 200(5 seconds}. After 3 connection attempts, the Platform Management shows the Agent as disconnected. In this example, after approximately 45 seconds (total duration of the 3 requests).

**Note:** Security events are immediately pushed to the Platform Management and are displayed in the UI.

**Note:** Agents that are shown as disconnected still perform actions according to the installed policy.

**Note:** Agents logs and messages are saved locally until communication with the Platform Management is restored.

## To Set the Connection Interval Duration

- In the Platform Management (Server) config.env file modify the following variables:

PERIODIC_REPORT_INTERV – Agent's periodic report interval (i.e connection interval)

AGENT_COUNT_FOR_PERIODIC_REPORT_INTERVAL – maximum number of Agents before lowering report interval (i.e. connection interval)

## Managing Integrations

In today's complex cybersecurity landscape, no single security tool can provide comprehensive protection against the ever-evolving threats. Connecting the Sepio Platform to other security products as part of a complete security solution stack provides multiple benefits including automated Incident Response (IR) and remediation, improved operational efficiency, cost savings and overall, better resiliency and security posture.

Integrations allow you to seamlessly connect to other security platforms. Several partner solutions like Syslog, Splunk, Guardicore and more require a configuration on both the Sepio Platform as well as the other tool. Other integrations are configured on the other tool's side only.

See the integrations section.

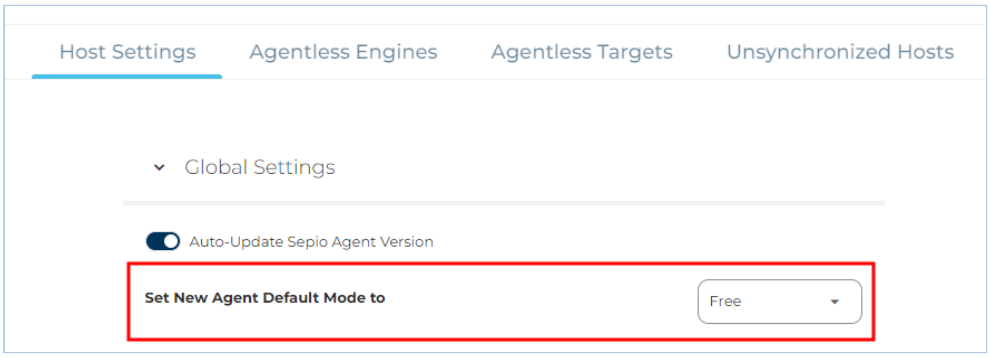
## Setting Host/s (Agent) Mode

The **Host (Agent) mode** defines how a Host behaves when detecting a risky Asset/Peripheral. An Agent is installed on a Host.
When connecting a new Host to the Sepio Managment Platform, you can define the default mode (and change it at a later stage).

| Mode | Description |
|---|---|
| Free | No action is performed on a Peripheral by the Platform, so all actions must be performed manually. |
| Armed | The Platform automatically 'Blocks' a 'Disapproved' Peripheral (it does not 'Block' an 'Approved' Peripheral). You can also manually 'Block' an 'Approved' Peripheral by selecting 'Disapprove'. |
| Block Known Threats | The Platform automatically 'Blocks' an Asset /Peripheral, known as an attack tool, whether its risk is 'Approved' or 'Disapproved'. **Note:** You can't 'Block' a Peripheral manually if the Host is set to this mode. |
| Block Mass Storage devices and Known Threats | The Platform automatically 'Blocks' an Asset /Peripheral that is classified as a USB Mass Storage Device (including thumb drives, disk on key, mobile phones with storage interfaces etc.) as well as any Asset /Peripheral known as an attack tool whether it's 'Approved' or 'Disapproved'. **Note:** You can't 'Block' a Peripheral manually if the Host is set to this mode. |
| None | Keep the mode that is defined on the Host itself |

## To Set a New Host Default Mode (to be activated when connecting a Host to Sepio)

1. From the Sepio menu, select **Settings** -> **Host Settings** -> **Global Settings**.
2. In the **Set New Agent Default Mode to** dropdown list, select the required option (see descriptions in the table above).

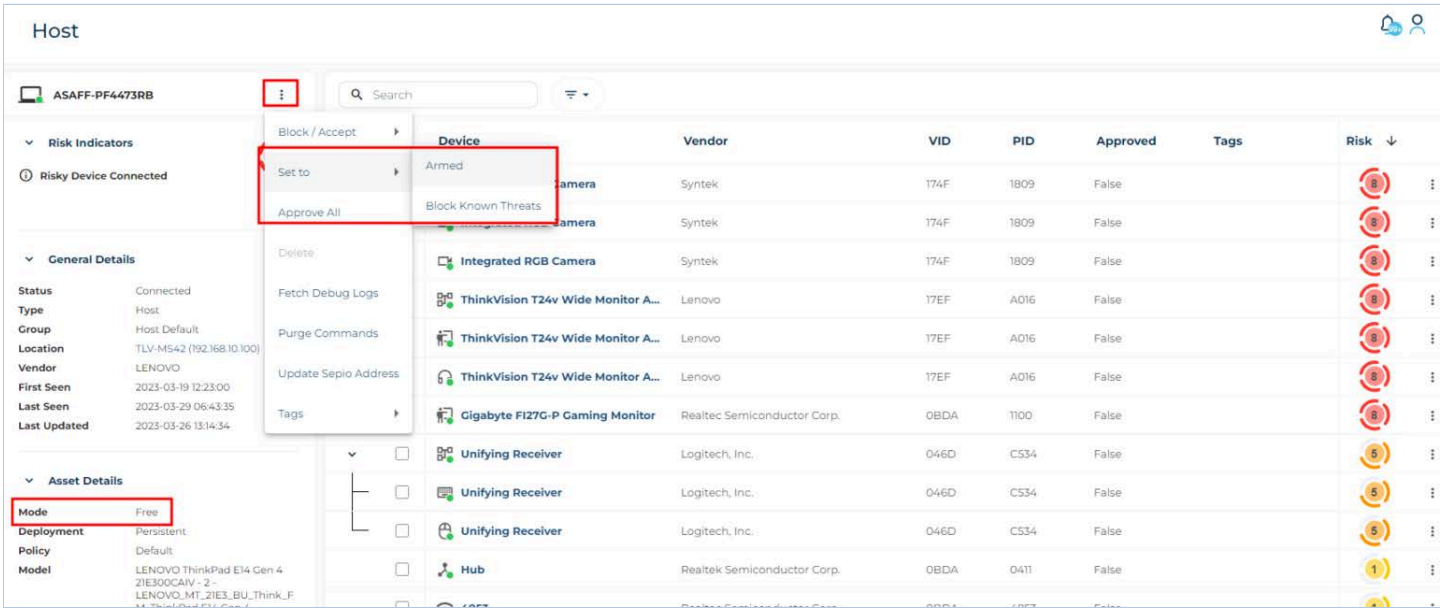



Set New Agent Default Mode to

## To Set a Host Mode

1. In the **Discovered Assets** or **Hosts visibility view**, click on the Host name for which you want to set the mode.
2. Click ⋮ then **Set to** and select required option, as described in the above table.

> **Note:** The Host mode is displayed in the **Asset Details** section.




Hosts visibility view

# Post Installation and Update Checklist

## Post-Installation Checklist

This **Post-Installation Checklist** provides a structured, step-by-step guide designed to validate the successful deployment of Sepio. It outlines a series of tests, verifications, and configurations that must be performed *immediately after* the installation to ensure the correct functionality.

The primary objective of this checklist is to:

- Confirm that all components have been properly installed.
- Validate that system functionality aligns with expected behavior.
- Ensure initial security and operational requirements are met.

> **Note:** Completion of this checklist is required before the system is moved to a production environment.

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 1 | Install environment | | | |
| 1.1 | | Install the environment using the latest version | Install process executed successfully | |
| 1.2 | | Check Visibility overview field | The data (online asset distribution and recent visible risk) appears as expected | |
| 2 | Deploy external Scan Engines (if applicable) | Deploy external Scan Engines | Scan Engine is installed and appeared as connected (after activation) | |
| 3 | KB upload (if applicable) | Upload the Knowledge Base (KB) to the environment | KB is successfully uploaded | |
| | Upload network infrastructure elements | Upload switches and WLC using bulk operation with a file | Switches and WLCs are created, appear as connected, and are successfully scanned | |
| 4 | Data verification | Verify data correctness on specific switches, | Data on the ports and in the switch modal corresponds to | Check ports (connection |

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| | | WLC | the expected values | status, risk, switch general data) |
| 5 | Change scan priority | Change network infrastructure scan priority | Switch and WLC are scanned according to new priority | |
| 6 | Change switch domain | Change switch domain | Switch domain changed successfully, and switch is scanned | |
| 7 | Manual switch scan | Perform switch scan “on demand” | Switch is scanned | |
| 8 | Move peripheral between ports | Move peripheral between ports | Asset is shown on new port | Scanning is required to complete this action. |
| 9 | Move peripheral between switches | Move peripheral between switches | Asset removed from previous switch and shown on relevant switch | Ensure a scan is performed after the action |
| 10 | Check switches for “error” statuses | Check switches for “error” statuses | No switches in “not supported” status | |
| 11 | Check location on devices connected to managed switch | Check location on devices connected to managed switch | Location is correct | |
| 12 | Check first seen for existing (pre upgrade) network asset | Check first seen for network asset | The timestamp is correct | Make sure “first seen” is prior to system upgrade |
| 13 | Check switch last scan and last updated | Check switch last scan and last updated times | No significant delays (more than a couple of minutes) between expected and actual times | Take scan priority into consideration |

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 14 | Fetch Scan Engine logs | | | |
| 14.1 | | On the network infrastructure, click “Fetch Debug Logs” | | |
| 14.2 | | Go to settings -> about -> system health -> Available Debug Logs (last 24 hours) | Scan Engine logs are there | It might take a few seconds |
| 15 | Download sepio agent | Download sepio agent using button | Agent installation file is downloaded (the version is official) | |
| 16 | Check “About” page | Check “About” page | All data is consistent (backend version as expected, and the KB version is recent) | |
| 17 | Export data from “all assets” | Add all columns to the UI. Filter some data from “all assets page” and export it once to csv and once to PDF | Filtered data is successfully exported | |
| 18 | Define, run, and send user query | Define user query on assets and set scheduled query time | The query is sent via email on time | |
| 19 | Run legacy report | Download Asset Visibility report | Report is created successfully | |
| 20 | Check event logs | Check event logs | Both agent and network events can be seen in event log | |
| 21 | Check audit logs | Check audit logs | Latest user actions can be seen in audit log | |
| 22 | Check environment dashboard | Grafana check environment dashboard | No services are down, and no bottlenecks exist for any services | On prem customers with deployed monitoring |

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 23 | Check Syslog/Splunk integration (if applicable) | Check Syslog/Splunk for incoming Sepio events | Events from the Sepio platform are visible in the system | |
| 24 | Install Sepio agent on host | | | |
| 24.1 | | Install agent | New agent successfully registered on host | |
| 24.2 | | Test a few commands (change agent mode, approve/disapprove peripheral) | | |
| 25 | New agent gets default mode | Check agent mode after install | Agent gets default mode (as defined in server settings) | |
| 26 | Check if the managed host has correct information | Verify data correctness on managed host | Ensure all agent properties exist and are correct: host identifier, status, vendor, first seen/last seen/ last updated , mode, deployment, model, ip, mac, software, uuid, assets number, version | |
| 27 | Detect USB device | | | |
| 27.1 | | Connect a usb peripheral to computer (like mouse) | The peripheral appears in the Host view in connected status and with correct details | |
| 27.2 | | Disconnect the device to computer | The device appears as disconnected | |
| 28 | Verify peripherals data on managed host | Verify peripherals data on managed host | Make sure all the peripheral properties exist and correct: vid, pid, first seen/last seen/ last updated, status, location | |

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 29 | Change agent mode | Change agent mode to one that differs from current | Agent mode is changed accordingly (Free/Armed/BKT/BST) | |
| 30 | Approve USB peripheral | Approve USB peripheral | Device is approved | |
| 31 | Fetch Agent debug logs | | | |
| 31.1 | | On server from hosts screen or the host itself, press “fetch debug logs” (make sure the agent is connected) | | |
| 31.1 | | Go to settings -> about -> system health -> Available Debug Logs (last 24 hours) | The agent log is there (it might take a few seconds) | |
| 32 | Verify environment health | Verify container health using Run “docker ps” commands | All containers appear healthy | |

## Post-Update Checklist

This **Post-Update Checklist** is a structured document intended to be executed following any software update, patch, or configuration change applied to Sepio’s components or the connected infrastructure.

Its primary objective is to confirm that:

- The update was applied successfully.
- No regressions or unintended issues were introduced.
- The system continues to operate correctly and securely with the updated version.

**Important**

**Before performing the update, it is essential to collect baseline system statistics.** We recommend documenting the following data points and comparing them after the update is successfully completed:

- Total number of assets – both connected and disconnected.

- Number and status of network infrastructure elements (e.g., switches, wireless LAN controllers).
- Number of supervised hosts – both connected and disconnected.

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 1 | Upgrade environment | | | |
| 1.1 | | Upgrade environment to the latest version | Upgrade process completed successfully | |
| 1.2 | | Check Visibility Overview field | The data (online asset distribution and recent visible risk) appears as expected | |
| 1.3 | | Check asset count by type (switches, WLCs, hosts, all assets) | After upgrade, asset count and connection status show no significant changes | |
| 1.4 | | Upgrade external Scan Engine to the latest version (if applicable) | Scan Engine upgraded and switches continue to be scanned | |
| 2 | KB upload (if applicable) | Upload the Knowledge Base (KB) to the environment | KB uploaded successfully | |
| 3 | Switch data verification | Verify data correctness on a specific switch | Data on the ports and in the switch modal corresponds to the expected values | Check ports (connection status, risk, general switch data) |
| 4 | Create switch | Upload switch from .csv (if applicable) | New switch is created, appears as connected, and is scanned successfully | |
| 5 | Change switch scan priority | Change switch scan priority | Switch is scanned according to the new priority | |
| 6 | Change switch domain | Change switch domain | Switch domain changed successfully and scanning continues | |

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 7 | Manual switch scan | Perform manual “on-demand” switch scan | Switch is scanned | |
| 8 | Move peripheral between ports | Move peripheral between ports | Asset appears on new port | Don’t forget to scan after the action |
| 9 | Move peripheral between switches | Move peripheral between switches | Asset appears under the new switch | Don’t forget to scan after the action |
| 10 | Check switches for “error” statuses | Check switches for “error” statuses | No switches in “not supported” status | |
| 11 | Check location on devices connected to managed switch | Check location on devices connected to managed switch | Location is correct | |
| 12 | Check first seen for existing (pre upgrade) network asset | Check first seen for network asset | The timestamp is correct | Make sure “first seen” is prior to system upgrade |
| 13 | Check switch last scan and last updated | Check switch last scan and last updated times | No significant delays (more than a couple of minutes) between expected and actual times | Take scan priority into consideration |
| 14 | Fetch Scan Engine logs | | | |
| 14.1 | | On the network infrastructure page, click “Fetch Debug Logs” | | |
| 14.2 | | Go to settings -> about -> system health -> Available Debug Logs (last 24 hours) | Scan Engine logs are there | It might take a few seconds |

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 15 | Download Sepio agent | Download Sepio agent using button | Agent installation file is downloaded (the version is official) | |
| 16 | Check “About” page | Check “About” page | All data is consistent (backend version as expected, and the KB version is recent) | |
| 17 | Export data from “all assets” | Filter some data from “all assets page” and export it once to csv and once to PDF | Filtered data is successfully exported | |
| 18 | Define, run, and send user query | Define user query on assets and set scheduled query time | The query is sent via email on time | |
| 19 | Run legacy report | Download Asset Visibility report | Report is created successfully | |
| 20 | Check event logs | Check event logs | Both agent and network events can be seen in event log | |
| 21 | Check audit logs | Check audit logs | Latest user actions can be seen in audit log | |
| 22 | Grafana – check environment dashboard | Grafana – check environment dashboard | No services are down, and no bottlenecks exist for any services | |
| 23 | Check Syslog/Splunk integration (if applicable) | Check Syslog/Splunk for incoming Sepio events | Events from the Sepio platform are visible in the system | |
| 24 | Update agent to newer version (if applicable) | | After a few minutes, the agent reports the latest version | |
| 25 | | Update the agent version | The agent version was updated | |

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 26 | | Test a few commands (change agent mode, approve/disapprove peripheral) | The commands work | |
| 27 | Check if the managed host has correct information | Verify data correctness on managed host | Ensure all agent properties exist and are correct: host identifier, status, vendor, first seen/last seen/ last updated, mode, deployment, model, ip, mac, software, uuid, assets number, version | |
| 28 | Detect USB device | | | |
| 28.1 | | Connect a USB peripheral to computer (like mouse) | The peripheral appears in the Host view with a connected status and displays the correct details | |
| 28.2 | | Disconnect the device from the computer | The device appears as disconnected | |
| 29 | Verify peripherals data on managed host | Verify peripherals data on managed host | Make sure all the peripheral properties exist and correct: vid, pid, first seen/last seen/last updated, status, location | |
| 30 | Change agent mode | Change agent mode to one that differs from current | Agent mode is changed accordingly (Free/Armed/BKT/BST) | |
| 31 | Approve USB peripheral | Approve USB peripheral | Device is approved | |
| 32 | Fetch Agent debug logs | | | |
| 32.1 | | On server from hosts screen or the host itself, press “fetch debug logs” (make sure the agent is connected) | | |

| # | Test | Steps | Expected | Comments |
|---|---|---|---|---|
| 32.1 | | Go to settings -> about -> system health -> Available Debug Logs (last 24 hours) | The agent log is there (it might take a few seconds) | |
| 33 | Check container status | Run “docker ps” command to verify container health | All containers appear healthy | |

# Sepio Platform SaaS

## Sepio Platform Managed from the Cloud – SaaS

Sepio Platform SaaS provides an integrated, turnkey solution managed from the cloud. To prepare for production, the following steps will be taken:

## Initial Access

Sepio Customer Success team will provide the initial credentials to access the system on Sepio Cloud. This will include the platform DNS name and authentication credentials. Administrators are requested to change their initial passwords upon first login.

> **Note:** additional information about platform security, privacy and compliance is available in the Sepio Trust Center.

## Corporate Connectivity Requirements

It is possible to limit access to the management interface by setting access control policies for authorized IP addresses that belong to the customer's corporate address range.

By default, the Sepio cloud will not initiate connections into customer's environment or other deployment components and thus there are no specific requirements. You should allow TCP 443/TLS connections from corporate networks towards the Sepio Management Platform DNS name.

> **Note:** Detailed connectivity diagram is available here: About Sepio > Connectivity Diagram.

## On Customer Premises Scan Engine

On premises Scan Engine (sometimes referred to as "external" or "external scan engine") are deployed on customer premises and connect to the network infrastructure in order provide DNA Asset related information. The Scan engine initiates outbound connections over TCP 443/TLS to the Sepio Platform in the cloud.

> **Note:** Detailed installation and configuration instructions are available here: Platform Installation and Update > Installation > Installing and Activating a Sepio Scan Engine.

## Host Agents

Sepio Host agents should be allowed to connect to the Sepio Platform in the cloud. Apart from setting up and configuring various agent parameters (such as the FQDN for the Sepio Platform's management interface and, optionally, for the Agent recovery server), no further action is required.

## Integrations

The Sepio Platform SaaS can be integrated with corporate services, including SAML/Active Directory, SIEM, SOAR, and more. Please refer to the integrations section of the manual for detailed configuration instructions.

## Proactive Monitoring and Maintenance, Platform, and Knowledge Base Updates

Sepio provides proactive environment monitoring and maintenance, along with regular SaaS platform updates as part of our continuous improvement process.
Customers are encouraged to report any issues and to open support tickets by contacting the Customer Success team at support@sepiocyber.com.

# Deep Dive

## Related Topics

- Agent Deep Dive
- Advanced Agent Security Model: Enhanced Host Agent Security
- Knowledge Base Deep Dive
- MAC Addresses Deep Dive
  - MAC Address Learning and Asset Visibility
- Deep Dive on Network Architecture
- Deep Dive: Campus and Data Center Switching
- Deep Dive on Switch Stacking
- USB Deep Dive
- USB Billboard Device
- Raspberry Pi Deep Dive
- Deep Dive on Mouse Jigglers
- Deep Dive on Cisco Switch Interfaces
- CDP and LLDP Protocols
- Deep Dive on WLC High Availability
- Deep Dive on First Hop Redundancy Protocols
- Deep Dive on 802.1X and Some of Its Limitations
- Anatomy of a “Duplicated MAC Address” Alert in High-Availability Networks

# Advanced Agent Security Model: Enhanced Host Agent Security

## Overview

Sepio's **Advanced Agent Security Model** is an operational enhancement designed to prevent **agent cross-tenant registration**, a configuration weakness that could allow a malicious or compromised agent to register with an unauthorized **Sepio Management Platform** server. This security model implements server-side authorization and cryptographic identity verification for each host agent. In practice, the Sepio host agent now furnishes a cryptographically signed identity token with every request, and the server strictly validates this token against the expected tenant.

This ensures that agents can only register with their intended **Management Platform** (sometimes being called or referenced as a tenant), and any attempt to alter the server fields in the request (for example, by a threat actor or an attacker) will be detected and rejected. By embedding strong identification into the agent's communication, the platform guarantees the **authenticity** of the agent and the **integrity** of its messages. In summary, this enhancement locks each agent to its proper destination through cryptographic means, addressing concerns about server isolation, impersonation, and tampering in the agent registration process.

## Solution Overview: Server-Side Authorization & Identity Verification

The Advanced Agent Security Model introduces **server-driven enforcement of agent identity**.
Sepio's Management Platform server requires agent to present a cryptographic proof of identity as part of the handshake. This is implemented through the use of secure tokens embedded in the agent's requests:

- **Unique Registration Token per Agent/Tenant**
  When a new agent is deployed, it is provisioned with a secure, tenant-scoped token that it must present during registration. This token is generated by the Sepio management platform (server side) and is cryptographically bound to the target Tenant (and optionally to that specific agent or installation instance).
- **Server-Side Validation**
  Upon each agent request to the server, the server extracts the token and verifies it. Because the token is signed by the server itself the server can detect if it's been forged or altered.
  The token's payload explicitly tells the server which Tenant and context this agent was authorized for. If the agent's request claims to be for a different tenant than what the token specifies – or if the token is missing/invalid – the server will reject the request outright.

## Requirements

- **Server Version:** Sepio platform V59 and above
- **Agent Version:** 17.2604.100 and above

## Token Fetching

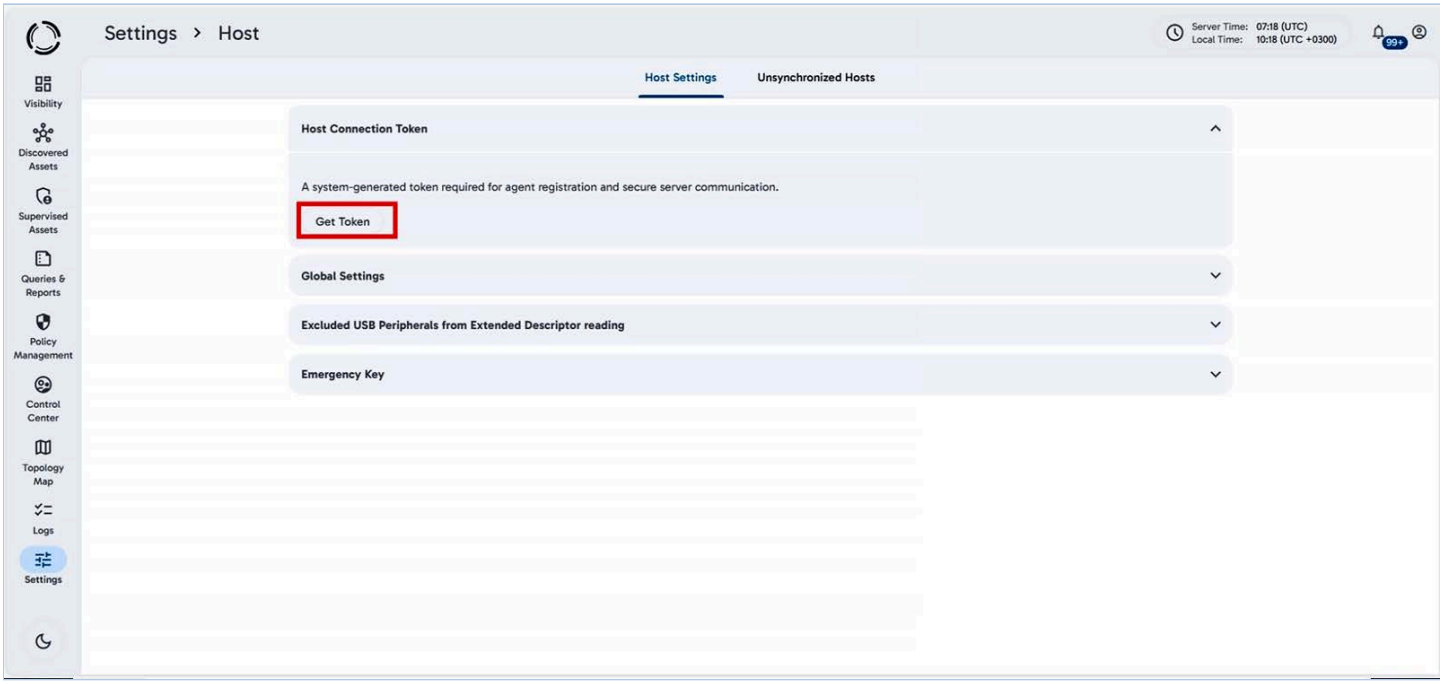
To enable token access:

1. Set the feature flag:
   `ENABLE_TOKEN_VALIDATION_VIEW = True`

> **Note:** This flag only enables token visibility in the UI. It does not enforce validation or block agents without tokens.

2. Navigate to:
   Settings -> Host

3. Click "**Get Token**" to retrieve the server token



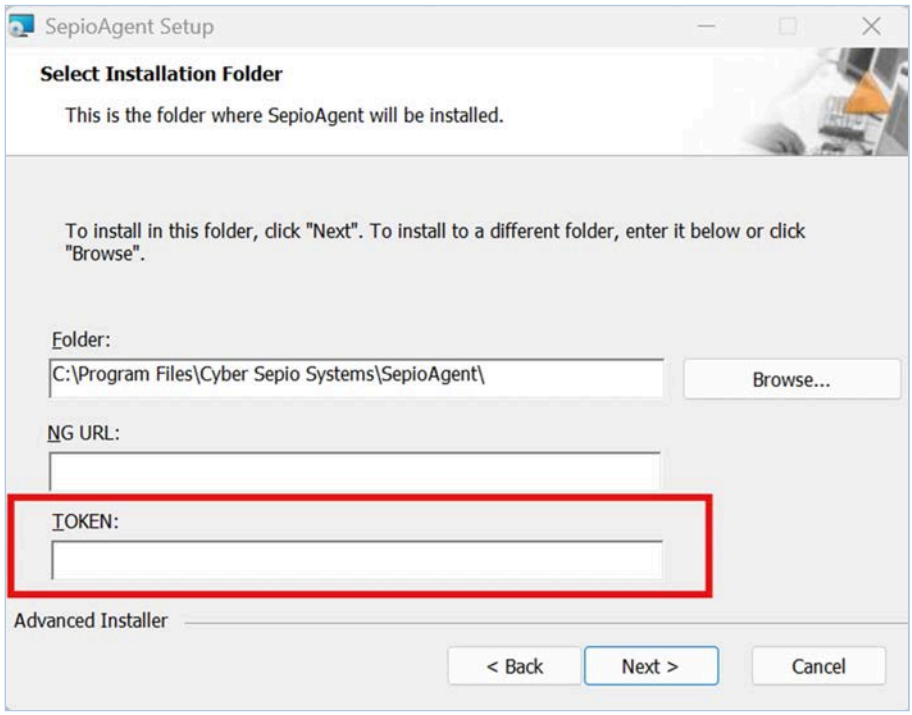

Get Token

## Agent Installation

### 1. Fresh Installation

During installation of a new agent:

- A dedicated field is available to input the **server token**
- The token must match the target server




Sepio Agent Installation – Input Token

### 2. Upgrading Existing Agents

When upgrading from an older agent version:

- **Windows agents:**
  Automatically receive the token during upgrade
- **macOS / Linux agents:**
  Require a **fresh installation** to receive the token

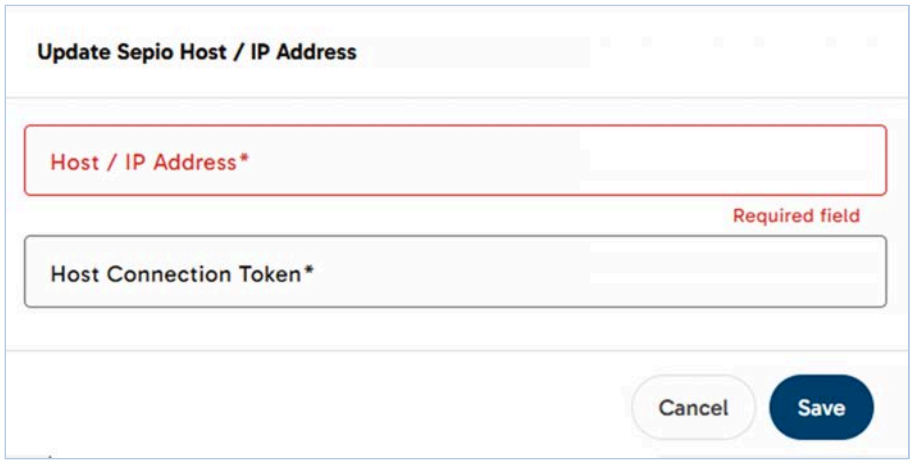
### Changing Agent Server (Update Sepio Address)

When using the **"Update Sepio Address"** capability:

- The agent **must include the token of the new server**
- Otherwise, the connection will be rejected

A new UI option allows specifying the token during the server update process.

> **Important:** The token must correspond to the **destination server.**



Update Sepio Host / IP Address

### Enabling Server-Side Token Enforcement

Once all agents are upgraded and properly configured:

1. Set the enforcement flag:
   `FORCE_TOKEN_VALIDATION = True`
2. After enabling:

- Any agent without a valid token will be **rejected**
- Any outdated agent version will be **blocked**
- Only properly authenticated agents can communicate with the server

> **Important:** This step should only be performed after ensuring full agent readiness across the environment.

### Logs

When token validation is enabled, the AgentsAPI service generates logs for rejected requests to assist with troubleshooting and validation.

### Missing Token

If an older agent version (that does not support token validation) sends a request without a token, the server will reject the request and log:

“`No token provided in the request headers.`”

### Token Mismatch

If an agent sends a request with an invalid or incorrect token, the server will reject the request and log:

“`Token mismatch detected. Extracted token: {Token}, does not match master token.`”

These logs can be used to identify:

- Agents that were not upgraded
- Misconfigured agents (e.g., incorrect server token)
- Potential unauthorized or tampered requests

# Deep Dive into Campus and Data Center Switching Architecture

## Overview

In modern networking, the term *switch* describes two very different design philosophies. **Campus switching** is optimized for people, mobility, and endpoint diversity, while **Data Center switching** is optimized for application throughput, deterministic latency, and scale. Both environments rely on Ethernet, but they use different topologies, buffering strategies, and security controls to solve very different operational problems.

This distinction matters because most enterprises operate in both environments simultaneously. Campus networks sit at the human edge, where the primary challenge is connecting diverse devices securely and reliably, while Data Center fabrics support applications, east-west traffic, and increasingly latency-sensitive workloads. That also creates a trust gap: the network may know where traffic is flowing, but not always what is physically connected to the port or whether that hardware should be trusted.

## Two Different Missions

Campus networks are built to connect people and mobile devices across buildings, floors, and shared spaces, connecting multiple LANs within a limited geographical area.They must support laptops, phones, printers, cameras, IoT devices, and wireless access points, often with Power over Ethernet and access controls at the edge. Depending on the use cases, campus networks may support IT, IoT and OT applications, although for OT it is more common to deploy dedicated, physically separated networks.

Data Center networks are built for application performance. Their priorities include high bandwidth, predictable latency, rapid failover, and scalable segmentation for servers, storage, and east-west traffic inside the fabric.

The following table summarizes the main differences between Campus and Data Center switching:

| **Dimension** | **Campus switching** | **Data Center switching** |
|---|---|---|
| Primary purpose | Connect people and endpoint devices | Connect applications, servers, and storage |
| Common traffic pattern | North–south | East–west |
| Typical topology | Hierarchical tree | Leaf-spine / Clos |
| Priority focus | Voice, video, endpoint access | Storage, compute, low latency |

| Dimension | Campus switching | Data Center switching |
|---|---|---|
| Security emphasis | Identity, access, segmentation | Fabric policy, multihoming, congestion control and protection |

Sepio's relevance spans both environments because device identity and hardware trust matter at every attachment point. In campus networks, this usually means identifying unmanaged or spoofed devices at the edge. In Data Centers, it means validating that connected infrastructure is truly what the environment expects it to be.

## Topology and Forwarding

Campus networks traditionally follow a hierarchical model with access, distribution (or aggregation), and core layers. This design maps well to physical buildings and user populations, and it was historically optimized for north-south traffic flowing from user devices toward shared applications or the internet. The model is modular and can be implemented as either a two-tier (collapsed core) or three-tier architecture, depending on the size and requirements of the deployment site.

**Figure 1. Campus networks use a hierarchical tree, while Data Centers use a leaf-spine fabric designed for symmetry, scalability, and low latency.**

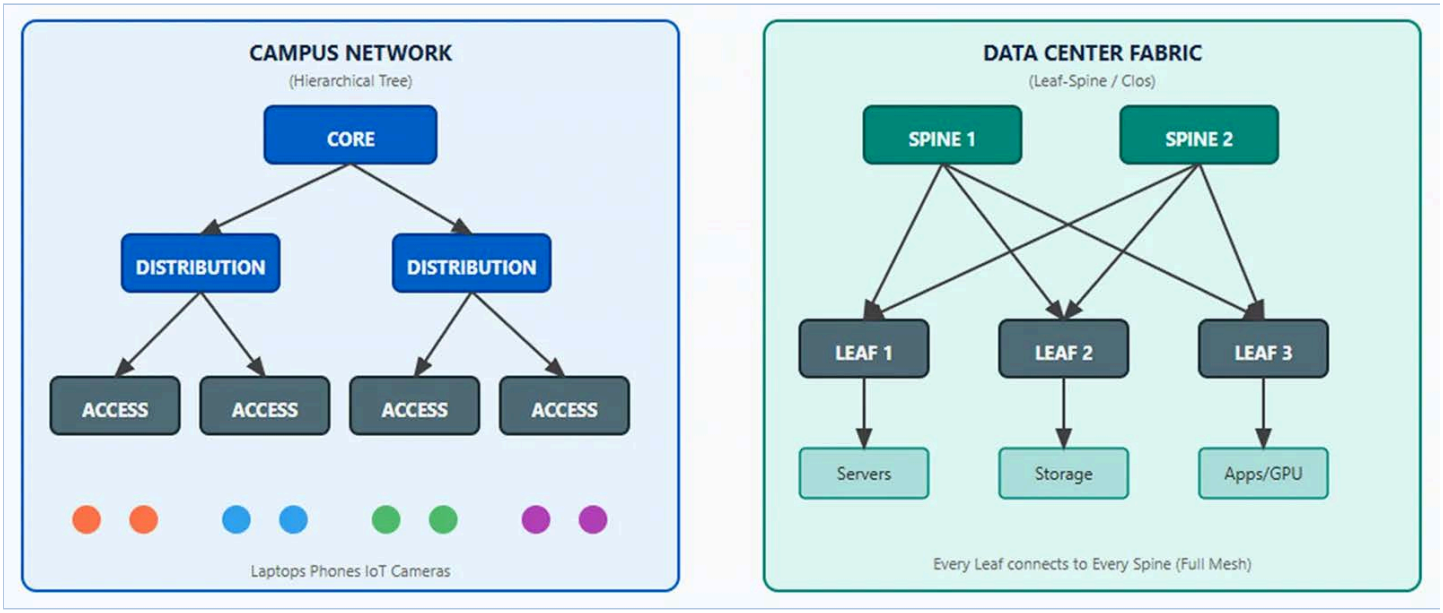



Figure 1. Campus networks use a hierarchical tree optimized for north-south user traffic, while Data Centers use a leaf-spine fabric designed for symmetric east-west application traffic, scalability, and low latency.

Data centers typically use leaf–spine architectures, where each leaf switch connects to every spine switch. This design creates predictable hop counts and more uniform latency between workloads, which is why it has become the dominant architecture for modern fabrics. See also the deep dive references for a detailed comparison of topology designs.

In the Data Center, the physical underlay is usually a Layer 3 routed IP, often using BGP, while the overlay commonly uses VXLAN. RFC 7348 defines VXLAN as a mechanism for extending Layer 2 networks across Layer 3 infrastructure using tunnel endpoints and a 24-bit VNI, providing significantly greater segmentation scale than VLANs. EVPN, standardized in RFC 7432, adds a BGP-based control plane for MAC and IP reachability, multihoming, and more deterministic endpoint distribution.

## Traffic Behavior

Campus traffic is usually dominated by north-south flows. Users access SaaS, browse the internet, connect to cloud applications, or reach centralized services outside the local segment.

**Figure 2. Campus traffic is primarily north-south, while Data Center traffic is predominantly east-west.**

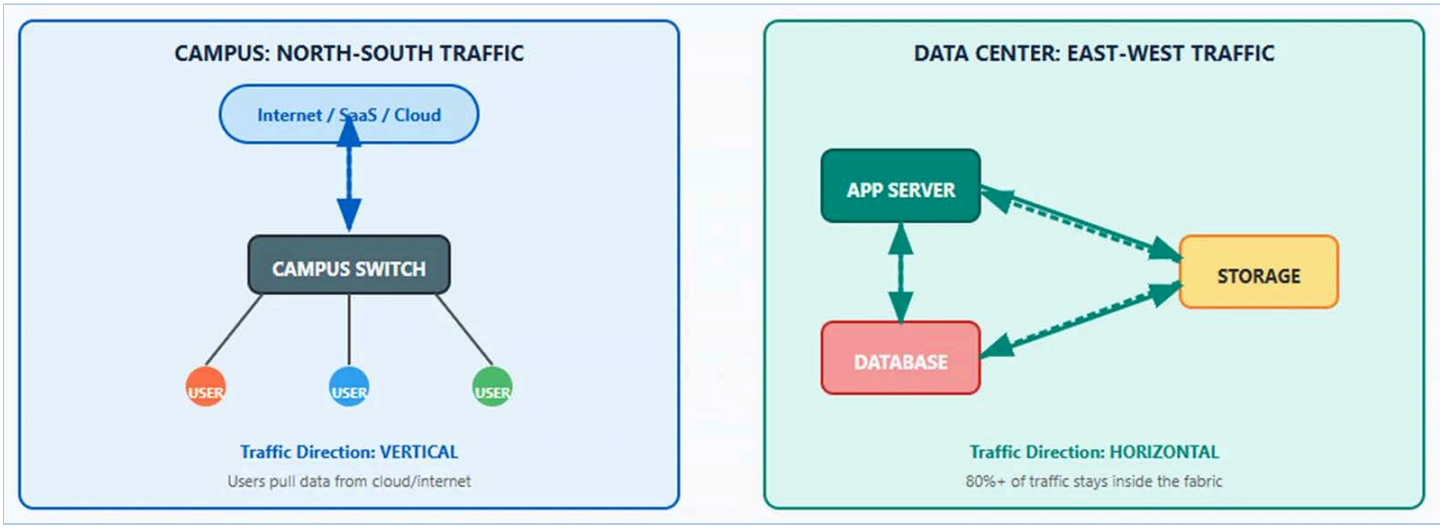



Figure 2. Campus traffic flows north-south between users and the cloud. Data Center traffic is predominantly east-west, with servers, databases, and storage communicating laterally within the fabric.

Data Center traffic is different. Much of it remains inside the fabric, with application servers communicating with databases, storage systems, hypervisors, or other microservices. As a result, east–west traffic patterns, rather than uplink bandwidth alone, define most Data Center switching requirements.

This difference in traffic patterns also changes the threat model. In campus environments, risk is concentrated at the edge, where unknown devices connect to access ports. In Data Centers, risk often shifts to trust in infrastructure nodes, control-plane consistency, and endpoint correctness inside the fabric.

## Congestion and Buffers

Campus networks typically tolerate unpredictable bursts by using deeper buffers and access-layer policies that absorb variations in user behavior. A large download, video stream, or roaming event may create temporary spikes, but the network is designed to smooth them out.

Data Center fabrics are optimized differently. They often prioritize low latency and fast forwarding over very deep buffers, which means congestion must be signaled quickly and handled precisely. ECN, defined in RFC 3168, allows network devices to mark packets instead of dropping them when congestion begins, giving the sender an early warning. RFC 8257 describes DCTCP, which uses those ECN marks to adjust transmission more precisely in shallow-buffered Data Center environments.

**Figure 3. ECN-based congestion signaling lets Data Center networks control microbursts before buffer overflow occurs.**

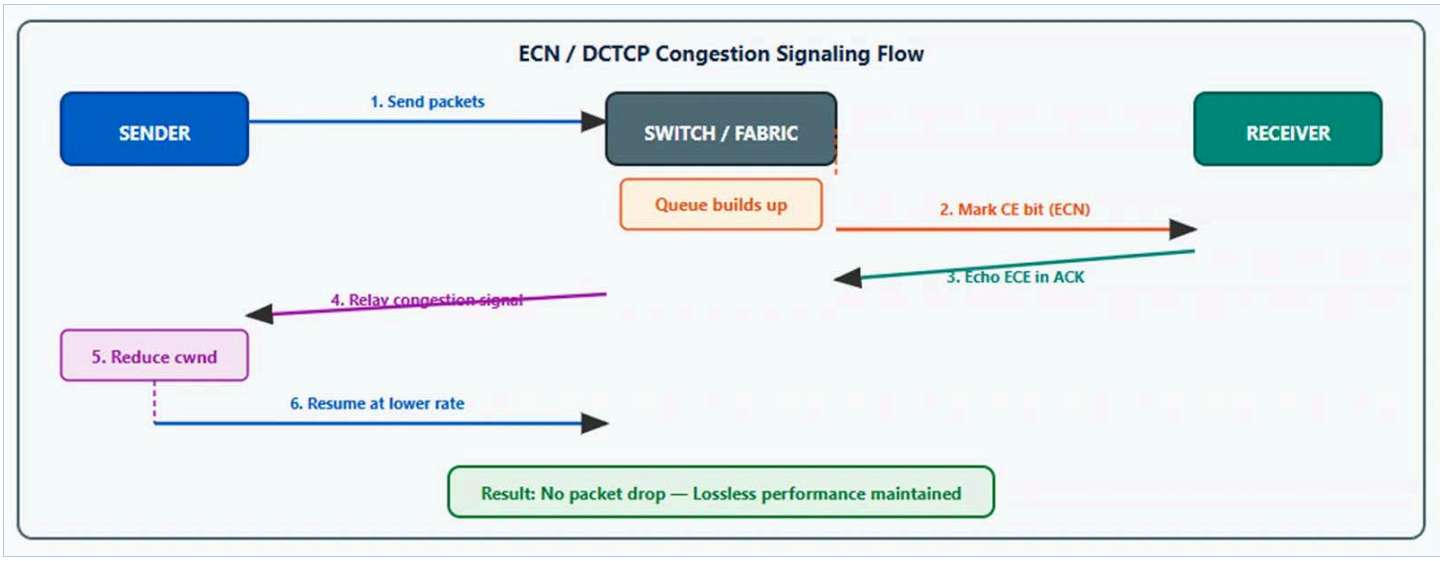



Figure 3. ECN marks packets instead of dropping them. DCTCP uses this signal to precisely reduce the sender congestion window, preventing buffer overflow in shallow-buffered Data Center fabrics (RFC 3168, RFC 8257).

This matters operationally because unexpected devices or misbehaving endpoints can disrupt these carefully tuned assumptions. In a campus environment, that might mean a rogue device generating abnormal traffic from an access port. In a Data Center, it may mean a badly behaving node contributing to congestion or pause events that affect many workloads.

## QoS and Traffic Classes

Campus QoS is generally human-centric. Voice and video traffic must be protected because delay and jitter are immediately visible to users. If a file transfer slows down, most people will not notice. If voice packets are delayed, the problem becomes obvious.

Data Center QoS focuses more on compute and storage behavior. IEEE 802.1Qbb Priority-based Flow Control allows pause behavior by traffic class rather than pausing the entire link, which is useful for loss-sensitive workloads. IEEE 802.1Qaz Enhanced Transmission Selection provides bandwidth management across traffic classes so multiple workloads can coexist more predictably.

The following table summarizes the main differences between Campus and Data Center QoS and traffic classes:

| Feature | Campus | Data Center |
|---|---|---|
| Main objective | Preserve user experience | Preserve application behavior |
| Sensitive traffic | Voice, video, collaboration | Storage, RPCs, RDMA |
| Typical method | Priority queuing | PFC, ETS, ECN-based control |

This is also where inventory accuracy matters. QoS policy assumes the network knows what kind of traffic and endpoint it is handling. Unknown hardware can undermine those assumptions, whether by generating unexpected classes of traffic or by bypassing intended policies.

## Security at the Edge and in the Fabric

Campus access control often begins with IEEE 802.1X, which provides port-based network access control and typically relies on RADIUS for authentication and policy decisions. This approach works well for managed endpoints, but it becomes more difficult when the network must accommodate printers, cameras, building systems, medical devices, and other headless systems that may not support full supplicant behavior.

IEEE 802.1AE (MACsec) adds confidentiality and integrity protection at the Ethernet layer, allowing line-rate encryption between peers such as switches or endpoints and switches. That helps protect traffic in transit, but it does not by itself prove that the connected device is the intended device.

**Figure 4. Network access is enforced in layers, from port authentication to encryption and policy-based segmentation.**

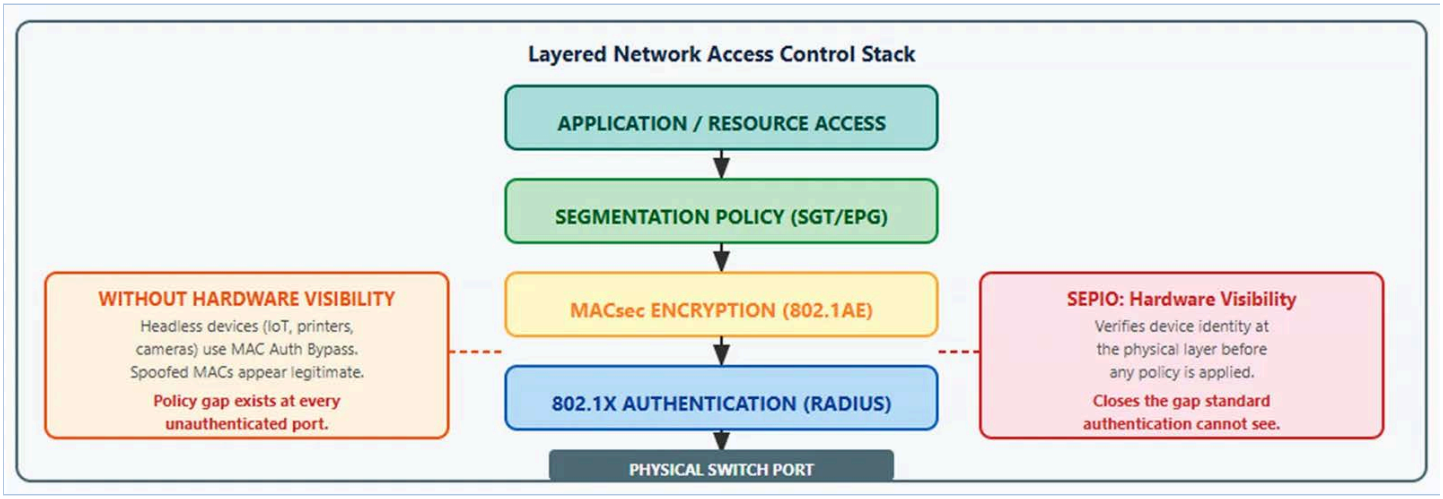



Figure 4. Network access is enforced in layers from physical port to application. IEEE 802.1X (port auth), 802.1AE MACsec (encryption), and segmentation policy work together — but none verify hardware authenticity. Sepio closes this gap at the physical layer.

In Data Centers, this layering extends deeper into the fabric through segmentation, routing policy, and the overlay control plane. EVPN helps advertise and synchronize endpoint state across the network, but that creates a dependency on control-plane correctness and infrastructure trust.

## Where the Security Model Breaks

Campus and Data Center networks fail in different ways.

In campus environments, the biggest challenge is often uncertainty at the edge. A port may be authorized for a known user or device class, but the actual connected hardware may be something else. Examples include a VoIP phone with a downstream Ethernet port feeding an unauthorized laptop, an unmanaged mini-switch hidden under a desk, a camera or printer using weaker fallback access methods, or a spoofed device presenting a familiar identity. In those cases, the network may allow access to something, but not necessarily to the device the organization believes is attached.

In Data Center, the risk shifts toward trust in the fabric itself. A VXLAN/EVPN design depends on accurate route distribution, endpoint reachability, and stable control-plane behavior. A rogue or misconfigured VTEP, a compromised automation workflow, or incorrectly advertised endpoint information can create traffic black holes, duplicate reachability, or policy drift across the fabric.

Lossless and low-latency features can also become a source of fragility. If pause mechanisms or congestion controls are abused by faulty or unexpected endpoints, the result can be disproportionate disruption in a highly optimized environment. Even encrypted links do not solve endpoint trust; MACsec protects the link, not the authenticity of the hardware connected to it.

**Figure 5. Security gap differences between campus and Data Center switching.**

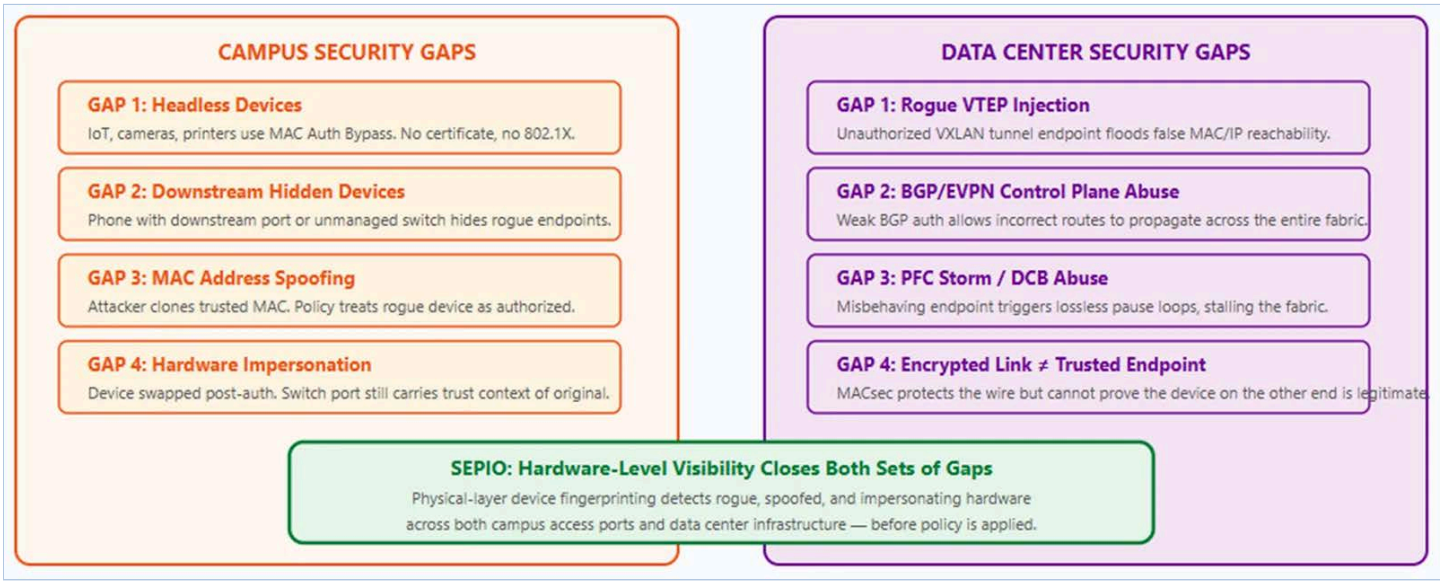



Figure 5. Campus security gaps originate at the physical edge; Data Center gaps originate inside the fabric. Both attack surfaces share a common root cause: insufficient hardware-level device identity assurance. Sepio addresses this across both environments.

This is where Sepio can be referenced without making the article product-heavy. The generic point is that policy alone is not enough when the network lacks trustworthy hardware visibility. Sepio addresses that gap by helping organizations validate the actual device connected to the network, rather than relying only on logical identifiers such as MAC addresses, certificates, or topology assumptions.

## VXLAN, EVPN, and the Modern Fabric

VXLAN and EVPN are central to modern Data Center switching because they separate physical transport from logical segmentation. VXLAN provides the tunnel mechanism, while EVPN provides the control plane that tells the network where MAC and IP endpoints reside.

The following table summarizes key technologies used in modern VXLAN/EVPN-based data center fabrics and their roles:

| Technology | Role | Key benefit |
|---|---|---|
| VXLAN | Overlay encapsulation | Large-scale Layer 2 over Layer 3 |
| EVPN | Control plane | MAC/IP distribution, multihoming, convergence |
| BGP | Routing protocol | Scalable reachability and policy control |
| ECN | Congestion signaling | Earlier response to fabric congestion |
| DCTCP | Sender reaction model | Fine-grained congestion response in Data Centers |

The important point for a broad audience is that these technologies improve scale and agility, but they also increase the importance of correctness. When logical overlays become richer, the consequences of a wrong endpoint, wrong advertisement, or wrong trust assumption become larger.

## Why Hardware Trust Matters in Both

A modern network can have excellent routing, segmentation, authentication, and encryption and still have a blind spot if it cannot reliably identify connected hardware. That is especially true for unmanaged, headless, or impersonating devices.

In campus networks, the problem usually appears as edge uncertainty. In Data Centers, it appears as trust assumptions in tightly orchestrated infrastructure. In both cases, hardware-level visibility complements protocol-based controls by helping the organization verify that the device at the port is truly the one it expects.

That framing lets the article remain generic while still pointing to problems Sepio can solve: discovering unknown assets, validating device identity, exposing hidden hardware risks, and reducing blind trust in the physical layer.

# USB Billboard Device

## Overview

The USB Billboard Device Class is a specialized USB device category (Base Class 0x11) introduced to support the USB Type-C ecosystem. Its primary function is to communicate the “Alternate Modes” (e.g., DisplayPort, Mobile High-Definition Link (MHL), Thunderbolt) supported by a device to a host system, particularly in scenarios where the host fails to negotiate these modes or lacks the physical hardware to support them.

## Core Functionality

A Billboard Device is typically a low-speed or full-speed USB 2.0 endpoint embedded within a more complex hardware container, such a docking station or a Type-C to HDMI adapter.

- **Capability Advertising:** It uses a Binary Object Store (BOS) descriptor to provide the host with a list of Alternate Modes the device can support.
- **Error Reporting:** If a device fails to enter an Alternate Mode within a specific timeout, the Billboard Device is mandated to expose itself to the host. This allows the Operating System to display a human-readable notification (e.g., “Display connection might be limited”) rather than leaving the user with a silent failure.
- **Informational Presence:** In many modern implementations, the Billboard Device remains enumerated even during successful operations to provide the host with ongoing status and configuration details.

## Technical Architecture

The Billboard Device Class is defined at the Device Descriptor level. Unlike many other classes that are defined at the Interface level, a device identifying as a Billboard Device must use specific class codes in its Device Descriptor. It also relies on specific Billboard Capability Descriptors which contains additional information such as string index pointing to a URL with additional support information.

# Anatomy of a “Duplicated MAC Address” Alert in High-Availability Networks

## Overview

Sepio’s “**Duplicated MAC Address**” risk indicator flags when a single hardware device appears on two different physical ports simultaneously. This could indicate MAC spoofing, cloning attacks, network misconfiguration, or poorly manufactured hardware device.




Notification for a Duplicated MAC Address Risk Indicator

However, in enterprise environments using **High Availability (HA)** network architectures, such as **Cisco vPC (Virtual Port Channel)**, a single device can legitimately appear active on two different switches at once. This deep dive article dissects a real-world scenario where a network device (Huawei switch) triggers this state not due to an attack, but due to a dual-homed redundancy configuration.

## The Detection Scenario

The Sepio platform observed a single device (Huawei Technologies, **MAC 48FD.8E6E.ABCD**) connected to two distinct physical locations:

- **Switch A (Switch01):** Interface **Ethernet1/33**
- **Switch B (Switch02):** Interface **Ethernet1/33**

Under normal circumstances, a device cannot be in two places at once. However, investigation reveals this is a **Layer 2 loop prevention and redundancy mechanism** in action.




Locations of a single asset connected to different switches simultaneously

## Investigation Details

To validate the duplication, the following commands were executed on the network switches. This evidence confirms that the device is dual-homed rather than spoofed.

### EVIDENCE A: MAC ADDRESS TABLE ANALYSIS

```
Switch01#show mac address-table

Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan,
        (NA)- Not Applicable
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
* 4001     48fd.8e6e.abcd   dynamic  NA         F      F    Eth1/33
+ 4002     48fd.8e6e.abcd   dynamic  NA         F      F    vPC Peer-Link


Switch02#show mac address-table

Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan,
        (NA)- Not Applicable
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
* 4002     48fd.8e6e.abcd   dynamic  NA         F      F    Eth1/33
+ 4001     48fd.8e6e.abcd   dynamic  NA         F      F    vPC Peer-Link
```

Partial output of `show mac address-table` command for the two switches

**Explanation of** `show mac address-table address 48fd.8e6e.abcd` **:**

**Switch A Output:**

- `4001 …abcd… Eth1/33` (* indicates a local, physical connection)
- `4002 …abcd… vPC Peer-Link` (+ indicates a virtual entry synced from Switch B)

**Switch B Output:**

- `4002 …abcd… Eth1/33` (* indicates a local, physical connection).
- `4001 …abcd… vPC Peer-Link` (+ indicates a virtual entry synced from Switch A).

### EVIDENCE B: INTERFACE CONFIGURATION VERIFICATION

**Command:** `show running-config interface Ethernet1/33`

- **Switch A Config:** `switchport access vlan 4001`
- **Switch B Config:** `switchport access vlan 4002`

**Forensic Conclusion:** The configuration confirms that the device is intentionally splitting traffic: **VLAN 4001** is handled by Switch A, and **VLAN 4002** is handled by Switch B. There is no channel-group configuration, confirming these are independent active links.

## Architecture Analysis: The “Split-Brain” Connection

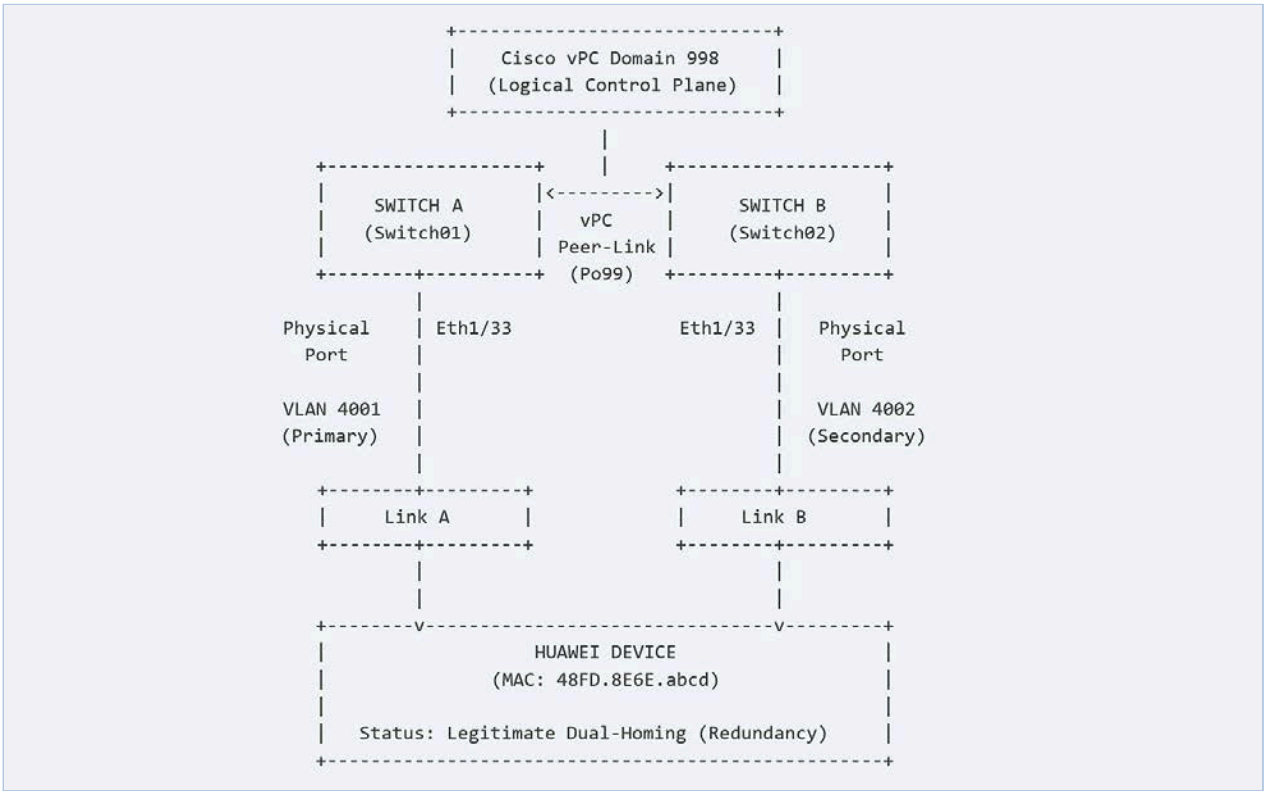
The device is **dual-homed**, meaning it has two physical cables connecting it to the network infrastructure. Unlike a standard bundled connection (LACP), where two cables act as one, this device is configured with two independent “legs”:

- **Leg 1 (Primary):** Connected to Switch A on VLAN 4001 (ISP/WAN Circuit 1).
- **Leg 2 (Secondary):** Connected to Switch B on VLAN 4002 (ISP/WAN Circuit 2).

Because traffic is separated by VLANs (Virtual Local Area Networks), the device is treating these as two separate pathways: one leg for VLAN 4001 traffic, and the other leg for VLAN 4002 traffic.

### Visual Topology

The following diagram illustrates the physical and logical connections derived from the switch configurations.




## The Reason for MAC “Ghosting”

A security analyst reviewing the switch configuration may see confusing data that mimics a spoofing attack. Here is how to decode it.

In a **Cisco vPC cluster**, switches synchronize their known MAC addresses over a dedicated connection called the **Peer-Link**, ensuring that if one switch fails, the other already knows where to send traffic.

**The “Crisscross” Effect**

- **The Real Connection:** Switch 01 sees the Huawei MAC on its local port (Ethernet1/33). This is the **true positive**.
- **The Ghost Connection:** Switch 01 also learns about the MAC from Switch 02. Switch 02 says, “I see this MAC on my side too (on VLAN 4002).”
- **The Result:** Switch 01 adds a secondary entry for the MAC, pointing to the Peer-Link.

**Analyst Reference Table:**

| Switch | VLAN | MAC Address | Interface | Type | Explanation |
|---|---|---|---|---|---|
| Sw 01 | 4001 | ...abcd | Eth1/33 | * (Dynamic) | Real: Physically connected here. |
| Sw 01 | 4002 | ...abcd | Peer-Link | + (Synced) | Virtual: Learned from neighbor switch. |
| Sw 02 | 4002 | ...abcd | Eth1/33 | * (Dynamic) | Real: Physically connected here. |
| Sw 02 | 4001 | ...abcd | Peer-Link | + (Synced) | Virtual: Learned from neighbor switch. |

## Conclusion

When the “**Duplicated MAC Address**” indicator triggers this specific pattern, it is **not malicious**. It is a signature of high-availability network design.
This alert represents a verified **redundant uplink configuration**. The detected duplicate presence is functional, not due to MAC spoofing or physical cloning.
**For future references, the following checklist can be used:**

- **Topology Check:** Are the two reporting switches part of a cluster (Stack/vPC)? (Confirmed: vPC domain 998).
- **VLAN Check:** Is the MAC appearing on different VLANs on each switch? (Confirmed: VLAN 4001 vs 4002).
- **Port Consistency:** Are port number identical or symmetric (e.g., Ethernet1/33 on both)? While not mandatory, this strongly suggests a planned redundant cabling standard rather than a rogue device plugged into a random wall jack.

# Deep Dive on 802.1X and Some of Its Limitations

## Overview

IEEE 802.1X is a standard for port-based network access control (PNAC) and is part of the IEEE 802.1 family of networking protocols.
It provides an authentication mechanism to devices attempting to connect to a Local Area Network LAN.

The standard directly addresses a common attack method in which an attacker who gains physical access to a network port, by posing as a legitimate guest, customer, or staff member, can connect to network services without authorization.

Over time, IEEE 802.1X has become a cornerstone technology for enforcing port-based authentication of users and devices across both wired and wireless networks.

> **Note:** For a detailed technical overview, visit IEEE 802.1X on Wikipedia.

## Short Overview of IEEE 802.1X

IEEE 802.1X is an industry-standard protocol for Port-Based Network Access Control (PNAC).
It defines how devices (known as supplicants) request network access through infrastructure devices (authenticators, such as switches or wireless access points), while user or device identities are verified against a central authentication server (typically RADIUS).

**802.1X Process at a Glance:**

- When a device connects, the network port blocks most traffic.
- The switch (authenticator) communicates with the device using EAP (Extensible Authentication Protocol) messages, directing authentication requests to a RADIUS server.
- Full network access is granted only after successful authentication and policy assignment.

## MAB (MAC Authentication Bypass)

Not all devices support 802.1X authentication. This is a significant challenge in modern converged networks that mix traditional IT, Internet of Things (IoT), and Operational Technology (OT) devices.

Examples of non-compliant devices are widespread and include:

- **Traditional IT Peripherals:** Network printers, scanners, and fax machines.

- **Corporate IoT:** IP-based security cameras, VoIP phones, smart building controls (e.g., HVAC systems, smart lighting), and digital signage.
- **Operational Technology (OT) / Industrial IoT (IIoT):** This represents a critical risk area. Devices in industrial environments, such as Programmable Logic Controllers (PLCs), Human-Machine Interfaces (HMIs), industrial sensors (flow meters, pressure transmitters), and Variable Frequency Drives (VFDs), often run on legacy hardware or specialized protocols that lack an 802.1X supplicant.

For these critical devices to operate in a protected network environment, alternative mechanisms are required.

Disabling 802.1X on that port is an option, but this is highly discouraged because it leaves the port unprotected and open for any rogue device to connect and gain network access.

A more common, although still weak, alternative is **MAC Authentication Bypass (MAB)**. When MAB is configured on a port, the port first attempts 802.1X authentication. If there is no 802.1X response (as with a PLC or a printer), the switch falls back to authenticating with the AAA server (e.g., RADIUS) using the connected device's MAC address as both the username and password.

The network administrator must then make provisions on the RADIUS server to authenticate these "known" MAC addresses. Usually by adding them to a static "allow list" or implementing logic to resolve the MAC against a network asset inventory database.

However, MAB relies on a single, static identifier that is trivial to counterfeit. An attacker can discover and **spoof the MAC address** of a trusted, MAB-authorized device (like a known PLC or security camera). By doing so, the attacker can connect a malicious device to the port, bypass the network access control, and gain an internal foothold. This is especially dangerous in OT environments, where an attacker spoofing a trusted device could gain direct access to the industrial control system, potentially causing physical disruption or halting operations.

## Key Benefits of 802.1X for Network Access Control

- **Improved Security:** Uses unique credentials or certificates to prevent unauthorized access, unlike shared-password methods.
- **Centralized Policy Management:** Integration with RADIUS/AAA allows granular access control based on user or device roles, simplifying compliance and auditing.
- **Dynamic Policy Enforcement:** Assign VLANs, ACLs, and firewall policies to authenticated sessions in real time.
- **Network Visibility and Segmentation:** Binds user and device identities to network sessions, improving visibility for forensics, monitoring, and threat response.
- **Supports Modern IT Needs:** Scales to both wired and wireless infrastructures, enables secure BYOD, and provides strong support for IoT/OT environments.
- **Regulatory Compliance:** Detailed logging and session management help meet HIPAA, PCI DSS, GDPR, and other mandates.

## Common Authentication Methods

### EAP-TLS (Transport Layer Security)

- **Description:** Uses client and server certificates for mutual authentication.
- **Advantage:** Strong cryptographic security, is passwordless, and resists to credential theft.
- **Consideration:** Requires robust Public Key Infrastructure (PKI) deployment and certificate management.

### PEAP (Protected EAP) / EAP-TTLS (Tunneled TLS)

- **Description:** Uses username and password authentication within a secure TLS tunnel.
- **Advantage:** Easier to deploy than EAP-TLS; credentials remain encrypted in transit.
- **Consideration:** May be vulnerable to attacks if weak inner authentication (e.g., MSCHAPv2) is used.

### EAP-FAST (Flexible Authentication via Secure Tunneling)

- **Description:** Developed by Cisco, uses PAC (Protected Access Credentials) instead of certificates.
- **Advantage:** Simplifies deployment and avoids the need for PKI.
- **Consideration:** Offers slightly lower assurance if PACs are compromised.

### MAC Authentication Bypass (MAB)

- **Description:** Used for legacy or IoT devices lacking 802.1X supplicant.
- **Advantage:** Enables onboarding of non-802.1X devices.
- **Consideration:** Highly vulnerable to MAC spoofing; should be tightly controlled and isolated

## Practical Implementation: Cisco & Juniper Example

### Cisco:

- **Enable AAA** and configure **RADIUS** integration.
- Activate **dot1x system-auth-control** and configure switch ports for 802.1X mode (single-host, multi-host, or MAB fallback).
- Support **dynamic VLAN and ACL assignment** via RADIUS, with full visibility through extensive debug and monitoring commands.

### Juniper:

- Configure **interface authentication mode, RADIUS groups**, and **fallback VLANs** e.g., guest, server-fail, or server-reject).
- Support **dynamic filtering** via RADIUS, **MAC RADIUS** for non-802.1X endpoints, and trunk limitations (Note that some fallback features apply only to access ports).

- Carefully manage guest and fallback VLANs along with authentication profiles to prevent accidental open points.

## Example Security Flows and Design Considerations

| Issue | Cisco | Juniper | Risk / Remediation |
|---|---|---|---|
| 802.1X on Trunks | Supported (configurable) | Limited, recent support | Juniper restricts to local config, disables fallback features; segment trunks carefully |
| Guest VLAN | Supported / critical fail VLAN | Supported | Should have ACLs to restrict access only to the Internet |
| MAC Authentication Bypass (MAB) | Supported (`mab` command) | Supported (MAC RADIUS) | Highly vulnerable — always use in isolated VLANs |
| Vendor-Specific Attributes (VSAs) | ACL and role assignment via RADIUS | Juniper Dictionary / filters | Strong access control if centrally managed; manage attribute policies carefully |

## Security Risks and Best Practices

- **Supplicant Support Gaps:** Legacy and IoT devices may lack 802.1X support. While MAC Authentication Bypass (MAB) can provide connectivity, it introduces additional security risks.
- **Trunk Port Limitations:** Some vendor implementations do not support guest or fail VLANs on trunk ports, limiting fallback flexibility.
- **EAP Method Selection:** Weak EAP methods (e.g., PEAP-MSCHAPv2) are vulnerable to credential theft. Use EAP-TLS in high-assurance environments for stronger protection.
- **Fallback & Guest Network Exposure:** Fallback networks must be isolated to prevent lateral movement or exploitation.
- **Configuration Complexity:** Manual errors can introduce vulnerabilities; use automation and centralized policy where possible.
- **MAC Spoofing (MAB):** A severe vulnerability, always combine MAB with complementary controls such as DHCP snooping, Dynamic ARP Inspection (DAI), and network segmentation.

## Conclusion

IEEE 802.1X is the backbone of secure enterprise network access control. Its adoption across all verticals is driven by strong, centralized authentication, flexible policy enforcement, and the ability to meet the highest security and compliance standards.

While technical and operational challenges remain, especially around legacy device support, trunk configurations, and fallback path exposure, a well-architected 802.1X deployment dramatically reduces attack surface and enables robust, scalable, and manageable network security.

# Raspberry Pi Deep Dive

## Overview

The Raspberry Pi is a series of low-cost, credit-card-sized single-board computers (SBCs) developed by the UK-based Raspberry Pi Foundation. Its original mission, rooted in philanthropy, was to promote the teaching of basic computer science in schools and developing countries.

## What is the Raspberry Pi?

The device is a complete, functioning computer, typically running a version of the Linux operating system (like the default Raspberry Pi OS). It is much smaller and more affordable than a traditional PC. Key features include:

- **System-on-a-Chip (SoC):** Integrates the processor, graphics processor, memory, and often wireless connectivity all on a single board.
- **General Purpose Input/Output (GPIO) Pins:** Allow the Raspberry Pi to interact with the physical world by connecting to and controlling electronic components, making it popular for Internet of Things (IoT) and hardware projects.
- **Connectivity:** Modern versions like the Raspberry Pi 5 include a quad-core processor, multiple USB ports (including USB 3.0), dual HDMI display outputs, true Gigabit Ethernet, and integrated Wi-Fi and Bluetooth.

## History and Popularity

### Early Days and Mission

The Raspberry Pi was officially launched in February 2012 with the initial Model B, priced at $35. It quickly generated massive public interest, far exceeding the creators' expectations. The foundation's goal was to provide an extremely low-cost platform to inspire a new generation of coders, helping to reverse a decline in student applications for computer science courses.

### Gaining Critical Mass

The device gained popularity rapidly for several key reasons:

- **Low Cost:** Its initial price point made it accessible to students, hobbyists, and those in developing nations who couldn't afford a full desktop computer.
- **Versatility and Size:** Its small form factor and processing power made it ideal for countless projects, from retro gaming consoles (**RetroPie**) and media centers to network-level ad blockers (**Pi-hole**) and sophisticated home automation systems.
- **Strong Community and Open-Source Ecosystem:** A large, active community quickly formed, sharing projects, tutorials, and providing extensive software support for the hardware, which has

been crucial to its sustained success.

- **Industrial Adoption:** With the introduction of the Compute Module in 2014, a bare-bones version designed for integration, the platform started to be adopted by businesses for embedded applications, industrial automation, and rapid prototyping. As of 2024, approximately 70% of Raspberry Pi Foundation's sales are to industrial customers.

## Manufacturing and Volume

The Raspberry Pi is manufactured under contract, primarily by **Sony** in the UK.

- **Annual Volume:** In the fiscal year 2024, Raspberry Pi sold approximately **7.0 million** single-board computers and compute modules.
- **Total Units Sold:** As of March 2025, Raspberry Pi had sold over **68 million** SBCs in total since its launch.

Due to the low cost of the core board, the Raspberry Pi platform provides an incredibly cheap basis for developing networking and other embedded devices, which is a major factor in its use as a "dual-use device", useful for both legitimate projects and malicious purposes.

## Raspberry Pi Models & Chipsets

| Model / Adapter | Connection Type | Chipset / Controller |
|---|---|---|
| **Pi 5** | Built-in Ethernet | Broadcom BCM54213PE (PHY) |
| **Pi 5** | Built-in Wi-Fi | Infineon CYW43455 |
| **Pi 5** | PCIe 2.5G Adapter | Realtek RTL8125 (Common) |
| **Pi 5** | PCIe 10G Adapter | Aquantia AQC113 (Common) |
| **Pi 4** | Built-in Ethernet | Broadcom BCM54213PE (PHY) |
| **Pi 4** | Built-in Wi-Fi | Infineon CYW43455 |
| **Pi 3 B+** | Built-in Ethernet | Microchip LAN7515 (via USB 2.0) |
| **Pi 3 B+** | Built-in Wi-Fi | Infineon CYW43455 |
| **Pi 3 B** | Built-in Ethernet | SMSC LAN9514 (via USB 2.0) |
| **Pi 3 B** | Built-in Wi-Fi | Broadcom BCM43438 |
| **Pi 2 B** | Built-in Ethernet | SMSC LAN9514 (via USB 2.0) |

| Model / Adapter | Connection Type | Chipset / Controller |
|---|---|---|
| **Pi 1 B/B+** | Built-in Ethernet | SMSC LAN9512 (via USB 2.0) |
| **Pi Zero 2 W** | Built-in Wi-Fi | Infineon BCM43430 (in SiP) |
| **Pi Zero W** | Built-in Wi-Fi | Infineon CYW43438 |
| **Adapter** | USB 3.0 (Gigabit) | Realtek RTL8153 (Common) |
| **Adapter** | USB 3.0 (2.5G) | Realtek RTL8156 (Common) |
| **Adapter** | USB 2.0 (Gigabit) | ASIX AX88179 (Common) |
| **Adapter** | USB 2.0 (10/100) | ASIX AX88772 (Common) |
| **Adapter** | SPI Module | WIZnet W5500 (Hardware TCP/IP) |
| **Adapter** | SPI Module | Microchip ENC28J60 (Software TCP/IP) |

Products that are created and built using those Raspberry Pi modules will be identified by Sepio as a specific Raspberry Pi module, and will trigger the dual use device Risk Indicator (if it is enabled) unless other L2, L3, or application information is available for better classification.

The Raspberry Pi's combination of low cost, size, portability, and a full Linux operating system makes it an excellent platform for building a variety of covert and multi functional hacking and penetration-testing tools, which are prime examples of "dual-use devices."

## Examples of Raspberry Pi OT and IoT

### Products

Here are three examples of IoT and OT products that are built around a Raspberry Pi:

#### KUNBUS Revolution Pi

- **Category:** Operational Technology (OT) / Industrial Automation
- **Description:** This is a perfect example of the Raspberry Pi in a rugged industrial setting. KUNBUS takes the Raspberry Pi Compute Module and builds it into a modular, DIN-rail-mountable industrial PC. It's used directly in factories and industrial environments to control machinery, monitor production lines, and act as an Industrial IoT (IIoT) gateway. It's designed to meet industrial standards such as EN 61131-2, and can be expanded with various digital and analog I/O modules, making it a direct competitor to traditional programmable logic controllers (PLCs).

#### Yodeck Digital Signage Player

- **Category:** Internet of Things (IoT) / Commercial
- **Description:** Yodeck provides a cloud-based digital signage service for businesses to display content on screens in restaurants, offices, and retail stores. Their "Yodeck Player" is a small, plug-and-play device you connect to a TV. This device is a Raspberry Pi (often a Pi 4) pre-configured with their software. It's a classic IoT device: it connects to the internet to pull content and schedules from the cloud and display them on commercial screens. They even provide the Raspberry Pi player for free with an annual subscription.

**Volumio Primo**

- **Category:** Internet of Things (IoT) / Consumer Electronics
- **Description:** This is a high-fidelity (hi-fi) network music streamer and server for audiophiles. At its core, the Volumio Primo uses a Raspberry Pi Compute Module as its main processor. Volumio then builds a custom case, a high-quality digital-to-analog converter (DAC) for superior sound, and other audio-grade components around the Pi. This creates a premium, user-friendly smart device for the home, focused entirely on high-quality audio streaming from services like Spotify and Tidal, or from a local network.

## Examples of Raspberry Pi Hacking Tools

The core of many Raspberry Pi hacking tools involves installing a specialized Linux distribution, such as **Kali Linux** or **Parrot OS**, which come pre-loaded with hundreds of penetration testing utilities. Beyond these general-purpose distributions, specific projects leverage the hardware's unique capabilities for targeted attacks:

### Covert USB Attack Platforms

These tools exploit the trust a computer has for a device plugged into a USB port by emulating a standard peripheral like a keyboard or Ethernet adapter.

| Tool Name | Raspberry Pi Model | Function / Attack Vector |
|---|---|---|
| **PoisonTap** | **Raspberry Pi Zero** | Exploits the USB interface to emulate an Ethernet adapter. It then spoofs DNS to hijack all web traffic, steal web cookies (even from locked machines), and install a persistent, cache-based web backdoor. |
| **P4wnP1 A.L.O.A.** | **Raspberry Pi Zero W** | A highly customizable framework that turns the Pi into a "Little Offensive Application." It can perform Plug & Play USB device emulation (e.g., a keyboard to inject keystrokes/HIDScript), set up Wi-Fi KARMA attacks, and create covert Wi-Fi and Bluetooth channels for remote access. |

### Network Scanning and Reconnaissance

The Pi, when deployed as a network tap or a rogue Wi-Fi access point, can perform deep network analysis.

| Tool Name | General Function | Attack Vector |
|---|---|---|
| **Pwnagotchi** | A passive Wi-Fi handshake capture device. | Uses the Wi-Fi card's monitor mode to sniff for handshake data from nearby Wi-Fi networks, which can then be used offline to crack WPA/WPA2 passwords. |
| **Nmap (via Kali Linux)** | Network Mapper | A classic tool used for scanning large networks, discovering active hosts, and identifying open ports and running services (vulnerability assessment). |
| **Aircrack-ng (via Kali Linux)** | Wireless Cracking Suite | Used to assess Wi-Fi network security, specifically for cracking WEP/WPA/WPA2-PSK keys by capturing data packets. |

### Hardware and Forensics Tools

The Raspberry Pi's General Purpose Input/Output (GPIO) pins allow direct interfacing with the components of other devices, making it a "poor man's" hardware-hacking tool.

- **JTAG/SWD debugging:** The Pi can be configured using tools like OpenOCD to act as a debugger interface. This allows an attacker to connect to the internal debug ports of a target device's processor to dump firmware, read internal memory, or perform dynamic changes while the device is running.
- **SPI/$I^2C$ flash dumping:** Using the GPIO pins and tools like flashrom, the Pi can physically connect to and read/write data from external flash memory chips (used for firmware storage) on various target devices, bypassing higher-level security controls.

These examples illustrate how the Raspberry Pi is a potent dual-use device, offering legitimate value in education and IoT development while simultaneously enabling low-cost, effective tools for covert cyber operations that target layers 1 and 2 of the network stack.

# Agent Deep Dive

## Agent Operating Modes

The Agent can operate in one of four modes. Each mode determines how the Agent monitors devices and enforces security policies on the host.

### Free Mode

In this mode, the Agent operates in **visibility-only** mode. It reports device activity to the Platform Management but does not take any enforcement actions.

All actions must be performed manually by the Sepio Administrator.

### Armed Mode

In Armed Mode, the Agent enforces device control policies based on approval status.

- Only peripherals **approved by Sepio** are allowed to operate on the host.
- Assets or peripherals that are **not approved** are automatically **blocked**.

> **Note:** A host is considered approved when you select **Approve All Peripherals** for that host.

Assets/Peripherals that are not **Approved** by Sepio will be automatically **Blocked**. The platform will automatically **Block** any peripheral that is **Disapproved**, but it will not block those that are **Approved**. The Agent will also automatically **Block** an Asset/Peripheral, whether it is **Approved** or **Disapproved**, after matching its DNA profile to the Agent's Known Threats List.

The order in which assets/peripherals are connected is not significant. For example, if four assets are connected and their peripherals are **Approved**, connecting a fifth asset that is not **Approved** will result in automatic **Blocking**.
Any asset/peripheral not **Approved** by Sepio is immediately and automatically **Blocked** upon connection to the host.
The Agent is not aware of the host (computer) ports. The actions **Approved** or **Disapproved** depend only on the device and host, not on which USB port the device is connected to.

### Block Known Threats (BKT) Mode

In BKT Mode, the Agent automatically 'Blocks' an Asset/Peripheral after matching its DNA profile to the Agent's 'Known Threats' List, regardless of 'Approval' status.

#### Block Mass Storage Devices and Known Threats (BST) Mode

In BST Mode, the Agent automatically 'Blocks' a USB Mass Storage Device (including thumb drives, disk on key, mobile phones with storage interfaces, etc.) and other Asset/Peripherals identified as attack tools, regardless of 'Approval' status, after matching their DNA profile to the Agent's 'Known Threats' List.

## Agent Behavior on Windows and Linux

The Windows and Linux Agents are designed to behave in the same way, however there are a few differences. At the operating system level, the Linux Agent's behavior when handling peripheral devices is slightly different from the Windows Agent's behavior.

## Agent Lists

The Agent collects and stores data in various lists and sub-lists. This data remains stored indefinitely unless the user configures a time period for automatic deletion. By default, there is no time limit, meaning the data is never deleted from the Agent, except for entries governed by the Asset Aging Configuration (described below).

> **Note:** This stored data is separate from the information recorded in the Sepio Event Logs.

#### Peripherals/Assets List

This list contains the following parameters:

- **First seen:** the first time (timestamp yyyy-mm-dd hh:mm:ss.) the Agent detects an Asset /Peripheral on the network. For example, if a mouse was installed on the network before the Agent was installed, it won't be listed in the 'Seen' Assets /Peripherals sub-list. It will only be listed in the ' first seen' sub-list once the Agent detects it.
- **Last seen:** the last time (timestamp yyyy-mm-dd hh:mm:ss) an Asset /Peripheral was 'seen' (detected) by the Agent on the network. The First/Last seen Asset listings are saved to the Platform even after an Asset is disconnected from it.
- **Online/offline:** shows if an Asset /Peripheral is currently online (connected to the network) or offline (disconnected from the network). If an Asset /Peripheral is currently online, the 'last seen' listing will be of the current time.
- **Peripheral/Asset Aging:** the Asset Aging settings define the time period after which the Platform Management automatically deletes Peripherals/Assets listings from the 'Peripherals/Assets' List. You set the Asset Aging in **Settings** -> **Server Settings** -> **Auto-delete Asset Configuration**.




Auto-delete Asset Configuration

- **Approved:** In Armed mode, every Peripheral/Asset must be 'Approved'; otherwise, it will be automatically 'Blocked'.

> **Note:** When an Agent is set to Free Mode no action is required.

### Peripherals/Assets List Continuity

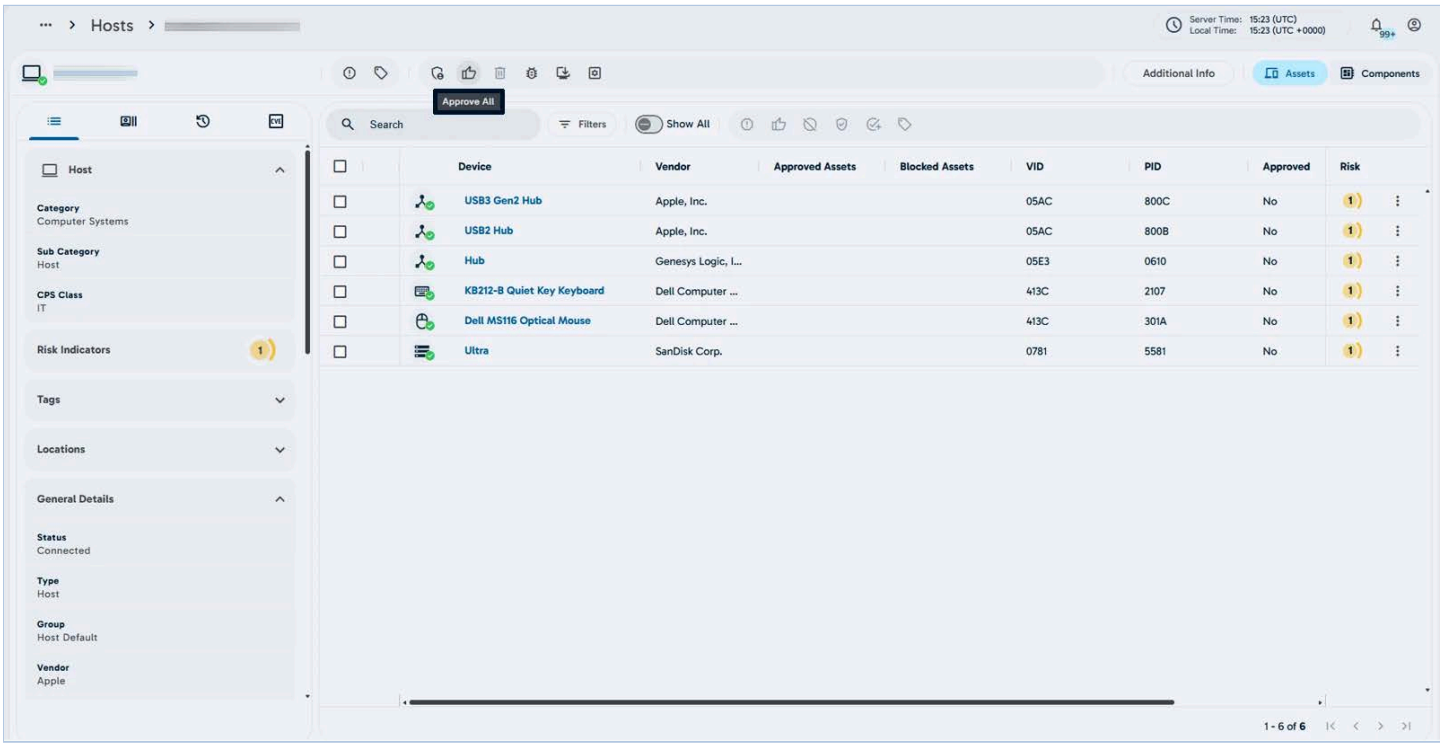
An Agent's 'Approved' status is replicated across each Platform Management instance where it is installed. When an Agent is connected to a Platform Management, a mechanism verifies that the 'Peripherals/Assets' List is received by that Platform Management.

If, for any reason, the Agent is disconnected from one Platform Management instance and later connected to another, the Peripherals/Assets list from its previous connection is transferred to the new Platform Management instance. This ensures continuity and integrity of asset management across different servers.
Each Platform Management system retains the Peripherals/Assets List of all Agents that have ever connected to it.

### Approve All Action

**Approve All:** Approves all of the Agent's Peripherals currently connected to the Platform Management.

When the **Approve All** option is selected, all peripherals connected at that moment are automatically marked as 'Approved'. However, any peripherals that are not connected during the Approve All action will be marked as 'Disapproved', even if they were previously approved. It is important to keep this in mind when using the 'Approve All' option.




Approve All option

### Components (BOM) List

This list is similar to the 'Peripherals/Assets' List with two differences:

- Difference between an Asset/Peripheral and a Component.
  - Asset/Peripheral: an object you can connect or disconnect to/from something.
  - Component: an integral part of a system, i.e., a built-in component.
- The Approval/Disapprove/Block options do not exist for built in Components. No enforcement actions are available for them. In the Peripherals/Assets List, "Assets" currently refer only to USB-connected devices.

### Agent Event History Log

This log records key events performed by the Agent, which operates autonomously. Once it is set to 'Armed' via the Platform Management, it automatically blocks any Assets/Peripherals/Built in components that are not approved, even when disconnected from the Platform Management.

The Agent Event Log includes:

- Event date and time.
- Event description.

The Agent stores its last 300 event listings in the Local Event History Log. Events are logged sequentially. It stops when the number of events in the file reaches maximum 300 events. There is no limit to the number of events written to the 'Peripherals/Assets' List. For example, if a user connects/disconnects an Asset to/from an Agent 310 times in one day, the Agent Local Event History Log only creates 300 listings. However, if a user connects/disconnects an Asset once during five years, the Peripherals/Assets List

creates and displays only those two listings. The user won't be able to see events from the Agent Local Event History Log that occurred while the Agent was connected to a Platform Management if there were more than 300 during that time.

### Agent Information Continuity

The Agent continuously updates the Platform Management. If disconnected for any period (e.g., an hour, a week, a month), once it reconnects, it sends the missing data to the Platform Management (e.g., Peripherals/Assets List, Component (BOM) List, Agent Event History Log). The Platform Management will successfully recover all missing information from the Peripherals/Assets List and the Components (BOM) List. However, recovery from the Agent Event History Log is subject to a maximum event limit. If the number of events generated while the Agent was disconnected exceeds this limit, some events will not be recovered.

### Known Threats List

Since Sepio Agent cannot approve or block devices that have not yet been detected, it uses the Known Threats List stored locally in the Agent. When a new Asset/Peripheral is connected, the Agent compares its DNA profile against the Known Threats List. If a match is found, the Agent automatically blocks the device, regardless of its approval status.

## Windows Device Manager

When the Agent is operating in Free mode, also known as visibility mode only, it monitors and reports device activity to the Sepio Platform Management without enforcing any actions. In this mode, if a user disables an Asset or Peripheral via the Windows Device Manager, the Platform Management interface will display the device as "Blocked", even though the action was not performed by Sepio.



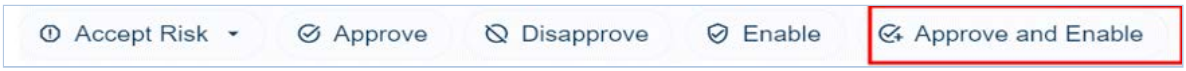
Asset/Peripheral is 'Blocked'

When the Agent is operating in Armed mode, the behavior changes: if an Asset or Peripheral is marked as 'Blocked', it is automatically disabled in the Windows Device Manager. Additionally, if a device is enabled in the Device Manager but has not yet been approved within the Sepio Platform Management, it is immediately marked as 'Blocked' and disabled in the Device Manager. To prevent this automatic enforcement, the user must switch the Agent back to Free mode.

The Windows Device Manager retains the state of a device after a system shutdown. For example, if a camera is manually disabled in the Device Manager before the system is powered off, it will remain disabled when the computer is restarted. The device will stay in this state until it is manually re-enabled through the Device Manager.

If an Asset or Peripheral is 'Blocked' via Sepio, it can still be manually enabled through the Device Manager, unless additional restrictions are enforced. In Armed mode, any newly connected Asset or Peripheral that has not been approved by the Sepio Administrator will be automatically blocked. For example, if a user connects a new camera without prior approval, the Agent will immediately block the device.

To streamline this process, Platform Management offers an 'Approve and Enable' action. This feature allows users or administrators to simultaneously add a device to the Approved list and enable it, eliminating the need to perform two separate actions.



Approve and Enable action

When the Agent is operating in Armed mode, it automatically blocks an unapproved Asset or Peripheral but does not automatically enable it; enabling must be done manually. Similarly, approving an Asset or Peripheral does not automatically result in it being enabled.

**USB Asset Identification and the Device Manager**

In addition to Sepio's proprietary Asset DNA profiling for device detection, the system also utilizes standard USB identification fields. These include:

- VID (Vendor Identification) mandatory field: might not be unique.
- PID (Product Identification) mandatory field: might not be unique.
- Serial number: optional field.
    - The vendor might:
        – not provide a serial number field.
        – provide a unique serial number.
        – provide a non-unique serial number (such as 1234).

If a connected USB device lacks a serial number, Windows generates an identifier based on the physical USB port it's connected to. As a result, if the device is disabled, disconnected, and later reconnected to a different port, Windows treats it as an entirely different device due to the change in identifier.

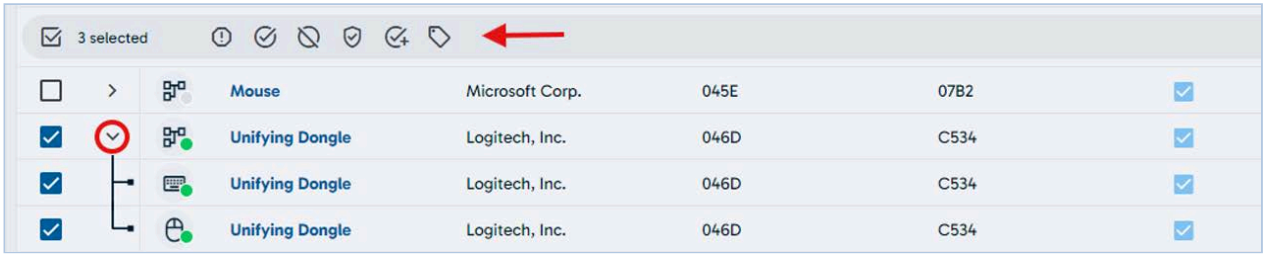
**Note:** There are some cases where Windows is unable to identify that the same device (without a serial number) was connected/disconnected to it multiple times, so it appears as different devices. However, Sepio can identify a device (without a serial number), if connected/disconnected multiple times, as the same previously connected device.

### Composite Devices (Assets)

A composite device, also known as an Asset, is a device that performs multiple functions. Examples include a multifunction printer that offers both printing and scanning capabilities, or a headset that provides audio output along with input functions like volume control. Structurally, a composite device is represented as a hierarchical tree, where a single 'parent' node is connected to one or more 'child' nodes, each representing a distinct peripheral function. The 'parent' node itself is nonfunctional and serves only as a container for its associated child peripherals. Whether a device is classified as composite is determined by the vendor, and in some cases, the 'parent' node may have only one 'child' node.

To approve or disapprove a composite device:

- Click on the expand mark of the composite device.
- Select the 'parent' and the 'children' nodes.
- Use the icons on the top to perform the required action.



Expand Composite Devices

**Note:** Selecting only the 'parent' will not apply the action on the 'children'.

To 'Approve' or 'Disapproved' only one functionally of the composite device, chose only the relevant 'child' node.

### Agent UUID Identifier

Each Agent has a unique identifier known as the UUID, which is derived from the computer's hardware. Sepio generates this UUID using the BIOS and motherboard IDs. Even if Sepio is uninstalled and then reinstalled on the same machine, the Agent retains its UUID. Data that the Agent stores locally, such as the computer name it is installed on and the data in its lists (as mentioned above) are lost when uninstalling an Agent. If the host computer's name or IP address changes, the UUID remains the same, allowing the Sepio Agent to continue functioning on the host without issue.
In some cases, custom-build devices like POS terminals and ATM might use the same BIOS ID. To support such use cases, Sepio added an optional installation parameter, that directs the Agent to use not only the BIOS ID, but also the serial number of the hard drive of the machine when generating the UUID.

To enable this, use the following parameter during installation:

```
EXTENDED_AGENT_UUID="T"
```

Append the parameter when using the installation command line. Consider the following example:

```
msiexec.exe /i "SepioAgent_Win_64_16.2403.9.msi" CENTRALIZEDIP="mysepioserver.mydomain.com"
EXTENDED_AGENT_UUID="T"
```

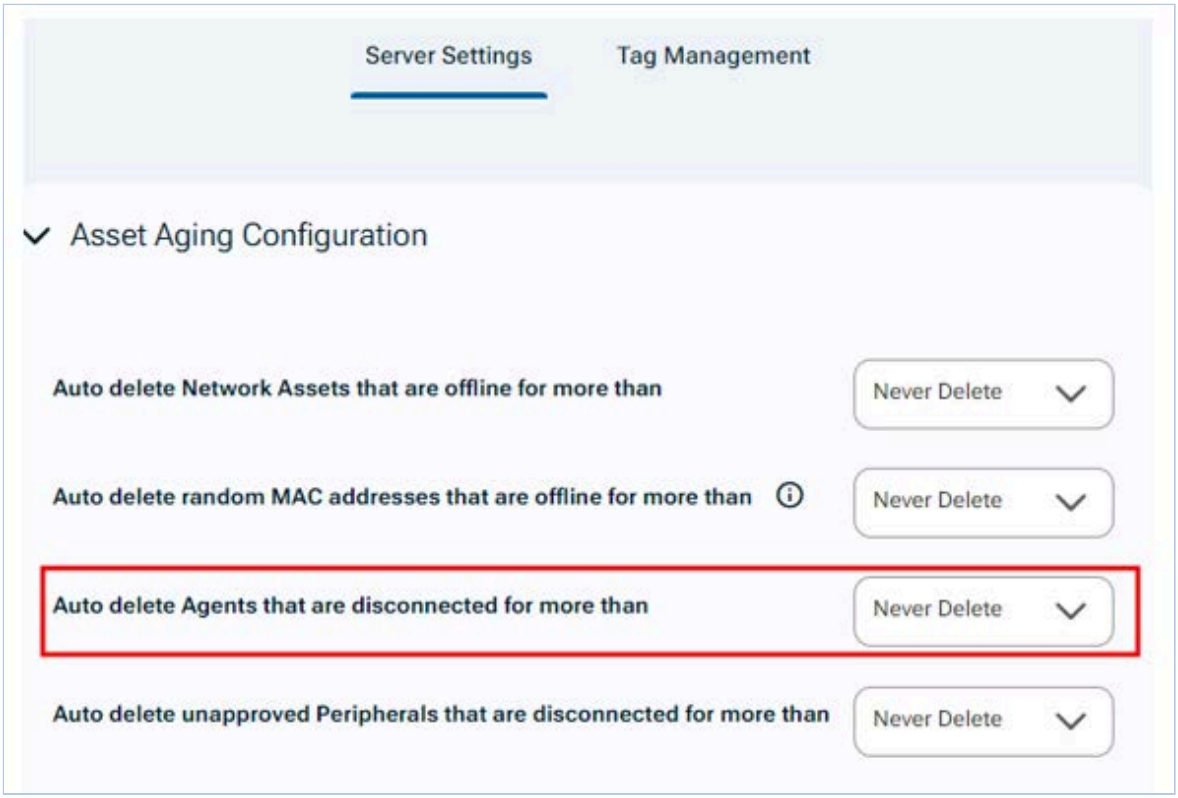
Using a “UUID” which is not unique is causing a duplicate asset in Sepio Platform. It might create issues with other security products as well. If the issue of non-unique UUID is discovered after the Agent was installed, the resolution is to reinstall the affected agents with this additional parameter. This will resolve the duplication of the assets but would keep the duplicated asset’s information in Sepio’s database and requires deleting the non-current assets. For example, if two POS terminals that have a non-unique UUID were installed without setting the parameter EXTENDED_AGENT_UUID=”T”, after fixing the problem the Sepio Platform will present the correct hosts with its correct status as well as a duplicated asset which will be in “disconnected” state and should be deleted manually.

### Agent Aging

The Agent Aging setting determines how long an inactive Agent, one that has been disconnected from the Platform Management, is retained in the Platform’s *Agent* list before being permanently deleted. By default, this setting is configured as Never Delete.

You can configure Agent Aging by navigating to:

**Settings** -> **Server Settings** -> **Asset Aging Configuration** -> **Auto delete Agents that are disconnected for more than.**




Asset Aging Configuration

# Knowledge Base Deep Dive

## Overview

The Knowledge Base (KB) is Sepio's proprietary intelligence data repository that enhances the platform's ability to classify assets, assign risk, and detect hardware-based threats. It is used as the reference source for classifying trusted assets, identifying known attack tools, and assigning appropriate Risk Indicators (RIs), in addition to Sepio's proprietary algorithms to generate hardware fingerprints (AssetDNA).

The Knowledge Base is a curated and continuously updated repository containing:

- **AssetDNA of Attack Tools:** Identifiers and fingerprints of known malicious hardware and spoofed devices.
- **AssetDNA of Trusted Assets:** Verified identifiers, fingerprints of common, benign hardware.
- **Risk Indicator Parameters:** Rules and logic for assigning specific Risk Indicators.
- **Common Vulnerabilities and Exposures (CVEs):** Public vulnerability references linked to device profiles.
- **Classification Data Rules:** Device types, categories, and typical behavior.
- **Vendors and Assets with Bad Reputation:** Policy rules used for proactive detection and blocking.

The Knowledge Base is also used as a vehicle to distribute the **latest version of the Sepio Agent**. Unlike the Network Scan Engine, which is typically updated during full Platform upgrades, the agent can be upgraded independently and might have more frequent updates.

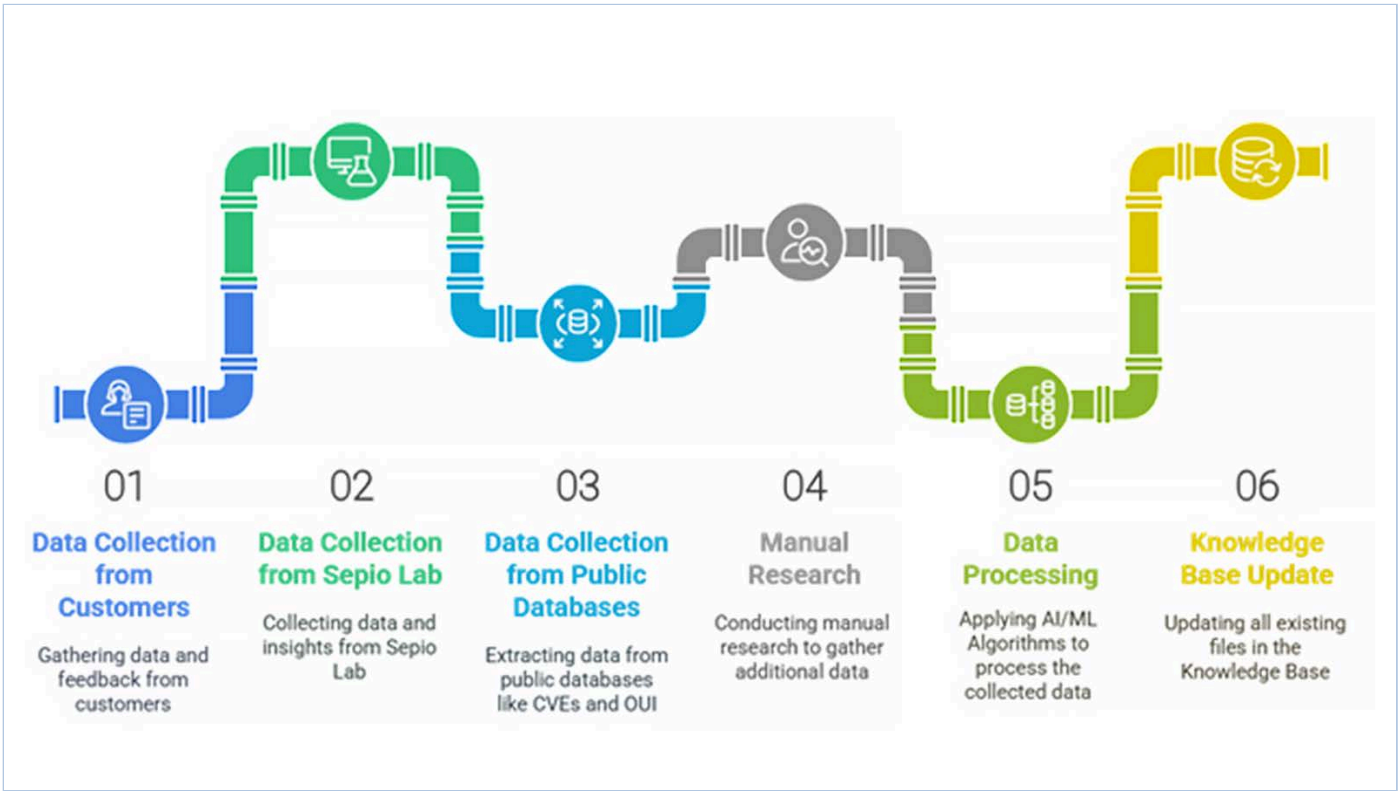
## Update Frequency and Process

The KB is regularly updated with a biweekly goal using the following process:

1. **Data Collection** from multiple sources:
    - Anonymized customer deployments
    - Sepio Lab Research
    - Open-source intelligence feeds

2. **Verification**

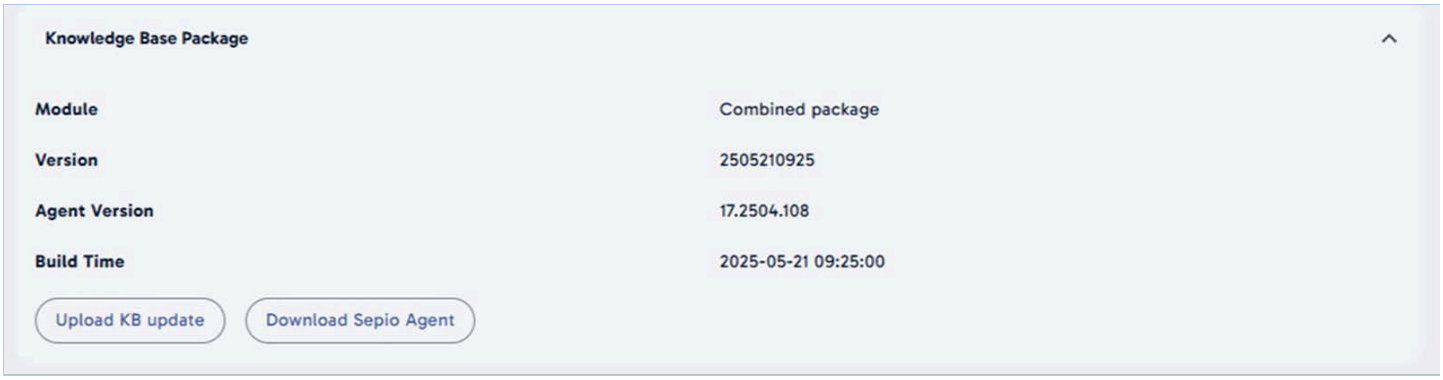
3. **Processing**
    - AI/ML models process the collected data.
    - Fingerprints and threat intelligence are validated and integrated into the Knowledge Base (KB).
    - Resulting updates span all KB components: DNA entries, risk logic, classifications, and reputation assessments.




Knowledge Base Update Process

**Note:** As a core component of the platform's classification and detection pipeline, the Knowledge Base and its update process include several security and governance checkpoints to validate the integrity and accuracy of its content.

4. **Deployment** of updates via a shared file system.




Knowledge Base Package

## Platform Dependency on the Knowledge Base

The Knowledge Base is essential for several core functions of the Sepio platform:

- **Agent Updates:** Ensures users receive the latest version of the Sepio Agent independently of platform upgrades.

- **Asset Classification:** Provides the intelligence to classify assets with high fidelity, distinguishing between benign and malicious devices.
- **Risk Indicators:** Supplies the contextual rules and fingerprints used to assign accurate Risk Indicators.

The Knowledge Base ensures the Sepio platform delivers full asset visibility and the hardware-level risk assessment capabilities it's known for.




Platform Dependency on the Knowledge Base

**Note:** Asset classification occurs when a device is detected during a scan. Sepio will not update the classification of offline devices. Therefore, if there is a Knowledge Base (KB) update and some devices that should have been updated are offline, their classification will remain unchanged.

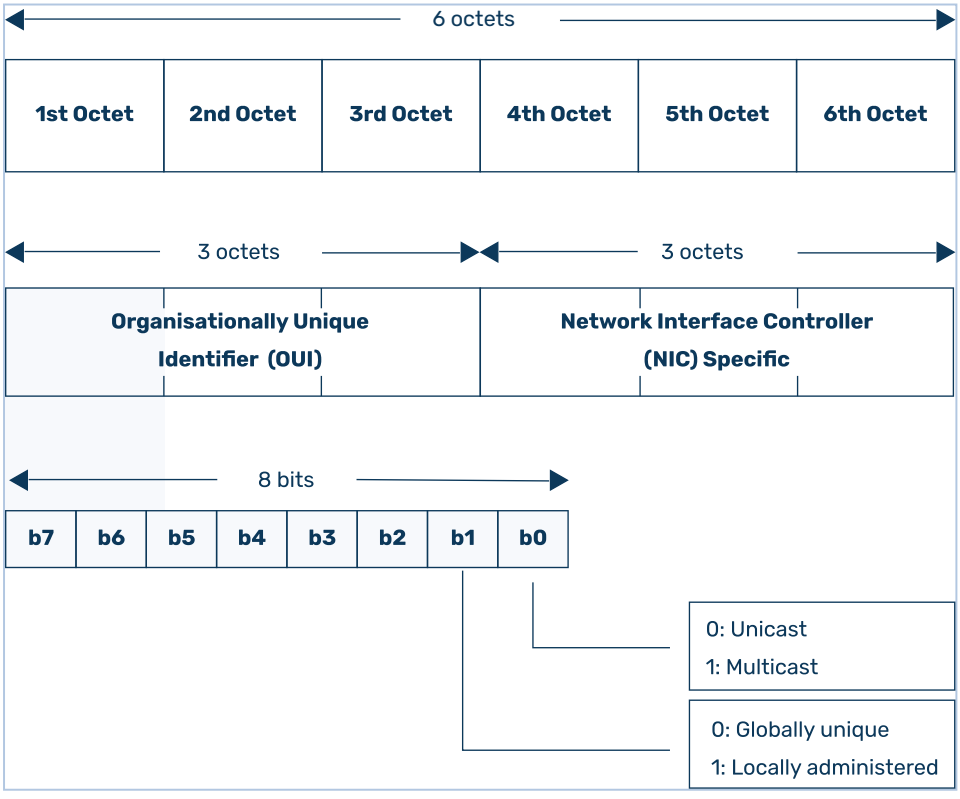
# MAC Addresses Deep Dive

A MAC address (media access control address) is a unique identifier assigned to a network interface card (NIC) for use as a network address in communications within a network segment. This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth. Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control (MAC) protocol sublayer of the data link layer.

Network nodes with multiple network interfaces, such as routers, laptops capable of connecting to a LAN and Wi-Fi network simultaneously as well as multi-homed servers and L3/L4 switches, must have a unique MAC address for each NIC in the same network. However, two NICs connected to two different networks can share the same MAC address.

A MAC address is a 48-bit (6-byte) hexadecimal number that is written in groups of two hexadecimal digits.

## MAC Address Format




MAC Address format

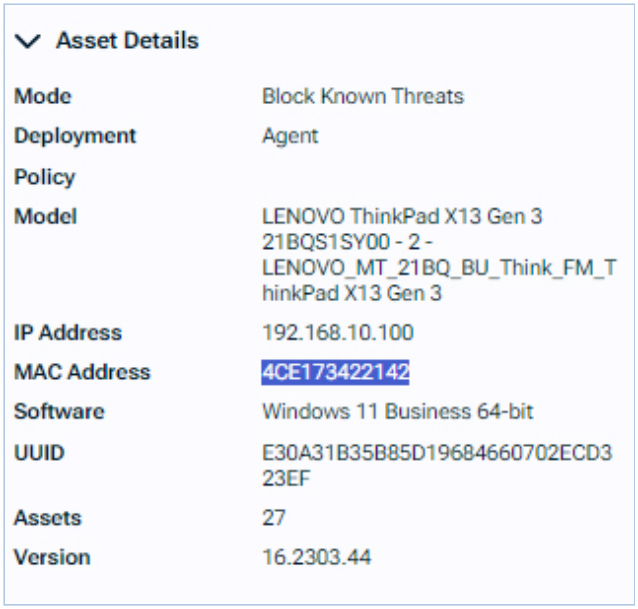
The MAC Address is a 48-bit Address, traditionally, 6 octets, 12-digit (6 bytes or 48-bit) hexadecimal number. The 48-bit space means there are potentially 281,474,976,710,656 MAC Addresses.

There are different formats to write the MAC Address. But it is usually written in one of the following ways.

- Hyphen-Hexadecimal notation = MM-MM-MM-SS-SS-SS

- Colon-Hexadecimal notation = MM:MM:MM:SS:SS:SS
- Period-separated Hexadecimal notation = MMM.MMM.SSS.SSS
- 12 digits: MMMMMMSSSSSS

**Sepio uses the 4th method. For example, see the following screenshot:**



Sepio uses the 4th method

MAC addresses are used for a variety of purposes, including:

- Identifying devices on a network
- Determining the path that data should take through a network
- Securing networks from unauthorized access
- Blocking unwanted traffic
- Diagnosing network problems

MAC addresses are considered permanent and unchangeable identifier for a device. However, some devices allow you to change the MAC address, which can be useful for bypassing network restrictions or for security purposes. In a virtualized environment it is more common to see duplicated MAC addresses.

## MAC Address Structure

The first three octets of a MAC address are assigned to the manufacturer of the NIC, and the last three octets are assigned by the manufacturer to uniquely identify each NIC.

## OUI MAC Address

An OUI (Organizationally Unique Identifier) is the part of the MAC Address that defines the hardware manufacturer. It is the leftmost six digits, also called prefixes, and is associated with the hardware manufacturer.

The IEEE is responsible for OUI distribution and issues it to their registered manufacturers. Sometimes, manufacturers possess several prefix numbers associated with their products. And it is common in large manufacturers to have more than one set of OUIs. For example, the prefixes 00-13-10, 00-25-9C, and 68-7F-74 (plus others) belong to Linksys.

The OUI of some well-known manufacturers are as follow

- Dell: 00-14-22
- Nortel: 00-04-DC
- Cisco: 00-40-96
- Belkin: 00-30-BD
- Huawei: 00-9A-CD
- Hewlett Packard: 3C-D9-2B

**The following screenshots is showing a sample report of devices and vendors:**

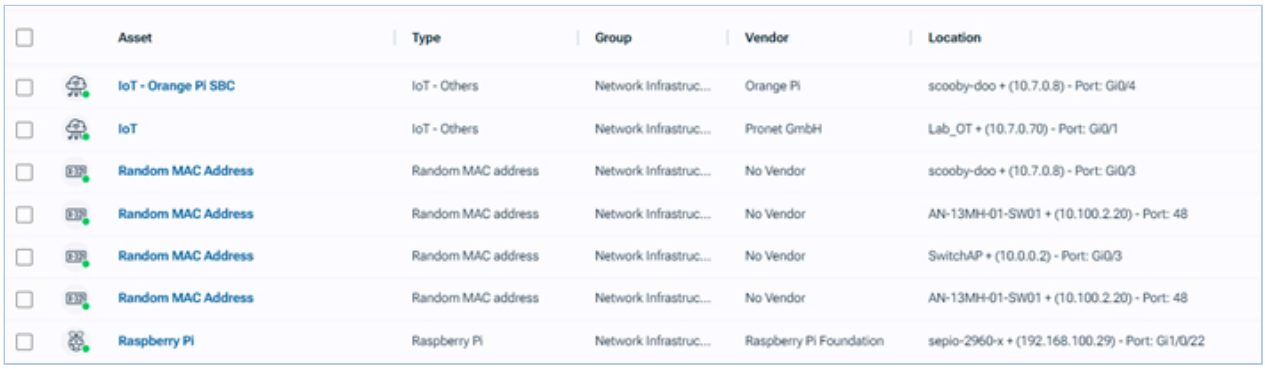


| Asset | Type | Group | Vendor | Location |
|---|---|---|---|---|
| Communication - CT2504 Access Point | Access Point | Network Infrastruc... | Cisco Systems | AN-13MH-01-SW01 + (10.100.2.20) - Port: 48 |
| Galaxy A5 (MTP) | Smartphone | | Samsung Electronics Co... | ANATS-PF3D1TKS |
| Communication - MR86 Access Point | Access Point | Network Infrastruc... | Cisco Meraki | AN-13MH-01-SW01 + (10.100.2.20) - Port: 13 |
| Communication - MR86 Access Point | Access Point | Network Infrastruc... | Cisco Meraki | AN-13MH-01-SW01 + (10.100.2.20) - Port: 14 |
| Raspberry Pi | Raspberry Pi | Network Infrastruc... | Raspberry Pi Foundation | sepio-2960-x + (192.168.100.29) - Port: Gi1/0/22 |
| AR9271 802.11n | Smartphone | | Qualcomm Atheros Co... | HP-ELITEDESK1 |
| IP Phone (7841) | IP Phone | Network Infrastruc... | Cisco Systems | Cat2960_1 + (192.168.10.43) - Port: Fa0/20 |
| Communication - Wireless | Router | Network Infrastruc... | Ubiquiti Networks Inc. | SwitchAP + (10.0.0.2) - Port: Gi0/4 |
| Communication - Aruba MODEL 105 Acc... | Access Point | Network Infrastruc... | Aruba Networks | AN-13MH-01-SW01 + (10.100.2.20) - Port: 48 |
| Mobile | Smartphone | Network Infrastruc... | ZTE | Lab02 + (10.9.0.2) - Port: Gi0/13 |
| Communication - MR86 Access Point | Access Point | Network Infrastruc... | Cisco Meraki | AN-13MH-01-SW01 + (10.100.2.20) - Port: 3 |
| IP Phone (eSpace 7950) | IP Phone | Network Infrastruc... | Huawei Technologies C... | 889-SW + (10.9.0.9) - Port: Fa2/0/7 |
| IoT | IoT - Others | Network Infrastruc... | Pronet GmbH | Lab_OT + (10.7.0.70) - Port: Gi0/3 |
| Communication - Aruba MODEL 105 Acc... | Access Point | Network Infrastruc... | Aruba Networks | AN-13MH-01-SW01 + (10.100.2.20) - Port: 48 |
| Mobile - Mate | Smartphone | Network Infrastruc... | Huawei Technologies C... | Lab02 + (10.9.0.2) - Port: Gi0/13 |

Sample report of devices and vendors

## Random MAC Addresses

A random MAC address is a temporary MAC address that is generated by a device when it connects to a network, in contrast to a permanent MAC address, which is assigned to a device when it is manufactured.



| Asset | Type | Group | Vendor | Location |
|---|---|---|---|---|
| IoT - Orange Pi SBC | IoT - Others | Network Infrastruc... | Orange Pi | scooby-doo + (10.7.0.8) - Port: Gi0/4 |
| IoT | IoT - Others | Network Infrastruc... | Pronet GmbH | Lab_OT + (10.7.0.70) - Port: Gi0/1 |
| Random MAC Address | Random MAC address | Network Infrastruc... | No Vendor | scooby-doo + (10.7.0.8) - Port: Gi0/3 |
| Random MAC Address | Random MAC address | Network Infrastruc... | No Vendor | AN-13MH-01-SW01 + (10.100.2.20) - Port: 48 |
| Random MAC Address | Random MAC address | Network Infrastruc... | No Vendor | SwitchAP + (10.0.0.2) - Port: Gi0/3 |
| Random MAC Address | Random MAC address | Network Infrastruc... | No Vendor | AN-13MH-01-SW01 + (10.100.2.20) - Port: 48 |
| Raspberry Pi | Raspberry Pi | Network Infrastruc... | Raspberry Pi Foundation | sepio-2960-x + (192.168.100.29) - Port: Gi1/0/22 |

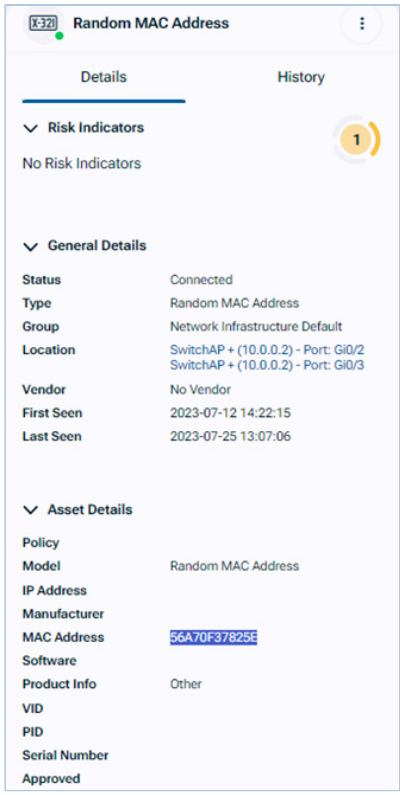
Random MAC Addresses

There are a few reasons why a device might use a random MAC address. One reason is to protect the device's privacy: when a device uses a random MAC address, it is more difficult for someone to track the device's activity on the network.

Another reason a device might use a random MAC address is to bypass network restrictions. Some networks restrict access to certain devices or applications. By using a random MAC address, a device can bypass these restrictions and gain access to the network.

The MAC specifications define that any MAC address' first octet that ends 2,6,A,E would be a random MAC address. For example, in 5**6**:A7:0F:37:82:5E the digit **6** in the first octet reveals this is a random MAC address.

**The following screenshot shows a Random MAC address in Sepio's Platform:**




Random MAC address in Sepio's Platform

# MAC Address Learning and Asset Visibility

## Overview: The Switch as the Source of Truth

To provide accurate asset visibility, it is critical to understand how network switches identify and track devices. At the heart of this process is the **MAC Address Table**.

Switches act as the "eyes" of the network infrastructure. They do not simply forward traffic blindly; they maintain a dynamic database that maps physical ports to the unique hardware identifiers (MAC addresses) of the devices connected to them.

## Dynamic Learning: How Switches See

Switches operate on a simple but powerful principle called **Source Address Learning**. This process is automatic and requires no human intervention.

When a device (like a laptop, printer, or rogue Raspberry Pi) is plugged into a port and sends its first packet, the switch will take the following actions:

- **Ingress & Learn:** The switch reads the Source MAC Address of the incoming frame. If the MAC is unknown, it adds an entry to its table: MAC Address X is on Port Y.
- **Update:** If the switch already knows the MAC but sees it coming from a different port, it updates the entry, indicating device movement.
- **Forwarding:** The switch looks at the **Destination MAC** to decide where to send the packet. If the destination is unknown, it "floods" the packet out to all ports in the same VLAN to find the target device.

### The Role of Timers (Aging)

Dynamic entries are temporary. To prevent the switch database from filling up with obsolete data, switches use an **aging timer**.

- **Default Behavior:** Usually set to 300 seconds (5 minutes).
- **The Process:** Every time a device sends traffic, its timer resets. If the device remains silent beyond the aging time, the switch deletes the entry.
- **Asset Tracking Implication:** If a device is passive (silent), it may disappear from the switch's live view even if physically connected.

> **Note:** Sepio can display devices even if they are dormant or inactive for longer than the switch's aging timer.

## Static MAC Assignment

Unlike dynamic learning, a **static MAC assignment** is a manual configuration performed by a network administrator. These entries do not expire and survive switch reboots.

**Typical Use Cases:**

- **Strict Security (Port Locking):** Administrators may lock a specific port so only a corporate printer can connect. Other MAC addresses are blocked.
- **Silent Devices (IoT/Industrial):** Some sensors only receive data and never transmit. Since they never send a source packet, the switch cannot learn them dynamically. Static entries define their exact location.
- **Blackholing (Security):** Administrators can assign a malicious MAC address to a Drop or Null interface to block it from communicating anywhere on the network.
- **Licensing Dongles:** Legacy software sometimes binds to a specific MAC. In virtual environments, a static MAC ensures the software sees the correct hardware ID.

> **Note:** There are additional use cases for static MAC address assignments. A switch can report how each MAC address is learned.

**Summary: Dynamic vs. Static MAC addresses**

| Feature | Dynamic Learning | Static Assignment |
|---|---|---|
| **Learning Method** | Automatically learned from incoming traffic | Manually configured by an administrator |
| **Creation** | Automatic (via traffic) | Manual (via Admin CLI or API) |
| **Persistence** | Temporary (lost on reboot) | Permanent (saved in configuration) |
| **Aging** | Subject to an aging timer (e.g., 5 minutes) | No aging; remains until manually deleted |
| **Flexibility** | High – devices can move between ports | Low – must be reconfigured to move |

## Special Interfaces & Concepts

### Trunk Ports

A **trunk port** connects two switches together and carries traffic for multiple devices and VLANs.

- **How MACs appear:** If Switch A connects to Switch B via Port 48, Switch A will learn the MAC addresses of devices that send traffic through Switch B via Port 48.
- **Visibility Implication:** Trunk ports can list hundreds of MAC addresses. When tracking assets (e.g., in Sepio), it is critical to distinguish between **edge ports** (where the device is physically plugged in) and **trunk ports** (which merely aggregate downstream traffic).

#### Software Defined Networks (SDN)

In modern data centers (Cisco ACI, VMware NSX), the concept of "learning" shifts from **Flood & Learn** to **Centralized Truth.**

- **Mechanism:** When an asset (for example, a virtual machine) is created, the central controller is notified immediately. It can program the switches with the device's location before the device sends any packets.
- **Visibility:** In these environments, asset queries are made to the **Global Endpoint Table** rather than individual switch MAC tables.

#### MAC Anomalies: Loops & Flapping

Anomalies in the MAC table are often indicators of misconfiguration or security threats. There are many reasons that can lead to such cases, for example:

- **MAC Flapping (Same Switch):** The switch sees MAC X rapidly appear on multiple ports. This usually indicates a network loop (e.g., a cable plugged into two ports) or a WiFi user roaming aggressively between Access Points.
- **Duplicate MACs (Different Switches):** MAC X appears on Switch A and Switch B simultaneously (in different locations). This is a high-severity alert, often indicating MAC spoofing (an attack) or Virtual Machine cloning errors.

## The Role of ARP (Address Resolution Protocol)

While switches operate at Layer 2 (MAC addresses), ARP links this to Layer 3 (IP addresses).

- **The Connection:** When a device joins the network, it often broadcasts an ARP Request (e.g., "Who has IP 10.0.0.1?").
- **Triggering Learning:** This ARP broadcast is frequently the first packet that triggers the switch to learn the MAC address.
- **Asset Context:** To get a full picture, we correlate the switch's MAC Table (location) with the router's ARP Table (IP context).

## From Switch to Database: Asset Tracking

Asset management systems like Sepio ingest MAC tables to maintain a historical record:

- **Polling:** The system reads the switch MAC table via SNMP or CLI.
- **Database Tracking:** Entries are stored in a history log.

**Why?** Switch memory is temporary. If a hacker connects for two minutes and disconnects, the switch forgets them. The asset database preserves a record (e.g. MAC X was on Port Y at 2:00 PM) for auditing and forensic analysis.

## Vendor Configuration Examples

### CISCO (IOS / NX-OS)

**View Table:**

```
show mac address-table
# Look for Type: DYNAMIC vs STATIC
```

**Set Static Entry:**

```
conf t
mac address-table static aaaa.bbbb.cccc vlan 10 interface GigabitEthernet1/0/1
# Syntax: mac address-table static vlan interface
```

### ARISTA (EOS)

**View Table:**

```
show mac address-table
```

**Set Static Entry:**

```
configure
mac address-table static 0011.2233.4455 vlan 100 interface Ethernet1
```

### JUNIPER (Junos – ELS Syntax)

**View Table:**

```
show ethernet-switching table
```

**Set Static Entry:**

```
edit
set switch-options interface ge-0/0/0.0 static-mac 00:11:22:33:44:55
commit
```

**Optional: Limit to a single MAC per interface:**

```
set switch-options interface ge-0/0/0.0 interface-mac-limit 1
```

# Deep Dive into Network Architecture

## Overview

Enterprise customers have a variety of needs, and the different network topology designs depend on those needs. An on-premises network refers to the physical infrastructure located within a company's own facilities, as opposed to the public cloud and is a mix of wired and wireless connectivity, with hardware-based offerings that can be a challenge to manage and modify to meet changing user connectivity needs. Key components of the network include the following:

- **Switches:** These devices connect devices on a network and intelligently route data packets.
- **Routers:** These connect different networks and direct data traffic to the appropriate destination network.
- **Firewalls:** These act as security barriers, controlling incoming and outgoing network traffic.
- **Servers:** These house applications, data, and resources for users on the network.
- **Workstations:** These are the personal computers used by employees.
- **Cables:** These physically connect devices on the network.
- **Wireless Access Points (WAPs):** These transmit and receive wireless signals, allowing devices to connect to the network.
- **Wireless Controllers:** These manage multiple WAPs centrally, simplifying configuration, security, and network traffic management for large deployments.

For OT (Operational Technology) environments (manufacturing, operations etc.), the network infrastructure includes additional components which depend on the size, complexity, and specific needs of the network.

- **Programmable Logic Controllers (PLCs):** These are industrial computers that control physical processes in factories, plants, and other automated environments. They can communicate with sensors and actuators on the network.
- **Human-Machine Interfaces (HMIs):** These provide operators with a graphical interface to monitor and control PLCs. They typically connect to the network to access data and send control signals.
- **Sensors and Actuators:** Sensors collect data from physical systems like temperature, pressure, or machine status. Actuators take physical actions based on control signals from PLCs, like opening valves, starting motors, or adjusting settings. These devices often connect to the network for monitoring and control.

**Additional IT Infrastructure Devices:**

- **Network Attached Storage (NAS):** These are specialized file-level data storage devices that connect to the network and provide shared storage for users and applications.
- **Load Balancers:** These distribute incoming network traffic across multiple servers to optimize performance and prevent any single server from becoming overloaded.

A robust network design must also be versatile to adapt to an organization's evolving needs based on the location of the network. It is often using the following key principles for crafting a reliable and adaptable network design:

- **Always-On Resilience:** Uninterrupted uptime and consistent availability are paramount.
- **Intelligent Adaptability:** The network should go beyond basic standards, dynamically adjusting to changing demands and leveraging insights from network activity.
- **Uncompromising Security:** Protect the organization and its users from cyber threats.

## (Main) Network Types Explained

- **LAN (Local Area Network):** A small network confined to a limited geographical area, like a single office building.
- **Campus Network:** Connects multiple LANs within a close geographical area, like a university campus or corporate headquarters.
- **Data Center:** A highly secure and controlled facility housing critical servers and network equipment.
- **Private Cloud:** A cloud computing environment created using on-premises hardware and software, offering similar benefits to the public cloud with greater control and security.
- **Branch / Remote Office Network:** A smaller network located at a remote company location, typically connected to the main network via the WAN (Wide Area Network).

While there are some general industry terms for network designs, networking vendors like Cisco, Juniper, Arista, HPE and others may have their own specific terminology and product lines focused on achieving those designs.

### General Network Designs

- **Hierarchical:** This is a layered approach with core, aggregation, and access layers. Common terminology across vendors.
- **Spine-Leaf:** A variation of hierarchical with high-bandwidth connections between core switches. Cisco uses the term ACI (Application Centric Infrastructure) for its data center spine-leaf solution.
- **Converged Network:** Combines data, voice, and video on a single network. May use vendor-specific technologies like Cisco's Convergence Networking System (CNS).
- **Fabric:** A high-performance, scalable network with many interconnected devices. Vendors may have specific fabric product lines like Cisco Nexus Fabric.

### Vendor Specifics

- **Cisco:** Often uses commercial names for its solutions alongside generic terms. For example, ACI for Spine-Leaf and DNA Center for network management.
- **Juniper:** Uses terms like QFX Series for high-performance switches and Contrail for their Software-Defined Networking (SDN) platform.

- **Arista:** Known for their high-density, low-latency switches. They may use terms like EOS (Extensible Operating System) for their switch software.
- **HPE:** Offers a broad networking portfolio, including Aruba for campus networks and SimpliVity for hyperconverged infrastructure.

## Campus Wired LAN

The campus wired LAN uses a hierarchical design model to break the design up into modular groups or layers allowing each layer to implement specific functions, which simplifies the network design and therefore the deployment and management of the network.

> **Note:** The network design and complexity impact device monitoring and the vendors ability to manage the risk of connected assets.

Modularity in network design allows you to create design elements that can be replicated throughout the network and thus provide an effortless way to scale the network as well as a consistent deployment method.

A hierarchical LAN design includes the following three layers:

- **Access layer** – Provides endpoints and users direct access to the network
- **Distribution / Aggregation layer** – Aggregates access layers and provides connectivity to services
- **Core layer** – Provides connectivity between distribution layers for large LAN environments

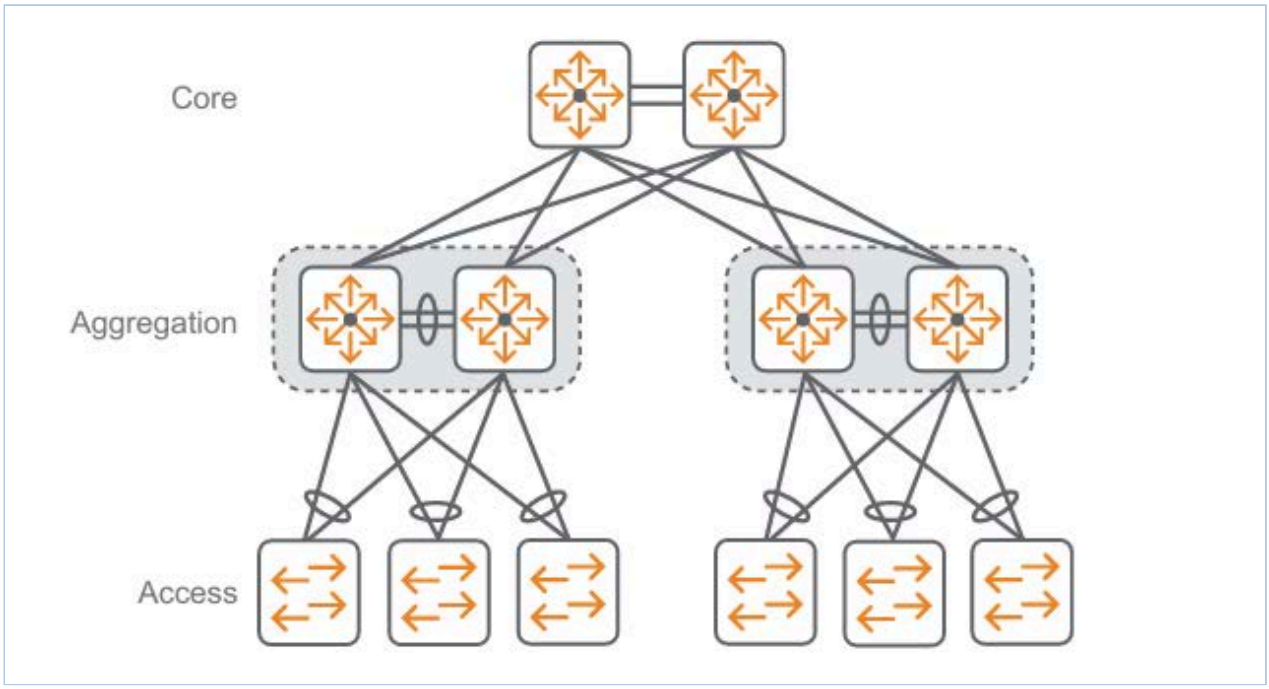



Diagram 1: LAN hierarchical design (source: HPE)

Each layer – access, distribution (or aggregation), and core – provides different functionality and capability to the network. Depending on the characteristics of the deployment site, you might need one, two, or all three of the layers. For example, a site that occupies a single building might only require the access and distribution layers, while a campus of multiple buildings will require all three layers.

Regardless of how many layers are implemented at a location, the modularity of this design ensures that each layer will provide the same services, and in this architecture, will use the same design methods.

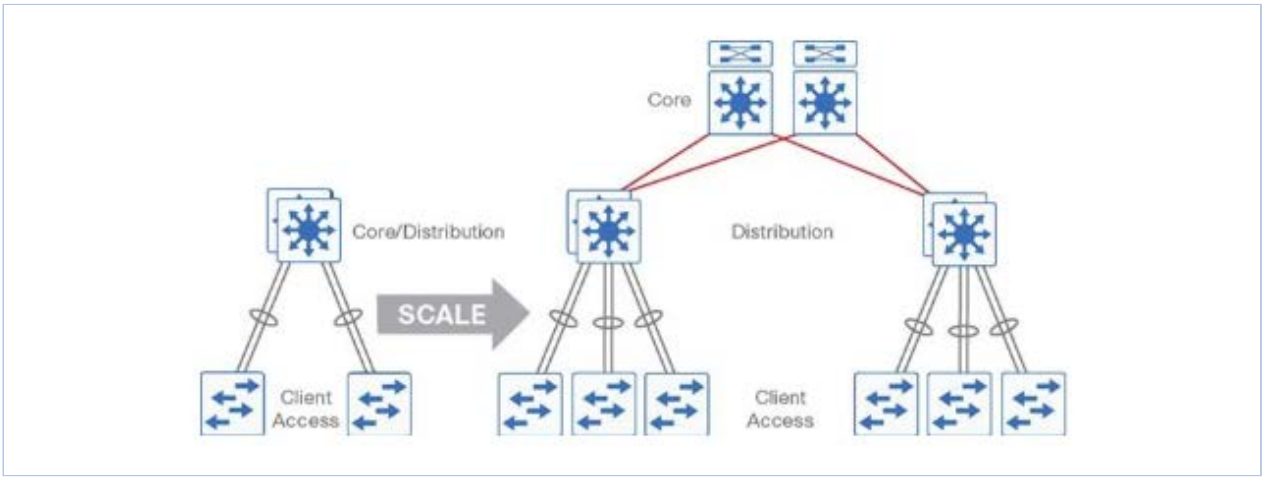



Diagram 2: Scalability by using a modular design (source: Cisco)

## Access Layer

The access layer is where user-controlled devices, user-accessible devices, and other end-point devices are connected to the network. The access layer provides both wired and wireless connectivity and contains features and services that ensure security and resiliency for the entire network.

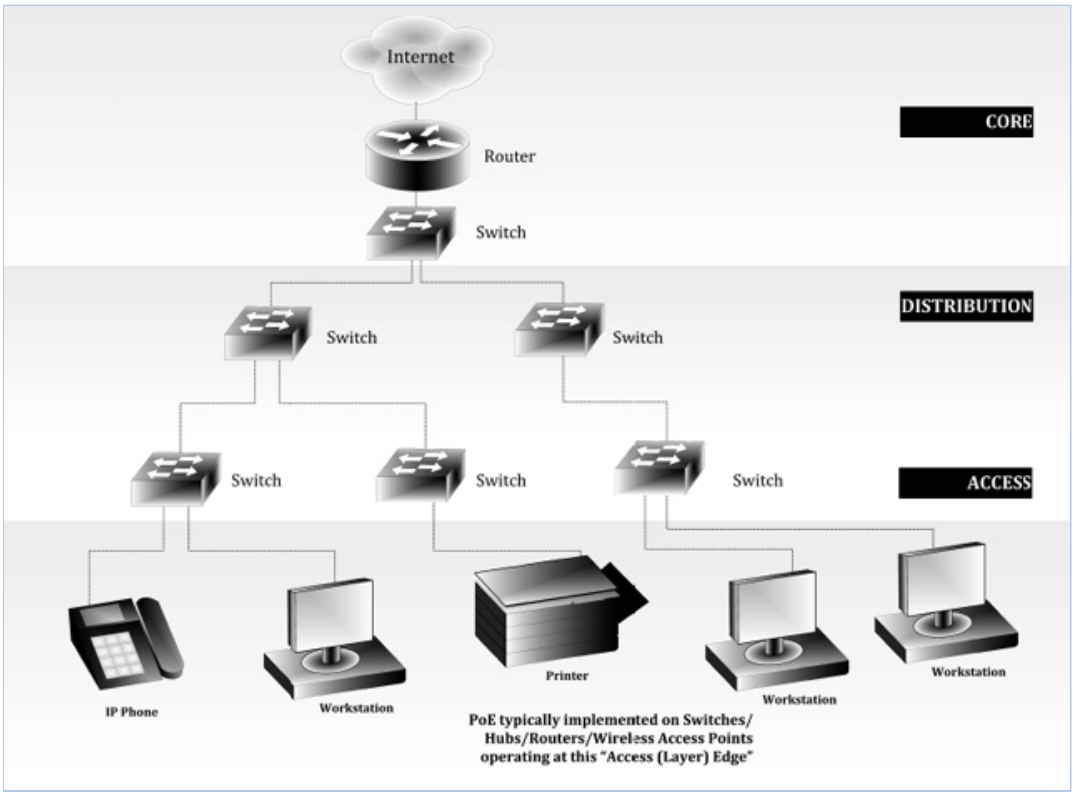



Diagram 3: Access layer connectivity (source: Oreilly)

### Switch Stack Configurations

To expand network capacity at the access-layer, switch stacks provide an effective and flexible solution:

- The switch stack behaves as a single device (characteristics and functionality of a single switch)
- The switch stack allows expansion of switch ports without having to manage multiple devices
- Switches can be added or removed from the switch stack without affecting the overall operation of the switch stack
- Depending upon the configuration of the switch stack, it can continue to transmit data even if a link or switch within the stack fails

When adding additional access layer switches in a stackable configuration, you should design the switch stack with the desired oversubscription ratio both during normal operations, and if there is a failure of a switch within the stack.

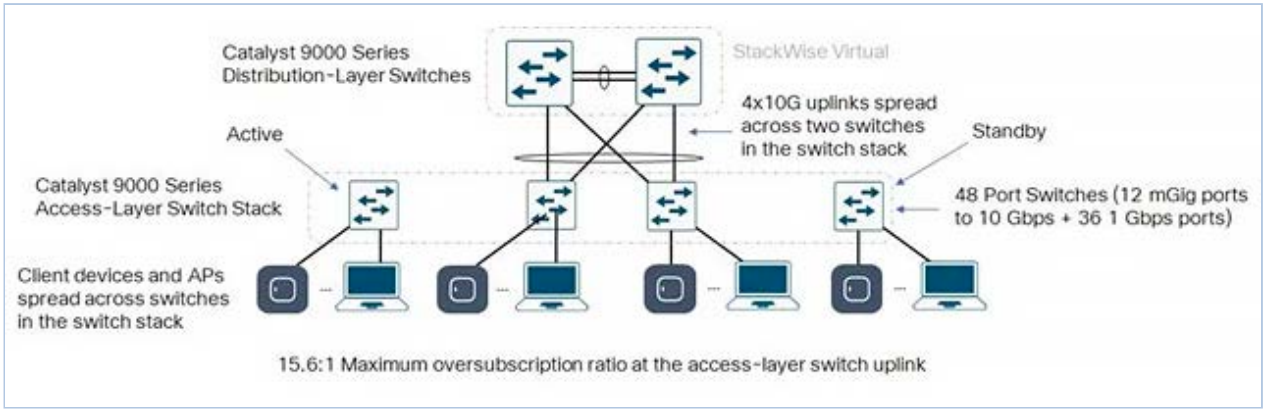



Diagram 4: Example of access-layer switch stack with oversubscription (source: Cisco)

## Distribution Layer

The distribution layer supports many important services. In a network where connectivity needs to traverse the LAN end-to-end, whether between different access layer devices or from an access layer device to the WAN, the distribution layer facilitates this connectivity.

- **Scalability** – At any site with more than two or three access-layer devices, it is impractical to interconnect all access switches. The distribution layer serves as an aggregation point for multiple access-layer switches.

The distribution layer can lower operating costs by making the network more efficient, by requiring less memory, by creating fault domains that compartmentalize failures or network changes, and by processing resources for devices elsewhere in the network. The distribution layer also increases network availability by containing failures to smaller domains.

- **Reduce complexity and increase resiliency** – The campus wired LAN has the option to use a simplified distribution layer, in which a distribution-layer node consists of a single logical entity that can be implemented using a pair of physically separate switches operating as one device or using a physical stack of switches operating as one device. Resiliency is provided by physically redundant components like power supplies, supervisors, and modules, as well as stateful switchover to redundant logical control planes.

#### Two-Tier Design

The distribution layer provides connectivity to network-based services, to the WAN, and to the Internet edge. Network-based services can include and are not limited to Wide Area Application Services (WAAS) and WLAN controllers. Depending on the size of the LAN, these services and the interconnection to the WAN and Internet edge may reside on a distribution layer switch that also aggregates the LAN access-layer connectivity. This is also referred to as a collapsed core design because the distribution serves as the Layer 3 aggregation layer for all devices.

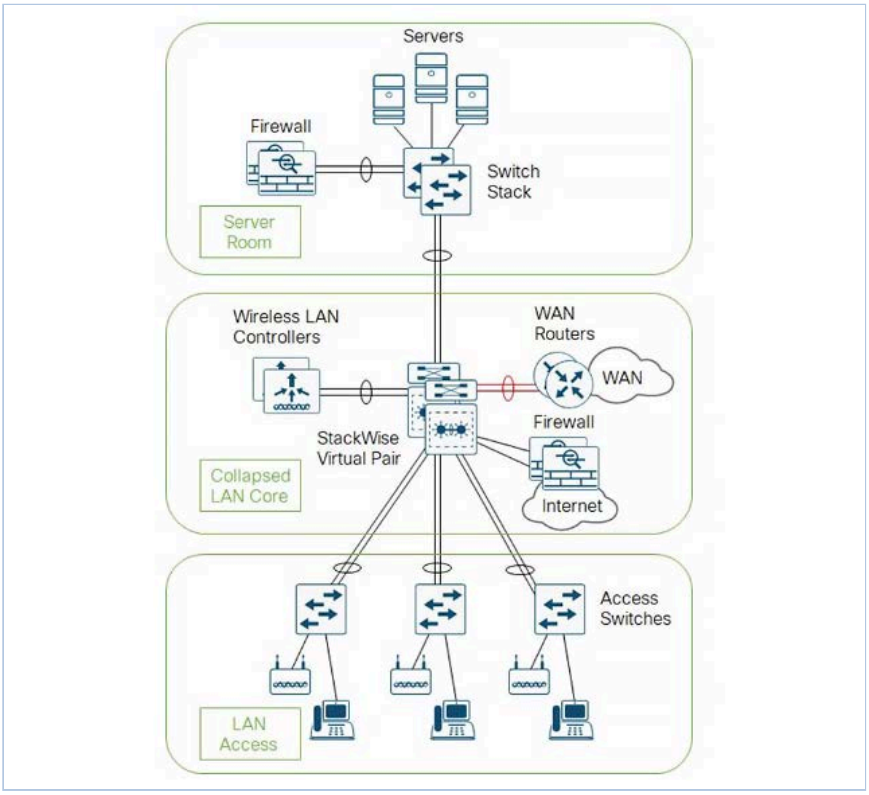


Diagram 5: Two-Tier Design: Distribution layer functioning as a collapsed core (Source: Cisco)

**Three-tier design**

Larger LAN designs require a dedicated distribution layer for network-based services versus sharing connectivity with access layer devices. As the density of WAN routers, WAAS controllers, Internet edge devices, and WLAN controllers grows, the ability to connect to a single distribution layer switch becomes hard to manage. When connecting at least three distributions together, using a core layer for distribution connectivity should be a consideration.

There are several factors that drive LAN design with multiple distribution layer modules:

- The number of ports and port bandwidth that the distribution layer platform can provide affects network performance and throughput.
- Network resilience is a factor when all LAN and network-based services rely on a single platform, regardless of that platform's design, it can present a single point of failure or an unacceptably large failure domain.
- Change control and frequency affects resilience. When all LAN, WAN, and other network services are consolidated on a single distribution layer, operational or configuration errors can affect all network operation.
- Geographic dispersion of the LAN access switches across many buildings in a larger campus facility would require more fiber optic interconnects back to a single collapsed core.

Like the access layer, the distribution layer also provides quality of service (QoS) for application flows to guarantee critical applications and multimedia applications perform as designed.

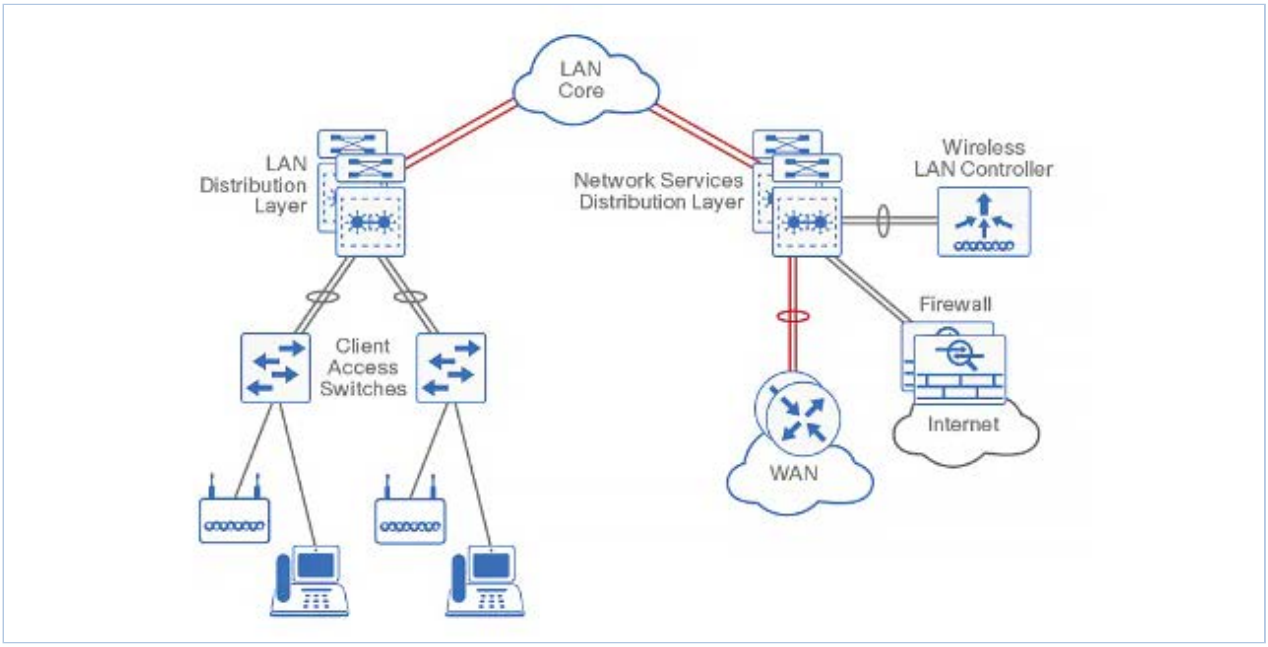



Diagram 6: Three-tier design with a network-services distribution layer (Source: Cisco)

## Core Layer

In a large LAN environment, there often arises a need to have multiple distribution layer switches. One reason for this is that when access layer switches are located in multiple geographically dispersed buildings, you can save potential costly fiber-optic runs between buildings by locating a distribution layer switch in each of those buildings. As networks grow beyond three distribution layers in a single location, organizations should use a core layer to optimize the design.

The core layer of the LAN is a critical part of the scalable network and, by design, is one of the simplest. The distribution layer provides the fault and control domains, and the core represents the 24x7x365 non-stop connectivity between them, which organizations must have in the modern business environment where connectivity to resources to conduct business is critical. Connectivity to and from the core is Layer 3–only, which drives increased resiliency and stability.

# Deep Dive on Switch Stacking

## What is Switch Stacking?

Switch stacking is a term that describes a technique for linking networking switches together. Stacked switches are connected in such a way that the multiple units operate as if they were a single device.

Switch stacking allows to expand network capacity without having to manage each switch individually. Switches that are designed for stacking can be easily put into a stack which saves time and energy with both planning and execution of network administration. In addition, it allows us to implement various high availability and redundancy scenarios.

## How Does Stacking Work?

Primarily, network stacking requires the switch manufacturer to design additional capabilities. Not all switches support any or all stacking capabilities. Stackable switches are designed to go into stacking mode easily. Some operate on a completely preconfigured design while others allow for more manual control. In either case, the switches will use designated ports (by the network admin or the manufacturer) to communicate with each other.

Ultimately, the stack is managed through a master switch. This is the switch that you configure and control directly. It's then disseminated configuration and instructions to the rest of the switches in the stack. You can control every unit in the stack by connecting to the master.

It is important to note that some switches come with built-in stacking capabilities, in software or with a separate hardware stacking module. Also, some switches require specific stacking cables.

## What Are the Major Advantages of Stacking?

The biggest reason to use stacking is for scalability. You can expand the network whenever you need to. If you have enough space, power, and cables, you can throw in another switch, up to the stack's maximum capacity.

That alone is a powerful motivator, but switch stacks bring other benefits to the table. They can improve network redundancy, flexibility, and ease of use.

## Redundancy

In a stack, if an individual stack fails, the rest of the stack can operate just fine. While part of the network might experience downtime, this prevents total failure from the loss of a central switch. With the use of a backup, the network has robust redundancy that can prevent network outages.

## Flexibility

Single switches in the stack can be removed or added ad hoc. This makes it easier to adjust network capacity. It also helps with repairs. If a single switch is failing, it can be replaced without taking the rest of the network offline. It is easier to manage and saves abundant time and energy in terms of network planning and strategy.

## Ease of Use

Stackable switches are designed for easy connection. Many of them can operate on a plug-and-play level if the master is up and running.

On top of that, they are designed for physical grouping. This allows you to centralize key parts of the network, so you don't have to run extra power and data infrastructure to accommodate more switches. Adding a stackable switch requires significantly less labor than adding individually managed switches.

## Switch Stacking Technologies

There are two main types of switches stacking technologies: backplane stacking and front-plane stacking. Each has its own advantages and disadvantages.

Backplane stacking:

- Uses dedicated stacking modules and cables plugged into the back of the switches.
- Creates a high-bandwidth, low-latency connection between switches, typically using proprietary protocols.
- Offers high scalability and redundancy, allowing for easy addition of more switches to the stack.

Front-plane stacking:

- Uses standard Ethernet ports and cables to connect the switches, often using Virtual Switching Framework (VSF) technology.
- More flexible and cost-effective than backplane stacking, as standard cables and ports are used.
- Offers slightly lower bandwidth and higher latency compared to backplane stacking.

## Common switches stacking technologies within each type:

Backplane Stacking:

- **Cisco StackWise®:** Proprietary technology used in Cisco Catalyst switches, offering high bandwidth and scalability.

- **HPE Intelligent Resilient Fabric (IRF):** Proprietary technology used in HPE Aruba switches, providing high availability and redundancy.
- **Extreme Networks SummitStack™:** Proprietary technology used in Extreme Networks switches, offering high-density stacking with low latency.

Front-plane Stacking:

- **Virtual Switching Framework (VSF):** An industry-standard protocol for stacking switches from different vendors, offering flexibility and cost-effectiveness.
- **Link Aggregation Control Protocol (LACP):** Used to combine multiple physical ports into a single logical trunk, increasing bandwidth and redundancy.

**Multi Chassis Link Aggregation (MC-LAG):** Extends LACP across multiple switches, creating a single, high-bandwidth logical link.

# USB Deep Dive

## Overview

USB stands for Universal Serial Bus. It is standard for connecting peripheral devices to computers. USB devices can be anything from keyboards and mice to printers and external hard drives. Overall, USB is a versatile and reliable standard for connecting peripheral devices to computers. It is easy to use, fast, and reliable. However, there are some limitations to USB, such as its limited power and the security risks associated with USB devices.

## How USB Works: Data Transmission and Communication

USB works by sending data in packets over a serial bus. A serial bus is a communication channel that allows two devices to send data to each other one bit at a time. The USB bus is a shared bus, which means that multiple devices can share the same bus. However, only one device can transmit data at a time. When a device wants to transmit data, it must first send a request to the bus controller. The bus controller then grants the device permission to transmit data.

### USB Cable Configuration

USB uses a four-wire cable to transmit data. The four wires are:

- **VBUS:** This wire provides power to the USB device.
- **D+:** This wire carries the data signal.
- **D-:** This wire carries the data signal in the opposite direction.
- **GND:** This wire is the ground wire.

### How the Computer Recognizes USB Devices

When a USB device is connected to a computer, the computer sends a signal to the device to identify itself. The device responds with its identification information, such as its manufacturer, product name, and product ID. The computer then assigns a unique address to the device. Once the device is assigned an address, it can start sending and receiving data. Data is sent in packets, which are small blocks of data. Each packet has a header that contains information about the packet, such as its size and destination address.
The device also sends a set of descriptors to the host. Descriptors are data structures that contain information about the device, such as its class, subclass, protocol, and capabilities. The host uses this information to determine what type of device is connected and how to interact with it.

The following are the types of descriptors that a USB device can send to the host:

- **Device descriptor**: This descriptor contains general information about the device, such as its manufacturer, product name, and product ID.
- **Configuration descriptor**: This descriptor contains information about the device's configuration, such as the number of interfaces and endpoints.
- **Interface descriptor**: This descriptor contains information about an individual interface on the device, such as the interface's class, subclass, and protocol.
- **Endpoint descriptor**: This descriptor contains information about an individual endpoint on the device, such as the endpoint's direction, transfer type, and maximum packet size.

Once the host has received the device's descriptors, it can determine what type of device is connected and how to interact with it. The host then loads the appropriate driver for the device and allows the user to interact with the device.

Here are some of the ways that a USB host can recognize what type of USB device is connecting to it:

- **Vendor ID and product ID**: The vendor ID and product ID are unique identifiers that are assigned to each USB device by the manufacturer. The host can use these identifiers to determine the type of device that is connected.
- **Class**: The class of a USB device is a high-level categorization of the device. There are many different classes of USB devices, such as human interface devices (HID), mass storage devices, and communication devices. The host can use the class of the device to determine how to interact with it.
- **Subclass and protocol**: The subclass and protocol of a USB device are more specific than the class. The subclass further categorizes the device, while the protocol specifies the specific protocol that the device uses. The host can use the subclass and protocol of the device to determine how to interact with it.

Overall, the USB host recognizes what type of USB device is connecting to it by using the device's descriptors and other identification information. This information allows the host to load the appropriate driver for the device and allow the user to interact with the device.

**Note:** This also means that attackers can spoof the identity of a device by changing the different descriptors.

**Note:** Sepio uses Asset DNA to classify and identify the USB device that is connected to the host. It will present both the DNA-based information as well as the data that is retrieved from the Vendor ID and product ID information reported by the USB device.

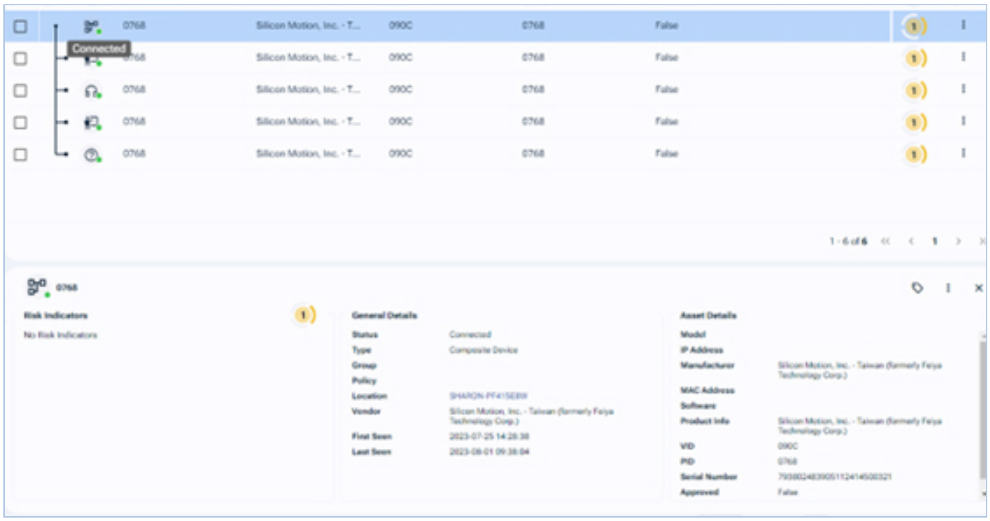
## What is a HID Composite Device?

A HID composite device is a USB device that combines two or more USB Human Interface Device (HID) interfaces into a single device. This allows the device to appear as multiple devices to the host computer, even though it is physically a single device. For example, a wireless mouse and keyboard combo might be implemented as a HID composite device. The host computer would see the device as two separate devices, a mouse and a keyboard, even though they are both physically connected to the same USB receiver.

The following screenshot shows a small subset of the USB composite device as it appears in the developer's debug tool and in Sepio's platform UI.




USB composite device




Sepio's platform UI

HID composite devices are often used to simplify the development of USB devices. By combining multiple HID interfaces into a single device, the developer can reduce the number of USB interfaces that need to be implemented. This can make the development process easier and faster.

Here are some of the benefits of using a HID composite device:

- **Simplicity**: It can simplify the development process by reducing the number of USB interfaces that need to be implemented.
- **Flexibility**: It allows the device to appear as multiple devices to the host computer, even though it is physically a single device.
- **Efficiency**: It can improve the efficiency of the device by reducing the amount of data that needs to be transferred over the USB bus.

Here are some of the limitations of using a HID composite device:

- **Complexity**: It can be more complex to implement than a single HID interface device.
- **Compatibility**: Some host computers may not support HID composite devices.
- **Performance**: The performance of the device may be reduced if the multiple HID interfaces are not well-optimized.

## Is keyboard a Composite Device?

A keyboard can be a composite device, but it doesn't have to be. A keyboard is a Human Interface Device (HID) device, which means that it is classified as a type of input device that sends data to a computer. HID devices are typically implemented as a single USB interface, but they can also be implemented as a composite device with multiple USB interfaces.

For example, a keyboard that has a built-in media control section might be implemented as a composite device. The keyboard would have two USB interfaces, one for the keyboard functionality and one for the media control functionality. The host computer would see the device as two separate devices, a keyboard and a media controller, even though they are both physically connected to the same USB connector.

However, a keyboard can also be implemented as a single USB interface device. In this case, the keyboard would only have one USB interface, and the host computer would see the device as a single keyboard.

## USB Descriptors

The USB specification defines the format of all of these descriptors. The format of a descriptor is always the same, regardless of the type of descriptor. The first two bytes of a descriptor contain the length of the descriptor in bytes. The next byte contains the type of descriptor. The remaining bytes of the descriptor contain the specific information for that type of descriptor.

USB descriptors are used by the USB host to enumerate and configure USB devices. The host uses the information in the descriptors to determine the capabilities of the device and to set up the appropriate drivers.

Here is a table that summarizes the different types of USB descriptors:

| Descriptor Type | Description |
| --- | --- |
| Device Descriptor | Provides basic information about the device, such as its vendor ID, product ID, and product version. |
| Configuration Descriptor | Describes the different configurations that the device can support. Each configuration can have multiple interfaces, and each interface can have multiple endpoints. |
| Interface Descriptor | Describes the different interfaces that the device supports. Each interface can have multiple endpoints. |
| Endpoint Descriptor | Describes the different endpoints that the device supports. Each endpoint has a unique address, a maximum packet size, and a transfer type. |
| String Descriptor | Provides human-readable strings, such as the device's manufacturer name and product name. |
| HID Descriptor | Used by Human Interface Devices (HIDs), such as keyboards and mice. |
| CDC Descriptor | Used by Communication Device Class (CDC) devices, such as modems and serial ports. |

## USB Hubs

A USB hub is a device that expands a single USB port into several so that there are more ports available to connect devices to a host system. Similar to a power strip, all devices connected through a USB hub share the bandwidth available to that hub.

USB hubs come in a variety of shapes and sizes, from simple devices with just a few ports to more complex devices with many ports and additional features like power switches, individual port power control, and more.

There are two main types of USB hubs:

- **Bus-powered hubs**: These hubs draw their power from the USB port they are connected to. They are typically limited to 500 mA of power, which means that they can only support a limited number of devices.
- **Self-powered hubs**: These hubs have their own power supply, which allows them to support more devices. They are typically powered by an AC adapter or a USB power adapter.

A USB hub includes multiple USB devices inside it.

USB hubs are a convenient way to add more USB ports to a computer. They are often used to connect peripherals such as printers, scanners, external hard drives, and flash drives. They can also be used to charge mobile devices.

# Deep Dive on Mouse Jigglers

## What is a Mouse Jiggler?

A mouse jiggler is a device or software designed to simulate mouse movement, preventing a computer from going into sleep mode or activating the screensaver. Mouse jigglers have been around for years, but they became more popular as working from home became mainstream. Initially, simple mechanical methods were used to move a physical mouse, such as placing the mouse on an analog watch or an oscillating fan. Over time, technology evolved to include software-based applications that mimic mouse movements, browser extensions, and small hardware devices that connect to a USB port. These USB devices, often built using microcontrollers like the ATtiny85, can emulate mouse movements by sending HID commands. Some advanced hardware jigglers can even be programmed to appear as a specific brand of mouse to a computer.

## Mouse Jigglers Security Risks

The use of mouse jigglers has introduced several security risks. Because they keep computers active, they can make systems vulnerable to unauthorized access, potentially exposing sensitive information. Additionally, the use of mouse jigglers can create a false impression of employee productivity, which can lead to trust issues and difficulties in evaluating employee performance. Employers may also struggle to maintain security certifications if employees are using these devices to bypass security protocols. Furthermore, some companies may monitor online status and have policies against installing unauthorized software or hardware, so using a mouse jiggler can be a violation of workplace policy.

## Advanced Mouse Jigglers: Features and Capabilities

Advanced mouse jigglers use sophisticated methods to simulate mouse movement and avoid detection. These devices have evolved from simple mechanical methods to include software, browser extensions, and specialized hardware. Here's a breakdown of advanced features and concepts:

- **Hardware-based Emulation:** Instead of physically moving a mouse, advanced jigglers directly inject emulated mouse movements via USB. These devices often utilize **microcontrollers like the ATtiny85** to send USB Human Interface Device (HID) commands.
- **USB HID Commands:** HID commands are part of the USB standard that allows devices like keyboards and mice to communicate with a computer. A mouse jiggler that sends HID commands can simulate the actions of a real mouse, moving the cursor and preventing the computer from going to sleep.
- **Customization and Discretion:**
    - Advanced hardware jigglers can be programmed to create randomized mouse movements to appear more like normal user activity.

    - Some advanced jigglers can be configured to appear as a specific brand or model of mouse to the computer's operating system.
    - These devices are often designed to be small and discreet, making them difficult to spot.
    - Some mouse jigglers can bypass USB restrictions.
- **Software and Scripting:**
    - Software-based jigglers can mimic mouse movements through programs installed on the operating system.
    - Scripts can be written to move the mouse cursor by a small number of pixels at set intervals.
    - Some software uses a "media is playing" flag to keep the screen active, using the same method as media players to prevent the screen from locking.
- **Detection Challenges:**
    - Advanced jigglers are designed to be hard to detect, making it challenging for employers to identify their use.
    - Some devices are designed to avoid detection by not leaving any obvious fingerprints in system logs.
    - Some may even use spoofed IDs to disguise themselves as legitimate devices.

**Note:** The evolution of mouse jigglers from simple mechanical devices to sophisticated hardware and software reflects efforts to bypass workplace monitoring systems.

# Deep Dive on Cisco Switch Interfaces

## Cisco Switch Interfaces

There are several types of interfaces for switches, each with its own purpose and capabilities. Most vendors have similar capabilities.
Here's a breakdown of the most common ones:

### Physical Interfaces

- **Ethernet interfaces:** These are the most common type of interface, used for connecting to LAN devices such as computers, servers, and other switches. They come in various speeds, including 10/100 Mbps (Fast Ethernet), 1000 Mbps (Gigabit Ethernet), 2.5 Gbps, 10 Gbps, 25 Gbps and higher.
- **Fiber interfaces:** These interfaces use fiber optic cables to connect to devices over longer distances and at higher speeds than copper Ethernet cables. They are typically used for connecting buildings or campuses together, or for providing high-bandwidth connections to critical servers.
- **Serial interfaces:** These interfaces use serial cables to connect to devices such as routers, modems, and consoles. They are not as common as Ethernet or fiber interfaces, but they are still used in some situations, such as for connecting to legacy equipment.

### Common Ethernet Interface Names

| Speed | Short Interface name | Longer Interface name |
|---|---|---|
| 10/100 M | Fa | FastEthernet |
| 1 G | Gi | GigabitEthernet |
| 2.5G | Tw | TwoGigabitEthernet |
| 10 G | Te | TenGigabitEthernet |
| 25 G | TF | TwentyFiveGigabitEthernet |
| 40 G | Fo | FortyGigabitEthernet |
| 50 G | Fi | FiftyGigabitEthernet |
| 100 G | Hu | HundredGigabitEthernet |
| 200 G | TH | TwoHundredGigE |
| 400 G | F | FourHundredGigabitEthernet |

There are additional interface types such as the Bundle-Ether Aggregated Ethernet (BE) and Bundle-POS Aggregated (BP) which are a group of one or more ports that are aggregated together and treated as a single link.

Besides the standard Ethernet interfaces like “Fa” (Fast Ethernet) and “Gi” (Gigabit Ethernet) for their speeds, Cisco switches have several special interface types for specific functionalities. The most relevant are listed below:

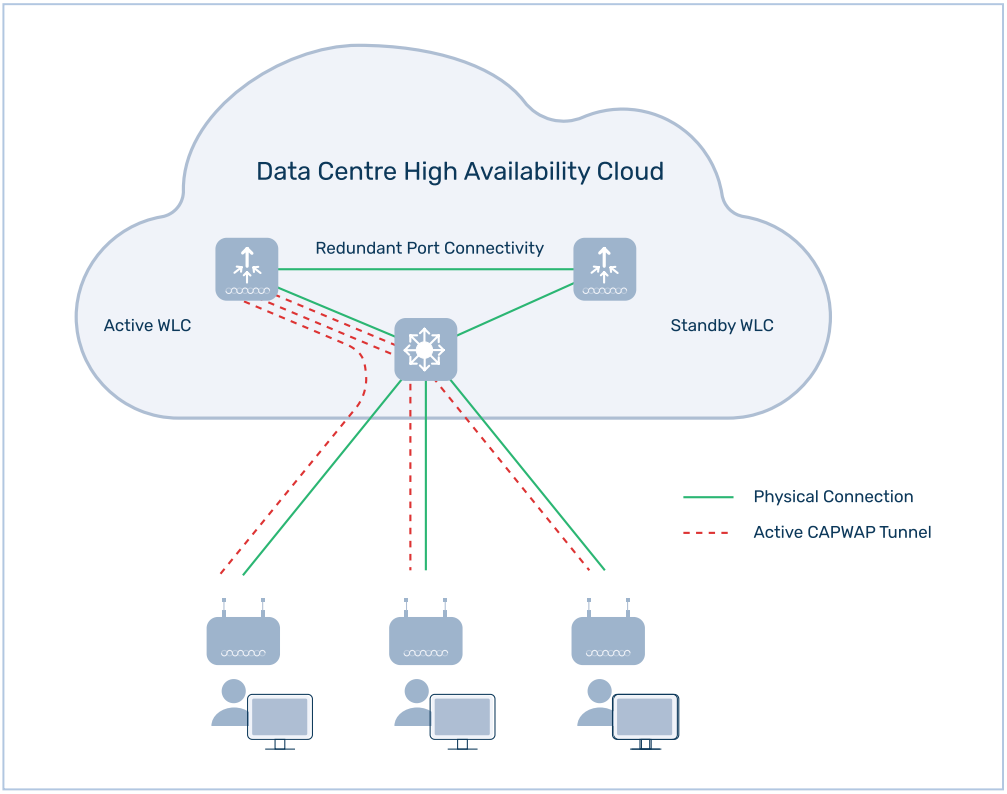
- **Trunk (Trunking):** Carries traffic for multiple VLANs (Virtual LANs) across a single physical link. It requires specific commands to enable trunking and define the VLANs allowed on the trunk port.
- **Tunnel Port:** Encapsulates traffic within another protocol for secure communication over a network.
- **HSRP (Hot Standby Router Protocol) Port:** Participates in HSRP, a protocol for providing router redundancy and failover.
- **VLAN Interface:** Represents a specific VLAN on the switch, used for managing and monitoring VLAN traffic. VLAN interfaces do not have a physical interface but are logically associated with a specific VLAN.
- **Port-Channel (EtherChannel):** Groups multiple physical ports together to create a logical high-bandwidth and fault-tolerant link.
- **SVI (Switch Virtual Interface):** Acts like a virtual router interface on a switch, allowing Layer 3 routing between VLANs.

# Deep Dive on WLC High Availability

## Overview

Wireless LAN Controller (WLC) High Availability (HA) addresses single points of failure inherent in centralized wireless network architectures. Without HA, failure of the primary WLC results in complete wireless network outage. WLC HA mitigates this through redundancy, providing a failover mechanism to maintain service continuity.

Vendors implement WLC HA primarily using two architectures: N+1 redundancy and Stateful Switchover (SSO).




Data Centre High Availability Cloud

## Data Centre High Availability Cloud

N+1 redundancy employs one or more backup WLCs. Under normal operation, these backups are inactive. Upon failure of an active WLC, a designated backup assumes control of the associated Access Points (APs). This provides a cost-effective HA solution, particularly for larger deployments where the cost of a fully redundant active system for every WLC might be prohibitive. The failover process involves the APs re-registering with the backup controller, which introduces a short service interruption.

## Cisco WLC SSO (Wireless LAN Controller Stateful Switchover)

Stateful Switchover (SSO) utilizes an active/standby WLC pair. The active WLC manages all APs and clients. The standby WLC maintains a real-time synchronized state with the active WLC, including configuration, client sessions, and operational data. In the event of active WLC failure, the standby immediately takes over, minimizing service disruption. This results in a significantly faster failover compared to N+1, as APs and clients do not need to re-establish connections.

Further enhancing failover are features like Access Point Stateful Switchover (AP SSO) and Client SSO. AP SSO maintains AP connectivity and configuration during WLC failover, preventing AP reboots and minimizing disruption. Client SSO ensures client sessions and IP addresses are preserved during failover, preventing client disconnections and minimizing application impact.

## Cisco WLC SSO Implementation

Here's a breakdown of the technical details of Cisco's WLC SSO implementation:

**1. Active/Standby Architecture:**

- SSO operates with two WLCs configured as an active/standby pair. Only one WLC actively manages the wireless network at any given time.
- The active WLC handles all client connections, AP management, and network operations.
- The standby WLC maintains a synchronized mirror of the active WLC's configuration and operational state.
- Initial setup for each WLC is separate. Each WLC will have its own IP address but once configured for SSO, there will be a single routable IP address for the active device.

**2. Synchronization Mechanisms:**

- **Control Plane Synchronization:** This involves replicating the WLC's configuration, including WLAN settings, security policies, and radio parameters, to the standby WLC. This ensures that both controllers have identical configurations.
- **Data Plane Synchronization:** This is the crucial aspect of SSO. It involves synchronizing real-time operational data, such as client session information, AP status, and radio resource management data. This ensures that the standby WLC has an up-to-date view of the network's state.

**3. Failover Trigger:**

- A failover is triggered when the active WLC becomes unavailable due to various reasons, such as:
  - Hardware failure
  - Software crash
  - Manual intervention
- The standby WLC detects the active WLC's failure through the loss of heartbeat messages.

**4. Failover Process:**

- Upon detecting a failure, the standby WLC immediately assumes the active role.
- Because of the continuous synchronization, the standby WLC already has the necessary information to take over seamlessly.
- APs maintain their connections with the newly active WLC, and client sessions are preserved.
- The failover time is typically very short, minimizing service interruption to a few seconds.

**5. Considerations:**

- SSO requires identical WLC models and software versions for compatibility.
- Proper network design and configuration are essential for optimal SSO performance.

## Cisco WLC SSO Limitations

When a Wireless LAN Controller (WLC) in SSO (Stateful Switch Over) Redundancy mode reports the Peer MAC Address as the same base MAC Address of the WLC, it typically indicates a configuration or connectivity issue. Here are a few potential causes:

**1. Redundancy Port Connectivity:**

- Ensure that the redundancy ports of both WLCs are properly connected. If there's an issue with the physical connection or the switch they are connected to, it can cause the WLCs to not recognize each other correctly.

**2. Configuration Mismatch:**

- Verify that both WLCs have the correct redundancy configuration. Any mismatch in the configuration can lead to issues with the SSO setup.

**3. Software Version Compatibility:**

- Check that both WLCs are running compatible software versions. Incompatible versions can cause synchronization issues and incorrect reporting of MAC addresses.

**4. Network Issues:**

- Ensure there are no network issues such as VLAN misconfigurations or IP address conflicts that could be affecting the communication between the WLCs.

# Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP)

## Overview

Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) are layer two discovery protocols designed to share information about network elements and infrastructure items to ease network management processes. CDP is a Cisco proprietary protocol while LLDP is a standard, formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in IEEE 802.1ab with additional support in IEEE 802.3 section 6, clause 79.

Cisco devices support the IEEE 802.1ab version of LLDP. This allows non-Cisco devices to advertise information about themselves to Cisco network devices.

Some network end devices (like IP Phones) can use LLDP for VLAN assignment or PoE (Power over Ethernet) requirements. To accomplish this, an enhancement was made which is called MED (Media Endpoint Discovery). This is typically known as LLDP-MED.

## Link Layer Discovery Protocol

LLDP uses TLVs (Type, Length, Value) attributes so that devices that support LLDP use TLVs to send and receive information to their directly connected neighbors. Some basic TLVs include:

- Port description TLV
- System name TLV
- System description TLV
- System capabilities TLV
- Management Address TLV

## Cisco Discovery Protocol

CDP employs a different approach called “packets” to exchange information. Cisco devices that support Cisco Discovery Protocol store the information received in a table which is refreshed every time an advertisement is received, and information about a device is discarded after three advertisements from that device are missed.

The information contained in Cisco Discovery Protocol advertisements varies based on the type of device and the installed version of the operating system. Some of the information that Cisco Discovery Protocol can learn includes:

- Cisco IOS version running on Cisco devices
- Hardware platform of devices
- IP addresses of interfaces on devices

- Locally connected devices advertising Cisco Discovery Protocol
- Interfaces active on Cisco devices, including encapsulation type
- Hostname
- Duplex setting
- VLAN Trunking Protocol (VTP) domain
- Native VLAN

## Benefits of using CDP and LLDP

- **Simplified Network Mapping:** CDP and LLDP automate the process of discovering network topology. This is helpful for network administrators to create network maps, visualize connected devices, and keep the information up to date.
- **Troubleshooting:** Information gathered through CDP or LLDP can pinpoint connectivity issues, such as mismatched duplex settings or port configuration errors.
- **Enhanced Network Management:** These protocols help administrators gather essential information like device types, capabilities, and software versions, simplifying inventory management and maintenance tasks.

## Main Differences Between CDP and LLDP

- **Vendor Support:** The key difference is that CDP is exclusive to Cisco devices, while LLDP is an industry standard supported by devices from a wide range of vendors.
- **Information Exchanged:** While both protocols share similar types of data, there can be minor differences in the specific details provided.
- **Security:** LLDP might be considered slightly more secure as it offers the option to disable the transmission of certain sensitive information.
- **Configuration:** Both CDP and LLDP can be enabled/disabled globally for the device, or individually for specific interfaces.

Sepio uses information collected from LLDP and CDP to improve the network location calculation, collect DNA data and identify additional unsupervised network infrastructure elements.

> **Note:** There are additional, proprietary Layer 2 discovery protocols like Foundry Discovery Protocol, Nortel Discovery Protocol and Microsoft's Link Layer Topology Discovery.

# Deep Dive on First Hop Redundancy Protocols

## Overview

First Hop Redundancy Protocol, or FHRP  is not a specific protocol itself. Instead, it's a category or group of protocols that are designed to provide redundancy for the default gateway in a network. In essence, if the primary router/switch serving as the default gateway fails, an FHRP ensures that another device can seamlessly take over its role, preventing a single point of failure and maintaining network connectivity for client devices.

## What is FHRP?

FHRPs solve the problem of a single point of failure at the first-hop router (the default gateway). In a typical network setup, client devices are configured with a single IP address for their default gateway. If that router goes down, all devices pointing to it lose their ability to reach other networks. FHRPs address this by:

1. **Providing a Virtual IP Address (VIP):** Client devices are configured to use a single virtual IP address as their default gateway.
2. **Providing a Virtual MAC Address (VMA):** This virtual IP address is associated with a virtual MAC address.
3. **Active/Standby or Load-Sharing Roles:** Multiple physical routers/switches participate in an FHRP group. One device takes on the "active" role (responding to ARP requests for the VMA and forwarding traffic for the VIP), while others are in "standby" or "backup" roles, ready to take over if the active device fails.
4. **State Synchronization (for some FHRPs):** For stateful FHRPs (like HSRP with SSO on Cisco Nexus/Catalyst platforms), the active and standby devices can synchronize state information (e.g., NAT translations, NetFlow entries) to minimize disruption during a failover.

## First Hop Redundancy Protocols

There are several FHRP implementations such as:

- Hot Standby Router Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Common Address Redundancy Protocol (CARP)
- Gateway Load Balancing Protocol (GLBP)

HSRP and VRRP are the most common.

## Main Differences Between HSRP and VRRP

While both HSRP and VRRP achieve first-hop redundancy, they have distinct origins and some key operational differences:

### 1. HSRP (Hot Standby Router Protocol)

- **Vendor Specific:** HSRP is a **Cisco-proprietary** protocol. It was developed by Cisco to address the single point of failure in their networks before a standardized protocol existed.
- **Active/Standby Model:** HSRP operates on an **active/standby** model.
    - One router is **Active**: Forwards traffic for the virtual IP and responds to ARP for the virtual MAC.
    - One router is **Standby**: Monitors the Active router and takes over if the Active fails.
    - Other routers in the group (if any) are in a "Listen" state.
- **Virtual MAC Address:** HSRP uses a specific, well-known virtual MAC address format: 0000.0C07.ACxx (where 'xx' is the HSRP group number). This means the virtual MAC address is consistent and always starts with 0000.0C07.AC.
- **Preemption:** By default, preemption is **disabled**. This means if the higher-priority active router fails and then recovers, it will NOT automatically take back the active role unless explicitly configured with standby preempt.
- **Authentication:** Supports clear text and MD5 authentication.
- **Load Balancing:** HSRP itself does not inherently support load balancing across multiple active routers for the same virtual IP. To achieve load balancing with HSRP, you typically configure multiple HSRP groups (each with a different virtual IP/MAC) and distribute VLANs/subnets across these groups, effectively making one router active for some VLANs and standby for others.
- **Groups:** Supports up to 256 HSRP groups per interface (HSRPv1) or 4096 (HSRPv2).

### 2. VRRP (Virtual Router Redundancy Protocol)

- **Open Standard:** VRRP is an **open standard** protocol, defined by IETF RFCs (RFC 3768, RFC 5798). This means it is supported by multiple vendors (Cisco, Juniper, Huawei, HP, etc.), making it suitable for multi-vendor environments.
- **Master/Backup Model:** VRRP operates on a **Master/Backup** (or Master/Standby) model.
    - One router is **Master**: Forwards traffic for the virtual IP and responds to ARP.
    - One or more routers are **Backup**: Monitor the Master and take over if the Master fails.
- **Virtual MAC Address:** VRRP uses a different, standard virtual MAC address format: 0000.5E00.01xx (where 'xx' is the VRRP group ID). This is a well-known standard MAC address block for VRRP.
- **Preemption:** By default, preemption is **enabled**. If a higher-priority router comes online or recovers, it will automatically take over the Master role. This behavior can be disabled.
- **Authentication:** Supports clear text, MD5 (RFC 3768), and often more robust authentication methods depending on vendor implementation and newer RFCs (RFC 5798 removes MD5 but allows other mechanisms).

- **Load Balancing:** Similar to HSRP, VRRP by itself doesn't offer direct load balancing for a single virtual IP. Multi-group configuration is used for load balancing.
- **Groups:** Supports up to 255 VRRP groups per interface.

**Key Differences Summary Table**

| Feature | HSRP (Hot Standby Router Protocol) | VRRP (Virtual Router Redundancy Protocol) |
|---|---|---|
| **Standard** | Cisco Proprietary | Open Standard (RFC 3768, RFC 5798) |
| **Roles** | Active, Standby, Listen | Master, Backup |
| **Virtual MAC** | 0000.0C07.ACxx | 0000.5E00.01xx |
| **Preemption Default** | Disabled | Enabled |
| **Authentication** | Clear text, MD5 | Clear text, MD5 (older), various (newer RFCs) |
| **Load Balancing** | Via multiple groups | Via multiple groups |
| **Usage** | Primarily Cisco-only networks | Multi-vendor networks, often preferred for compliance |

# Release Notes

## Release Versioning

Sepio is updating its release methodology to better support diverse customer upgrade cycles. We now release a **Major Version** once per quarter, designed for enterprises preferring a quarterly upgrade cadence. Between major versions, we provide **Minor Releases** on the regular release schedule, delivering continuous improvements. If needed, patches and fixes can be provided for customers that do not upgrade frequently.

The versioning format is **VV.YYMM.NNN**. The middle component (**YYMM**) reflects the year and month of the build, rather than the significance of the release. **VV** represents the version family, and **NNN** is a build number counter for a specific release. To assist with planning, the release notes for every version clearly designate the release **type** (major or minor).

> **Note:** Please contact Sepio support with any questions.

## Release Availability

The preferred deployment mode for Sepio is SaaS. Customers who, due to internal regulations or compliance requirements, must operate the platform in their own data centers or private clouds may select alternative deployment options that best meet their needs. While the Sepio Management Platform is identical across all deployment types, the installation and delivery methods vary.

The following table outlines the current availability of the different deployment options.

| Deployment | Packaged release for distribution | Notes |
|---|---|---|
| Sepio SaaS | v60 (build 17.2604.632) | Upgrades performed by Sepio, coordinated with the customer during a maintenance window |
| Other public clouds | v60 (build 17.2604.632) | |
| On-premises installation on customer hardware | v60 (build 17.2604.632) | Offline or air-gapped deployments |
| On-premises installation using Sepio's virtual appliance (OVF) | v60 (build 17.2604.632) | |

**Notes:**

- Please contact Sepio support with any questions.
- US Government and Federal customers should contact Sepio Federal Support.

## Related Topics

- Sepio Platform
- Sepio Agent
- Sepio Knowledge Base

# Known Limitations

## Overview

This page lists known limitations for Sepio Platform. For clarifications and other related issues, please contact Sepio Support.

## known Limitations

| Limitation | Issue ID | Applicability |
|---|---|---|
| When creating a saved query and selecting the displayed columns, all user defined attributes will be added to this newly created query. | Q-4304 | All versions of Sepio Platform |
| Can't export data for a query with modified columns from the query results screen. It is possible to download the report that contains the query results in CSV or PDF format. | Q-4305 | All versions of Sepio Platform |
| Saving a query does not keep the selected columns. The Sepio Administrator should define which columns the results page should present in the query configuration "Columns" section. | Q-4306 | All versions of Sepio Platform |
| When creating a scope, the query evaluation is case-sensitive, while the preview results are not. This causes a mismatch between the assets that actually belong to the scope and the assets displayed in the preview screen. | Q-4280 | Sepio Platform builds 17.2510.523 and 17.2511.510. |
| In some cases, when an asset was connected to a switch that was migrated to a different platform but remains in the same location, the asset may appear as connected on two different ports (previous and current) on the same switch. | Q-3867 | All versions of Sepio Platform |
| In some cases, offline assets that were migrated in a specific time have no asset name. | A-2370 | Sepio Platform build 17.2507.514 |
| In some cases, when using LDAP, sessions are automatically terminated after 8 minutes, even when the user remains active. | O-1326 | Sepio Platform builds 17.2504.926 to 17.2506.503 |

| Limitation | Issue ID | Applicability |
|---|---|---|
| Linux Host Agents are not upgraded by the Sepio Management Platform and thus should be upgraded by the administrator via the shell or using any configuration tool. | Q-2093 | All versions of Sepio Linux Agent and All versions of Sepio Platform |
| When more than a single asset is reporting CDP/LLDP to a port and this information does not include a MAC address, Sepio will present the discovered information but will not use the CDP/LLDP data to enrich the connected asset attributes. | A-1700 | All versions of Sepio Platform |
| Disabling local users using the configuration property DISABLE_LOCAL_USERS=true has no effect. Local users can be disabled by Sepio Support directly on Sepio Platform's database. | Q-1817 | All versions of Sepio Platform |
| When changing the scan priority of a network device and this device is scheduled for a scan already, the change will be reflected in the UI after the scheduled scan task is completed, yet the audit record will be updated as soon as the administrator has asked for the change. | Q-1944 | All versions of Sepio Platform |
| To configure two switches with the same IP address but different domains, the user should first upload the first switch and wait for its status to change to "connected." Once this is confirmed, the second switch can then be added. | CPO-1118 | All versions of Sepio Platform |
| When connecting a switch with insufficient access level, the status may display as "Unsupported". The specific command requiring permissions can be identified in the switch logs. | I-1413 | All versions of Sepio Platform |
| Sepio configuration for high performance environments will not be updated during the version upgrade. The configuration should be performed manually after the upgrade is completed. | Q-2836 | Sepio Platform builds 17.2306.697 to 17.2306.732 |
| When connecting a switch with incorrect credentials, the status may display as "Unable to Connect" rather than "Authentication Failed". The underlying cause of the switch connection issue can be extracted from the switch logs. | Q-1777 | Sepio Platform builds 17.2306.429 to 17.2306.675 |
| When integrating Sepio with the Meraki API, if multiple switches are assigned the same IP address within the same domain, the onboarding process for those switches may experience delays. | N-908 | All versions of Sepio Platform |

| Limitation | Issue ID | Applicability |
|---|---|---|
| Sepio dev tools page does not load. | Q-4294 | Sepio Platform builds 17.2511.510 and 17.2511.603 |
| Enabling multiple peripherals at the same time is not supported. | Q-4491 | All agent macOS versions |
| When attempting to disable multiple peripherals simultaneously, the agent blocks them sequentially rather than all at once. | Q-4491 | All agent macOS versions |
| When updating the KB automatically, the Version field is updated correctly in the UI, but the Build Time will not update (it only updates when manually uploading a KB) | Q-4563 | Sepio Platform builds 17.2601.508 |
| Automatic KB updates only update the internal server KB. For a new Agent Version update, a manual KB upload is required. | Q-4563 | Sepio Platform builds 17.2601.508 |
| In environments where the host has Federal Information Processing Standards (FIPS) mode enabled and services run in .NET containers using OpenSSL 3.1 or higher, FIPS enforcement inside the container is disabled to prevent service communication failures. | Q-4781 | Sepio Platform build 17.2602.516 or higher |
| Port configuration not presented for N9K-C93180YC-EX. | Q-4905 | Sepio Platform build 17.2602.627 or higher |
| USB hubs are not blocked on macOS, as the operating system does not treat hubs as enforceable peripheral devices. | Q-4255 | All agent macOS versions |
| When switching between agent modes, enforcement on already connected devices may be delayed and, in some cases, will only apply to newly connected peripherals. | Q-4255 | All agent macOS versions |
| Blocking a child interface of a composite USB device results in blocking the entire device, including all associated interfaces. | Q-4255 | All agent macOS versions |
| If a peripheral driver fails to load properly on macOS, the device will be reported as blocked, since devices without a functioning driver are considered disabled by the operating system. | Q-4255 | All agent macOS versions |
| Exporting audit or even logs to is limited to 10,000 events. | I-2941 | All versions of Sepio Platform |

**Note:** For any questions, please contact support@sepiocyber.com.

# Sepio Agent

## Related Topics

- Sepio Agent
  - Sepio Agent 17.2602.229 Release Notes
  - Sepio macOS Agent 17.2511.160 Release Notes
  - Sepio Agent 17.2511.124 Release Notes
  - Sepio Agent 17.2509.101 Release Notes
  - Sepio Agent 17.2506.520 Release Notes
  - Sepio Agent 17.2504.108 Release Notes
  - Sepio MacOS Agent 17.2501.104 Release Notes
  - Sepio Agent 17.2409.14 Release Notes
  - Sepio Agent 17.2306.385 Release Notes
  - Sepio Agent 17.2306.352 Release Notes
  - Sepio Agent 17.2306.292 Release Notes
  - Sepio Agent 17.2306.275 Release Notes
  - Sepio Agent 17.2306.273 Release Notes
  - Sepio Agent 17.2306.252 Release Notes

# Sepio macOS Agent 17.2604.118 Release Notes

This release introduces major stability improvements and bug fixes.

## System Requirements

- **macOS Version:** macOS 14 and above
- **Supported Devices:** MacBook Pro with M-series processors

## Release Highlights

### macOS Agent Stabilization

This release introduces major architectural improvement to the macOS agent's low-level components. The device handling mechanism has been re-built to provide more accurate and consistent reflection of device states.

Ticket ID: Q-4545

## New Features, Changes and Bug Fixing

| Item | Task ID |
| --- | --- |
| **Fixed:** Resolved an issue where printers and devices operating in DFU mode were incorrectly displayed as disabled. | Q-4255 |

## Known Limitations

See the list of known limitations.

# Sepio Agent 17.2602.229 Release Notes

This release introduces several enhancements and fixes.

## Release Highlights

### Agent Events Enhancement

Added support for the enhanced event and logging system introduced in Sepio Platform V56.
For more information on Peripheral Policy, see Enhanced Event and Logging System.

**Task ID:** A-1197

## Mouse Jigglers Detection Enhancement

Sepio Agent now includes a behavioral detection capability to identify potential mouse jiggler activity based on mouse movement patterns. This enhancement complements Sepio's existing AssetDNA-based detection and improves coverage for both dedicated mouse jiggler devices and mouse movers.

When suspicious activity is detected, the agent assigns a **"Potential Mouse Jiggler"** risk indicator to the asset, enabling administrators to enforce policy actions such as **block** or **notify**.




Potential Mouse Jiggler

For more information, see Mouse Jiggler Detection.

**Limitations:** This capability is supported only on Windows 7, Windows 10, and Windows 11 (32-bit and 64-bit).

### Prerequisites & Configuration Requirements:

- `JIGGLER_DETECTION_ENABLED` and `RI_MOUSE_JIGGLER` flag must be true
- `JIGGLER_DETECTION_MOVEMENT_WINDOW` should be set to 8
- `JIGGLER_DETECTION_PAUSE_THRESHOLD` should be set to 30

**Task ID:** IN-2220

## New Features, Changes and Bug Fixing

| Item | Task ID |
| --- | --- |
| **Behaviour change:** USB Peripheral Connected and USB Peripheral Disconnected events are now generated for agents operating in Policy Mode. | A-1258 |
| **Fixed:** Resolved an issue in which agent log files grew excessively when the Sepio Platform Server was unavailable. | Q-4255 |
| **Fixed:** Resolved an issue where the USB Peripheral Enabled event was not generated when the agent was operating in Policy Mode. | A-1261 |

# Sepio macOS Agent 17.2511.160 Release Notes

This version of the macOS agent introduces several enhancements and fixes.
See the list of supported hardware and software.

## Release Highlights

### Peripheral Policy

This agent version supports the new Peripheral Policy capability, introduced in Sepio Platform version 50. For more information, see Peripheral Policy Introduction.

Ticket ID: I-1986

### Silent Installation

This version introduces a new silent installation method that supports deployment through endpoint management tools such as Intune and Jamf, in addition to the existing installation flow.

To install macOS agents using endpoint management tools, you must use both the agent PKG installation file and the installation script, which should be executed by the management tool.

For more information, please contact Sepio support at support@sepiocyber.com.

Ticket ID: I-1687

## Modifications and Bug Fixing

| Item | Task ID |
|---|---|
| **Fixed:** In some cases, USB storage devices were miscategorized as Composite Devices. | Q-3902 |
| **Fixed:** Misrepresentation of the “blocked” indication for MalDuino devices: (1) In rare cases, the “blocked” status may not display properly despite the device being blocked. (2) In rare cases, a device may be shown as offline and blocked even though it is connected and blocked. | A-850 |

## Specific Limitation

| Item | Task ID |
| --- | --- |
| Detecting a WiFi keylogger on the macOS agent is not supported. | I-1686 |
| The agent requires a valid server certificate for operation. | CPO-I-401 |
| If the agent is redirected to a server it previously connected to, it will automatically revert to the last operational mode used on that server. | Q-4350 |
| Intermittent recognition of Samsung Electronics USB-C headphones (VID: 04E8, PID: A057). The device may initially be detected and audio may function as expected, but it often disconnects unexpectedly after a short period. | Q-4351 |
| In some cases, composite devices may show a different number of child elements on macOS compared to Windows due to OS-level differences in device mapping behavior. | Q-4316 |
| Silent upgrade requires a complete cleanup of older macOS agents using the `clean.sh script`. | CPO-1123 |
| Logs related to CPU and memory usage are not collected automatically. | A-854 |

## Known Limitations

See the list of known limitations.

# Sepio Agent 17.2511.124 Release Notes

This release introduces several enhancements and fixes.

## Release Highlights

### Peripheral Policy

This agent version supports the new **Peripheral Policy** capability, which was introduced in Sepio Platform V50.
For more information on Peripheral Policy, see Peripheral Policy Introduction.

Task ID: I-1986

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **Fixed:** Agent version 17.2544.120 was not calculating the Risk Indicator (RI) for vulnerable devices correctly. | Q-4236 |
| **Fixed:** After a specific Windows update, the agent service fails to automatically start | Q-4103 |
| **New:** Improved logging to provide better visibility into cases where the agent loses its connection to the server | Q-4067 |

## Known Limitations

| Item | Task ID |
|---|---|
| In some cases, the Linux installation files will not get execution permissions. For all Linux platforms, it is required to manually add execution permission (`chmod +x`) for the files that were extracted before performing the installation. For example, of RedHat Enterprise Linux:<br>`tar xvzf sepioagent#redhat#17.2306.292#.tar.gz`<br>`chmod +x *`<br>`sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=FQDN_of_sepio` | CPO-I-214 |

| Item | Task ID |
| --- | --- |
| **All platforms:** Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from the currently installed version to the latest Agent version. While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to “install” or “modify” the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent. | O-315, A-603, CPO-A-275 |
| The agent requires that a valid server certificate must be used. | CPO-I-401 |

# Sepio Agent 17.2509.101 Release Notes

Supported platforms: see Supported Operating Systems for Sepio Host Agent.

This release introduces several enhancements and fixes.

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Introduced functionality to **Exclude USB Devices from Sepio Agent Asset DNA Reading** | A-1049 |
| **New:** Agent now reports peripherals shortly after reconnecting online | A-1091 |
| **New:** Added protection for cases where Windows does not allow disabling a connected device | A-1086 |
| **New:** Enhanced Agent logging to provide better insights | A-1092 |
| **Fixed:** Resolved issue causing Agent high CPU utilization | A-1087, A-1054 |
| **Fixed:** Improved handling of failed device descriptors | A-1088 |
| **Fixed:** Resolved issue where the Agent sometimes sent incorrect “new peripheral connected” event | Q-3753 |

## Known Limitations

| Item | Task ID |
|---|---|
| **Changed behavior:** USB composite devices will now generate a single disconnect/reconnect event for all associated internal interfaces. | A-992 |
| **New:** Enhanced debug logs have been added. | A-967 |
| **Fixed:** Improved stability of agent reporting mechanism. | Q-3039 |

# Sepio Agent 17.2506.520 Release Notes

Supported platforms: see Supported Operating Systems for Sepio Host Agent.

This release introduces several enhancements and fixes.

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **Changed behavior:** USB composite devices will now generate a single disconnect/reconnect event for all associated internal interfaces. | A-992 |
| **New:** Enhanced debug logs have been added. | A-967 |
| **Fixed:** Improved stability of agent reporting mechanism. | Q-3039 |

## Known Limitations

| Item | Task ID |
|---|---|
| In some cases, the Linux installation files will not get execution permissions. For all Linux platforms, it is required to manually add execution permission (chmod +x) for the files that were extracted before performing the installation. For example, of RedHat Enterprise Linux:<br>`tar xvzf sepioagent#redhat#17.2306.292#.tar.gz`<br>`chmod +x *`<br>`sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=FQDN_of_sepio` | CPO-I-214 |
| **All platforms:** Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from the currently installed version to the latest Agent version. While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to “install” or “modify” the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent. | O-315, A-603, CPO-A-275 |
| The agent requires that a valid server certificate must be used. | CPO-I-401 |

# Sepio Agent v17 for Windows (build no. 17.2306.252) Release Notes

## Release Highlights

**This Release Introduces a New Policy Mode for Blocking Mass Storage Devices**

In this mode the Sepio Agent automatically blocks an Asset/Peripheral that is classified as a USB Mass Storage Device (including thumb drives, disk on key, mobile phones with storage interfaces etc.) as well as other Asset /Peripheral that are identified as attack tools whether it's `Approved' or 'Disapproved', after matching its DNA profile to the Agent's 'Known Threats' List.

This mode is available for Sepio Platforms Version 15 or above. The Sepio Platform is backwards compatible with Sepio Agent Version 16.

Operating this mode is the same as other ARM, Block Known Threats and FREE modes. Blocking a Mass Storage Device according to the policy will generate system events but will not introduce Risk Indication.

The Hardware Compatibility List (HCL) and list of Supported Windows OS are not changed. Please see the relevant sections in the Sepio Technical documentation.

## Notes

1. Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from 16.2303.44 to the latest Agent version.
2. While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to "install" or "modify" the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent.

Task IDs: O-315, A-603

## Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **Changed behavior:** ARM mode operations while device manager provides user pop up for USB mass storage devices. Previously, Agent in Armed mode allowed new storage device on the first connection and blocking on the second attempts onwards (Effect of BitLocker enabled on the OS). | A-366 |
| **Fixed:** Mass Storage Devices with BitLocker enabled blocking issues in ARM mode. | CPO-A-366 |

# Sepio Agent v17 for Windows (build no. 17.2306.273) Release Notes

This release introduces a fix for Windows Descriptors Issue.

## Changes and Bug Fixing

| Item | Task ID |
| --- | --- |
| Fixed: Windows related USB descriptors | A-622 |

# Sepio Agent v17 for Linux and Windows (build no. 17.2306.275) Release Notes

## Release Highlights

### This Release Introduces Block Mass Storage Devices for Linux

**Reminder:** In this mode the Sepio Agent automatically blocks an Asset/Peripheral that is classified as a USB Mass Storage Device (including thumb drives, other storage known as “disk on key”, mobile phones with storage interfaces etc.) as well as other Asset /Peripheral that are identified as attack tools whether it’s `Approved’ or ‘Disapproved’, after matching its DNA profile to the Agent’s ‘Known Threats’ List.

This mode is available for Sepio Platforms Version 15 or above.

Operating this mode is the same as other ARM, Block Known Threats and FREE modes. Blocking a Mass Storage Device according to the policy will generate system events but will not introduce Risk Indication.

## Notes

1. **Linux:**
   For all platforms, it is required to manually add execution permission (chmod +x) for the files that were extracted **before** performing the installation. For example, of RedHat Enterprise Linux:

   ```
   tar xvzf sepioagent#redhat#17.2306.275#.tar.gz
   chmod +x *
   sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=FQDN_of_sepio
   ```

2. **Windows:**
   a. There are no changes comparing with the previously released windows agent, yet we provide the same version for simplified operations of our customers.

   b. Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from the currently installed version to the latest Agent version.

   c. While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to “install” or “modify” the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent.

Task IDs: O-315, A-603, CPO-A-275

## Changes and Bug Fixing

| Item | Task ID |
| --- | --- |
| Linux Agents support for BST mode | CPO-A-275 |

# Sepio Agent v17 for Linux and Windows (build no. 17.2306.292) Release Notes

This release includes multiple fixes and minor updates to improve the backend processing and operations.

## Changes and Bug Fixing

| Item | Task ID |
|---|---|
| Resolved: Fixing an issue with Linux Descriptors. | A-622 |
| Resolved: In some cases, Sepio Agent 17 does not create the service after an upgrade. | Q-1722 |
| Resolved: To support limited bandwidth, Agent events are sent to the backend in chunks. | A-627 |
| Resolved: Excessive Agents downloads, install attempts and failures when the Agent version 17.X.X and Agent on server version 16.X.X with Auto update on. The agent was trying to downgrade its version and pull the install version continuously.<br>Error message in WindowsStartUpAndUpdaterManager.cs<br>Message: Updater couldn't install updates, error code: , . Exceptions Messages: [] " | Q-1744 |
| Changed behavior: EULA file is updated. | A-579 |
| Resolved: Sometimes, Agent update fails due to a deadlock condition. | A-637 |
| Resolved: Sometimes, Agent upgrade or change agent mode operations will not provide UI notifications. | Q-1904 |

## Known Limitations

| Item | Task ID |
|---|---|
| In some cases, the Linux installation files will not get execution permissions.<br>For all Linux platforms, it is required to manually add execution permission (chmod +x) for the files that were extracted **before** performing the installation. For example, of RedHat | CPO-I-214 |

| Item | Task ID |
| --- | --- |
| Enterprise Linux:<br>`tar xvzf sepioagent#redhat#17.2306.292#.tar.gz`<br>`chmod +x *`<br>`sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=FQDN_of_sepio` | |
| **All platforms:** Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from the currently installed version to the latest Agent version.<br>While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to “install” or “modify” the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent. | O-315, A-603, CPO-A-275 |

# Sepio Agent v17 for Linux and Windows (build no. 17.2306.352) Release Notes

This release includes multiple fixes and minor updates to improve the backend processing, performance and operations.

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **Resolved:** Agents get disconnected from server and sometimes get back due to https timeout when SSL connection could not be established. (error: Unable to read data from the transport connection: An established connection was aborted by the software in your host machine) `"Message: Failed POST StatusCode: , to call to report: , URL: <://FQDN/prime/agentsapi/v2/heartbeat>, with Result: []. Exceptions Messages: System.Net.Http.HttpRequestException: No such host is known. (FQDN:443)"` | Q-1948 |
| **New:** Agent 17 added event “New Sepio agent associated”. | Q-2008 |
| **Resolved:** In some cases, on Ubuntu/Debian, the Agent keeps downloading in a loop an update version from backend. | Q-1991 |
| **Resolved:** Ubuntu agent became disconnected due to a denied permission issue. | Q-1950 |
| **New:** In addition to timestamp, date added to Agent logs for better analysis of host events investigations. | Q-1951 |
| **Resolved:** Win Agent becomes disconnected -configuration decrypt error. In some cases, when automatic upgrade fails, some files with configuration data cannot be read. “The provided payload cannot be decrypted because it was not protected with this protection provider”. | Q-1945 |
| **New:** Support extended UUID calculation: The Agent UUID is based on a computer’s hardware. Sepio uses the BIOS and motherboard IDs to create an Agent UUID. If Sepio is uninstalled then reinstalled on an Agent, it still remembers its UUID. Data that the Agent stores locally, such as the computer name it is installed on and the data in its lists (as mentioned above) are lost when uninstalling an Agent. This new feature allows us to create UUID based on additional parameters for hosts that use exact clone of hardware elements. | A-647 |

| Item | Task ID |
| --- | --- |
| **Resolved:** Linux Agent is not upgraded to 17.2306.292 | Q-1946 |
| **New:** Agent detection of flapping peripheral events. In some cases, mostly as an effect of hardware or an OS driver failure, a USB peripheral will generate a lot of connection attempts to the host. When it happens, the result will be a flood of Agent events that will propagate to the server as well.<br>When the same peripheral keeps connecting and disconnecting “too many times too frequently” during a window of more than 5 times in 10 seconds, the Agent will create a “peripheral flapping” event once and will stop generating connect/disconnect events for a time window of 30 min. | Q-1746 |

## Known Limitations

| Item | Task ID |
| --- | --- |
| In some cases, the Linux installation files will not get execution permissions.<br>For all Linux platforms, it is required to manually add execution permission (chmod +x) for the files that were extracted **before** performing the installation. For example, of RedHat Enterprise Linux:<br>`tar xvzf sepioagent#redhat#17.2306.292#.tar.gz`<br>`chmod +x *`<br>`sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=FQDN_of_sepio` | CPO-I-214 |
| **All platforms:** Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from the currently installed version to the latest Agent version.<br>While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to “install” or “modify” the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent. | O-315, A-603, CPO-A-275 |
| The agent requires that a valid server certificate must be used. | CPO-I-401 |

# Sepio Agent 17.2306.385 Release Notes

This release introduces several fixes.

## Changes and Fixes

| Item | Task ID |
|---|---|
| Fixed: HBOM components falsely shown as disconnected (Windows) | Q-2074 |
| Fixed: “Agent configuration update” event message is missing the newly configured mode | Q-1771 |
| Fixed: In some cases, when the Agent blocks an attack tool, while in Block Known Threats mode (BKT), it also blocks additional peripherals. | Q-2095 |

## Known Limitations

| Item | Task ID |
|---|---|
| In some cases, the Linux installation files will not get execution permissions.<br>For all Linux platforms, it is required to manually add execution permission (chmod +x) for the files that were extracted **before** performing the installation. For example, of RedHat Enterprise Linux:<br>`tar xvzf sepioagent#redhat#17.2306.292#.tar.gz`<br>`chmod +x *`<br>`sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=FQDN_of_sepio` | CPO-I-214 |
| **All platforms:** Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from the currently installed version to the latest Agent version.<br>While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to “install” or “modify” the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent. | O-315, A-603, CPO-A-275 |
| The agent requires that a valid server certificate must be used. | CPO-I-401 |

# Sepio Agent 17.2409.14 Release Notes

This release introduces several enhancements and fixes.
Starting with this release we are using a different versioning methodology for system components.

## Release Highlights

### HBOM Components Improve

This version of Sepio Agent provides more granular information regarding the memory, storage and CPU components of a Windows Host. The storage section now displays the model, size, and media type; the memory section shows memory type, speed, and capacity; and the CPU section provides information on name, speed, and core count.



HBOM Components new information

Task ID: A-749, A-750, A-751

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| Fixed: After a reboot, the Agent occasionally lost the server IP address | Q-2274 |
| Fixed: Resolved an issue where the Agent service sometimes failed to stop properly | Q-2187 |

## Known Limitations

| Item | Task ID |
|---|---|
| In some cases, the Linux installation files will not get execution permissions.<br>For all Linux platforms, it is required to manually add execution permission (chmod +x) for the files that were extracted **before** performing the installation. For example, of RedHat Enterprise Linux:<br>`tar xvzf sepioagent#redhat#17.2306.292#.tar.gz`<br>`chmod +x *`<br>`sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=FQDN_of_sepio` | CPO-I-214 |

| Item | Task ID |
| --- | --- |
| **All platforms:** Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from the currently installed version to the latest Agent version.<br>While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to “install” or “modify” the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent. | O-315, A-603, CPO-A-275 |
| The agent requires that a valid server certificate must be used. | CPO-I-401 |

# Sepio macOS Agent 17.2501.104 Release Notes

This release introduces **Agent support for macOS hosts** with the following minimal requirements.

## System Requirements

- **macOS Version:** macOS 14 and above
- **Supported Devices:** MacBook Pro with M-series processors

## Features

The macOS Agent comes equipped with the same features and capabilities as the Linux and Windows Agents, ensuring a consistent and unified experience across platforms.

## Known Limitations (for macOS Agent only)

| Packaged release for distribution | Notes |
|---|---|
| Logs regarding CPU and memory usage are not being collected | A-854 |
| Misrepresentation of “blocked” indication for MalDuino devices: 1. In rare cases, the “blocked” status may not display properly despite the device being blocked. 2. In rare cases, a device may be shown as offline and blocked, even though it is connected and blocked. | A-850 |
| Detecting a WiFi Keylogger on macOS Agent is not supported | I-1686 |
| The macOS Agent can only be installed manually; installation via software distribution platforms is not supported. | I-1687 |
| The Agent requires a valid server certificate for operation. | CPO-I-401 |

# Sepio Agent 17.2504.108 Release Notes

This release introduces several enhancements and fixes.

## Release Highlights

### Armed Mode Modifications

This version of Sepio Agent introduces enhancements to Armed mode, which now includes the Block Known Threats (BKT) functionality. In Armed mode, the Agent not only blocks unapproved peripherals but also cross-checks each device against its Known Threats list using the device's AssetDNA profile. If a match is found, indicating that the device is recognized as malicious, it will be blocked regardless of its approval status.

The following table outlines the actions taken by the Agent based on its operating mode:

| Agent mode / Action | Free | Block Mass Storage Devices and Known Threats (BST) | Block Known Threats (BKT) | Armed |
|---|---|---|---|---|
| Approved device | No blocking actions. The agent will provide visibility reports | No blocking actions. The agent will provide visibility reports | No blocking actions. The agent will provide visibility reports | No blocking actions. The agent will provide visibility reports |
| Disapproved device | | No blocking actions. The agent will provide visibility reports | No blocking actions. The agent will provide visibility reports | Block |
| Approved/disapproved device that match to a known threat based on AssetDNA | | Block | Block | Block |
| Disapproved device that is classified as a USB Mass Storage Device | | Block | No blocking actions. The agent will provide | Block |

| Agent mode / Action | Free | Block Mass Storage Devices and Known Threats (BST) | Block Known Threats (BKT) | Armed |
|---|---|---|---|---|
| | | | visibility reports | |

Task ID: A-857

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** HID, USBSTOR, and USB BOM objects will no longer be displayed as part of BOM. | A-907, A-908, A-909 |
| **New:** Added default values for BOM objects. | A-910 |
| **Changed behavior:** Peripheral Flapping criteria – More than 10 'Disconnect' events (same peripheral) within a 15-minute period during a sliding 24-hour window. | A-889 |
| **New:** Added additional logging to enhance bug tracking and improve troubleshooting capabilities. | Q-2819 |
| **Fixed:** Improved support for Eperdia slide printers. | Q- 3405 |
| **Fixed:** Improved support for MediaTek/TECNO smartphones. | A-872 |
| **Fixed:** Google DNS server is no longer used to determine connectivity. | A-937 |

## Known Limitations

| Item | Task ID |
| --- | --- |
| In some cases, the Linux installation files will not get execution permissions.<br>For all Linux platforms, it is required to manually add execution permission (chmod +x) for the files that were extracted **before** performing the installation. For example, of RedHat Enterprise Linux:<br>`tar xvzf sepioagent#redhat#17.2306.292#.tar.gz`<br>`chmod +x *`<br>`sudo ./LinuxInstallationRh.sh CENTRALIZEDIP=FQDN_of_sepio` | CPO-I-214 |
| **All platforms:** Sepio Agents version 16 can be upgraded to version 17. It is recommended to upgrade from the currently installed version to the latest Agent version.<br>While using the Windows installer for agent downgrade (i.e. from version N to a lower version) is not supported, administrators can still try to modify an existing installation by trying to “install” or “modify” the current installed agent using a different Sepio Agent MSI. This would result in an unstable agent. | O-315, A-603, CPO-A-275 |
| The agent requires that a valid server certificate must be used. | CPO-I-401 |

# Sepio Platform

## Related Topics

- Sepio Platform
  - Sepio Platform v60
  - Sepio Platform v59
  - Sepio Platform v58
  - Sepio Platform v57 (17.2602.517)
  - Sepio Platform v57
  - Sepio Platform v56
  - Sepio Platform v55
  - Sepio Platform v54
  - Sepio Platform v53
  - Sepio Platform v52
  - Sepio Platform v51
  - Sepio Platform v50
  - Sepio Platform v49
  - Sepio Platform v48
  - Sepio Platform v47
  - Sepio Platform v46
  - Sepio Platform v45
  - Sepio Platform v44
  - Sepio Platform v43
  - Sepio Platform v42
  - Sepio Platform v41
  - Sepio Platform v40
  - Sepio Platform v39
  - Sepio Platform v38
  - Sepio Platform v37
  - Sepio Platform v36
  - Sepio Platform v35
  - Sepio Platform v34
  - Sepio Platform v33 (17.2411.120)
  - Sepio Platform v33
  - Sepio Platform v32
  - Sepio Platform v31
  - Sepio Platform v30

# Sepio Platform v60 (build 17.2604.632) – Release Notes

This is a **Minor Release.**

It introduces several enhancements and fixes.

- Platform build: 17.2604.632
- Scan Engine build: 17.2602.3
- Default Host Agent build:
  - Windows: 17.2602.229
  - macOS: 17.2601.190
- KB version: 2605061019
- Build Time and Numerator: 2026-05-11 15:20:46 (77)

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **Modified:** Enhanced unmanaged switch detection logic | I-2611 |
| **Modified:** Minio container disk optimization | Q-5017 |
| **Fixed:** In some cases, LDAP Authentication Failures Caused by Active Directory DNS Zone Referrals | Q-4874 |
| **Fixed:** Asset query filters do not work after executing a saved query | Q-5001 |
| **Fixed:** In some cases, event cleanup process deletes the latest event/audit history | Q-5005 |

## Known Limitations

See the list of known limitations.

# Sepio Platform v59 (build 17.2604.620) – Release Notes

This is a **Major Release**.

This version of Sepio introduces important enhancements and represents a stabilized, thoroughly validated release intended primarily for on-premises deployments.

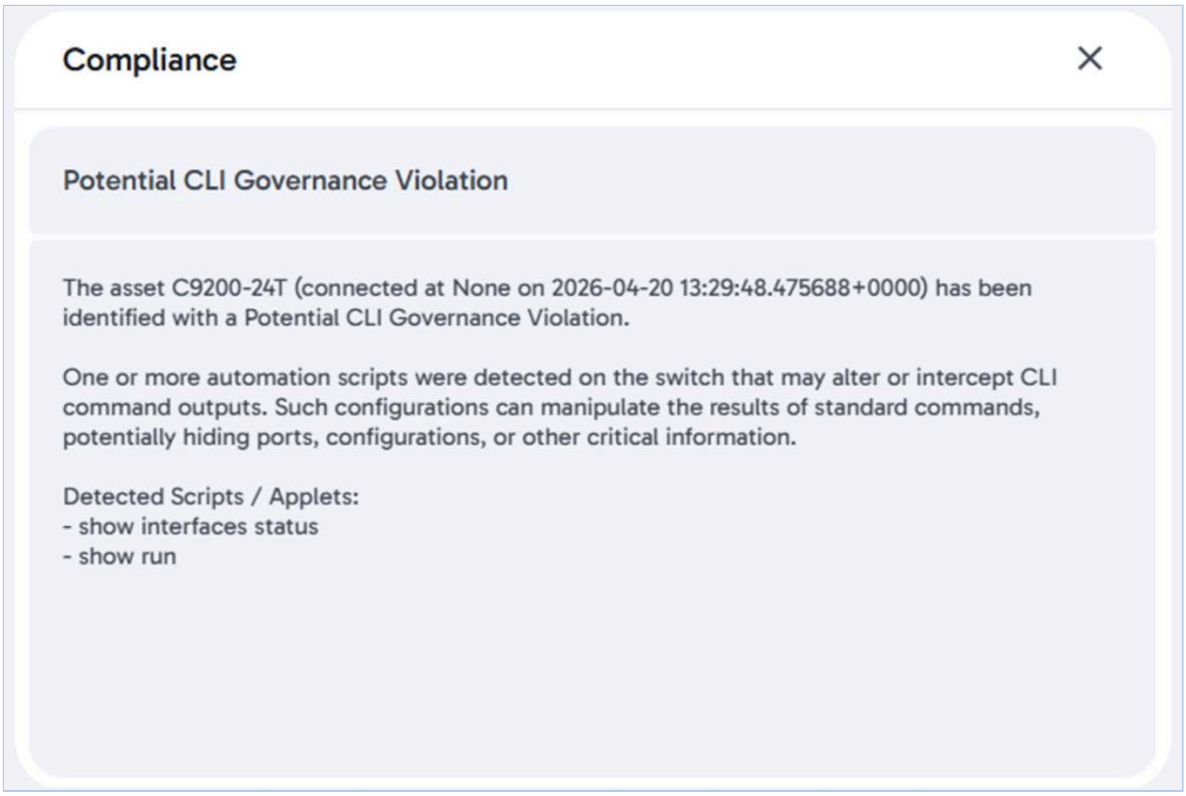
For cloud customers who update on a regular cadence, this release is similar to a standard incremental update. Fixes and enhancements are continuously delivered through minor releases, and no special actions are required to upgrade the system.

- Platform build: 17.2604.620
- Scan Engine build: 17.2604.2
- Default Host Agent build:
  - Windows: 17.2602.229
  - macOS: 17.2601.190
- KB version: 2604281009
- Build Time and Numerator: 2026-04-28 19:20:23 (77)

## Release Highlights

### Switch Manipulation Detection

This release introduces **CLI Governance Validation**, a capability that enables organizations to detect potential manipulation of switch CLI outputs caused by automation scripts such as EEM applets.
With CLI Governance Validation, Sepio analyzes switch configurations retrieved via SSH
to identify applets that may intercept or alter command results, potentially hiding critical information.
When such behavior is detected, Sepio raises a dedicated Sub Risk Indicator named **“Potential CLI Governance Violation”** on the relevant switch asset.




Potencial CLI Governance Violation

**Prerequisites & Configuration Requirements:** `RI_POTENTIAL_CLI_GOVERNANCE_VIOLATION` should be turned on.
**Limitations:** Supported only for Cisco switches
**Documentation:** Risk Indicator Groups

**Ticket IDs:** IN-2871

### Hardened Agent-to-Server Authentication Framework

Sepio Agent now includes an Advanced Agent Security Model that introduces token-based validation to ensure secure agent-to-server communication. Each agent is cryptographically bound to its designated Sepio Management Platform (SMP) tenant. This framework ensures tenant isolation by validating that the platform exclusively accepts communications from verified agents.

**Prerequisites & Configuration Requirements:** A dedicated agent will be released
**Documentation:** Advanced Agent Security Model: Enhanced Host Agent Security

**Ticket IDs:** IN-2101

## New Features, Changes and Bug Fixing (in This Release)

| Item | Task ID |
|---|---|
| **Modified:** User CRUD endpoints authentication hardening | O-1771 |

| Item | Task ID |
| --- | --- |
| **New:** Port detected assets filtering supports ‘more than’, ‘less than’ and range operators | UI-27 |
| **Modified:** Container images updated | I-2472, I-1084 |
| **Modified:** Improved assets delete mechanism efficiency to enhance system performance | Q-4532 |
| **Modified:** PDF generation optimization | O-1783 |
| **Modified:** User authentication error messages, due to wrong username or password, have been unified to a non-specific response during failed login attempts | I-2870, Q-3576, I-2869 |
| **Modified:** Dual use risk indicator logic was improved | K-1888 |
| **Modified:** Remove irrelevant files when downloading MacOS Agent version | UI-31, Q-4663 |
| **Modified:** Update the name “Traffic Type” to “Interface Type” within Location Details | UI-28 |
| **Modified:** Enhanced secret management | I-1270 |
| **Modified:** Interface Type now includes an “Is not” operator | U-35 |
| **Modified:** Enhanced dynamic detection for the Asset DNA Anomaly Risk Sub-Indicator | I-2910 |
| **Modified:** Default value of `RI_COMMUNICATION_ANOMALY_SLEEPING_THRESHOLD` changed to 4 (instead of 0) | K-1964 |
| **Fixed:** Access Points not displayed in SSID Window within Wireless Network Settings | Q-4260 |
| **Fixed:** KB auto-pull mechanism fails when not having a KB installed | Q-4743 |
| **Fixed:** Visibility Overview layout shift | Q-4851 |
| **Fixed:** Event details are empty for “Switch added by Administrator” log | Q-4674 |
| **Fixed:** An empty column appeared on the queries page | Q-4532 |
| **Fixed:** Port description was sometimes not displayed correctly in exported logs | Q-4547 |
| **Fixed:** Access Point’s client count differed from the client list in some cases | A-2633, Q-4850 |

| Item | Task ID |
| --- | --- |
| **Fixed:** WLC scans fail due to stale sessions in some cases | Q-4838 |
| **Fixed:** Report creation remains stuck in the queue | Q-2790 |
| **Fixed:** Event details missing for “Switch added by Administrator” log entry | Q-4674 |
| **Fixed:** Serial Number attribute missing on several pages | Q-4804 |
| **Fixed:** Spacing issues in Notification Center view | Q-4845 |

## Included Since Previous Major Release

This section provides a consolidated view of all changes delivered through minor releases since the previous Major Release. All of these changes are included in this version.

### Key Highlights

- Hardened Agent-to-Server Authentication Framework
- Port Compliance Verification
- Static API Keys Creation
- Filter and Display Assets by Location Details

### Detailed Change History

- Sepio Platform v57
- Sepio Platform v57 (17.2602.517)
- Sepio Platform v58

## Known Limitations

See the list of known limitations.

# Sepio Platform v58 (build 17.2602.627) – Release Notes

This is a minor release.
It introduces several enhancements and fixes.

- Platform build: 17.2602.627
- Scan Engine build: 17.2603.12
- Default Host Agent build: 17.2602.229
- KB version: 2603201427
- Build Time and Numerator: 2026-03-24 10:59:01 (74)

## Release Highlights

### Port Compliance Verification

This release introduces Port Compliance Verification, a port configuration validation capability that enables organizations to control port-level security, compliance, and governance standards based on connected device characteristics.
With Port Compliance Verification, administrators can define rules to validate whether switch port configurations comply with organizational policies when devices with specific MAC prefixes connect directly.
When a configuration violation is detected, Sepio raises a dedicated Sub Risk Indicator named “Port Compliance Violation” on the relevant asset.



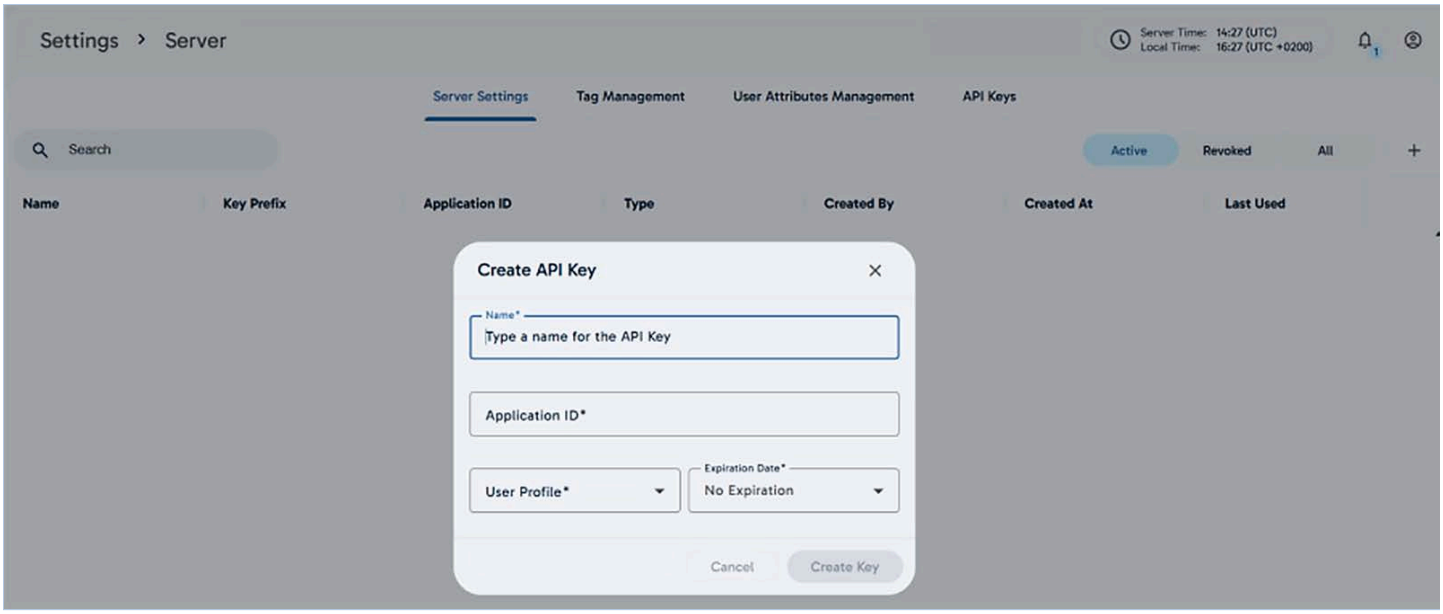
Port Compliance Violation

**Prerequisites & Configuration Requirements:** `RI_PORT_COMPLIANCE_VIOLATION` and `PORT_VERIFICATION` should be turned on.
**Documentation:** Port Compliance

**Ticket ID:** IN-86

### Static API Keys Creation

Sepio now supports Static API Keys, enabling secure, long-lived authentication for automated systems, scripts, and third-party integrations without requiring interactive user logins or managing authentication for automation processes. Administrators can create named keys with scoped permissions, optional expiration, full auditability, and instant revocation – making it easier and safer to manage machine-to-machine access across integrations.




Create API Key

**Prerequisites & Configuration Requirements:** `API_KEY_ENABLED` (it is false by default)
**Documentation:** API Key Management.

**Ticket ID:** IN-2375

### Filter and Display Assets by Location Details

Asset queries now extend beyond asset-only attributes to include network location intelligence. With the new Location Details query field, users can filter and search assets based on where they are connected in the network – such as switch or WLC identity, vendor, model, port speed, interface, and traffic type. This enables powerful new use cases, like identifying all assets connected to 1 Gbps ports or assets connected through a specific switch model, delivering richer context, faster investigations, and more precise asset visibility.

**Prerequisites & Configuration Requirements:** NA

**Ticket IDs:** IN-2069, IN-2479

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Sepio artifacts are now digitally signed | IN-2455 |
| **New:** Added support for fetching IP data via SNMP for Aruba CX devices | N-1080 |
| **New:** Meraki discovery logs are now available when fetching SE logs | N-1085 |
| **Modified:** Time zones have been aligned across all services | IN-2599 |
| **Modified:** Optimized performance of risk calculations | K-1872 |
| **Modified:** Agent event priorities were adjusted to improve alert clarity | Q-4760 |
| **Fixed:** Events generated in JSON format were missing fields | Q-4749 |
| **Fixed:** Serial Number attribute is missing on some UI pages | Q-4804 |
| **Fixed:** In some cases, after V56 installation, the Knowledge Base package may not auto-update | Q-4736 |
| **Fixed:** When a host is removed from the scope, associated policies remain assigned | Q-4707 |
| **Fixed:** Multiple IP phones connected via an unmanaged switch, but only one is displayed | Q-4570 |
| **Fixed:** An error notification appears in an incorrect location when adding a tag | Q-4715 |

## Known Limitations

See the list of known limitations.

# Sepio Platform v57 (build 17.2602.517) – Release Notes

This is a minor release.
It introduces several enhancements and fixes.

- Platform build: 17.2602.517
- Scan Engine build: 17.2602.11
- Default Host Agent build: 17.2511.124
- KB version: 2603101746
- Build Time and Numerator: 2026-03-12 17:50:26 (73)

## New Features, Changes and Bug Fixing

| Item | Task ID |
| --- | --- |
| **Fixed:** In some cases, SAML authentication was failing with `ERR_UNMATCH_ISSUER` due to the service was not correctly recognizing the identity provider's response | Q-4807 |

## Known Limitations

See the list of known limitations.

# Sepio Platform v57 (build 17.2602.516) – Release Notes

This is a minor release.
It introduces several enhancements and fixes.

- Platform build: 17.2602.516
- Scan Engine build: 17.2602.11
- Default Host Agent build: 17.2511.124
- KB version: 2602251023
- Build Time and Numerator: 2026-03-09 15:05:17 (73)

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Host classification enhanced using external data from CrowdStrike | A-2619 |
| **New:** Scan Engine will collect LLDP messages in addition to CDP messages from Cisco switches. Previously, only CDP messages were collected from Cisco switches | N-1070 |
| **New:** Sepio now supports IP address extraction for assets connected to network switches monitored via SNMP | I-2215 |
| **Modified:** PolicyAPI and PolicyEngine upgraded to Microsoft .NET 8 | O-1520 |
| **Modified:** The severity of some Agent events was updated | Q-4635 |
| **Modified:** Improved mechanisms for sending large number of reports | Q-4182 |
| **Modified:** Email notification for a ready report will not be sent for scheduled reports | Q-3235 |
| **Fixed:** A timeout banner appears during login with 2FA | Q-4685 |
| **Fixed:** Submenu opens without hover in the Actions menu under the Discovered Assets view | Q-4681 |

| Item | Task ID |
| --- | --- |
| **Fixed:** Query boxes are misaligned in the Rule screen when creating a policy | Q-4217 |
| **Fixed:** In some cases, offline peripherals were missing some events | O-1479 |
| **Fixed:** Risk Indicators events were being sent every scan without any asset change | Q-4607 |
| **Fixed:** In some cases, Search form on the “Events Log” page didn’t return results | Q-4689 |
| **Fixed:** Policy value in events is missing | Q-4746 |

## Known Limitations

See the list of known limitations.

# Sepio Platform v56 (build 17.2601.719) – Release Notes

This is a **Major Release.**
This version of Sepio introduces important enhancements and represents a stabilized, thoroughly validated release intended primarily for on-premises deployments.

For cloud customers who update on a regular cadence, this release is similar to a standard incremental update. Fixes and enhancements are continuously delivered through minor releases, and no special actions are required to upgrade the system.

- Platform build: 17.2601.719
- Scan Engine build: 17.2602.2
- Default Host Agent build:
  - Windows: 17.2511.124
  - macOS: 17.2601.190
- KB version: 2602052009
- Build Time and Numerator: 2026-02-06 17:36:21 (72)

## Release Highlights

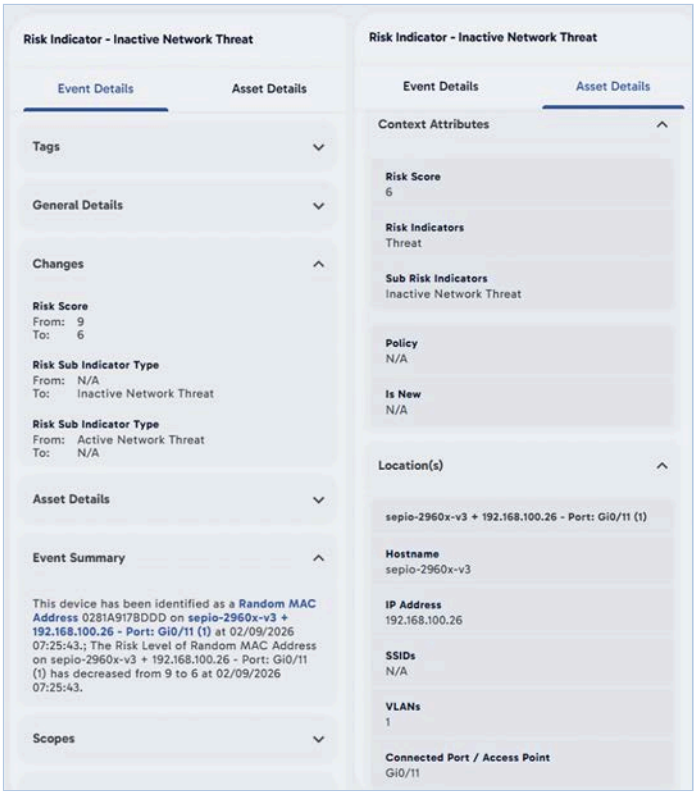
### Enhanced Event and Logging System

This release introduces a significantly **enhanced event and logging system**, delivering richer, **fully contextualized** security events across the Sepio platform.

Events now include comprehensive asset, network, and risk context in a single, standardized log entry, **aggregating simultaneous events** into a concise, asset-centric view that improves investigation, correlation, and audit readiness.

Administrators can also configure event severity and delivery channels directly from the UI, enabling more precise alerting and seamless SIEM integrations.

This enhancement can be enabled by setting the `EVENTS_AGGREGATION_PROCCESS_ENABLED` flag value to `TRUE` (default value `OFF`).



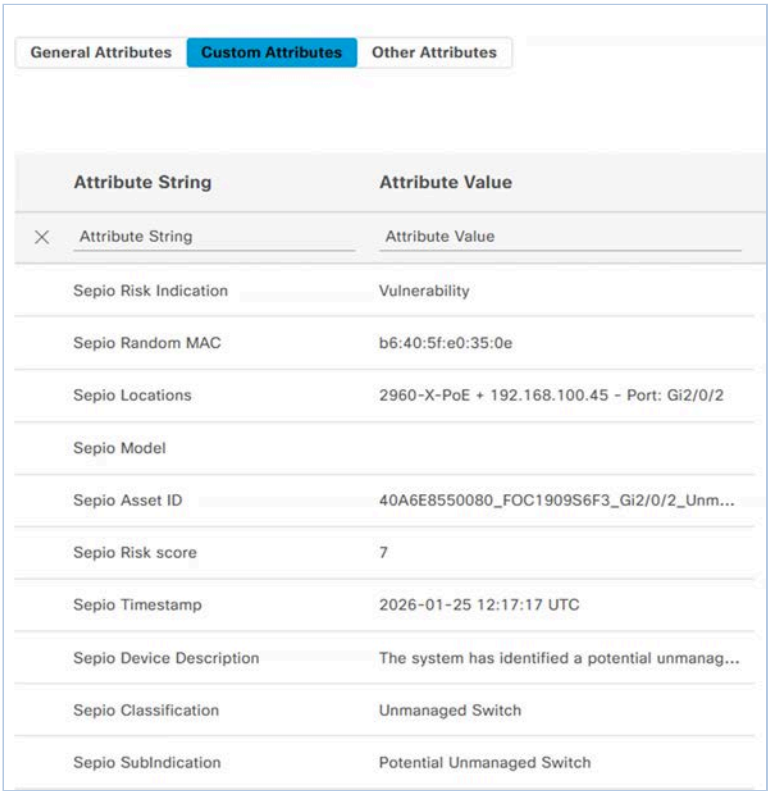
Enhanced Event and Logging System

**Documentation:** Enhanced Event and Logging System

Ticket IDs: IN- 2494

## Cisco ISE Integration

Customers can now configure an integration between Sepio and Cisco ISE, providing the ability to manage the risk of assets that cannot be detected or managed by Cisco ISE alone. This integration allows Cisco ISE to retrieve additional information from Sepio. Using this integration, enterprises can enrich information about existing endpoints or create new endpoints in Cisco ISE, including support for MAC-less devices such as unmanaged switches.



Cisco ISE Integration

**Prerequisites & Configuration Requirements:** Detailed prerequisites and configuration instructions are provided in the documentation.
**Documentation:** Sepio and Cisco Identity Services Engine (ISE) NAC Integration

Ticket IDs: IN-1035

## Support ALT MGMT LAN IP for Meraki Devices

Meraki Cloud provides two IP address sources for switches: **LAN IP** and **ALT MGMT LAN IP**. By default, Sepio uses the **LAN IP** for discovery and scanning.

In this release, Sepio introduces a **new configurable parameter** that allows users to select which IP address source – **LAN IP or ALT MGMT LAN IP** – should be used.

**Prerequisites & Configuration Requirements:** A dedicated Scan Engine configuration required.
**Documentation:** Adding and Configuring a Meraki Switch

Ticket IDs: IN-2462

## Display Serial Number of Hosts

In this release, the Serial Number of hosts is now visible in the UI, enhancing host identification and enabling easier correlation and integration with other IT and security tools.



| Name | Last Seen | BIOS Serial Number |
|---|---|---|
| SOC-PC-5 | 2026-02-07 01:17:01 | 3RL03Z3 |
| DINISC-PF40BC6P | 2026-02-06 18:33:30 | PF40BC6P |
| LIOR-PF446XK9 | 2026-02-03 08:13:54 | PF446XK9 |
| SHIRIS-PF3X62KW | 2026-02-02 08:04:31 | PF3X62KW |
| BRODER-DESKTOP | 2026-02-09 08:26:47 | GQN9YD3 |
| PEDROC-KHI4T6IE | 2026-02-06 16:58:54 | PF60NA1T |
| SHLOMI-PF5Y79G6 | 2026-02-09 08:26:51 | PF5Y79G6 |
| ORENM-51ZJ8S3 | 2026-02-02 08:04:32 | 51ZJ8S3 |
| DANB-PF5JAESH | 2026-02-06 12:01:38 | PF5JAESH |
| SOC-PC-2 | 2026-02-09 08:26:52 | BT5MFV2 |
| GILAOS-PF3JH7LH | 2026-02-02 08:04:30 | PF3JH7LH |

Bios Serial Number of Hosts

Ticket IDs: IN- 2468

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Scan Engine configuration parameter, `NETPOLLER_MERAKI_ENABLE_VLAN_RETRIEVAL`, that controls VLAN retrieval from the Meraki Cloud (False by default) | Q-4569 |
| **New:** Added support for the “distinguishedName” Active Directory attribute for LDAP login | Q-4032 |
| **New:** SepioCTL now supports Root CA certificate deployment to all containers at once | I-1215 |
| **New:** The Notification Center now displays an indicator for unread notifications and offers an easier way to pin notifications | O-1501 |
| **New:** Improved UI indication for the inability of users with insufficient privileges to trigger a Scan engine upgrade | Q-4115 |
| **New:** An indication for success and failure of Knowledge Base update has been added | Q-2452 |

| Item | Task ID |
|---|---|
| **New:** libicu library has been added to Sepio's offline installation package | N-1065 |
| **Modified:** The 'Risk' tab on the Notification Center modal has been renamed to 'Activity' | Q-4646 |
| **Fixed:** In some cases, the Topology Map fails to render after version upgrade | Q-3733 |
| **Fixed:** Build Time not updated when Auto Updating KB | Q-4563 |
| **Fixed:** Wrong audit message when disabling/enabling event from notification panel | Q-4599 |
| **Fixed:** In some cases, Policies disappear after deleting and re-adding agent | Q-4591 |
| **Fixed:** In some cases, "Check for New KB" button does not update existing KB | Q-4559 |
| **Fixed:** In some cases, searching for specific Host in Topology Map does not work | Q-4022 |
| **Fixed:** In some cases, event log messages do not arrive in syslog, when using "TLS over TCP" | Q-4641 |

## Included Since Previous Major Release

This section provides a consolidated view of all changes delivered through minor releases since the previous Major Release. These changes are all included in this version.

### Key Highlights

- New Risk Indicator – Duplicated MAC Address
- Backup and Restore Capability
- Unmanaged Switch Creation Logic Enhancement: new Sepio "Approved" Groups
- Configurable Meraki Cloud URL
- macOS Agent Upgrade via Server
- High Availability
- Fetch Platform Logs Directly from the UI

- Knowledge Base Auto-Pull Update

#### Detailed Change History

- Sepio Platform v51
- Sepio Platform v52
- Sepio Platform v53
- Sepio Platform v54
- Sepio Platform v55

## Known Limitations

See the list of known limitations.

# Sepio Platform v55 (build 17.2601.508) – Release Notes

This is a **minor release.**
It introduces several enhancements and fixes.

- Platform build: 17.2601.508
- Scan Engine build: 17.2512.16
- Default Host Agent build: 17.2511.124
- KB version: 2601141613
- Build Time and Numerator: 2026-01-15 16:52:22 (70)

## Release Highlights

### High Availability

In this Sepio Platform version, Sepio introduces a **High Availability** (HA) capability that allows Sepio Security administrators to automatically back up an active node and restore it on a passive node.

**Prerequisites & Configuration Requirements:** In the event of an active node failure, a manual DNS update is required to redirect the agents and scan engines to the passive node.
**Documentation:** Backup, Redundancy and High Availability.

Ticket IDs: IN-1906

### Fetch Platform Logs Directly from the UI

Sepio Security administrators can now retrieve all service logs directly from the Sepio Platform.
This functionality is available via **Settings** -> **About** -> **Platform Logs.**



Request Packing

**Prerequisites & Configuration Requirements:** This capability is available only to users with **Manager** or **Administrator** permissions. Log retention is limited to the **three most recent log packages.**

### Knowledge Base Auto-Pull Update

With this platform release, Sepio Security administrators can opt to have the **Knowledge Base** (KB) automatically updated whenever a new version is available for download. Alternatively, administrators

can manually check for a new version using the "**Check for New KB Version**" button, which will prompt whether the new KB should be auto-pulled and installed.

To enable auto-updates, set the `KB_AUTO_PULL_SCHEDULER_ENABLED` flag to **true** (default is **false**). If the flag is disabled, users can still use the "**Check for New KB Version**" button to manually update the KB.




Check for new Knowledge Base (KB) Version

Ticket IDs: IN-1372

**Known Limitations:**

- When updating the KB automatically, the **Version** field is updated correctly in the UI, but the Build Time will not update (it only updates when manually uploading a KB) – Q-4563.
- Automatic KB updates only update the internal server KB. For a new **Agent Version** update, a manual KB upload is required.

## New Features, Changes and Bug Fixing (in This Release)

| Item | Task ID |
|---|---|
| **New:** Added asset location information to event records | A-2588 |
| **New:** Data masking (bleaching) option added to host report exports | A-1192 |
| **Modified:** Unmanaged Switch was created on port with only Virtual Machines | Q-4300 |
| **Fixed:** In some cases, switch JSON files could not be downloaded for large-scale environments | Q-4355 |

## Known Limitations

See the list of known limitations.

# Sepio Platform v54 (build 17.2512.611) Release Notes

This is a minor release.
It introduces several enhancements and fixes.

- Platform build: 17.2512.611
- Scan Engine build: 17.2512.16
- Default Host Agent build: 17.2511.124
- KB version: 2512191044
- Build Time and Numerator: 2026-01-05 15:26:50 (69)

## Release Highlights

### Configurable Meraki Cloud URL

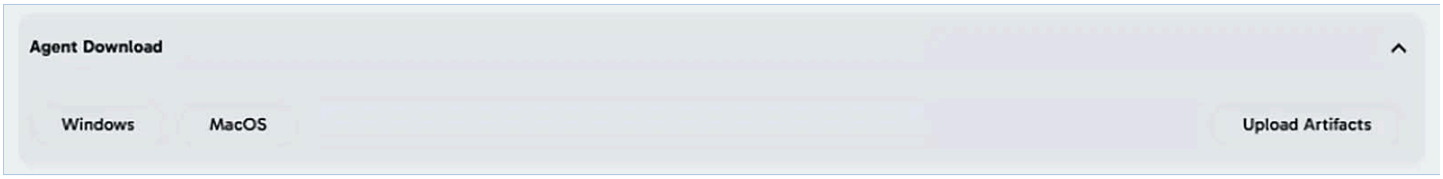
Sepio Security administrators can now configure the Scan Engine to use an alternative URL for Meraki Cloud integration (for example, the Meraki Government API).

**Prerequisites & Configuration Requirements:** A configuration change in the Scan Engine is required. For detailed instructions, please refer to the documentation below.
**Documentation:** Adding and Configuring a Meraki Switch

**Ticket IDs:** N-1058

### macOS Agent Upgrade via Server

In this Sepio Platform version, Sepio now supports the auto-update feature for macOS agents, in addition to Windows agents. This is enabled by uploading a macOS agent installation file.




macOS Agent Upgrade via Server

**Prerequisites & Configuration Requirements:** To enable this feature, a macOS agent that supports remote upgrade must first be installed. For further information, please contact support@sepiocyber.com.
**Documentation:** Updating a Sepio Agent

**Ticket IDs:** N-1058

## Modifications and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Ability to search attributes in Table Setting modal | O-1459 |
| **New:** Added support for Authentication Details on Huawei switches | N-1040 |
| **Modified:** Improved the aging mechanism to increase Dormant Device detection accuracy | Q-4113 |
| **Modified:** Updated descriptions for selected console configuration flags | Q-4180 |
| **Modified:** Scan engine command default timeout updated to 10 seconds | N-1064 |
| **Modified:** Improve agent remote update mechanism | A-1187, A-1155 |
| **Modified:** SepioCTL stability improvement | Q-4411 |
| **Fixed:** In some cases, an asset of type “Other” is incorrectly created and associated with a port that already has other assets connected | Q-4158 |
| **Fixed:** Local and remote MAC address fields are incorrectly parsed from CDP messages | Q-4285 |
| **Fixed:** In some cases, Dell PCs receive a “Rare asset” risk incorrectly | Q-4150 |
| **Fixed:** In some cases, wireless assets appear on a switch port instead of the Access Point | Q-4160 |
| **Fixed:** Right panel flickers when no switch is selected | Q-4130 |
| **Fixed:** Policy attribute of supervised hosts shows Auto-Tagging rule names instead of the governing Policy name | Q-4195 |
| **Fixed:** An irrelevant toggle appears for tag propagation when deleting host tags | Q-1361 |
| **Fixed:** Duplicated MAC Risk Indicator is raised for Wireless Lan Controllers | A-2691 |
| **Fixed:** The sort option does not work in the Policy Management page | Q-4184 |
| **Fixed:** In some cases, DNA reading is done only to first switch in an Aruba stack | Q-4282 |
| **Fixed:** Some Cisco 1121 devices are not scanned successfully | Q-4358 |
| **Fixed:** The About screen resolution is not adjusted correctly | Q-4445 |
| **Fixed:** Unmanaged Switch was not created when CDP from an IP Phone is received | Q-4488 |

## Known Limitations

There are no new known limitations introduced in this release.

See the list of known limitations.

# Sepio Platform v53 (build 17.2511.709) Release Notes

This is a minor release.
It introduces several enhancements and fixes.

- Platform build: 17.2511.709
- Scan Engine build: 17.2512.1
- Default Host Agent build: 17.2511.124
- KB version: 2512151803
- Build Time and Numerator: 2025-12-16 10:40:30 (68)

## Release Highlights

**New Risk Indicator – Duplicated MAC Address**

This version of Sepio introduces a new Risk Indicator that is triggered when the same MAC address (that does not belong to a network switch) is detected as being connected directly to more than one port simultaneously. When this condition occurs, the asset is marked with the "**Duplicated MAC Address**" Risk Indicator and assigned a **Risk Score of 5**.

**Prerequisites & Configuration Requirements:**

- The `RI_DUPLICATED_MAC` flag must be set to `TRUE`.
- To apply the risk indicator to Random MAC Address, the `RI_DUPLICATED_RANDOM_MAC_ADDRESS` flag must be set to `TRUE`.

**Default mode:** Disabled by default.
**Documentation:** Risk Indicator Groups.
**Known limitations:** The Duplicated MAC Address Risk Indicator is limited to non-supervised network elements.

**Ticket IDs:** A-2474, I-2132, O-1469

## Modifications and Bug Fixing

| Item | Task ID |
|---|---|
| **Modified:** `TOGGLE_USER_ATTRIBUTES` default value was changed to `TRUE` | Q-1468 |
| **Modified:** Updated default retention values for logging:<br>• Audit logs and user events are saved for 180 days (`DAYS_REPORT_LOGS`)<br>• Up to 3,000,000 user event records are retained (`EVENT_ROW_LIMIT`) | Q-1462 |

| Item | Task ID |
| --- | --- |
| **Modified:** Agent log structure adjusted to optimize resource utilization | A-1161 |
| **Fixed:** Dev Tools page was inaccessible | Q-4294 |
| **Fixed:** Packet distribution was not being sent to the server | Q-4303 |
| **Fixed:** In some cases, host IP field displayed an incorrect IPv6 address | Q-4122 |

## Known Limitations

There are no new known limitations introduced in this release.

See the list of known limitations.

# Sepio Platform v52 (build 17.2511.603) Release Notes

This is a minor release that includes several enhancements and fixes.

- Platform build: 17.2511.603
- Scan Engine build: 17.2511.12
- Default Host Agent build: 17.2511.124
- KB version: 2511281653
- Build Time and Numerator: 2025-11-24 14:08:12 (67)

## Modifications and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Added validation for duplicate PID/VID pairs on the “Excluded USB from DNA Reading” list | A-2493 |
| **New:** Added ability to set a limit on the maximum time the system waits for the CLI switch scan response | N-1015 |
| **Modified:** `ENABLE_EVENT_BASED_SCANNER` flag should be TRUE by default | Q-4129 |
| **Fixed:** In some cases, USB peripherals remain connected, although the host reports to a different environment | Q-4240 |
| **Fixed:** In some cases, some services were crashing following a data restore process | Q-4046 |
| **Fixed:** In some cases, when scanning a Cisco C9200L-48P-4G switch failed, its status was presented as “unsupported” even though scans were successful | Q-3992 |
| **Fixed:** Scope query should be case-insensitive | Q-4280 |
| **Fixed:** In some cases, tags disappear from USB peripherals after being blocked by a Policy | Q-4265 |
| **Fixed:** In some cases, the Rare Device risk indicator was being falsely associated with assets | Q-4159 |
| **Fixed:** The Scope functionality was enabled even though the Scope flag was set to false | Q-4179 |

| Item | Task ID |
| --- | --- |
| **Fixed:** The Internal Scan Engine was set to simulation mode by default on a fresh install | I-1140 |

## Known Limitations

There are no new known limitations introduced in this release.

See the list of known limitations.

# Sepio Platform v51 (build 17.2511.510) Release Notes

This release introduces several enhancements and fixes.

- Platform build: 17.2511.510
- Scan Engine build: 17.2511.5
- Default Host Agent build: 17.2509.101
- KB version: 2511181218
- Build Time and Numerator: 2025-11-19 16:00:01 (66)

## Release Highlights

### Backup and Restore Capability

This version of Sepio introduces a new capability that allows backing up a Sepio server and restoring it on a different server using SepioCTL CLI commands.

**Key Benefits & Impact:** Enables seamless migration or recovery of a Sepio server with minimal manual intervention.

**Prerequisites & Configuration Requirements:** The target server must have identical specifications and run the same Sepio version as the original server. Additionally, a DNS update is required to redirect Agents and the Scan Engine, ensuring that new data is correctly forwarded to the restored environment.

For full details, see the Backup, Redundancy and High Availability.

Ticket IDs: I-1115

### Unmanaged Switch Creation Logic Enhancement: new Sepio “Approved” Groups

Approved groups represent combinations of assets that are legitimately connected in a chain within the network. As a result, when such groups are detected, they should not trigger a potential unmanaged-switch risk indicator. Starting with this version, the following asset combinations have been added to the Approved Groups list:

- Printer + IoT RFID Reader Ethernet Interface
- NetAlly + Random MAC Address

Ticket IDs: A-2540

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Ability to customize UI components for specific integrations | O-1434 |
| **Modified:** When a supervised WLC is being removed from the platform, the platform turns its connected access points from Supervised to Unsupervised state | A-2560 |
| **Modified:** Persistent Unmanaged Switches will always be directly connected to the port where they were created | A-2512 |
| **Modified:** BOM components that were removed from a host, will be removed from the host's component list | A-2526, A-2527 |
| **Modified:** Peripheral data for all agents is now available for extraction from Cloud data lake | A-1143 |
| **Modified:** Data indexing improvements to optimize memory utilization | O-1461 |
| **Modified:** When LDAP is failing, it is possible to revert to older LDAP integration methods. To do so, please reach out Sepio Support | Q-4032 |
| **Modified:** Starting with this version, asset Scopes is on by default (ENABLE_SCOPES = True) | A-2571 |
| **Modified:** Health checks have been added to ArtifactsApi | N-1044 |
| **Fixed:** In some cases, hosts appear offline even though they were online and reporting correctly to the platform | Q-4059 |
| **Fixed:** In some cases, supervised hosts appear twice, once as supervised and once as unsupervised, when different NICs are used | A-2529 |
| **Fixed:** Port Scan Status is "connected" even when the link is down | A-2566 |
| **Fixed:** In some cases, license counts for supervised ports and hosts were not accurate | O-1458, Q-4119, Q-3253 |
| **Fixed:** The Auto-Tagging Policies screen now displays all available policies, not just the first 15 | Q-4212 |
| **Fixed:** Scoping host by Agent version doesn't work | Q-4216 |
| **Fixed:** In some cases, sorting assets by Scopes returns no results | Q-4165 |

| Item | Task ID |
|---|---|
| **Fixed:** The input and output packet counters of the application protocol values in Asset Details were inverted | O-1447 |
| **Fixed:** In some cases, platform Administrator cannot delete users | Q-4117 |
| **Fixed:** Enabling a composite device on the Host page does not result in the sub-interfaces being enabled | Q-2374 |
| **Fixed:** In some cases, the Last Successful Port Scan and Last Port Scan Attempt attributes were not populated | A-2516 |
| **Fixed:** In some cases, scan engine IP address was not presented correctly on Sepio platform | Q-4135 |
| **Fixed:** In some cases, scanning C9200L-48P-4G switch failed | Q-3992 |
| **Fixed:** In some cases, MAC addresses generated internally by Arista access points were falsely identified as unmanaged switches | A-2515 |
| **Fixed:** In some cases, hosts with assigned Peripheral Policies lose their tags | Q-4157 |
| **Fixed:** The LOGIN_SESSION_TIMEOUT is deleted when trying to revert to Default via UI consul | Q-4254 |
| **Fixed:** In some cases, the “Policy” attribute value was incorrectly set to the name of the governing Auto-Tagging policy | Q-4195 |
| **Fixed:** Hosts running Agent version 17.2509.101 were previously allowed to be moved to Policy Mode, even though this agent version does not support Peripheral Policy enforcement | Q-4110 |
| **Fixed:** Unnecessary logs generated when setting host mode to Policy | Q-4146 |

## Known Limitations

There are no new known limitations introduced in this release.
See the list of known limitations.

# Sepio Platform v49 (build 17.2509. 803) Release Notes

This release introduces minor enhancements and several fixes. Please note the changes section below.

- Platform build: 17.2509.803
- Scan Engine build: 17.2509.15.0
- Default Host Agent build: 17.2509.101
- KB version: 2510141038
- Build Time and numerator: 2025-10-14 10:38:00 (63)

## Release Highlights

### Event-Based Scan Engine

We're excited to introduce a new capability in the Scan Engine – **event-based scanning**. With this enhancement, Sepio Security Administrators can now configure network switches to send trap events directly to the Sepio Scan Engine. Upon receiving a trap event (Linkup/Linkdown), the Scan Engine immediately performs a targeted scan on the relevant port instead of scanning the entire switch. This enables faster, more efficient, and event-driven visibility into network changes.

As part of this enhancement, two new port attributes have been added to the platform: **Last Successful Port Scan** and **Last Port Scan Attempt**.

| | | Port | Port ID | Name | Detected Devices | Last Successful Port Scan | Last Port Scan Attempt |
|---|---|---|---|---|---|---|---|
| ☐ | | | | | | | |
| ☐ | | 6 | Gi1/0/6 | | 0 Detected Devi... | 2025-09-17 07:32:25 | 2025-09-17 07:32:25 |

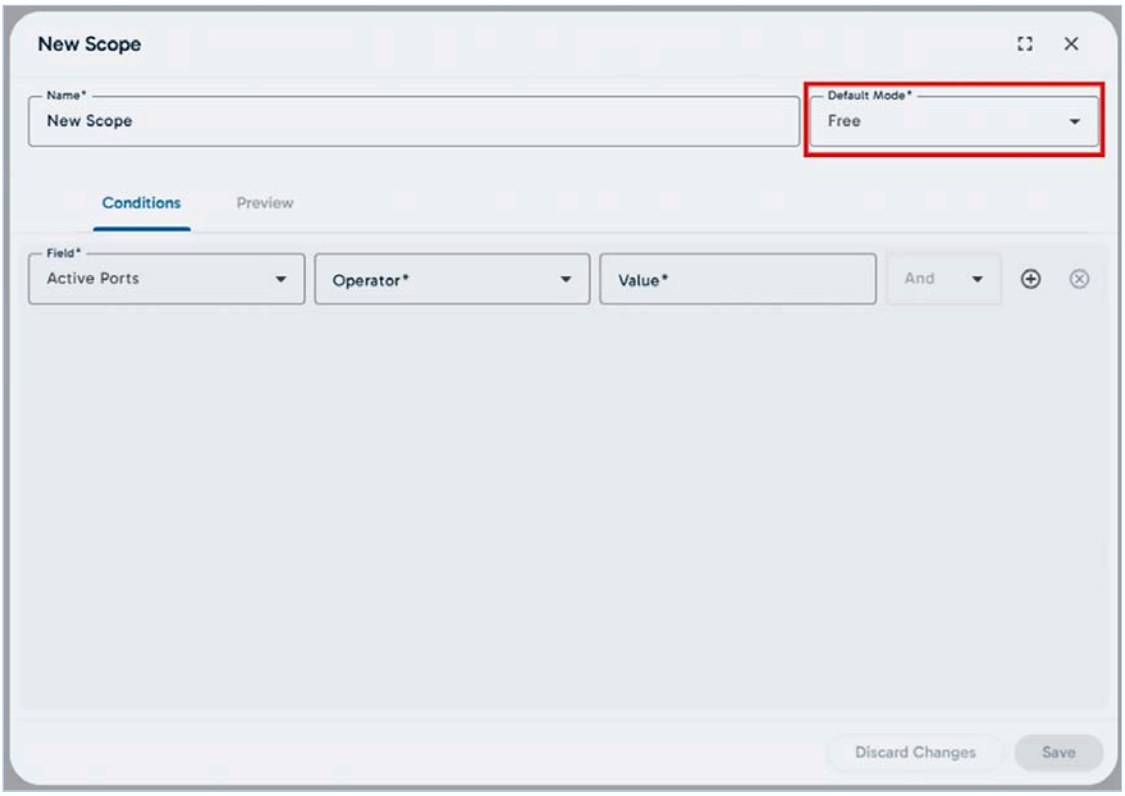
New port attributes: Last Successful Port Scan and Last Port Scan Attempt

Further information and prerequisites for enabling this capability can be found here: Event Based Scan Engine.

Task IDs: IN-1960

## Scopes and Agent Mode Control

Starting from Sepio Platform V49, Scopes have been enhanced to allow centralized control of Agent Modes. Scopes can now define a **default Agent Mode**, ensuring that all agents under the scope operate consistently in accordance with organizational policy. This eliminates manual misconfiguration errors, as agents automatically inherit the scope's defined mode, and manual changes are restricted while the scope is applied.



Default Agent Mode

Further information and prerequisites for enabling this capability can be found here: Scopes and Agent Mode in Sepio Platform.

Task IDs: IN-1986

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Switch physical location attribute (SNMP sysLocation) is now displayed and can be used for queries and reporting, in addition to the connected location | O-1381 |
| **New:** Indication when a password does not meet complexity requirements | Q-3969 |
| **Behavior change:** When an Access Point detected in a previous scan is no longer present in the subsequent WLC scan, it will now be automatically removed | A-2471 |
| **Fixed:** Login issues to Sepio's Platform | Q-3928 |
| **Fixed:** Issue where updating an existing filter did not apply changes correctly | Q-3987 |

| Item | Task ID |
| --- | --- |
| **Fixed:** In some cases, missing UI indications appear when a Sepio Security Administrator attempts an action without the required permissions | O-1399 |
| **Fixed:** In some cases, the change password after first login feature did not work | Q-3970 |
| **Fixed:** Some CEF messages are missing timestamps | Q-4006 |
| **Fixed:** Audit logs of agent mode change to BST are missing | A-1122 |
| **Fixed:** Issues in downloading cloud data lake from the platform | N-998 |
| **Fixed:** Issues in scheduled report emailed timelines | Q-3707 |

## Known Limitations

There are no new known limitations introduced in this release.
See the list of known limitations.

# Sepio Platform v48 (build 17.2508.608) Release Notes

This release introduces minor enhancements and several fixes. Please note the changes section below.

- Platform build: 17.2508.608
- Scan Engine build: 17.2508.503
- Default Host Agent build: 17.2509.101
- KB version: 2509081251
- Build Time and numerator: 2025-09-16 07:26:57 (61)

## Release Highlights

### Enhanced Asset Classification

This release of Sepio introduces an improved four-layer asset classification framework. Assets are now categorized by Cyber-Physical System (CPS) class (IT/OT/IoT), category, and sub-category, in addition to the previously provided type and asset name (see image below). The framework aligns with industry standards and delivers top-down CPS inventory visibility, starting from the broadest classification and narrowing down to specific instances. This structured approach enhances reporting capabilities (e.g., management and audit reports) and enables smoother integration and correlation with other tools across the organization's ecosystem. The currently used icons, asset types, and naming conventions remain unchanged. Asset metadata will be updated when it is online (status: connected) after the first scan with a Knowledge Base package that includes the changes.

| Asset | CPS Class | Category ↓ | Sub Category |
|---|---|---|---|
| Camera | IoT | Physical Security | Security Camera |
| Camera - Bosch OEM | IoT | Physical Security | Security Camera |
| Mobile - iPad | IT | Phones and Tablets | Tablet |
| Communication - FortiGate-3... | IT | Network Infrastrac... | Network Router |
| IP Phone (7965) | IT | IP Telephony | IP Phone |
| SEP1cdea782e211 | IT | IP Telephony | IP Phone |
| IP Phone (ATA 190) | IT | IP Telephony | Analog Telephone ... |
| IoT - Industrial PLC and TeSys... | OT | Industrial Automati... | PLC |
| Virtual Machine | IT | Computer Systems | Virtual Machine |

Enhanced Asset Classification

Task IDs: O-1353, A-2384, A-2438

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Asset lists can be sorted by location | Q-3735 |
| **Fixed:** In some cases, when a user attribute is added to an asset, the audit log incorrectly references a different asset | Q-3833 |
| **Fixed:** When trying to set SMTP configuration, it would only work if the user provided the sender's email address first | O-1379 |
| **Fixed:** In some cases, the Unsupervised Network Infrastructure risk indicator is not applied to manageable unsupervised switches detected by Sepio | A-2435 |
| **Fixed:** For certain Wi-Fi connected assets, the SSID is shown in the Location but is missing in the Connected SSID attribute | A-2441 |
| **Fixed:** In some cases, assets did not change to a disconnected status, although they have not been seen for a long time | Q-3893, A-2447 |
| **Fixed:** In some cases, multiple assets were presented as a single asset on the asset topology map | A-2429 |
| **Fixed:** Event logs are missing when changing Sepio Agent mode to Block Mass Storage Devices and Known Threats (BST) mode | O-1350 |
| **Fixed:** When exporting a network infrastructure report from the Supervised Network Infrastructure view, additional MAC address attribute is missing | Q-3820 |
| **Fixed:** When duplicating a Saved Query, the email recipients are not being copied to the new query | Q-3884 |
| **Fixed:** In some cases, when using the Splunk integration with the Sepio app, events were not being sent. | O-1376 |
| **Fixed:** In some cases, scheduled reports are emailed at a different time than the one configured | Q-3707 |
| **Changed:** Severity of some EMERGENCY syslog message is changed to "INFORMATIVE" | Q-3857 |

## Known Limitations

There are no new known limitations introduced in this release.
See the list of known limitations.

# Sepio Platform v47 (build 17.2508.504) Release Notes

This release introduces minor enhancements and several fixes. Please note the changes section below.

- Platform build: 17.2508.504
- Scan Engine build: 17.2508.11
- Default Host Agent build: 17.2504.108
- KB version: 2507151620
- Build Time and numerator: 2025-08-26 14:12:30 (60)

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** Users' last login time is logged and displayed in the Users table under **Settings → Users** | O-1375, O-1362 |
| **New:** The Sepio Scan engine now fetches application protocol information from Cisco switches using the Cisco NBAR | N-959 |
| **New:** Sepio Scan engine is now fetching device authentication information from Cisco switches | N-956 |
| **Fixed:** In some cases, DP information is not shown on Port Details | O-1370 |
| **Fixed:** In some cases, the asset topology map fails to render | Q-3733 |
| **Fixed:** Cisco Nexus port data parsing error | Q-3869 |
| **Fixed:** In some cases, a device connected to the management port is incorrectly shown as connected to a different port | Q-3868 |
| **Fixed:** Offline assets remain in the system beyond the configured retention period | Q-3653 |
| **Fixed:** In some cases, assets are incorrectly flagged with the Rare Asset RI despite having more instances than the defined threshold allows | A-2389 |
| **Fixed:** Corrected a typo in the Risky Asset Connected RI description | A-2421 |
| **Fixed:** Exported reports from the Network Infrastructure page do not include the Additional MAC field as expected | Q-3820 |

## Known Limitations

There are no new known limitations introduced in this release.

See the list of known limitations.

# Sepio Platform v46 (build 17.2507.615) Release Notes

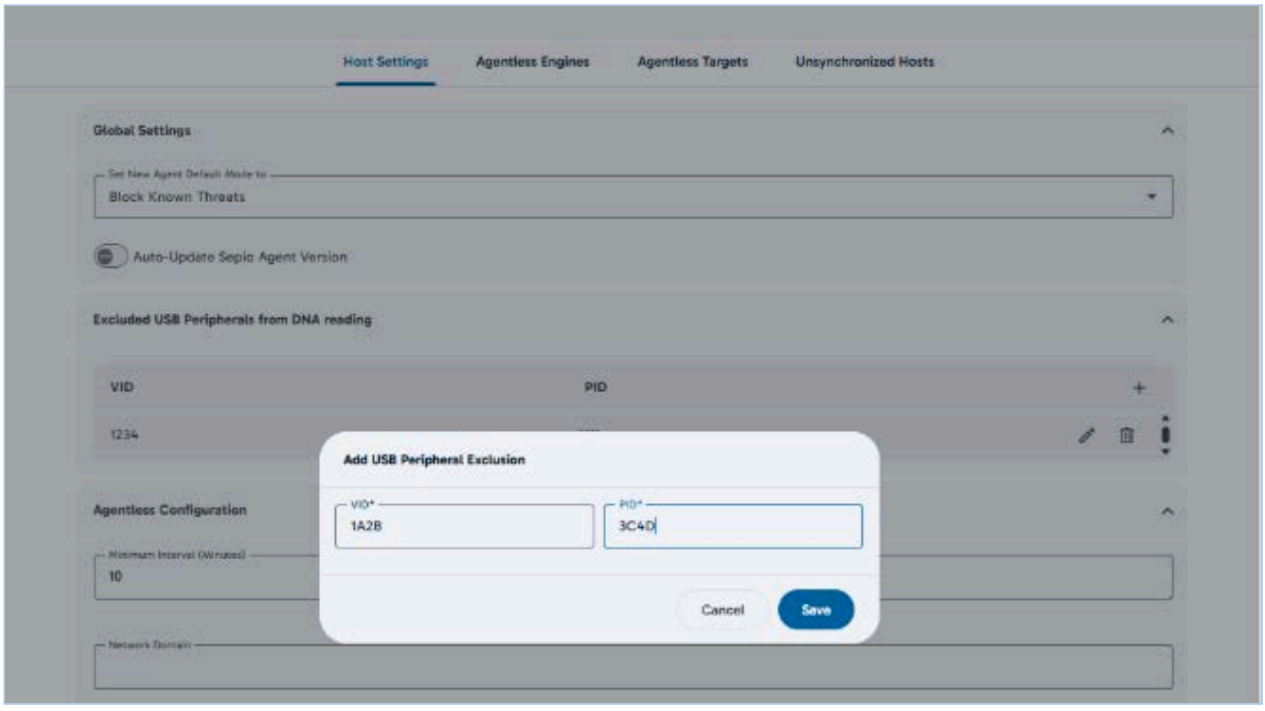
This release introduces minor enhancements and several fixes. Please note the changes section below.

- Platform build: 17.2507.615
- Scan Engine build: 17.2507.512
- Default Host Agent build: 17.2506.520
- KB version: 2508111240
- Build Time and numerator: 2025-08-11 12:40:00 (58)

## Release Highlights

### Exclude USB Devices from Sepio Agent Asset DNA Reading

Starting with this version, Sepio Security administrators can manage exclusions for trusted USB peripherals directly form the Sepio platform UI. By navigating to Settings → Host and adding the VID and PID of the relevant devices to the 'excluded from Asset DNA Reading list'.




Task IDs: O-1368, A-1065, I-2070, A-1051, A-1052, A-2419, A-1049

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **Fixed:** In some cases, the system experiences lag when uploading a new KB | A-2395 |

| Item | Task ID |
| --- | --- |
| **Fixed:** In some cases, data from CrowdStrike is linked to the wrong asset | A-2387 |
| **Fixed:** In some cases, disconnected assets are shown online | A-2351 |
| **Fixed:** Ports are shown on the Client tab in the Network Details modal of physical WLCs | Q-3780 |
| **Fixed:** The 'Copy GraphQL Request' button functions only on the Saved Queries page | O-1364 |
| **Fixed:** User Defined Attributes columns cannot be removed from asset lists. | O-1365 |
| **Fixed:** Typo in the Aruba Wi-Fi integration successful connection test message | Q-3566 |
| **Fixed:** When attempting to add a new user attribute from within the switch screen, clicking the Save button has no effect | Q-3832 |
| **Fixed:** In some cases, due to a parsing error, the Cisco Catalyst C9300-48UXM switch is incorrectly displayed as unsupported by Sepio | N-910 |
| **Fixed:** In certain cases, some ports of a supervised Juniper EX4300-48P switch are missing from the switch view in the Sepio platform UI | Q-3382 |
| **Fixed:** Schedule Reports are being emailed at wrong time | Q-3707 |
| **Fixed:** In some cases, VLAN table shows VLAN monitoring as 'Some' although monitoring is turned on for all switches associated with it | Q-2433 |
| **Fixed:** Assets cannot be filtered by the RI 'Reason' field in asset lists on Saved Queries | Q-3748 |
| **Fixed:** In some cases, DP information is missing from the Port Details modal, although being available | O-1370 |
| **Modified:** Meraki API calls optimization | N-933 |
| **Modified:** Juniper SSH session optimization | N-931 |

## Known Limitations

There are no new known limitations introduced in this release.

See the list of known limitations.

# Sepio Platform v45 (build 17.2507.514) Release Notes

This release introduces minor enhancements and several fixes. Please note the changes section below.

- Platform build: 17.2507.514
- Scan Engine build: 17.2507.501
- Default Host Agent build: 17.2504.108
- KB version: 2507151620
- Build Time and numerator: 2025-07-16 10:33:41 (57)

## Release Highlights

### Scan Engine to Meraki Cloud Proxy Configuration

Sepio customers can now connect to the Meraki Cloud through an authenticated proxy. Instructions for configuring the Scan Engine proxy are available under Network HTTP Proxy

Task IDs: N-835

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** It is now possible to review the Sepio agent CPU consumption in the UI as a table element. | O-1351 |
| **Modified:** When an active network asset becomes dormant, the Platform will retain its attribute values as long as the port it is connected to remains active. In such cases, a 'Dormant Asset' risk indicator will be assigned to the asset. | CPO-07281 |
| **Modified:** The label 'Risky Child Connected' in the filter bar has been updated to 'Risky Asset Connected'. | A-2312 |
| **Fixed:** Users with "User" privileges now have access to the Topology Map view. | CP-07282 |
| **Fixed:** In some cases, assets are presented as if they are connected to a different port than the one they are actually connected to. | A-2192 |
| **Fixed:**In some cases, the Communication Anomaly Risk Indicator did not function on assets connected to switches running ArubaOS-S and ArubaOS-CX. | A-2220 |

| Item | Task ID |
|---|---|
| **Fixed:** Disconnected assets are not deleted even when their Last Seen exceed the configured asset auto-deletion threshold. | Q-3653 |
| **Fixed:** In some cases, offline assets are missing their last known location. | Q-3669 |
| **Fixed:** Event log entries are not being purged as per the configured time-based and size-based retention policies. | Q-2411 |
| **Fixed:** Some Access Points were being merged under the same MAC Address and appearing in different physical locations. | Q-3279 |
| **Fixed:** In certain cases, different assets were merged into a single asset. | A-2094, A-2131 |
| **Fixed:** Some devices were being created based on wrong CDP/LLDP parsing. | A-2315 |
| **Fixed:** In certain cases, the location of online wireless assets is missing the Access Point to which they are connected. | A-2316 |
| **Fixed:** In some cases, supervised assets are presented as unsupervised. | Q-3608, A-2309 |
| **Fixed:** Disabling local users has no effect. | Q-1817 |
| **Fixed:** In some cases, SSID is not available in the SSID field but is available in the location field. | Q-3648 |
| **Fixed:** In some cases, assets with CDP records do not display the MAC address. | A-2336 |
| **Fixed:** In some cases, Access Point are shown in two locations. | A-2339 |
| **Fixed:** In some cases, assets connected to supervised Access Points are shown in two locations. | A-2310 |
| **Fixed:** In some cases, Arista asset DP is not being correctly parsed. | A-2365 |
| **Fixed:** In some cases, the additional MAC field contains strings of non-MAC addresses. | A-2048 |

## Known Limitations

There are no new known limitations introduced in this release.
See the list of known limitations.

# Sepio Platform v44 (build 17.2506.603) Release Notes

This release introduces minor enhancements and several fixes. Please note the changes section below.

- Platform build: 17.2506.603
- Scan Engine build: 17.2506.6
- Default Host Agent build: 17.2504.108
- KB version: 2506271517
- Build Time and numerator: 2025-06-26 10:16:46 (56)

## Release Highlights

### Enhancements to Unmanaged Switch Detection

To improve unmanaged switch detection operations, this version of Sepio introduces several enhancements to the detection algorithm:

#### Expansion of Approved Groups

Approved groups refer to combination of assets that are legitimately connected to the network as a chain. Therefore, when these are detected, a potential unmanaged switch risk indicator should not be created. Starting with this release, the approved groups are:

1. Multiple assets connected through network infrastructure elements
2. Network assets connected through an IP phone
3. Printers connected through Printronix/ST Printer IC
4. Siemens PLCs (often presenting multiple MAC addresses)
5. Virtual Machines and hosts

#### DNA Based Consistency

When an Unmanaged Switch has been previously detected, the Platform will continue to retain it as long as the DNA observed by Sepio on the corresponding port remains unchanged, regardless of any changes in the connected assets (i.e., assets being connected or disconnected).

*Sepio does not create unmanaged switches on ports configured as trunk or routed ports.* Starting with this release, Sepio does not create an unmanaged switches in cases where multiple assets are connected through trunk or routed ports.

Task IDs: A-2302

## Additional Context to User Events

Starting from this version of Sepio, asset 'tags' and 'user attributes' are now included in user events. These details are accessible on the User Event page in the Sepio UI, as well as through Syslog and Splunk integrations.

Task IDs: O-1296

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **Modified:** When an active network asset becomes dormant, the Platform will retain its attribute values as long as the port it is connected to remains active. In such cases, a 'dormant asset' risk indicator will be assigned to the asset | A-2303 |
| **Modified:** Administrator can now delete users directly from the user management page. | O-1327 |
| **Modified:** Users with "User" privileges now have access to the Topology Map view. | Q-3636 |
| **Fixed:** In some cases, the "accept risk" option is not applicable to hosts running the Sepio Agent and to the peripheral assets connected to them. | Q-3640, A-2173 |
| **Fixed:** In some cases, notifications regarding potential threats are not being sent by e-mail. | Q-3605 |
| **Fixed:** LDAP sessions are being automatically terminated, even while the user remains active. | O-1326, O-1325 |
| **Fixed:** In some cases, access points with the same name presented as one asset. | Q-3279, A-2131 |
| **Fixed:** In some cases, when filtering for unsupervised network infrastructure, result contains supervised network infrastructure. | A-2311 |
| **Fixed:** Administrator is unable to change users' password. | Q-3497 |
| **Fixed:** In certain cases, page navigation button is disabled on the 'network infrastructure' and 'Queries' page. | Q-3639, Q-3613 |
| **Fixed:** In some cases, the 'first successful scan' attribute remains 'Never" although switch has been scanned before. | Q-2516 |
| **Fixed:** Inability to filter hosts by 'Last Updated'. | Q-3523 |

## Known Limitations

There are no new known limitations introduced in this release.

See the list of known limitations.

# Sepio Platform v43 (build 17.2506.510) Release Notes

This release introduces minor enhancements and several fixes. Please note the changes section below.

- Platform build: 17.2506.510
- Scan Engine build: 17.2506.5.0
- Default Host Agent build: 17.2504.108
- KB version: 2506121051
- Build Time and numerator: 2025-06-19 09:08:36 (55)

## New Features, Changes and Bug Fixing

| Item | Task ID |
|---|---|
| **New:** audit record for tag operation now includes the asset's MAC address. | A-1315 |
| **New:** New TAGS API cache configuration options added:<br>• TAGS_API_CACHE_MAX_SIZE: Defines the maximum cache size (in number of assets) for Tags requests by AssetProducer to TagsAPI. Default value is 10000<br>• TAGS_API_CACHE_TTL: Defines the cache TTL (in seconds) for Tags requests by AssetProducer to TagsAPI. Default value is 600 | A-2267 |
| **Modified:** Do not send enrichment event for disconnected asset. | Q-3653 |
| **Fixed:** User type "User" now has access to the Topology Map. | Q-3636 |
| **Modified:** Added additional MFA controls. | Q-3567 |
| **Fixed:** In some authentication scenarios, Sepio WebUI does not allow login, and the "System is Loading" message appears for a very long time, due to sepioprime-auth-1 early exit. | Q-3524 |
| **Fixed:** In some conditions, the disabled Admin local user action has no effect. | O-1322 |
| **Fixed:** In some cases, LLDP is not parsed correctly. | Q-3616 |
| **Fixed:** In some cases, assets with recent scan missing are not showing SSID and their Access Point in the location is listed as unidentified. | Q-3644 |
| **Fixed:** In some cases, after scrolling pages in the network infrastructure section, then leaving and returning to the page will result in the scroll back option grayed out. | Q-3639 |

| Item | Task ID |
| --- | --- |
| **Fixed:** Previously scanned switch (C9300-48UXM) is showing “unsupported” due to improper parsing of a critical “show interfaces” command that includes an escape character. | N-887 |
| **Fixed:** In some cases, online Wireless assets are missing SSID info. | O-1247 |
| **Fixed:** Previously scanned switch (WS-C4506E) is showing “unsupported” due to improper parsing of a critical command that includes an escape character. | Q-2736 |
| **Fixed:** External data stream is consuming large amounts of memory. | Q-3326 |
| **Fixed:** Access point misclassification. | Q-3364 |
| **Fixed:** In some cases, assets on a supervised Access Point will have a wrong location due to wrong CDP name parsing. | Q-3590/8698qu8zt |
| **Fixed:** In some cases, due to Q-3590 an Access Point will appear on different sites. | Q-3279 |
| **Fixed:** Supervised Access Point name should be validated against the list taken from WLC. | A-2179 |
| **Fixed:** Merging wrong assets and location due to wrong Access Point name truncation. | A-2131 |
| **Fixed:** In some cases, wireless assets do not show updated status or location when the WLC is connected and not updated. | A-2161 |
| **Fixed:** In some cases, wireless assets do not show updated status or location when the WLC is in “Unable to Connect” state. | A-2160 |
| **Fixed:** Devices are not being disconnected, although having last seen in the past. | A-2194 |
| **Fixed:** In some cases, the location of unsupervised assets is empty because of an issue with disconnecting the last known parent. | Q-3606, A-2193 |

## Known Limitations

There are no new known limitations introduced in this release.
See the list of known limitations.

# Sepio Knowledge Base (KB) Change Log

This page documents changes and updates to classification categories provided as part of Sepio Knowledge Base (KB) updates.

## KB 20260506

**Changed Classifications:**

- IoT – Unified Security Platform

## April 2026 Knowledge Base Change Log

Expand All

**KB 20260428**

**KB 20260424**

**KB 20260416**

**KB 20260414**

**KB 20260413**

**KB 20260410**

**KB 20260407**

**KB 20260402**

## March 2026 Knowledge Base Change Log

Expand All

**KB 20260327**

**KB 20260320**

**KB 20260317**

**KB 20260313**

**KB 20260310**

**KB 20260305**

**KB 20260304**

## February 2026 Knowledge Base Change Log

Expand All

**KB 20260225**

**KB 20260219**

**KB 20260216**

**KB 20260212**

**KB 20260205**

## January 2026 Knowledge Base Change Log

Expand All

**KB 20260123**

**KB 20260115**

**KB 20260107**

## December 2025 Knowledge Base Change Log

Expand All

**KB 20251215**

**KB 20251211**

**KB 20251209**

## November 2025 Knowledge Base Change Log

Expand All

**KB 20251125**

**KB 20251120**

**KB 20251117**

**KB 20251113**

**KB 20251111**

**KB 20251105**

**KB 20251103**

## October 2025 Knowledge Base Change Log

Expand All

**KB 20251028**

**KB 20251023**

**KB 20251020**

**KB 20251015**

**KB 20251008**

**KB 20251002**

## September 2025 Knowledge Base Change Log

Expand All

**KB 20250926**

**KB 20250915**

**KB 20250909**

**KB 20250903**

**KB 20250902**

**KB 20250901**

## August 2025 Knowledge Base Change Log

Expand All

- KB 20250822
- KB 20250819
- KB 20250813
- KB 20250811
- KB 20250806
- KB 20250804
- KB 20250801

## July 2025 Knowledge Base Change Log

Expand All

- KB 20250729
- KB 20250722
- KB 20250715
- KB 20250714
- KB 20250711
- KB 20250709

**KB 20250708**

**KB 20250707**

**KB 20250702**

## June 2025 Knowledge Base Change Log

Expand All

**KB 20250627**

**KB 20250626**

**KB 20250625**

**KB 20250623**

**KB 20250620**

**KB 20250612**

**KB 20250609**

**KB 20250604**

**KB 20250602**

## May 2025 Knowledge Base Change Log

Expand All

**KB 20250527**

KB 20250519

KB 20250513

KB 20250512

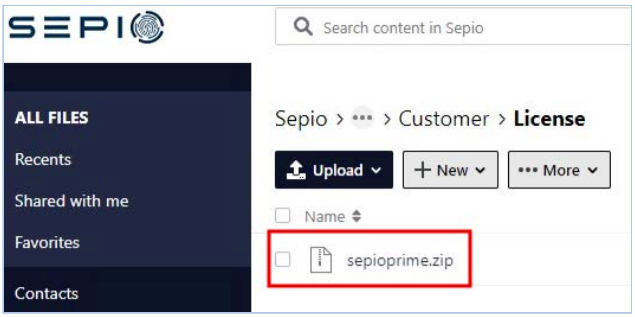
KB 20250505

# Logging into Sepio for the First Time

We recommend using **Google Chrome** or **Microsoft Edge** to log in to Sepio. After your first login, you can create a user profile for each new user.

## On-premises Log in

To operate Sepio on-premises, you must install a license after your initial login.
Before logging in, download your zip license file from sepiofiles.com



Download your zip license

**To log in to Sepio for the first time on-premises:**

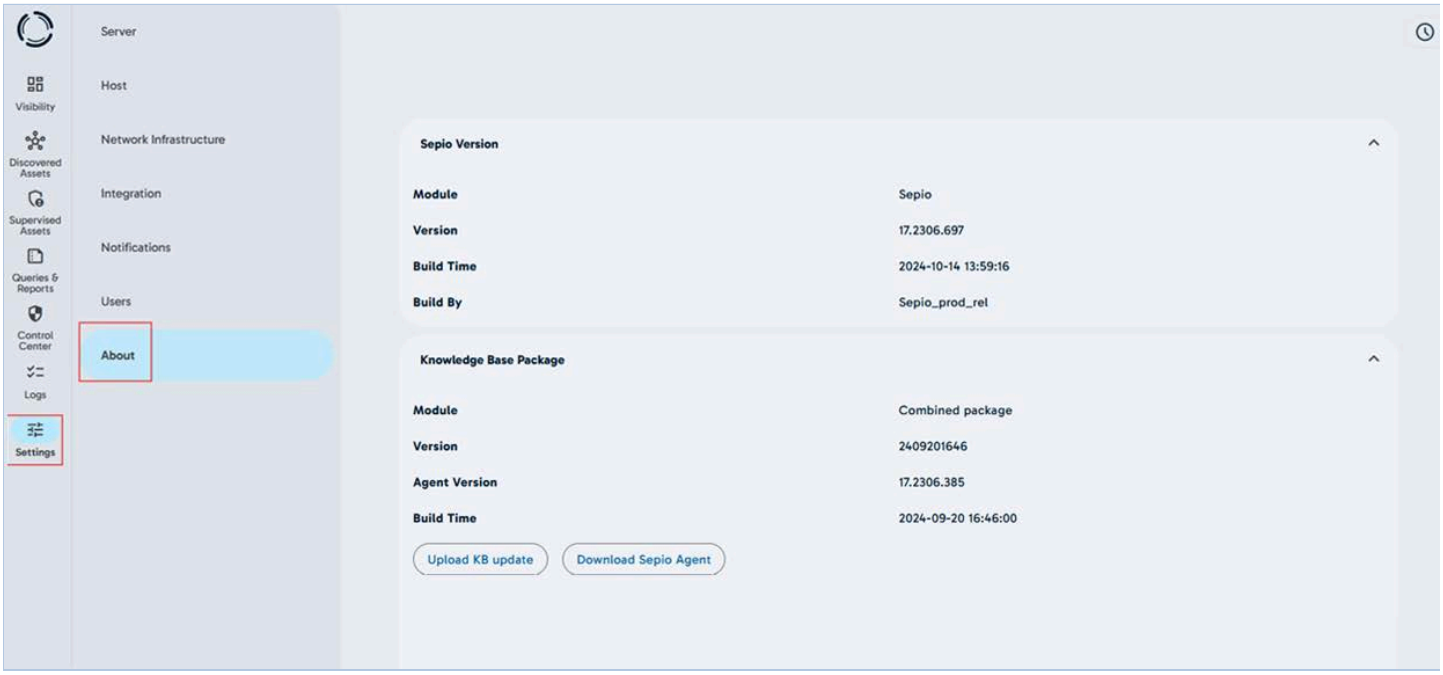
1. In the browser address bar, enter the fully qualified domain name exactly as entered in the Agent installation.



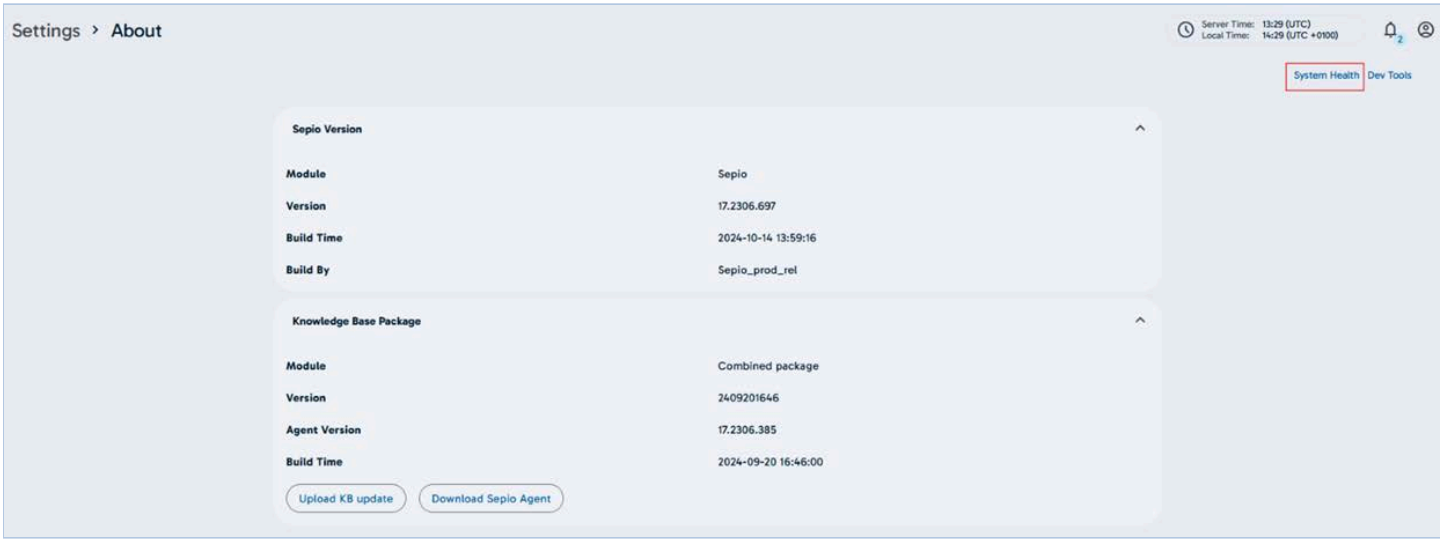
Log in to Sepio

2. Enter the following credentials:
    - **Username:** Administrator
    - **Password:** SepioSystems
    - Click **Sign In.**
3. Import the Sepio license:

- The license file should be available and ready. Import the License (ZIP format) to your server following the steps:
- **Settings** -> **About** -> **System Health** -> **General** -> **Import**




Settings -> About




Settings -> About -> System Health




Settings -> About -> System Health -> General -> Import

4. Click **Import**, then navigate and select the downloaded ZIP file.

**Note:** Do not unzip the file.

## Sepio Cloud Login

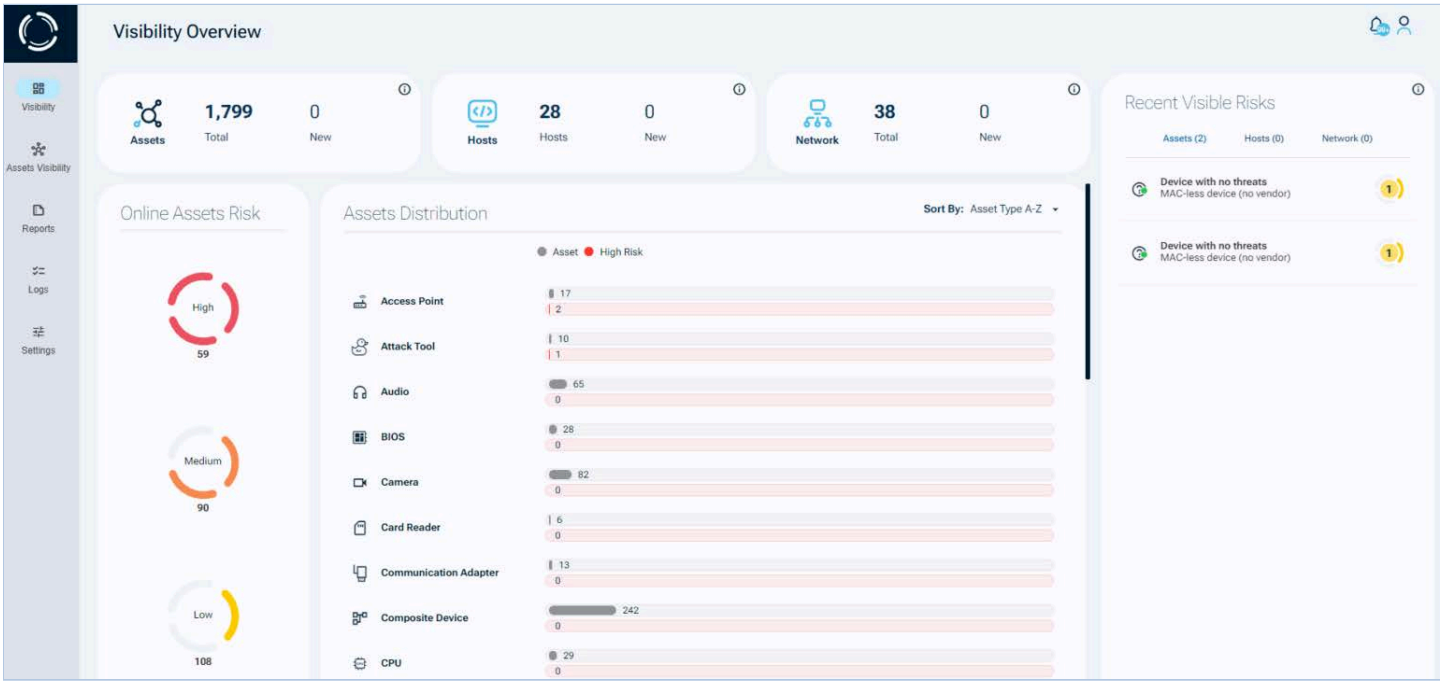
### To log in to Sepio for the first time on Sepio Cloud:

1. In the browser address bar, enter the fully qualified domain name.




Log in to Sepio

2. Enter the Username and Password provided on sepiofiles.com. We will notify you when your credentials are ready to be used.
3. Click **Sign In**. The **Visibility Overview** view will appear.



Visibility Overview

# Logging into Sepio

## Overview

We recommend using **Google Chrome** or **Microsoft Edge** to log in to Sepio.
When you receive your username and password, you can log in to the platform.

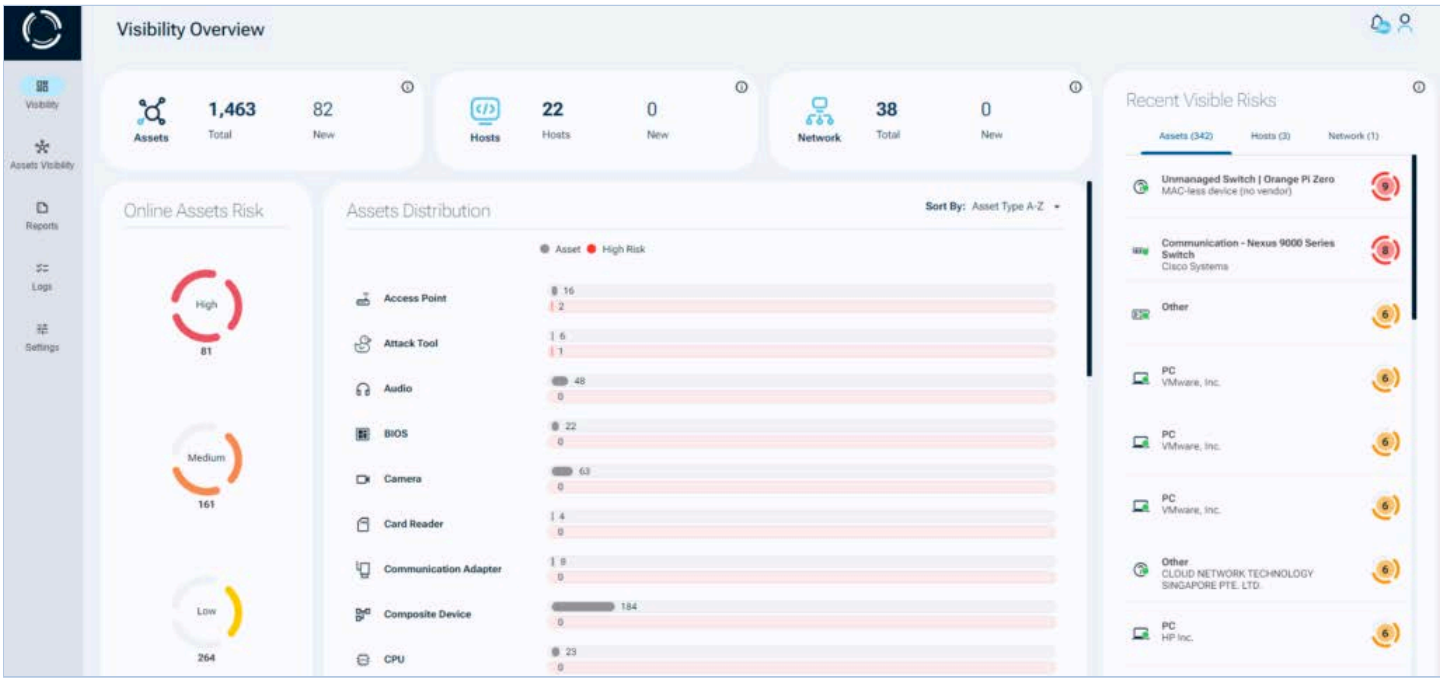
## Steps to Log into Sepio

1. In your browser's address bar, enter the fully qualified domain name (FQDN) of the Sepio platform.
2. Enter your username and password.




Enter your username and password

3. Click **Sign In**. The **Visibility Overview** page will appear after successful login.




Visibility Overview

# Monitoring Overall Assets and Risks

## Related Topics

- About Monitoring Overall Assets and Risks
- Opening the Visibility Overview View

## About Monitoring Overall Assets and Risks

You monitor Sepio overall Assets and Assets risks via the Visibility Overview.

The Visibility Overview is the central hub for monitoring your organization's Asset Inventory and Asset Risk. Here, you can sort the overall asset distribution in various ways, view recent visible risks, and perform additional monitoring tasks.

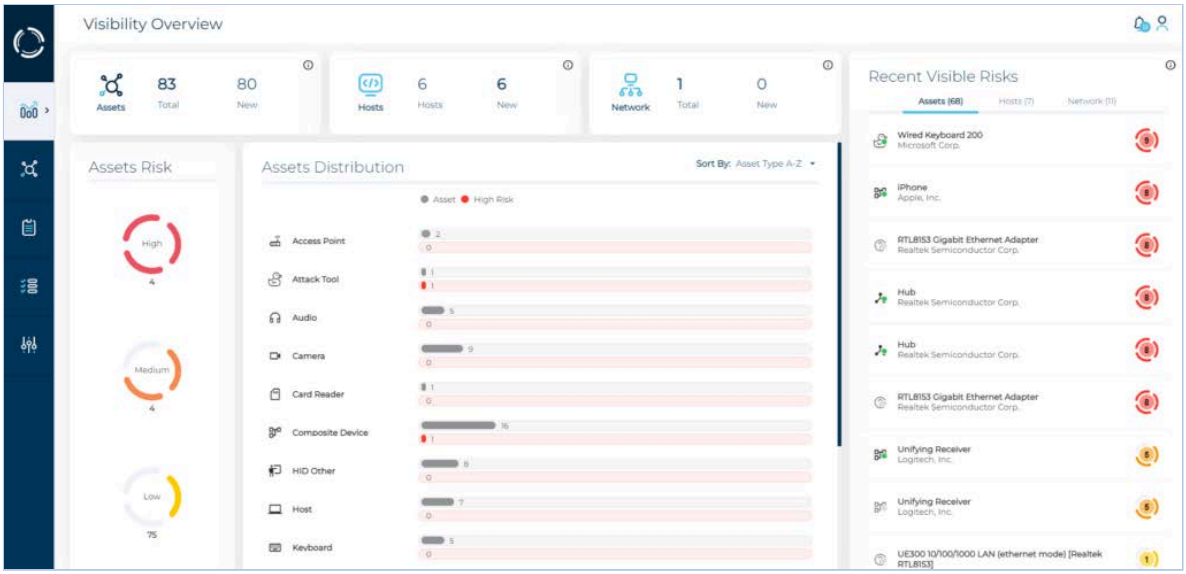
Use this view to:

- View the number of:
  - Current Assets on your Hosts, and on your Network Infrastructure
  - Assets that have been discovered in the last 24 hours
  - Assets which risk scores were updated in the last 72 hours
  - Recent visible risks by Asset group
  - Assets in each risk group and display each Asset risk score
- Drill down to the Asset details in the different Asset groups, via these views:
  - Discovered Assets
  - Hosts Assets Visibility
  - Network Infrastructure Assets Visibility
- Sort Assets, alphabetically, by Risk score and by Asset type count

# Opening the Visibility Overview View

To open the Visibility View:

- Login to Sepio
- – Or-
- From Sepio menu select **Visibility->Visibility Overview**



Visibility Overview

# Asset Management

## Related Topics

- About Assets
- About the Assets Visibility Views
- Opening the Assets Visibility Views
- Customized Views
  - Creating and Opening a Custom View
  - Customized Table View
- Visibility Views Interface Description
  - Discovered Assets Visibility View Interface
- Assets Actions
  - Managing Risky Assets
    - Managing Discovered Risky Assets
  - Displaying Assets Details
    - Displaying Discovered Asset Details
    - Displaying an Asset Historical Events
  - Sorting, Searching and Filtering Assets
  - Adding and Deleting User Defined Attributes
  - Adding and Deleting Tags
  - Exporting Asset/s Details to a CSV or PDF
- Network Topology Views
- Application Visibility
- Asset Identity
  - Improving Network Security with Sepio's Asset Identity Feature
  - Identity Related issues
  - Ensuring Visibility and Compliance for Enforced Authentication (802.1X/MAB)

# Asset Identity and Authentication Details

## What is Asset Identity?

In modern networking, knowing a device's **MAC address** or **IP address** is only part of the story. This information tells you that a device exists on your network, but not what it is, who is using it, or whether it's trusted.

**Asset Identity** is the next layer of visibility. It enriches basic device data by correlating it with high-trust information from your network's authentication systems. This authenticated identity acts as a powerful signal that works alongside with Sepio's existing classification methods.

By integrating this authenticated data, the feature increases the confidence level of Sepio's asset classification. Instead of only seeing the MAC address, you can now view the authenticated **user or host associated** with that device, as reported directly by the network itself.

This higher-confidence classification **strengthens your security posture**. It ensures that your access policies are applied to accurately identified and verified devices, while making it easier to detect anomalies, such as a device acting outside of its authenticated identity. This new feature in the Sepio platform provides a critical link, delivering immediate, high-confidence context about your assets.

## How Modern Switches Establish Identity

Your network switches are a key source of identity-related information. They act as gatekeepers for the network, using port-based authentication protocols to validate devices as they connect.

The most common protocol is **IEEE 802.1X** (also called "dot1x"). Here's a typical workflow:

1. A device (like a user's laptop) connects to a switch port.
2. The switch challenges the device to provide credentials (e.g., a username, password, or a digital certificate).
3. The switch passes these credentials to a central authentication server (such as a RADIUS server, e.g., Cisco ISE or ClearPass).
4. The server validates the credentials and, if successful, tells the switch that the device is **authorized**.
5. Crucially, the server also passes back the device's **identity** (like the username) and other policy details.

When devices don't support 802.1X (such as printers, OT or simple IoT devices), the switch can use other methods like **MAC Authentication Bypass (MAB)** to authenticate the device using its MAC address as its identity. This entire authentication process creates a session on the switch that contains a rich set of data about the connected asset.

## How Sepio Collects and Displays Asset Identity

Sepio's platform automates this discovery process. Our system polls your network infrastructure devices, and when a device is authenticated on a port (using protocols like 802.1X or MAB), the switch stores that session information.

If your network administrator has configured switch authentication policies or integrated them with NAC, Sepio will collect this data, parse the key details, and correlate them with the asset's existing profile (which already includes L1-L3 information such as MAC address, IP address, VLAN, DP, PoE etc.) and any other data collected.

The result is a simple, clear **Authentication Details** card in the Sepio UI. For example, the identity data pulled from the switch's session table is presented like this:

**Authentication Details:**

```
Identity: grow5129315
Status: Authorized
Domain: DATA
```

> **Note:** While this example data (e.g., grow5129315) may come from a Cisco device, Sepio developed this feature to be vendor-agnostic and not limited to Cisco devices. The release notes will provide information about supported vendors.

**A Note on the 'Identity' Field:** The information displayed in the **Identity** field depends on the switch's configuration and the authentication method used.

- It may be the **end-user ID** from an 802.1X authentication (such as grow5129315 in the example).
- It could be the **hostname** of the device generating the traffic.
- In other cases, especially with MAB, the identity may be the **asset's MAC address**. The MAC address format can also vary, appearing either as 12 concatenated hexadecimal digits (e.g., 38CA84DDABC1) or with each pair of digits separated by a dash (e.g., 38-CA-84-DD-AB-C1).

## The Value of "Status" and "Domain" Details

Knowing the authenticated **identity** is a major step forward, but the **Status** and **Domain** fields provide critical, real-time context for your security and IT operations teams.

### 🛡 Security Benefits

- **Identify Unauthorized Devices:** Quickly filter and investigate any device connected to the network but has a **Status** of Unauthorized or Pending. This could indicate a failed authentication attempt or a

device in a “guest” or “quarantine” state that requires immediate attention.

- **Detect Policy Violations:** The **Domain** field (e.g., DATA vs. VOICE) helps you spot anomalies. For example, if a device known to be an IP phone (which should reside in the VOICE domain) suddenly appears in the DATA domain, it could signal a spoofing attempt or a misconfiguration that a threat actor could exploit.

### ⚙ Operational Benefits

- **Faster Troubleshooting:** When a user reports a connectivity issue, you can instantly check their asset’s **Status**. If it’s Unauthorized, the issue is likely related to authentication rather than a physical port or cable. This significantly reduces mean time to resolution (MTTR).
- **Verify Network Segmentation:** The **Domain** field provides immediate confirmation that your network segmentation policies are working as intended. You can easily verify that specific device types (like VoIP phones) are correctly being placed in the VOICE domain, and that user devices reside in the DATA domain.

# Ensuring Visibility and Compliance for Enforced Authentication (802.1X/MAB)

**Note:** This pages applies to Cisco IOS XE (Catalyst 9000 Series)

## The Challenge: Invisible Non-Compliance

Many organizations configure 802.1X or MAB (MAC Authentication Bypass) on their switch ports but fail to realize that the switch is not actually **enforcing** these protocols. On modern Cisco platforms, simply adding the mab or dot1x command is insufficient to initialize an active authentication session.

Without the explicit enforcement trigger, the switch treats the port as a standard Layer 2 port. This results in:

- **Zero Visibility:** The command show authentication sessions will return "No sessions match supplied criteria," even if a device is connected.
- **Security Gaps:** Unauthorized devices may bypass security checks because the switch isn't actively managing the port state.

## Comparative Port Configurations

The following examples illustrate the difference between a compliant, enforced port and a non-compliant, unenforced port as seen in the switch configuration. Let's compare two different ports on the same switch.

#### Example A: Compliant/Enforced Port (Te1/1/4)

This port is correctly configured for Identity-Based Networking Services (IBNS). The inclusion of the port-control auto command ensures that the switch actively manages the device session.

Plaintext

```
interface TenGigabitEthernet1/1/4
description *** ENFORCED PORT - VISIBLE IN SEPIO ***
switchport access vlan 10
switchport mode access
mab
access-session port-control auto  <-- CRITICAL ENFORCEMENT COMMAND
dot1x pae authenticator
spanning-tree portfast
```

```
end
```

**Example B: Non-Compliant/Unenforced Port (Gi1/0/1)**

While this port has authentication methods defined, it is missing the enforcement trigger. The switch will allow traffic, but it will **not** track the authentication session in the internal database.

Plaintext

```
interface GigabitEthernet1/0/1
description *** UNENFORCED PORT - INVISIBLE SESSION ***
switchport access vlan 10
switchport mode access
mab
dot1x pae authenticator
spanning-tree portfast
! MISSING: access-session port-control auto
end
```

## Implementing Sepio Port Compliance for Enforcement

Sepio's **Port Compliance** feature allows you to automatically detect ports that lack this critical enforcement command by performing an exact text match against the retrieved configuration.

**Configuration in Sepio Control Center**

1. **Enable Prerequisites:** Ensure `RI_PORT_COMPLIANCE_VIOLATION` and `PORT_VERIFICATION` are enabled.
2. **Define the Rule:** Navigate to **Control Center** -> **Port Compliance** and create a new rule:
    - **Name:** "Cisco Authentication Enforcement"
    - **Condition Field:** Must Contain
    - **Value:** access-session port-control auto
3. **Result:** If an asset connects to a port like **Gi1/0/1** (Example B), Sepio identifies the missing string and raises a **Port Compliance Violation** sub-risk indicator for that asset.

## Best Practices

- **Verify Exact Syntax:** Use Sepio's **View Port Configuration** tool to confirm how your specific Cisco IOS version displays the command. Older versions may display authentication port-control auto instead of access-session....
- **Scope by Vendor:** Create dedicated Port Compliance configurations for different switch models or OS versions to avoid false negatives caused by syntax variations.

**Need Help?** Contact support@sepiocyber.com.

# Identity Related Issues

**Note:** This page lists common behaviors related to identity and authentication mismatches in network environments using 802.1X.

## Identity Mismatch

In some cases, the identity reported by the switch and the identity of the asset (hostname) and/or the identity of the OS user (username or login name) may differ. This is common behavior and, depending on your internal security strategy, may be intentional. Sepio is an ideal tool to detect such behavior and can help enhance your network security design when implementing 802.1X.

The primary reason for an identity mismatch is the distinction between **machine authentication** and **user authentication**, both of which use the 802.1X protocol. The switch reports the identity of the last successful authentication it received from the RADIUS (NAC) server.

As a result, the switch and NAC (Network Access Control) continue to show the original user's identity.

## Key Reasons for the Identity Mismatch

The identity you see on the switch port is the **User-Name** attribute from the RADIUS **Access-Accept** packet. This username can come from several sources, leading to a "mismatch":

### Machine Authentication (Most Common Reason)

- **What it is:** In corporate environments, Windows and macOS devices are often configured to authenticate to the network before any user logs in. This is called machine authentication.
- **Identity Used:** The identity is the computer's own Active Directory account. This is often formatted as **host/PC-NAME.domain.com** or just **PC-NAME$**.
- **Why it is done:** This is crucial. It allows the PC to get on the network to contact domain controllers. Without it, a user could not log in for the first time, receive Group Policy updates, or run boot-up scripts.
- **The "Mismatch":** A user (**jsmith**) logs into the PC, but the PC has already authenticated to the switch as **host/PC-001**. The OS user **jsmith** and the 802.1X user **host/PC-001** are different.

### User Authentication (Second Stage)

- **What it is:** After the user successfully logs into Windows, the 802.1X supplicant (client) can be configured to re-authenticate to the network, this time using the user's credentials.

- **Identity Used:** The identity is now the user's account, such as **jsmith@domain.com** or **DOMAIN\jsmith**.
- **The "Mismatch":** If this second-stage authentication is successful, the switch log will now show **jsmith@domain.com** on that port. An advanced NAC can use this new identity to change the port's VLAN or access (see NAC section below). If this user-level authentication fails (e.g., bad password), the port will remain authenticated as the machine (**host/PC-001**), creating a clear mismatch: **jsmith** is at the keyboard, but the network only sees the PC's identity.

#### Certificate-Based Authentication (EAP-TLS)

- **What it is:** Instead of a username and password (as in PEAP-MSCHAPv2), 802.1X can use digital certificates.
- **Identity Used:** The "username" is pulled from the certificate's **Subject** or **Subject Alternative Name** (SAN) field.
- **The "Mismatch":** If machine certificates are used, the certificate's subject will be the PC's Fully Qualified Domain Name (FQDN), such as pc-001.domain.com. This will be reported as the 802.1X user, which will not match the OS user (**jsmith**).

#### Fallback to MAC Authentication Bypass (MAB)

- **What it is:** If a device fails 802.1X (or doesn't support it), the switch can be configured to **fall back** and attempt authentication using the device's MAC address.
- **Identity Used:** The NAC/RADIUS server is configured to use the MAC address itself as the username.
- **The "Mismatch":** The switch will report the user as **aa-bb-cc-dd-ee-ff** (or a similar MAC format, depending on switch model and OS version), which matches neither the PC name nor the OS user. This commonly occurs with printers, IoT devices, or misconfigured PCs.

## How Common Is This Issue?

It is very common. In most enterprise environments, this is expected behavior rather than an actual "issue." The "issue" is often a misinterpretation of what is being observed.

#### Working as Designed

A helpdesk technician looks at a switch port and sees the user is **host/PC-012**, even though **jsmith** is logged in. This is normal if the network policy is machine-based, or if the user-authentication step has not occurred or is not required.

#### When it's a Real Problem

The real problem arises when the user-authentication step fails. For example, the user is supposed to land in the Corporate User VLAN, but their user-auth fails (due to a bad password or expired certificate). They then fall back to the Machine Auth VLAN, which has limited access (e.g., only to domain controllers).

The user complains that they “cannot access the file server,” and the “mismatch” (switch reports machine, user is logged in) is simply the symptom of the failed user authentication.

## Identity Differences based on OS and NAC Implementation

The possible differences in the identities that the switch is providing to Sepio vary based on implementation and your NAC solution:

**Windows 10 vs. Windows 11:**

- **No significant differences.** Both use the same underlying **Windows EAPHost service and supplicant logic.**
- Configuration via Group Policy (GPO) or MDM (Intune) is identical.
- Both fully support the “User or Computer” authentication mode, which leads to this behavior.

**Windows vs. macOS:**

- **Windows:** Deeply integrated with **Active Directory**. The “User or Computer” authentication is a standard, built-in setting that is easily deployed via **GPO.** It handles the machine-to-user authentication handoff reliably.
- **macOS:** Fully supports 802.1X for both user and machine (certificate) authentication. However, its integration is less seamless than that of a domain-joined Windows client. To achieve a reliable machine-then-user authentication flow, you almost always need an **MDM** to push a configuration profile. Manual configuration on a Mac is more complex and less reliable.

**The Role of the NAC**

- The operating system acts only as the supplicant. The NAC (e.g., Cisco ISE, Aruba ClearPass, FortiNAC, or even basic Windows NPS)  is the decision-maker, while the switch functions as the enforcer.
- Basic RADIUS (e.g., Windows NPS): You might just have a policy such as “Allow devices in the ‘Domain Computers’ group.” In this case, the PC authenticates as the machine, and that’s it. The switch will always report the machine name, regardless of who logs in.
- Advanced NAC (e.g., Cisco ISE, Aruba ClearPass): These systems are designed for this purpose. They perform identity stitching.
    - The PC boots, authenticates as **host/PC-001** (machine authentication).
    - The NAC sees this, checks its posture, and places the switch port in a “Base Access” VLAN (VLAN 10).
    - The user **jsmith** logs in, and the PC re-authenticates as **jsmith@domain.com** (user authentication).
    - The NAC sees this new authentication from the same MAC address and “stitches” the identities: “Ah, jsmith is on PC-001.”

- The NAC then sends a **Change of Authorization (CoA)** command to the switch, instructing it to dynamically move the port to the “User Access” VLAN (VLAN 20). All without the port ever going down.

## Stale 802.1X user session scenarios

A stale 802.1X user session occurs when a user logs into a PC, authenticates to the network, and their identity is successfully recorded on the switch port. However, when that user logs out and a new user logs in, the PC’s 802.1X supplicant (network client) fails to re-authenticate and update the switch.

As a result, the switch and NAC (Network Access Control) continue to display the previous user’s identity.

## How to Fix This (and Prevent the Mismatch)

If the switch supports re-authentication, the fix must be with the NAC (RADIUS) server or the client PC configuration (GPO/MDM).
Here are the solutions, listed from most common to most ideal.

#### Solution 1: Enforce Re-authentication from the NAC

Configuration options instruct the switch, “Don’t use your own local timer; wait for the RADIUS server to tell you how long the session should last.” The NAC server is likely not sending a session timeout.

**The Fix:**

- Log in to your NAC (e.g., Cisco ISE, Aruba ClearPass, FortiNAC, etc.).
- Locate the **Authorization Profile** (or Policy) applied to your wired 802.1X data users.
- In that profile, set a **Session Timeout.** A common value is **28,800 seconds (8 hours)** or **3,600 seconds (1 hour).**

After the session timeout, the NAC will force the switch to re-authenticate the user. This updates the User-Name to the currently logged-in user, or falls back to machine authentication if no one is logged in, automatically cleaning up stale sessions.

#### Solution 2: Force Re-authentication from the Client

The Windows 802.1X supplicant may not be configured to re-authenticate when the OS user changes.

**The Fix:**

- Modify the GPO profile SSO settings to perform re-authentication when a user logs on, forcing the PC to re-authenticate as the new user immediately upon login.

This synchronizes the OS login event with the network authentication event, ensuring the switch always reflects the most current user.

**Solution 3: Simplify to Machine Authentication Only**

If you don't need to track individual users and only care that the device is a trusted corporate PC, you can disable user-level authentication entirely.

**The Fix:**

- Update the GPO to perform **"Computer authentication"** only.

The User-Name reported on the switch will always be the PC's hostname (e.g., host/PC1010). This may create a different kind of mismatch (PC name vs. OS user), but it will be consistent and will never show a stale username.

# Improving Network Security with Sepio's Asset Identity Feature

## Overview

Modern networks often rely on basic asset data, such as MAC and IP addresses, to monitor devices. While useful, this data alone does not reveal who is using the device, what the device actually is, or if it's properly authenticated. Sepio's Asset Identity feature bridges this gap by correlating device details with authenticated identity data directly from your network infrastructure.

## How Asset Identity Strengthens Security

### Auth-Integrated Asset Discovery

Sepio automatically polls network switches to retrieve authentication session data from the 802.1X implementation. This adds a high-trust identity layer to your asset inventory, mapping each device to its authenticated username, machine name, or MAC address.

### Improved Classification Confidence

With authentication details included (Username, Hostname, or MAC), Sepio's classifications are far more accurate. Access policies can be tied to verified identities, making it much harder for rogue or misconfigured devices to evade detection.

### Policy Enforcement

By viewing both "Status" (Authorized/Unauthorized) and "Domain" (DATA/VOICE), you can ensure your segmentation and authentication policies are being enforced consistently. Any device in a domain where it shouldn't be will stand out for immediate review.

## Identifying Security Gaps Using Sepio

### Unauthorized Device Detection

Use Sepio's Status field to instantly find devices that failed authentication or remain in a "Pending" or "Quarantine" state. Investigate these endpoints to prevent unauthorized network access.

### Policy Violation Alerts

The Domain field helps spot segmentation anomalies. For instance, a VoIP phone showing up in "DATA" instead of "VOICE" can signal a configuration issue or possible spoofing attempt by a threat actor. Rapid detection helps block lateral movement and targeted attacks.

### Real-Time User Mapping

If asset identity does not match expected users (as with a user/host mismatch detected on the network), Sepio flags potential security gaps which could be device sharing, cached credentials, or user spoofing. Teams can then audit authentication logs and endpoint management data to resolve discrepancies.

## Using Sepio to Improve Network Security

1. **Turn On Authentication Data Collection**
   Integrate Sepio with your switches, ensure 802.1X and MAB logging are enabled. Confirm that Sepio can connect to network infrastructure to poll session data.
2. **Use the Authentication Details Card**
   Sepio's UI presents a clear view of each asset's session status, identity, and domain. Use this card during troubleshooting to quickly focus on authentication issues rather than physical or Layer 2 problems.
3. **Regularly Audit Authorized Devices**
   Use Sepio to review devices with an "Authorized" status and cross-reference them with user and asset profiles. Confirm that all devices passing authentication truly belong to their intended users.
4. **Monitor the Domain Field**
   Validate that devices are appearing in their correct network segments (DATA for computers, VOICE for phones, etc.). Investigate anomalies immediately.
5. **Automate Alerts for Gaps**
   Using SOC/SOAR integration, alert your team whenever:
   - A device is authorized with the wrong user/hostname.
   - Assets appear in unexpected domains.
   - Authentication sessions reflect stale or inaccurate credentials.

# Application Visibility

## Application Visibility and Classification in Sepio

Sepio delivers enhanced application visibility, providing insights that go beyond traditional network Layers 1–3. By leveraging technologies embedded within the network infrastructure, Sepio performs Layer 7 inspection to classify application traffic and uses Protocol Discovery to precisely identify which protocols are running on network interfaces.

### What is Application Classification?

Application Classification is an intelligent mechanism that transforms raw data packets into actionable visibility by analyzing and categorizing network traffic based on the specific applications and protocols that generate it. Rather than relying solely on traditional Layer 3 (IP addresses) and Layer 4 (port numbers), Application Classification employs Deep Packet Inspection (DPI) to examine traffic at Layer 7 (the application layer). This capability is essential for identifying applications that use non-standard ports, dynamically assigned ports, web-based methods, or encryption.

While switch vendors integrate their own DPI solutions, Sepio's platform harnesses these native capabilities to provide a unified solution that supports all major vendors.

## How Application Classification Enhances Asset Classification in Sepio

Application Classification delivers significant value to Sepio customers by providing additional data points about asset behavior and improving the ability to validate asset classification based on actual activity. This comprehensive application data dramatically enhances device contextualization and automated asset profiling.

By leveraging the existing network infrastructure, customers eliminate the need for dedicated collectors for application monitoring. Sepio achieves this by using data collected directly from network devices.

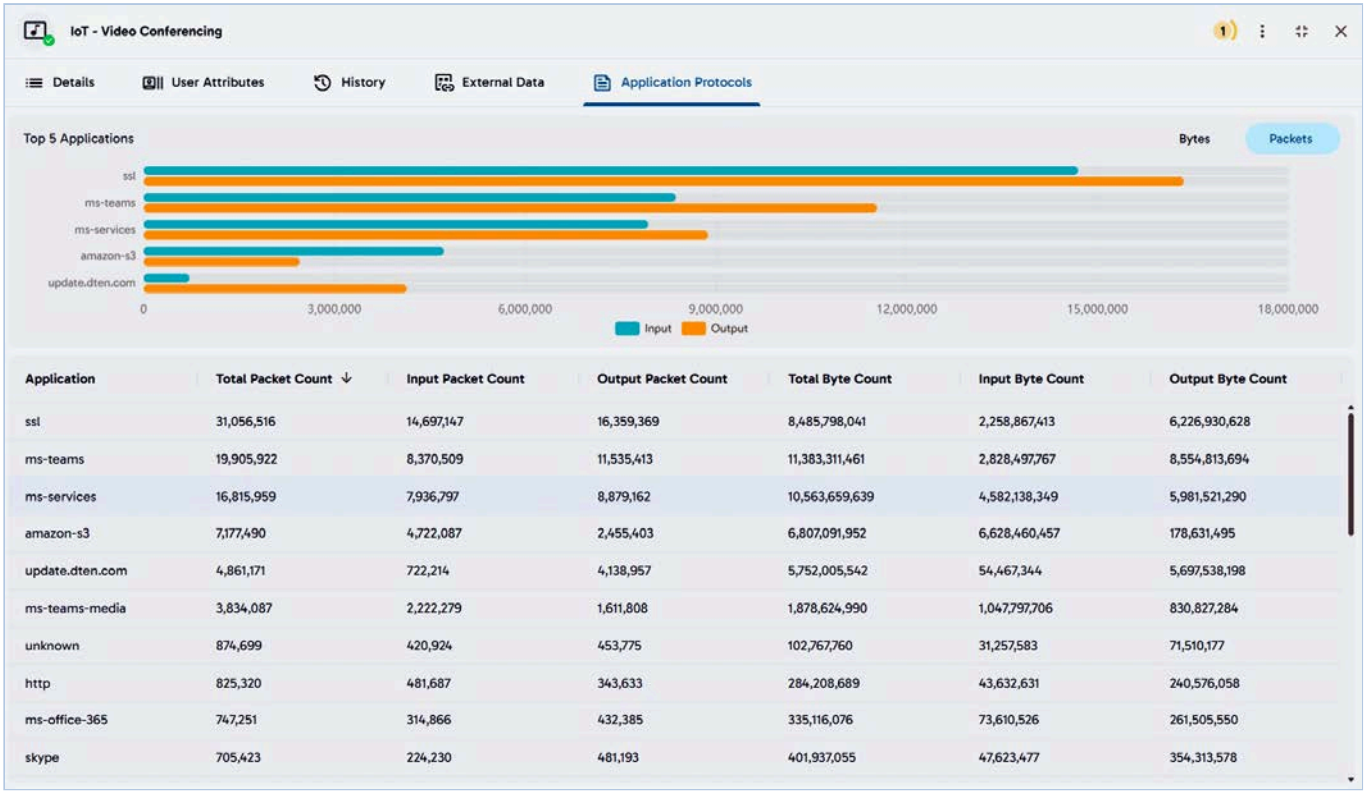
By analyzing the application traffic profile observed on a specific switch port, Sepio gains deep insight into the connected asset's function and role. This precise application-layer understanding significantly enhances Sepio's ability to accurately classify assets:

- **Behavioral Identification:** The composition of application traffic serves as a strong identifier of the device type. For example, traffic containing a high volume of Microsoft services (MS-Update, Windows Azure, MS-Services, and MS-Office-365) strongly indicates a Windows workstation or PC. Similarly, the presence of specific consumer protocols (like Skype and YouTube) combined with high packet counts is a strong indicator of an end-user device rather than a server, switch, or printer.
- **Higher Confidence Scoring:** The detailed data derived from Application Classification feeds directly into Sepio's analytical models, enhancing the confidence score for an asset's identity, type, and role.

## Key Benefits for Sepio's Platform

By leveraging native network technologies like Cisco NBAR, application classification offers several key benefits for the Sepio platform:

- **Granular Traffic Recognition:** Classify traffic accurately based on Layer 7 inspection (DPI), recognizing applications that might otherwise be masked by standard ports or encryption.
- **Enhanced Device Context:** Map observed application traffic to expected device roles to achieve highly accurate and detailed asset classification, directly informing device identity, behavior, and functionality.
- **Extensible Protocol Support:** Application recognition relies on a Protocol Pack of application signatures. This list can be regularly and easily updated without major system reconfigurations, ensuring continuous visibility as application landscapes evolve.
- **Customization Capabilities:** Define custom applications to identify and categorize internal, proprietary, or organization-specific traffic, ensuring all relevant activity is correctly classified.




| Application | Total Packet Count ↓ | Input Packet Count | Output Packet Count | Total Byte Count | Input Byte Count | Output Byte Count |
|---|---|---|---|---|---|---|
| ssl | 31,056,516 | 14,697,147 | 16,359,369 | 8,485,798,041 | 2,258,867,413 | 6,226,930,628 |
| ms-teams | 19,905,922 | 8,370,509 | 11,535,413 | 11,383,311,461 | 2,828,497,767 | 8,554,813,694 |
| ms-services | 16,815,959 | 7,936,797 | 8,879,162 | 10,563,659,639 | 4,582,138,349 | 5,981,521,290 |
| amazon-s3 | 7,177,490 | 4,722,087 | 2,455,403 | 6,807,091,952 | 6,628,460,457 | 178,631,495 |
| update.dten.com | 4,861,171 | 722,214 | 4,138,957 | 5,752,005,542 | 54,467,344 | 5,697,538,198 |
| ms-teams-media | 3,834,087 | 2,222,279 | 1,611,808 | 1,878,624,990 | 1,047,797,706 | 830,827,284 |
| unknown | 874,699 | 420,924 | 453,775 | 102,767,760 | 31,257,583 | 71,510,177 |
| http | 825,320 | 481,687 | 343,633 | 284,208,689 | 43,632,631 | 240,576,058 |
| ms-office-365 | 747,251 | 314,866 | 432,385 | 335,116,076 | 73,610,526 | 261,505,550 |
| skype | 705,423 | 224,230 | 481,193 | 401,937,055 | 47,623,477 | 354,313,578 |

Application Protocols

# About Assets

## Overview

In Sepio, Assets are devices that communicate at the physical layer over Ethernet (defined by the IEEE 802.3 standard), Wi-Fi (defined by the IEEE 802.11 standard), or USB, as defined by the Universal Serial Bus (USB) Specification, published by the USB Implementers Forum (USB-IF).

In other words, a Sepio **Asset** is anything that:

- can be connected to or disconnected from your organization's network infrastructure,
- is built into or added internally to a host.

## In Sepio Assets Include

A **Network Infrastructure** is a collection of **Network Elements (NEs)** that work together to run an IT network. In the Sepio platform, it includes Network Elements such as switches, controlled access points, assets that can be connected or disconnected to switch ports, and more.

Network Elements can be either **Supervised**, meaning that Sepio has the credentials to collect asset information such as AssetDNA, network information, etc., or **Unsupervised**.

A Sepio **Host** is any computer with a Sepio Agent that communicates with the Sepio platform. You can connect or disconnect Assets, such as USB devices, mice, and others, to or from a Host via a USB connection.

A Host has **Peripherals**, which are components built into it or devices connected to it.

In Sepio, a **Device** is composed of at least two Peripherals. For example, a wireless mouse is composed of the mouse itself and its USB receiver.

You can connect or disconnect Assets, such as servers, computers, switches, IoT or OT Assets, and others, to or from your organization's network infrastructure via an Ethernet connection.

There are different asset types, and for each type, Sepio collects different data elements. These elements are presented in the user interface in addition to metadata information, which is stored and used by Sepio for additional calculations and tasks. The presentation of the data depends on the asset type and the method by which it is connected to your organization and its network.

The list below summarizes the information collected and presented by the Sepio platform.

**Note:** In some cases, when not all data elements are available, the UI will indicate that the data is not available (N/A).

## Device Identity & Classification

- **Type** (Sepio Classification)
- **Asset** (Name or Sepio category)
- **MAC Address**
- **Vendor**
- **Model** (For Supervised network Infrastructure)
- **Serial Number** (For Peripherals and Supervised network switches)
- **UUID** (For Sepio Host Agents)
- **PID** (For Peripherals)
- **VID** (For Peripherals)
- **Approved** (USB/peripherals status)
- **Asset DNA** (Details of devices connected to the network)

## Network & Connection Details

- **IP Address**
- **Connected VLAN**
- **Connected SSID** (For Wi-Fi devices)
- **Location** (Network location: switch, port, managing WLC for AP, Host for peripheral)
- **SNMP Location** (Physical location of network infrastructure)
- **Peer MAC Address** (For Wireless LAN Controllers configured in HA mode)
- **Additional MAC Address**
- **Transport** (How Sepio collected the data)
- **Connection Type** (Network, Wi-Fi, USB)
- **Redundancy Mode** (Supervised network assets)
- **Application Protocols**
- **PoE Info** (Power over Ethernet information from the switch)
- **DP Info** (Discovery Protocol data reported by the asset to the switch)
- **Scope**
- **Domain** (Logical entity managed by the Scan Engine)
- **CPU Environment** (Supervised Network devices)
- **CPU Utilization** (Supervised Network devices)
- **Boot Info** (Supervised Network devices)
- **Hardware Version** (Supervised Network devices)

## Security, Authentication & Status

- **Policy** (Name of relevant policies associated with this device)
- **Status** (Connected or Disconnected)
- **Authentication Identity** (Device identity if available from network infrastructure)
- **Authentication Status** (If available from network infrastructure)
- **Authentication Domain** (If available from network infrastructure)
- **Risk** (Device's Risk Score)
- **Risk Sub Indicators** (Detailed names of Risk Indicators by family)
- **External Sources** (If collected by Sepio)
- **Tags**
- **User-Defined attributes**
- **Agent Policy name**
- **Blocked Assets**

## Administrative & Operational Metrics

- **Group**
- **First Seen**
- **Last Seen**
- **Last Updated** (For supervised Assets)
- **Agent Version** (For Sepio Agents)
- **Firmware** (For supervised devices)
- **Software** (For supervised devices)
- **Product Info**
- **Deployment** (For Sepio Agents)
- **Mode** (For Sepio Agents)
- **Version ID** (For Sepio Agents)
- **Number of Active Ports** (Supervised network devices)
- **Number of Total Ports** (Supervised network devices)
- **Scan Priority** (Supervised network devices)
- **Image** (Supervised network devices)
- **Number of Assets** (Supervised network devices)
- **CVE ID** (Supervised network devices)

## Related Topics

- About Assets Visibility Views
- Opening the Assets Visibility Views
- Discovered Assets View Interface

## Asset Actions

- Managing Discovered Risky Assets
- Sorting Searching and Filtering Assets
- Adding and Deleting Tags
- Exporting Assest Details to CSV or PDF

# About the Assets Visibility Views

The Platform provides three built-in Asset views, and enables creating custom views.
The built-in Asset views are:

## Discovered Assets

This view displays all the Assets in the platform. In the Discovered Assets view, you can:

- Set asset status
- View asset risk indicators and details
- Filter assets
- Add tags to assets
- Drill down to view peripherals and port levels

## Hosts

The Hosts view displays hosts within the platform. A host consists of:

- **Devices** – Comprising at least two peripherals (e.g., a wireless mouse and its USB receiver).
- **Peripherals** – Components either built into a host or connected to it.

In the Hosts view, you can:

- Set statuses for hosts, devices, and peripherals
- View host risk indicators and details
- Set a host mode
- Filter hosts and peripherals
- Add tags to hosts and peripherals
- Drill down to view devices and peripherals

## Network Infrastructure

The Network Infrastructure view displays network infrastructure assets, such as switches and wireless LAN controllers. In this view, you can:

- Set network equipment (NE) status
- View NE indicators and details
- Filter NEs
- Add tags to NE/s
- Drill down to port level
- Set port status

## Related Topics

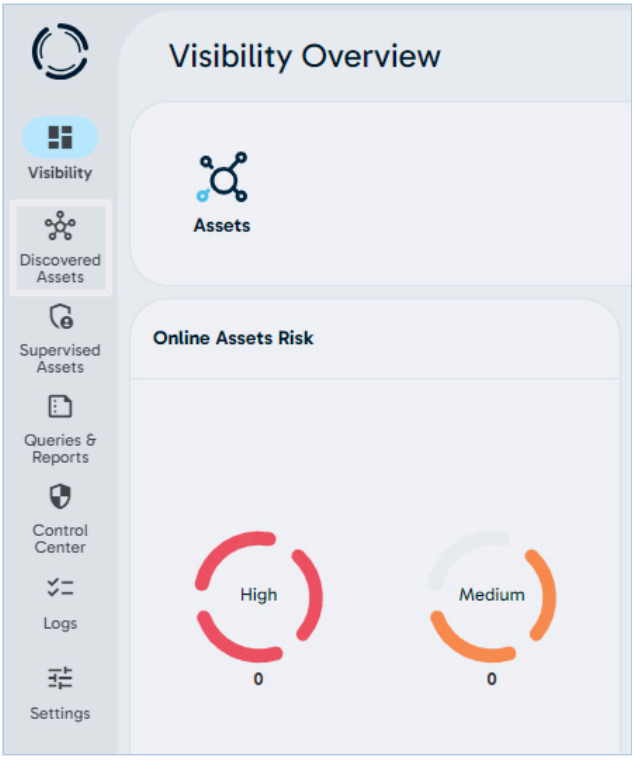
- Opening the built-in Assets Visibility Views
- Discovered Assets Visibility View Interface
- Creating and Opening a Custom View

# Opening the Assets Visibility Views

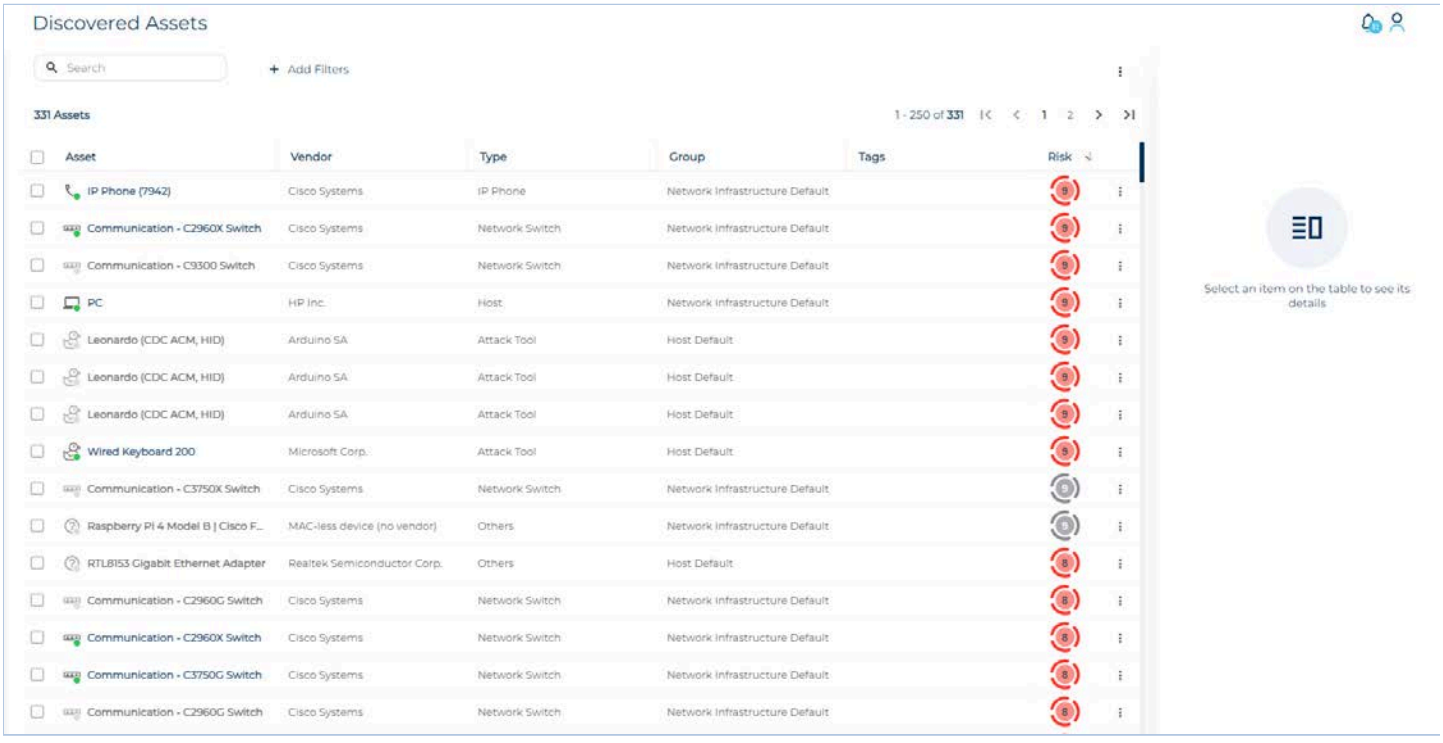
## Open the Discovered Assets View

To view discovered assets:

- **From the Sepio menu (navigation bar)**, select **Discovered Assets.** This will provide a visibility overview of all discovered assets.




Sepio menu (navigation bar)

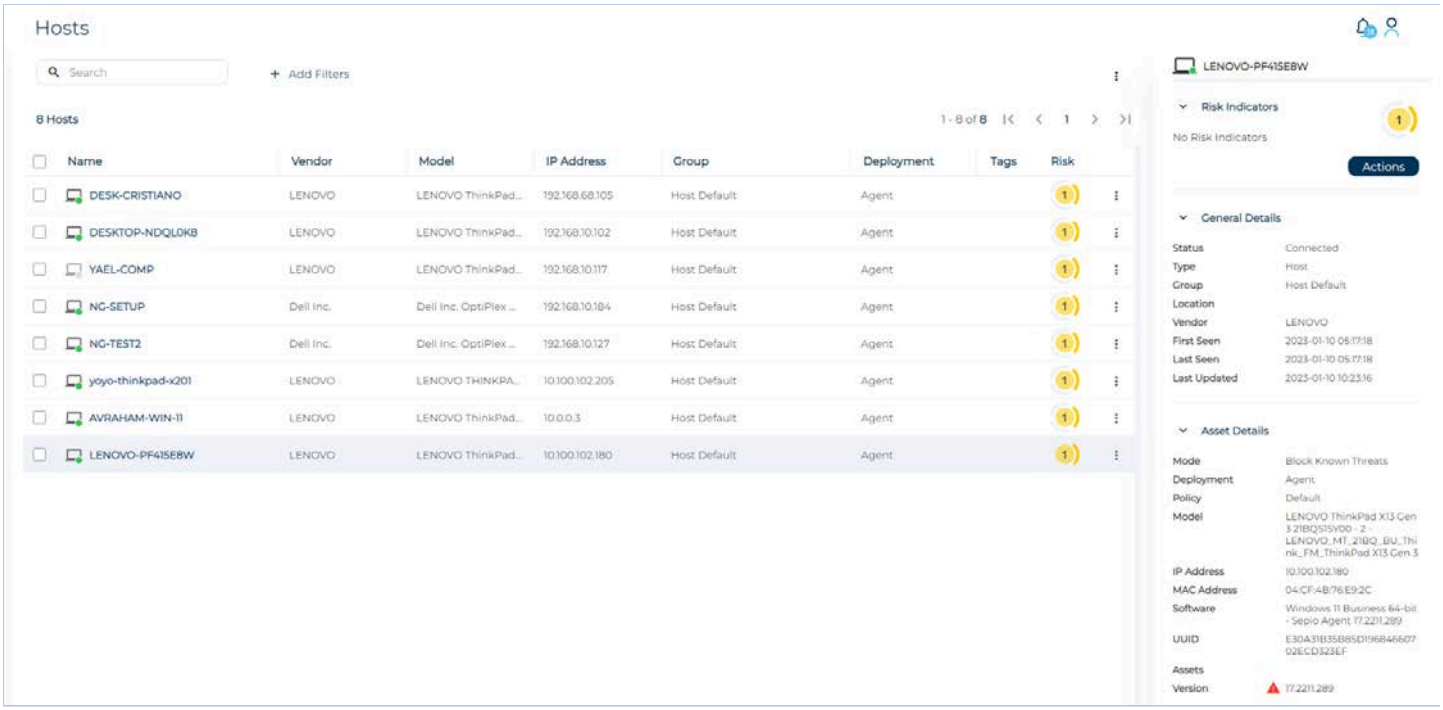



Discovered Assets View

## Open the Hosts View

To view hosts under supervision:

- **From the Sepio menu (navigation bar)**, select **Supervised Assets -> Hosts.** This will display the **Hosts View**, offering details on all supervised hosts.

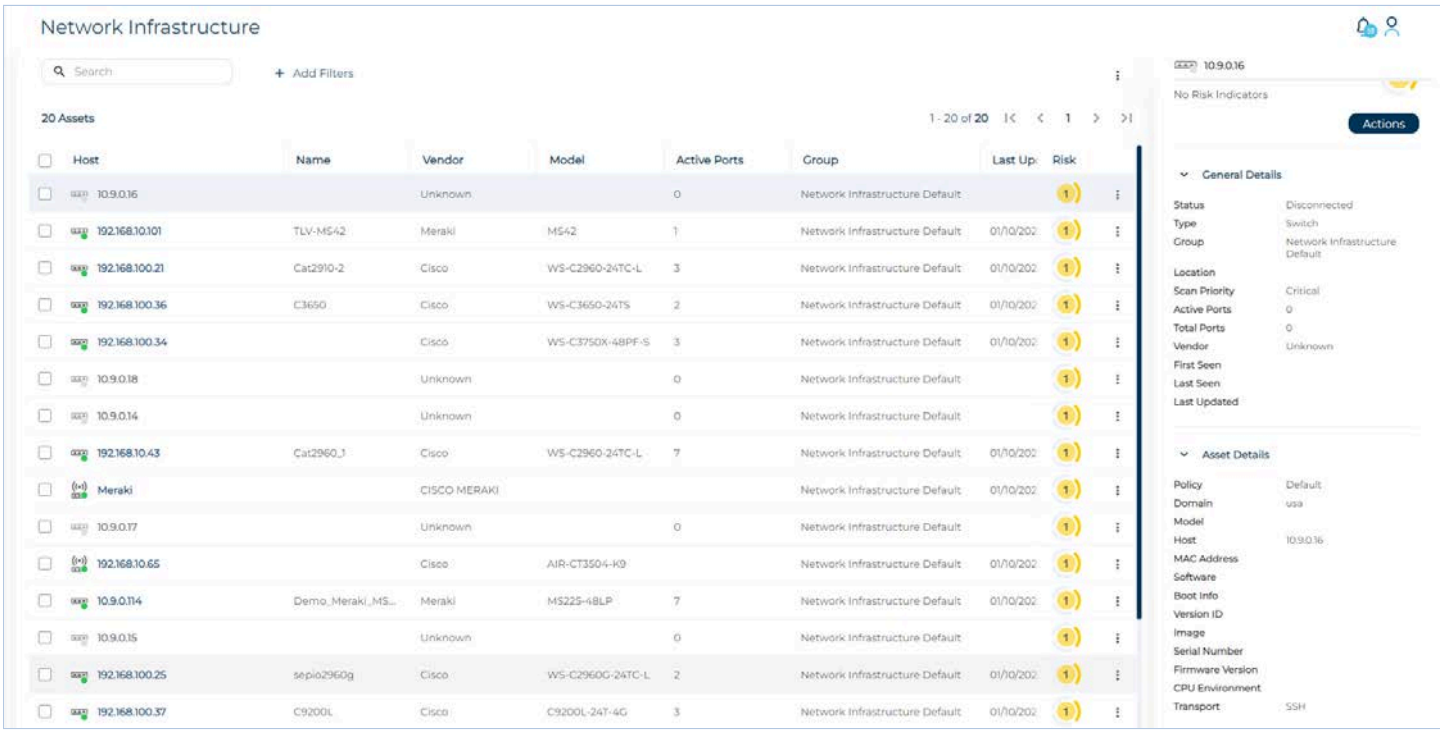



Hosts View

## Open the Network Infrastructure View

To view the network infrastructure:

- **From the Sepio menu (navigation bar)**, select **Supervised Assets -> Network Infrastructure.** This will open the **Network Infrastructure View**, allowing insight into the managed network infrastructure components.




Network Infrastructure View

# Customized Views

## Related Topics

- Customized Views
  - Creating and Opening a Custom View
  - Customized Table View

# Creating and Opening a Custom View

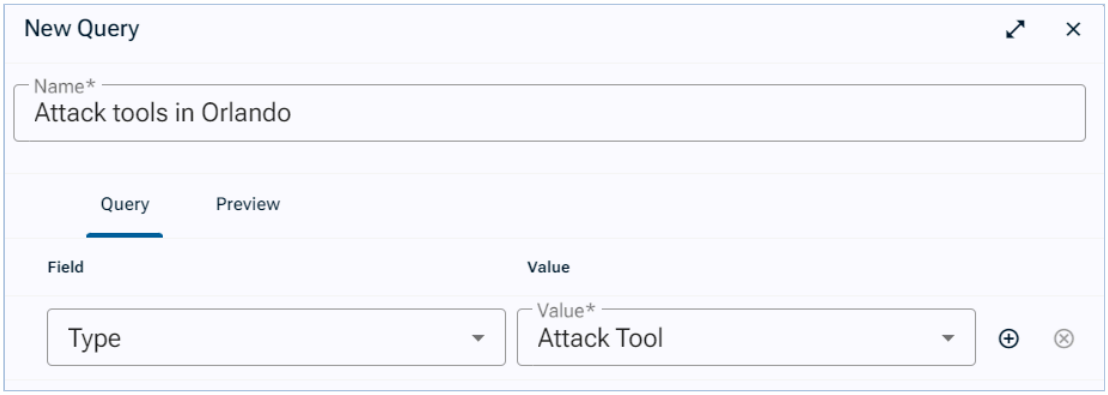
## Create a Custom View Using Queries

A custom view is a query stored in the Platform that returns specific results. By creating and saving these queries, you can generate custom views for future use.

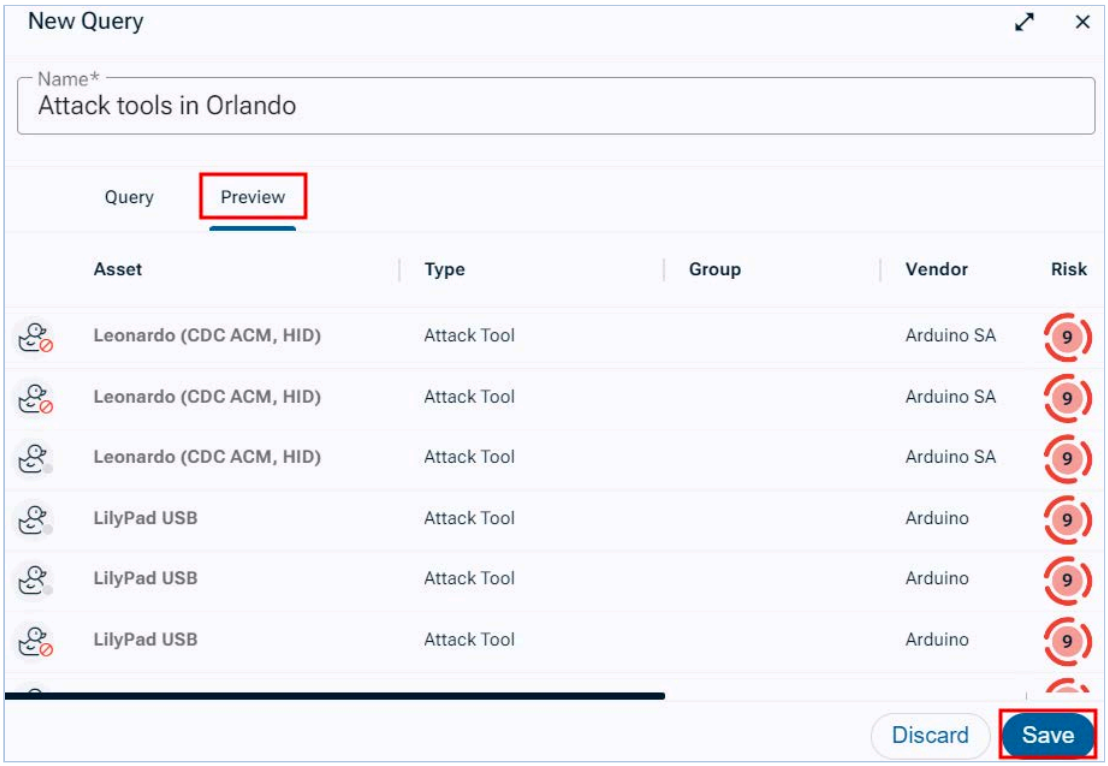
- From Sepio menu select **Assets Visibility** ->**Queries**
- Click **+ New Query**



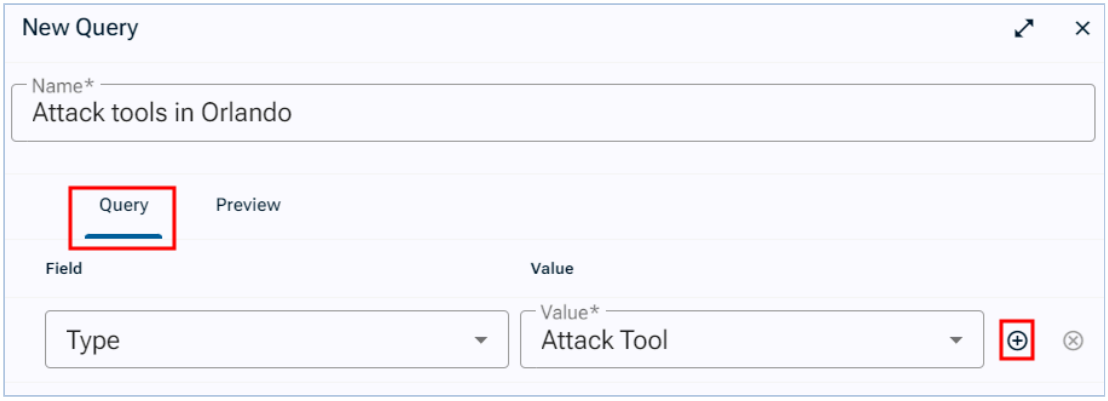

- Enter and select the following:
  - Meaningful query name
  - Select a query type
  - Select a value



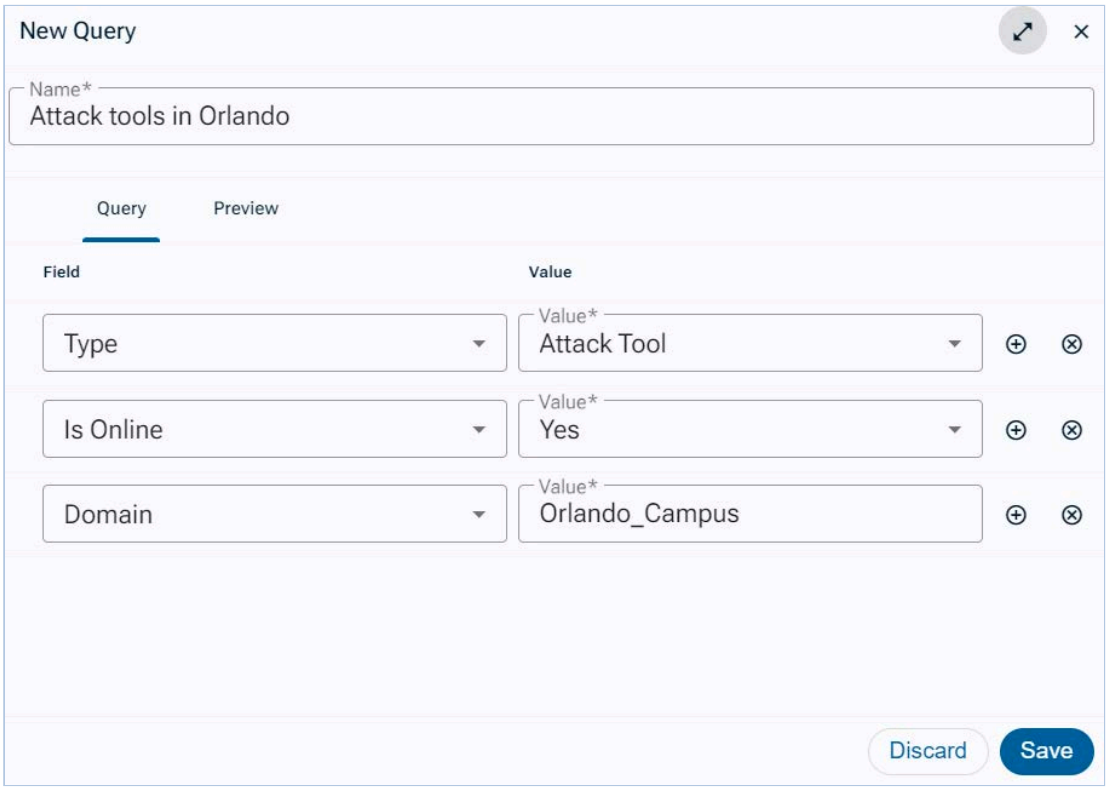

- Click **Preview** to view the results, then click **Save.**




- Or, click **Query**, then add more queries to this view.




- Click **Save.**




## Open a Custom View

- From Sepio menu select **Assets Visibility ->Queries**
- In the **Queries** list click ▷ next to the query which results you want to view.




Queries

## Edit a Custom View

- From Sepio menu select **Assets Visibility ->Queries.**
- In the **Queries** list, click ⋮ next to the query to edit, then select **Edit.**
- Edit as required, then click **Save Changes.**

## Delete a Custom View

- From Sepio menu select **Assets Visibility ->Queries.**
- In the **Queries** list, click ⋮ next to the query to delete, then select **Delete.** A message is displayed, click **Delete.**

## Customized Table View

It is possible to customize the different asset view tables by editing each table setting. Sepio Security administrators can create their most useful views by adding, removing, or reordering different table columns. The views are saved for every administrator.

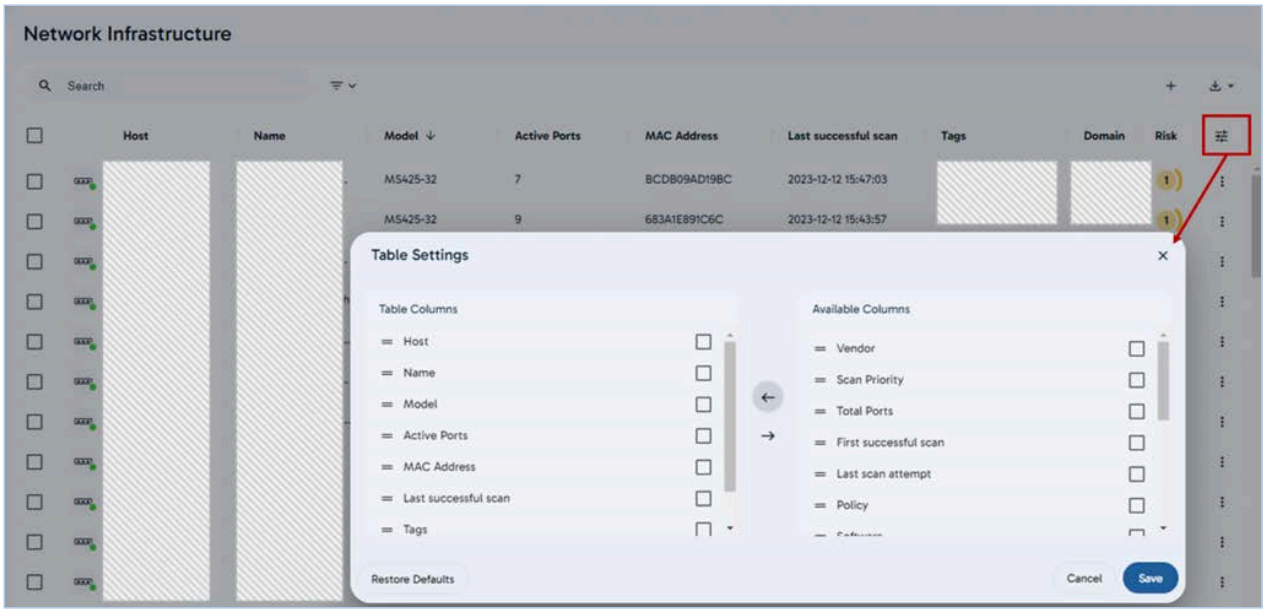



Table settings

# Visibility Views Interface Description

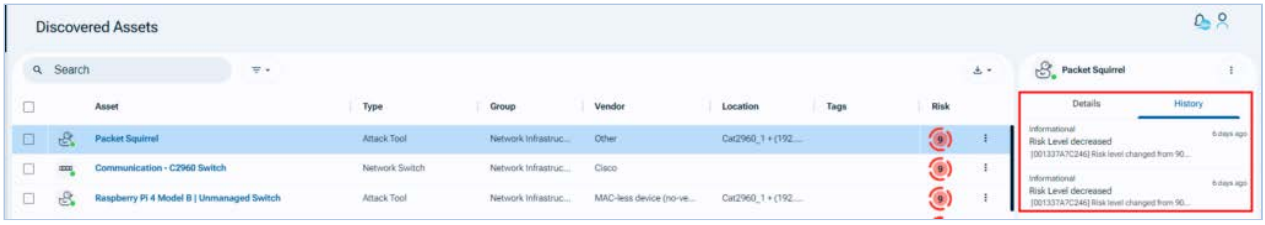
# Discovered Assets Visibility View Interface

## Discovered Assets Visibility View with Details Tab Open




Discovered Assets – Details tab

## Discovered Assets Visibility View with History Tab Open




Discovered Asset – History tab

## Discovered Assets Table

| Column | Description |
|---|---|
| Asset | Name of the Asset |
| Vendor | Vendor name of the Asset |
| Type | Type of the Asset |
| Group | The logical group the Asset belongs to |

| Column | Description |
| --- | --- |
| Tags | You use Tags for filtering Assets. You add tags in the Tags Management tab, or in the Assets Visibility views. |
| Risk | The Asset Risk Score |
| Actions  | ◦ Enables you to change a Risky Asset status<br>◦ Enables you to add and delete Tags |

## Risk Indicators

| Field | Description |
| --- | --- |
| Risk Indicator Score | Displays the Risky Asset Score |
| Risk indicator group | The Risk Indicators groups that make up a given Asset potential risk to your organization. |

## Asset General Details

| Column | Description |
| --- | --- |
| Type | Type of the Asset |
| Group | The logical group the Asset belongs to |
| Location | Asset location in a Host. Click the Asset link to display its Host |
| Vendor | Vendor name of the Asset |
| First Seen | Time and date the Asset was first detected by Sepio |
| Last Seen | Time and date the Asset was last seen in the platform |

## Asset Details

| Column | Description |
|---|---|
| Policy | The policy applied to the Asset |
| Model | Asset model information |
| IP Address | IP address of the Asset |
| Manufacturer | Name of the Asset manufacturer |
| MAC Address | The Asset MAC address on the network |
| Software | Asset software version information |
| Product Info | Miscellaneous Asset information |
| VID/PID | A USB Asset that is connected to a Host identifies itself by its VID/PID combination. A VID is a 16-bit vendor number (Vendor ID)<br>A PID is a 16-bit product number (Product ID)A Host uses the VID/PID combination to find the drivers (if any) that are to be used for the USB Asset |
| Serial Number | The serial number of the Asset |
| Approved | Asset status |

## Asset History

Display an Asset historical events.

# Assets Actions

## Related Topics

- Assets Actions
  - Managing Risky Assets
    - Managing Discovered Risky Assets
      - Blocking Peripherals
  - Displaying Assets Details
    - Displaying Discovered Asset Details
    - Displaying an Asset Historical Events
  - Sorting, Searching and Filtering Assets
  - Adding and Deleting User Defined Attributes
  - Adding and Deleting Tags
  - Exporting Asset/s Details to a CSV or PDF

# Managing Risky Assets

## Related Topics

- Managing Risky Assets
  - Managing Discovered Risky Assets
    - Blocking Peripherals

# Managing Discovered Risky Assets

## Overview

Each Risky Asset has a status, which you can change according to your requirements.
You can change a single Risky Asset status, or multiple Risky Assets statuses simultaneously.

## Accepting a Single Risky Asset

**In the Discovered Assets table:**

**In the Discovered Assets view, on the right side pane:**

## Accepting Multiple Risky Assets

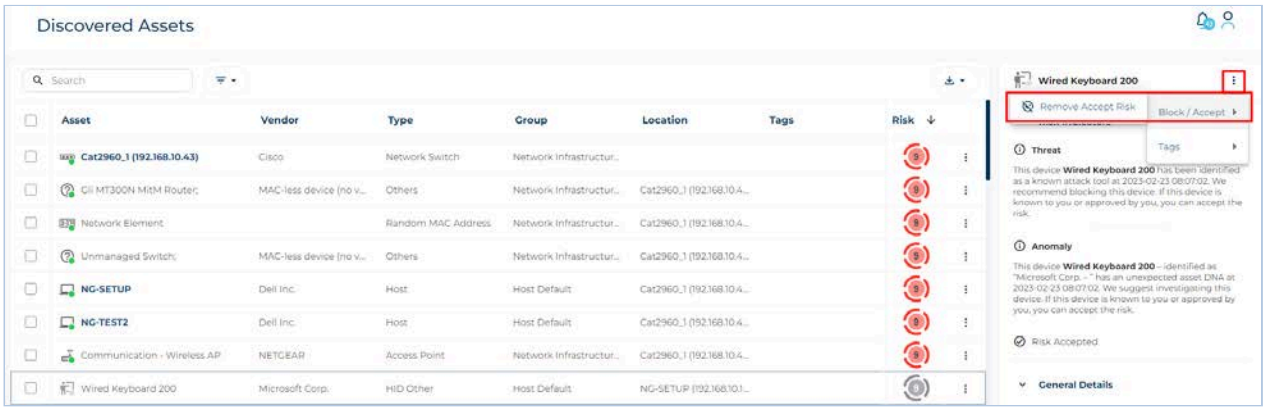
**In the Discovered Assets view:**

**To accept all multiple Risky Assets on a page, in the Discovered Assets view:**

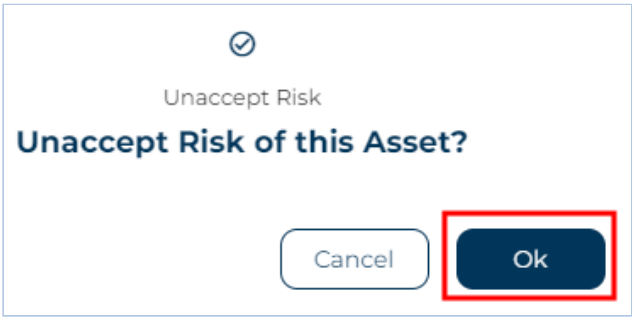
## Removing “Accept” Status from a Risky Asset

To remove the Accept status from a risky asset in the Discovered Assets view, follow these steps:

1. Open the Discovered Assets view.
    - Access the view where all discovered assets are listed.
2. Click on the row containing the asset.
    - Locate and select the row corresponding to the risky asset.
3. On the right-side pane, click the icon, then select **Block/Accept** -> **Remove Accept Risk**.
4. Confirm the action.
   A confirmation message will appear. Click **OK** to proceed.




Remove Accept Risk

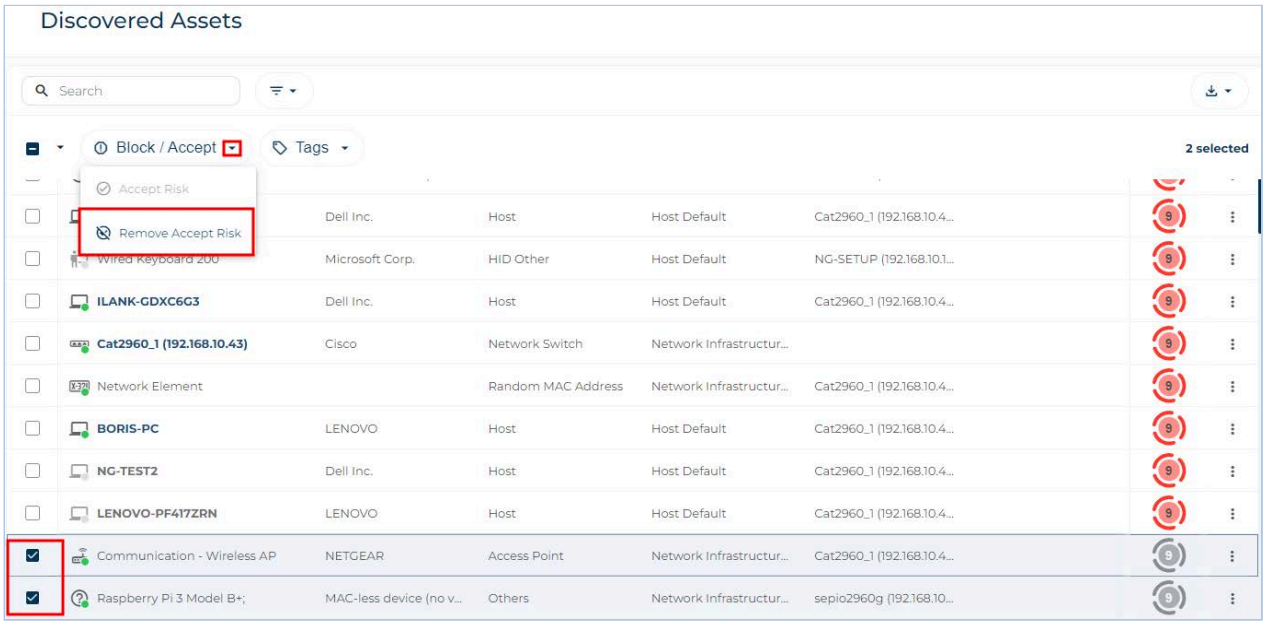



Click OK to proceed

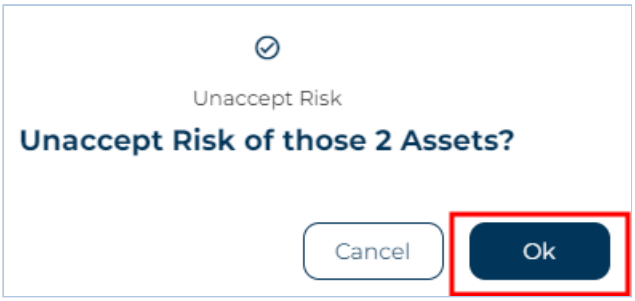
## Removing “Accept” Status from Multiple Risky Assets

To remove the **Accept** status from multiple risky assets, follow these steps:

1. Open the Discovered Assets view.
    - Access the view where all discovered assets are listed.
2. Select all the Assets
    - Check the risky assets you want to modify.
3. Click on **Block/Accept**.
    - From the available options, select **Remove Accept Risk**.
4. **Confirm the action.**
    - Click **OK** to proceed.




Remove Accept Risk

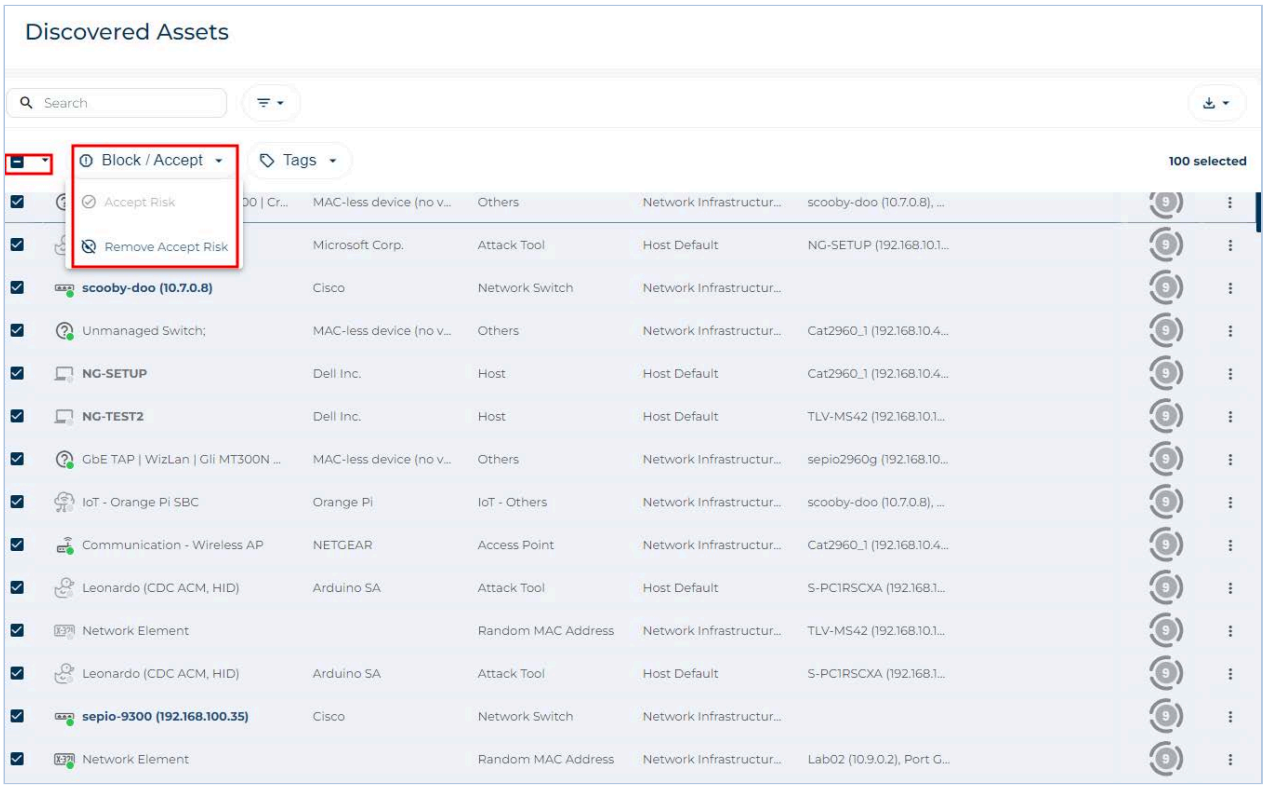



Click OK to proceed

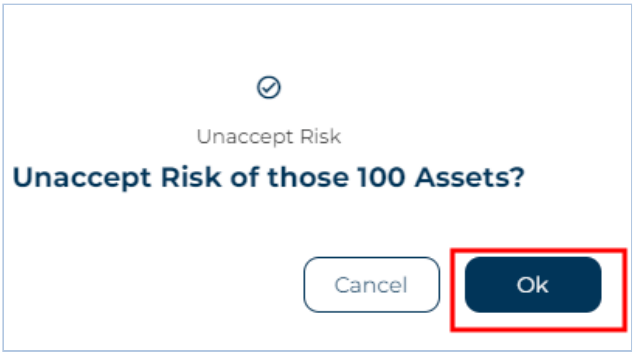
## Removing “Accept” Status from All Risky Assets on a Page

To remove the **Accept** status from all risky assets, follow these steps:

1. Open the Discovered Assets view.
    - Access the view where all discovered assets are listed.
2. Select all the Assets on the Page as shown below.
3. Click on **Block/Accept**.
    - From the available options, select **Remove Accept Risk**.
4. **Confirm the action.**
    - Click **OK** to proceed.




Remove Accept Risk




Click OK to proceed

# How to Block a Peripheral Device

## Overview

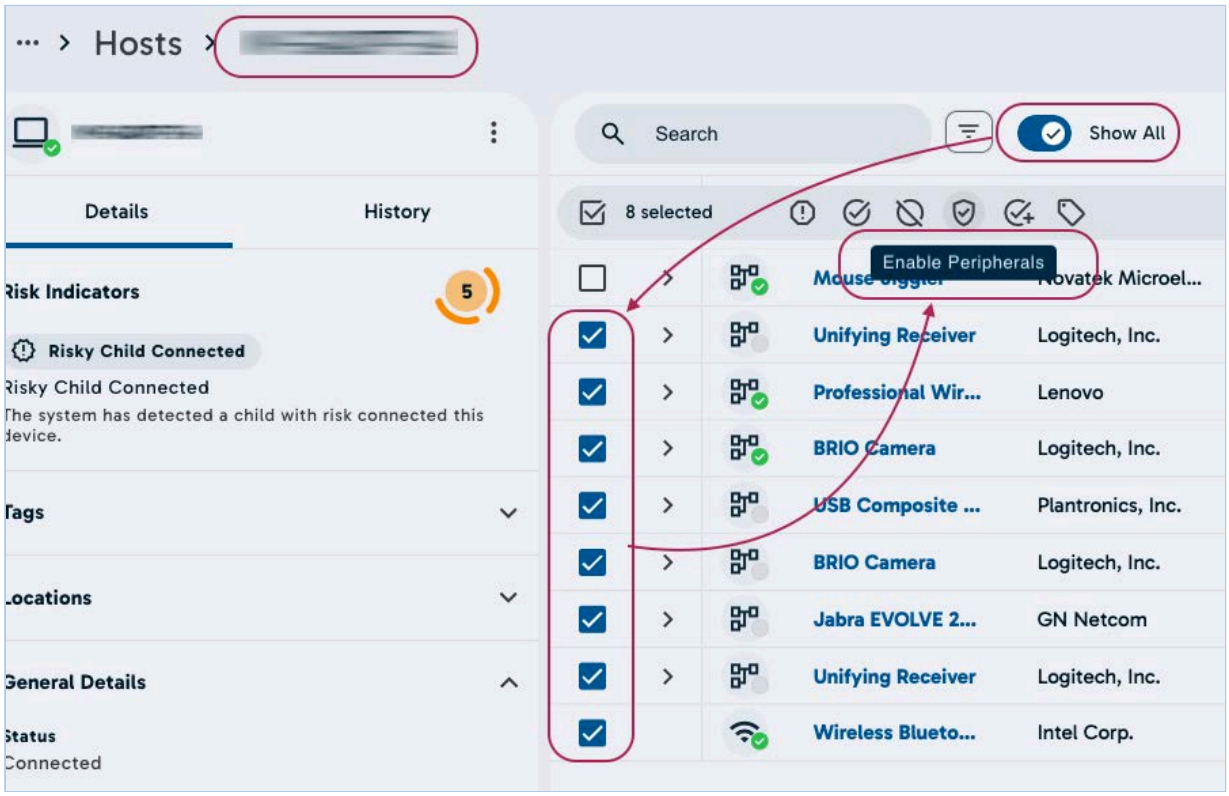
This guide provides a method to block a **specific** peripheral device on an **endpoint** using Sepio's Agent in Armed Mode.

## Scenarios Where This Method May Be Useful

- **Restrict Access to Certain Peripherals**
  Block peripherals or media devices but allow others. This applies for exposed sensitive endpoints such as:
  - Kiosks
  - ATMs
  - Point of Sales (POS).
- **Enforce Organizational Policies**
  Block specific peripheral that violates organization policies, such as:
  - Mouse Jigglers
  - Unapproved Bring Your Device (BYOD) peripherals
- **Control Media or Storage Devices**
  - Restrict access to specific media or storage devices while allowing others

## Example Scenario: Blocking a Mouse Jiggler on a Specific Endpoint

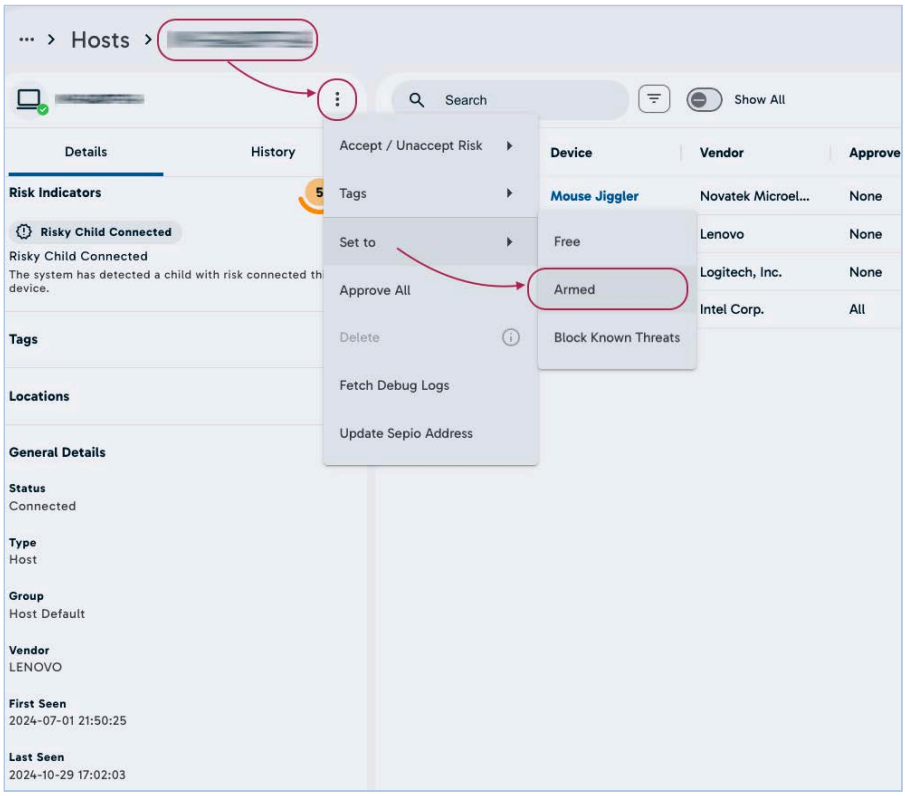
1. **Approve All Devices Except the Mouse Jiggler**
   - Use the **Show All** button to review and capture the device history on the endpoint.
   - Approve all devices on the endpoint except the Mouse Jiggler.




Use **Show All** button

2. **Change the Agent's Mode to Armed Mode**
    - Switch the agent to Armed mode.
    - After switching, a small yellow mark will appear on the Jiggler icon.

**Note:** In Armed mode, any unapproved device will be automatically blocked unless explicitly enabled.



Change agent's mode to Armed

### 3. If Needed, Change the Agent Mode Back to BST or BKT

**Note:** For more information about the agent in Armed mode, refer to the Agent Deep Dive.

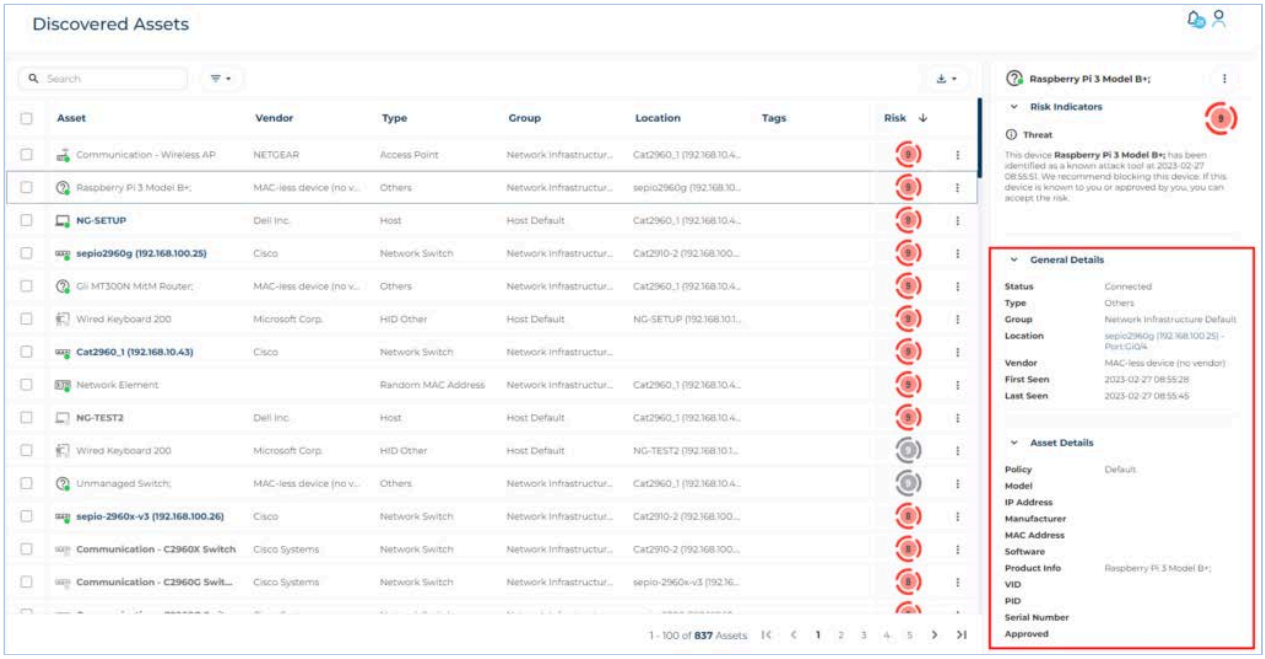
# Displaying Assets Details

# Displaying Discovered Asset Details

Sepio platform provides diverse discovered Asset and general details as listed in Discovered Assets View Interface.

To display general and Asset details in the Discovered Assets view:

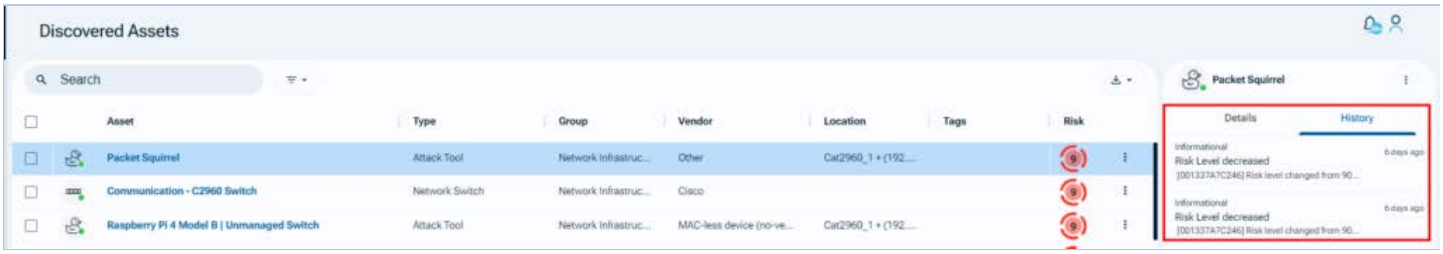
1. Open the Discovered Assets view.
2. Click the row containing the Asset which details you want to display.



# Displaying an Asset Historical Events

To display an Asset historical events in the Discovered Assets view:

1. Open the Discovered Assets view.
2. Click the row containing the Asset which historical events you want to display, then click the History tab.




Asset history events

# Sorting, Searching and Filtering Assets

There are a few things that you can do that will help you scan, find, and limit Assets on a list or in a table. These include sorting, searching, and filtering. You can apply some or all of these simultaneously to quickly find or analyze your data. You perform the actions listed in this topic in Assets Visibility views.

## Sorting

Sorting helps you quickly get an overview of your assets. For example, you could sort your Assets by Vendor, Type, or Risk indicator to get the overview you need.

**To sort a list:**

- Click a column header text to toggle between ascending and descending order.

## Rearranging the Order of Columns in a Table

**To rearrange the order of columns in a table:**

- Drag a column header and drop it in the position that you want.

## Searching

At the top of each list page, there's a Search action that provides a quick and easy way to reduce the Assets in a list and display only those Assets that contain the data that you're interested in seeing.

**To search for specific Assets:**

- At the top of the view, in the search box, type the text that you're looking for.

> **Note:** Generally, search will attempt to match text across all fields. It doesn't distinguish between uppercase and lowercase characters (case-insensitive) and will match text placed anywhere in the field, at the beginning, end, or in the middle.

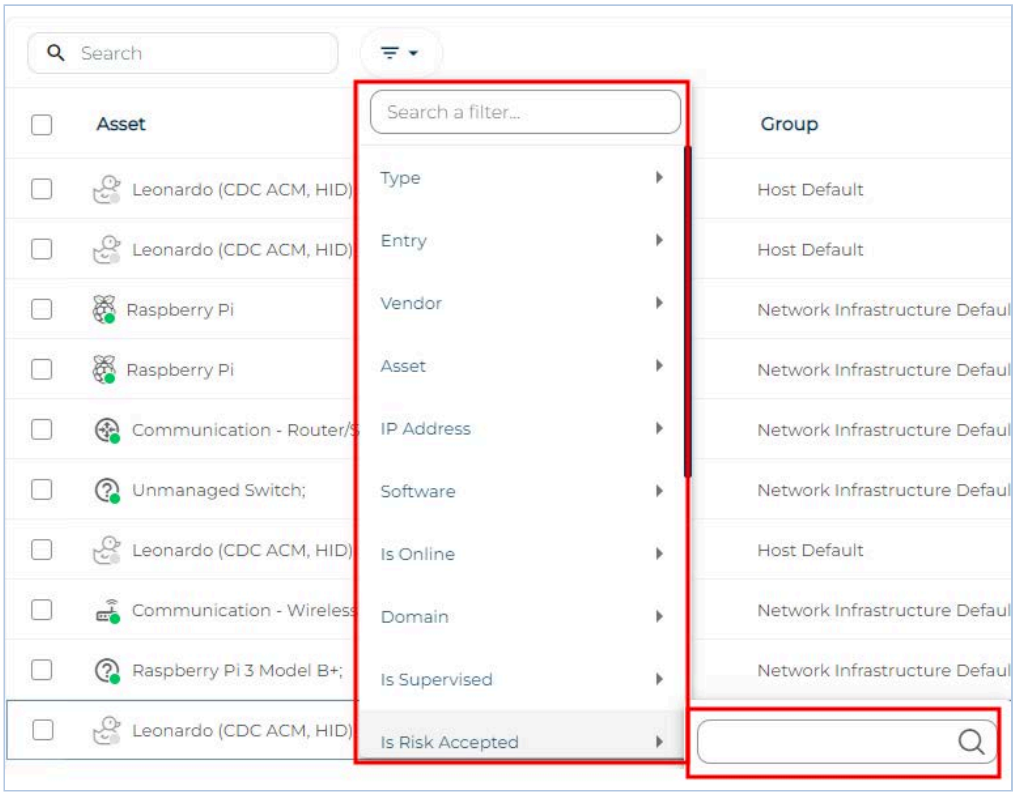
## Adding and Clearing Filters

Filtering provides a more advanced and versatile way to control which Assets are included in a list. You can customize the filters by using Tags.

**Note:**You can use multiple filters to narrow down your results.

## Add a Filter

1. At the top of the view, click 




.....

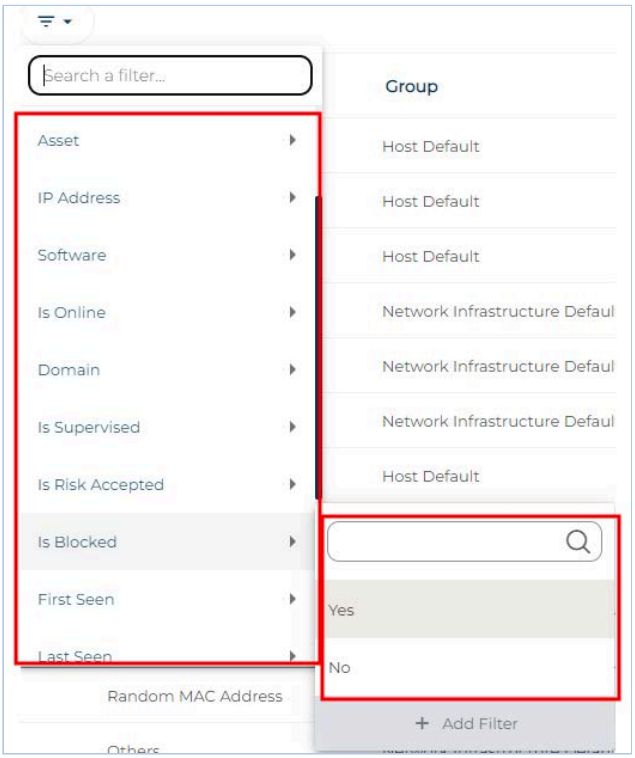
2. Enter a filter name in the search box, then enter or select the sub filter values, if required select Add Filter, otherwise select a filter value.




.....

– Or –

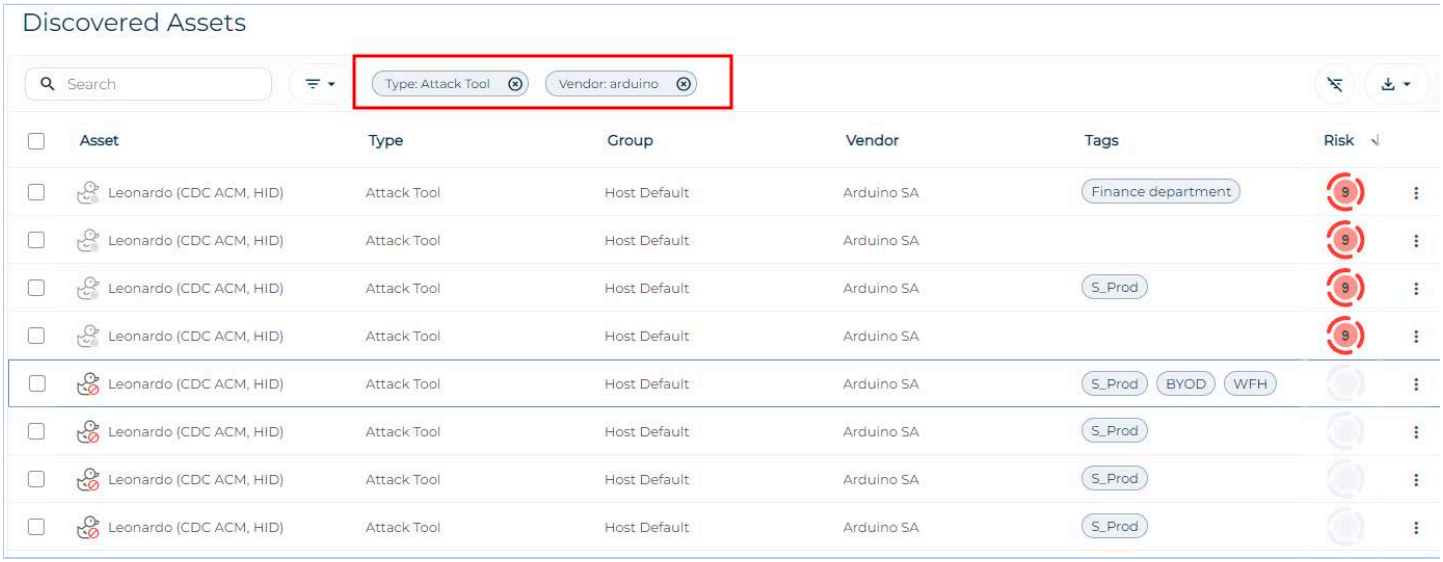
Select a filter name from the filter list, then enter or select the sub filter values.




.....

The filter/s appear/s at the top of view.

After adding a filter the list is filtered accordingly.




Discovered Assets

## Remove a Filter

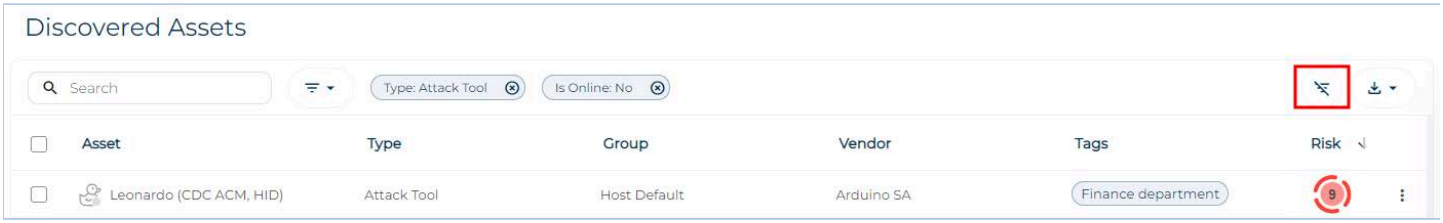
At the top of the view, click ⊗ next to the filter to remove.




Remove a filter

## Remove Multiple Filters at Once

At the top of the view, click .




Remove Multiple Filters at Once

## Filtering with Tags

Tags enable you to customize the Sepio Platform.

You can add and delete Tags in the Assets Visibility views and in the Tags Management tab. You can edit Tags in the Tags Management tab.

## Related Topics

- Managing Tags
- Adding and Deleting Tags

# Adding and Deleting User-Defined Attributes

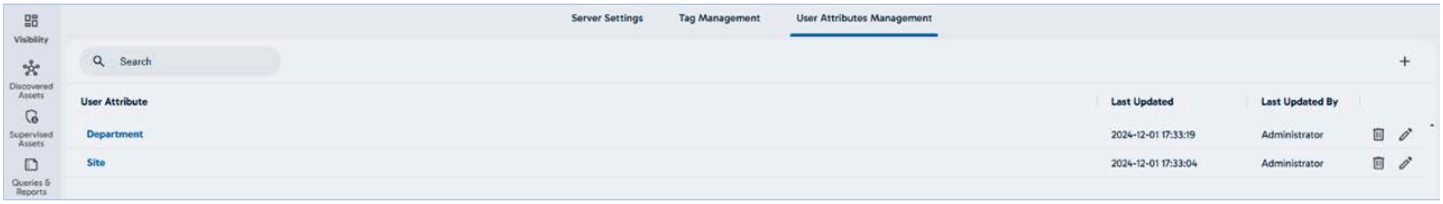
## User Attributes for Assets

Like their name suggests, the user attributes for assets are created by the Platform Administrators to define custom attributes for assets. It extends the list of pre-defined attributes that are provided by default.
These user-defined attributes are text-based key-value fields that apply to all assets and are accessible in the asset details panel. Additionally, these attributes can be displayed as columns in asset lists, used for sorting and filtering, and included in Sepio's reports.
Both Keys and attributes values can be created using ASCII characters. While values are case-sensitive, the keys are not.

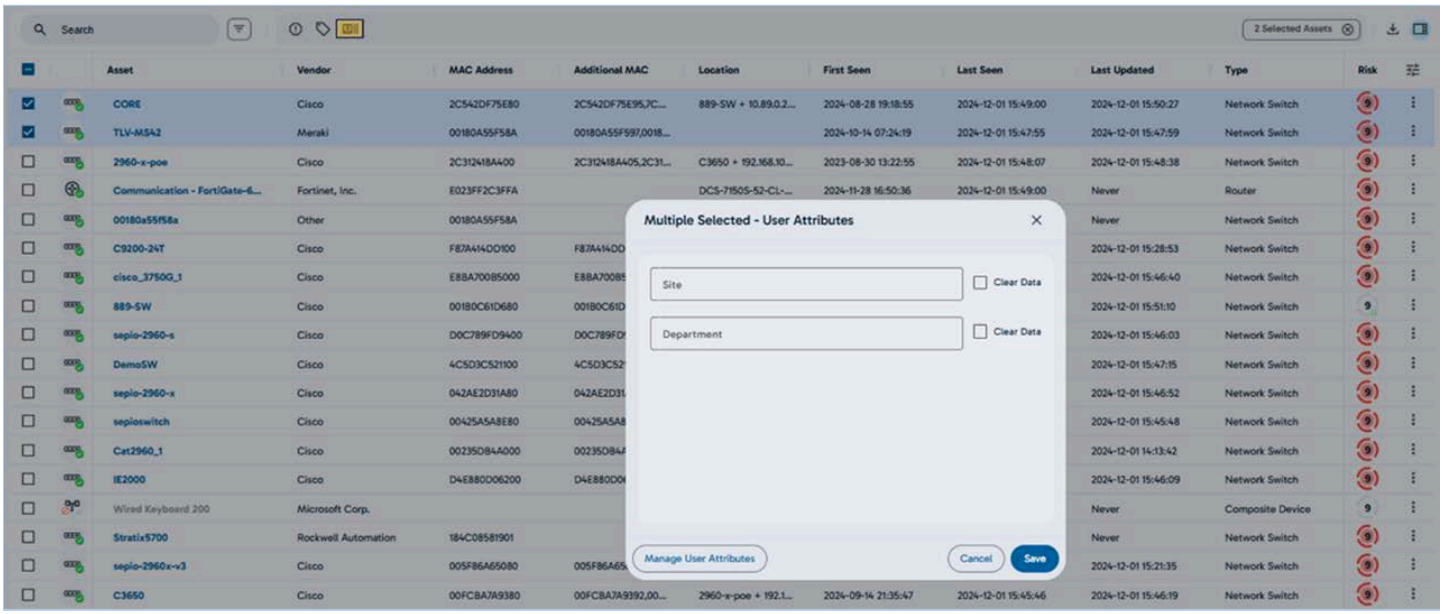
### What is the Difference Between Tags and User Defined Attributes?

Tags provide "marks" and are useful to provide fixed and simple context to assets. It is possible to create and remove tags, search and create policies for auto-tagging.
User Defined Attributes are much more sophisticated and powerful and are created to extend the definition of an asset. User Defined Attributes are great for custom integration with external systems.

The creation of new attributes is performed in the **Settings** -> **Server** -> **User Attributes management** tab. There is no limit on the number of attributes that can be defined.




Managers or Administrators can manage user attributes by navigating to the User Attributes Management tab under **Settings** -> **Server**, where they can add, edit, or remove attributes.




To edit user attribute values, **select the desired assets**, click the **button in the upper ribbon** to open the User Attribute modal, modify the attributes, and **click Save.**




You can display assets located at the LIS or ROC sites.

# Adding and Deleting Tags

You use Tags for filtering Assets. Filtering provides a more advanced and versatile way to control which Assets are included on a page.
After adding Tag/s to Assets, which you do in the Tags Management tab, or in the Assets Visibility views, you can filter the Assets page using those Tags.
You add and delete Tags in the Assets Visibility views. You edit Tags in the Tags Management tab.

#### Add Tag/s to a single Asset

#### Delete Tag/s from a Single Asset

#### Add Tag/s to multiple Assets

#### Delete Tags from multiple Assets

## Related Topics

- Managing Tags
- Sorting, Searching and Filtering Assets

# Exporting Asset/s Details to a CSV or PDF

You can export:

- a single Asset details,
- multiple Assets details,
- all the Assets on a page details, to a CSV or PDF file.

Assets are Hosts, Devices, Peripherals and Network Elements. The Discovered Assets Visibility view is used an example in the following procedures.

### Export a Single Asset details

### Export Multiple Asset Details

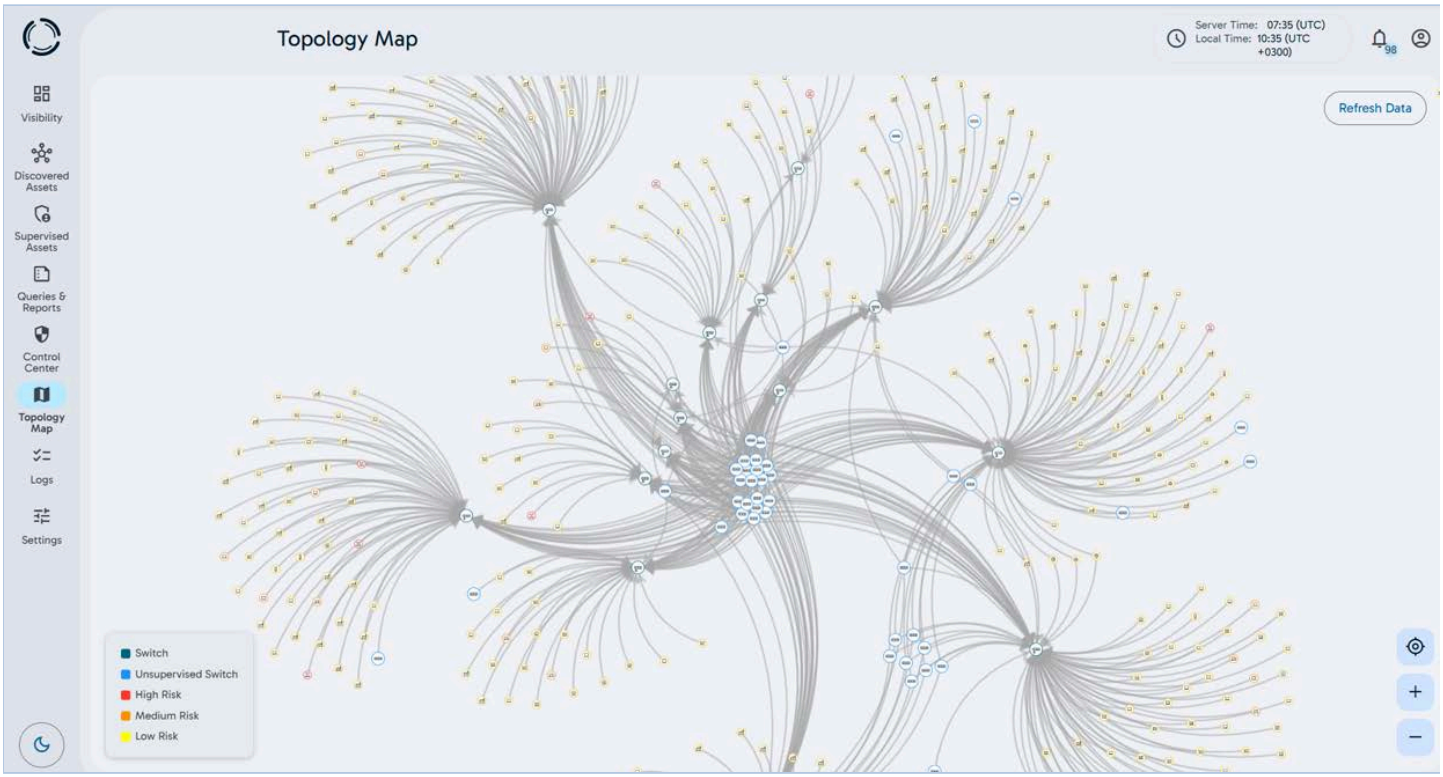
### Export all Assets

## Network Topology Views

Network Topology View provides a connectivity map of the networked assets that are physically connected (layer 1) to network switches. The maps are created automatically based on location calculation and can be filtered based on the type of infrastructure and the asset's risk level.

## Maps Overview

The Topology map folder will present all the networked assets connected as a graph. The view is created automatically and includes all the assets. It is possible to zoom in and out, filter and reload the maps. The graph end nodes are the networked assets which are connected to their network infrastructure according to the network layer 1 switch.

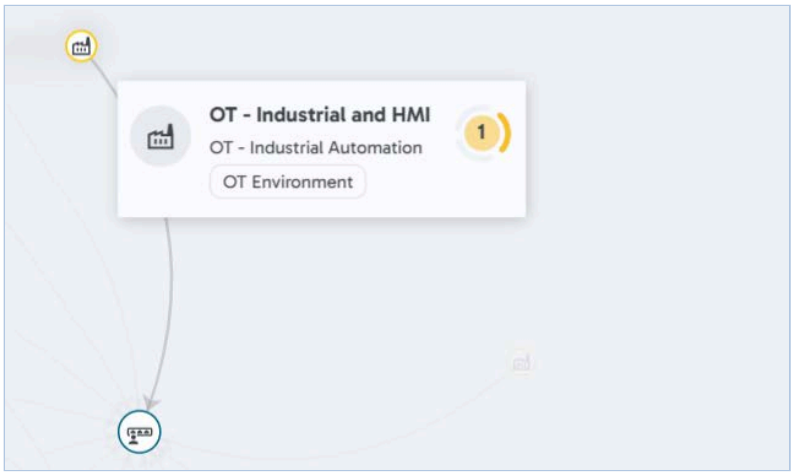



Topology Map overview

## Nodes and Connectors

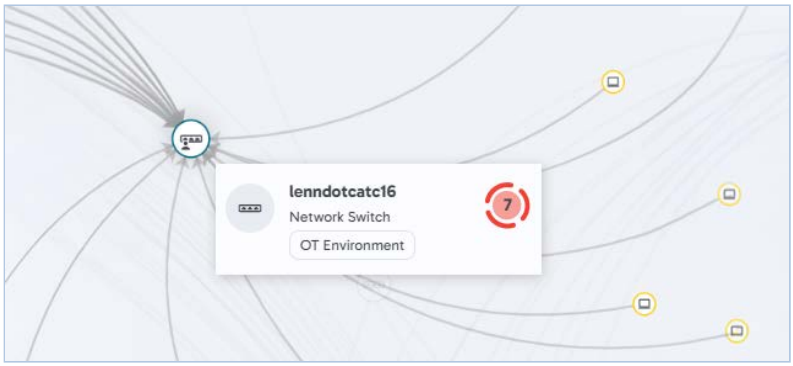
Map nodes are either assets or switches. Nodes can be located at the graph edge or as part of a graph hub.

Each asset will have its name, classification, risk score and labels. The arrow shows how the asset is connected to the network infrastructure.



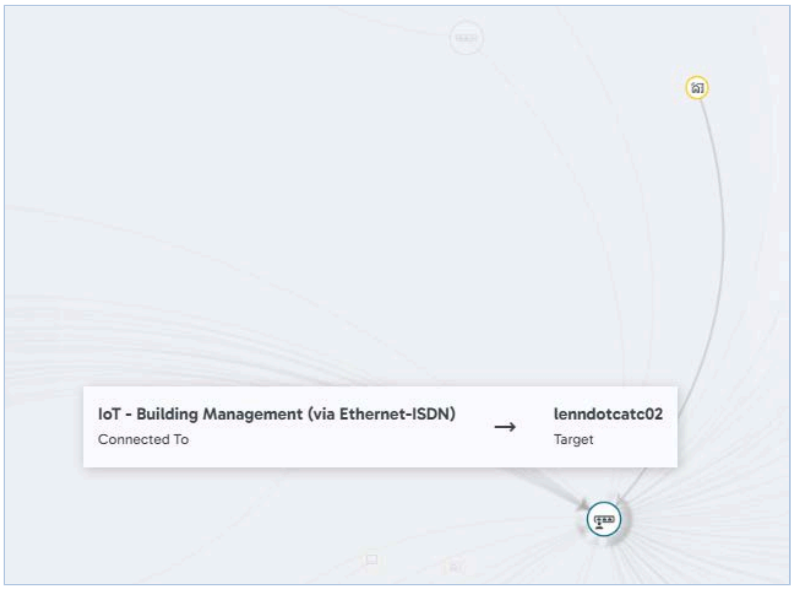
Asset at the map's edge

Each network switch will have its name, classification, risk score and labels. The arrow shows how the network switch is connected to other switches and edge assets.



Network switch connected to multiple assets and network infrastructure

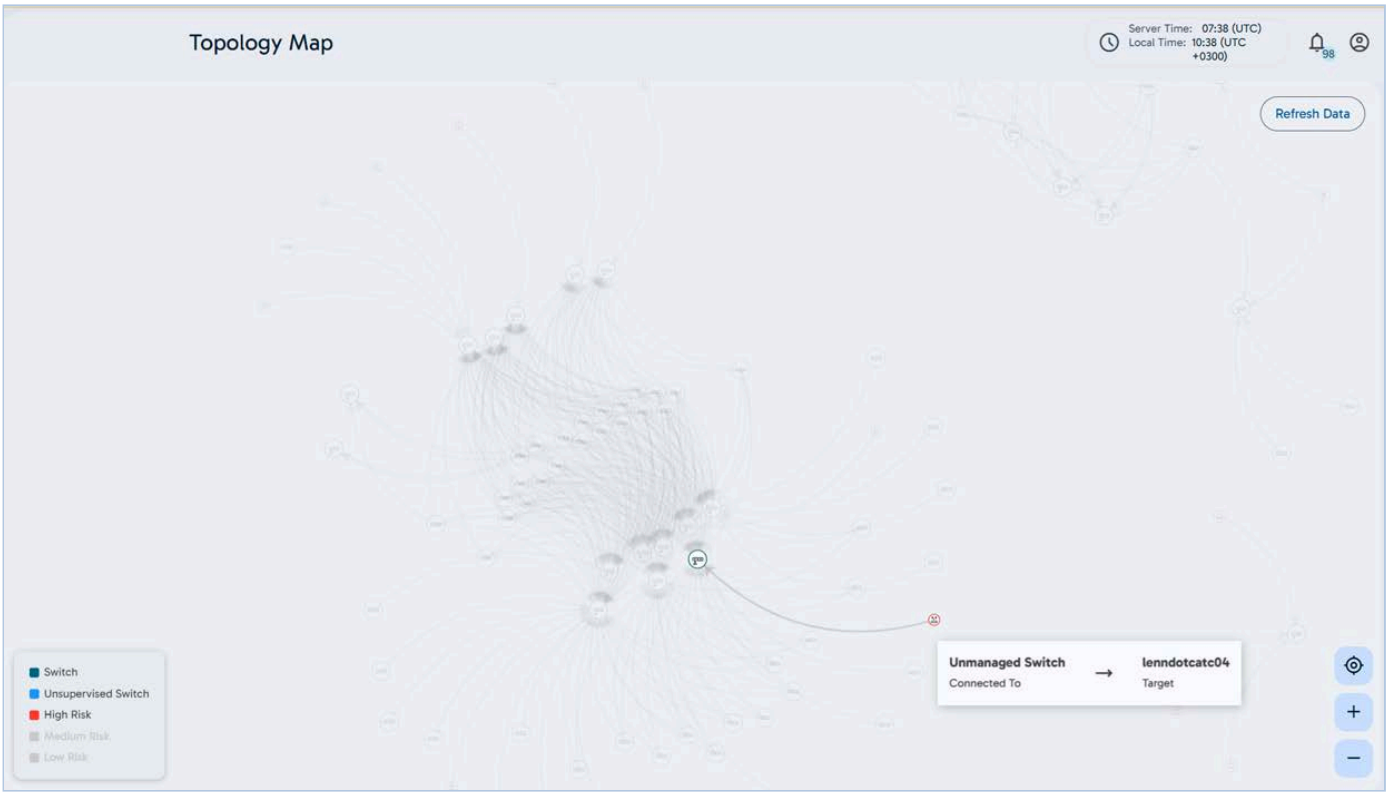
Connectors link between assets which can be network switches or edge devices. Each connector will list the assets at both ends.



Asset connected to network infrastructure switch

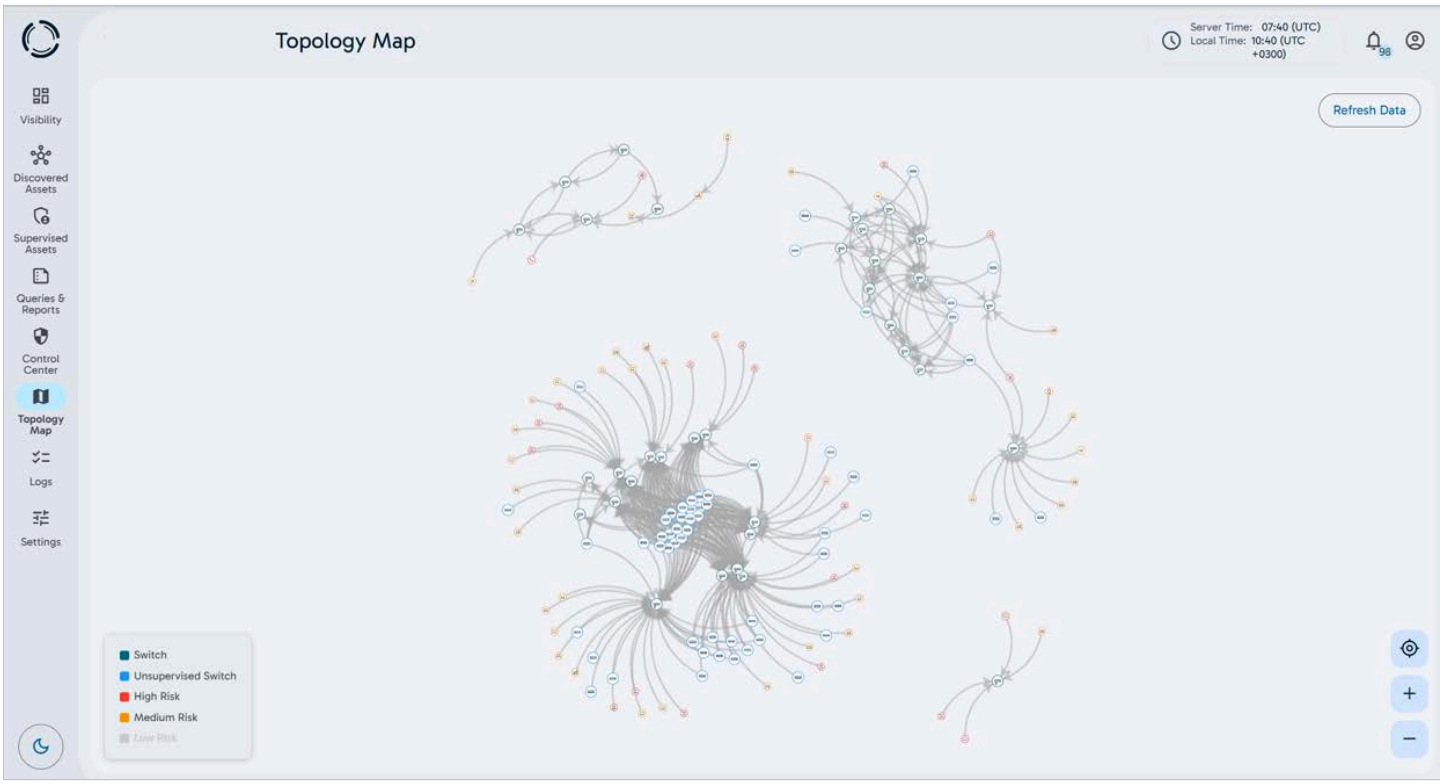
## Filtering

The color-coded categories at the bottom left-hand side of the topology map can be selected and deselected. Based on this selection, the map will be filtered accordingly.




Filtered map showing switches and high-risk assets

Using the filters it is easier to focus on specific areas of the network that require attention and more important, it allows you to identify where to start. For example, the picture below shows assets with high and medium risk. The shown clusters are the areas where one should focus on to reduce the risk.




Filtered map with focus areas

**Note:** The map layout is loaded dynamically; therefore, upon refreshing the page, the locations of assets might change. The visual asset connectivity diagram, however, remains accurate.

# Risk Management

## Related Topics

- About Risk Management
  - About Risk Indicators and Risk Scores
  - Risk Indicator Groups
  - Mouse Jiggler Detection
- Risky Assets Statuses
- Risky Device Connected

# About Risk Management

Risk management is the process of identifying threats to your organization's assets, analyzing vulnerabilities to assess threat levels, and determining strategies to manage these risks.

Sepio enhances this process by utilizing Risk Scores and Risk Indicators to monitor and manage risky assets effectively. You can perform risk management using the Asset Views.

## The Risk Management Process

- **Identify** risks to your organization's assets.
- **Determine the level of risk your organization is willing to accept** (your risk appetite).
- **Establish response** plans for handling risk events that exceed your risk appetite.

## Related Topics

- About Risk Indicators and Risk Scores
- Risk Indicator Groups

# Mouse Jiggler Detection

## Prerequisites

- **Sepio Agent (Windows Only):** Version 17.2602.229 or higher
- **Sepio Platform:** Version 56 or higher

## Overview

The **Mouse Jiggler Detection** capability enables Sepio to identify assets designed to simulate user activity by generating artificial mouse movement.

Sepio uses two complementary detection methods:

- **AssetDNA-based detection:** Identifies known mouse jiggler hardware using AssetDNA.
- **Behavioral Detection**: Detects suspicious mouse activity patterns using pattern analysis

This combined approach improves detection coverage for both dedicated mouse jiggler devices and mouse mover tools that use legitimate pointing devices.

A detailed explanation of mouse jiggler devices can be found in Deep Dive on Mouse Jigglers.

## Detection and Risk Assignment Logic

Sepio continuously analyzes mouse activity patterns reported by the agent. When abnormal movement behavior is detected, Sepio flags the device with a Potential Mouse Jiggler sub risk indicator.



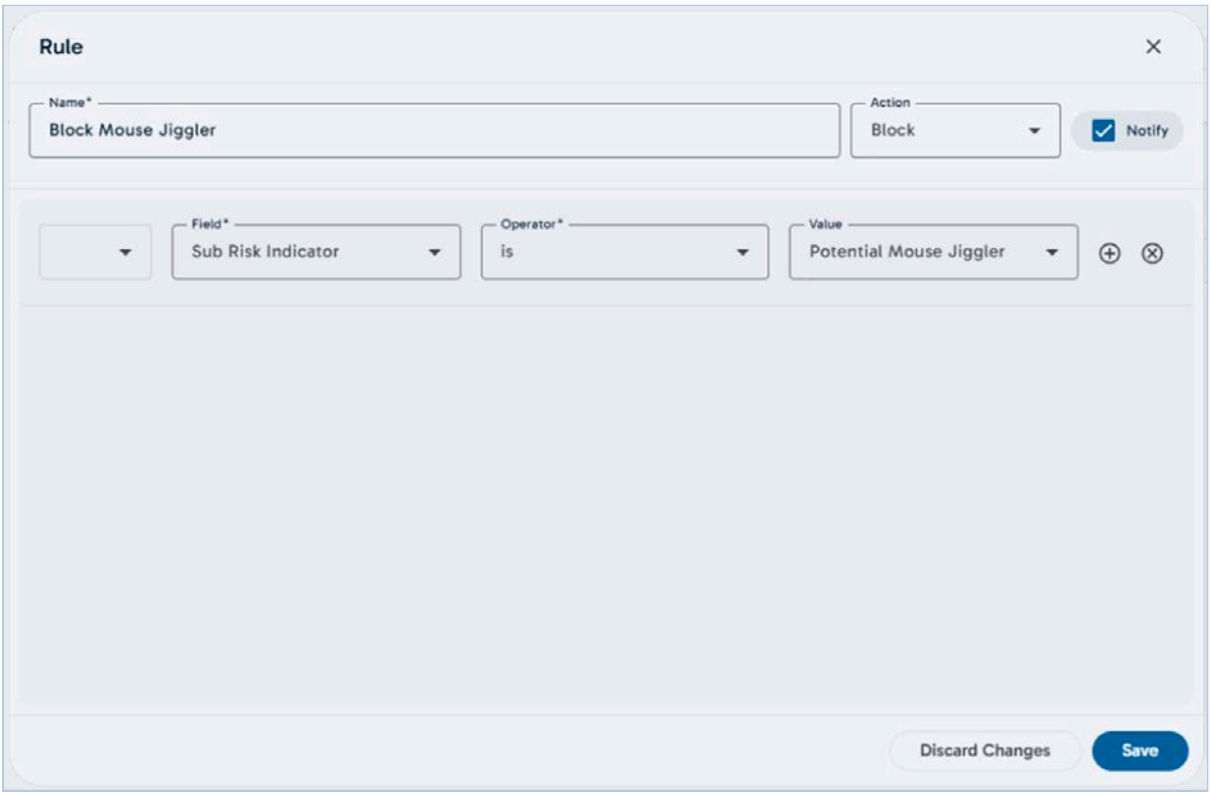

Potential Mouse Jiggler

## Creating Policies for Controlling Potential Mouse Jiggler Activity

Administrators can define policies to control and enforce actions when mouse jigglers are detected.

For example, policies can **block** or **notify** mouse jiggler upon their detection.

The following example demonstrates how to Sepio Security Administrators can set a policy rule that blocks mouse jiggler using the Potential Mouse Jiggler Sub risk indicator.



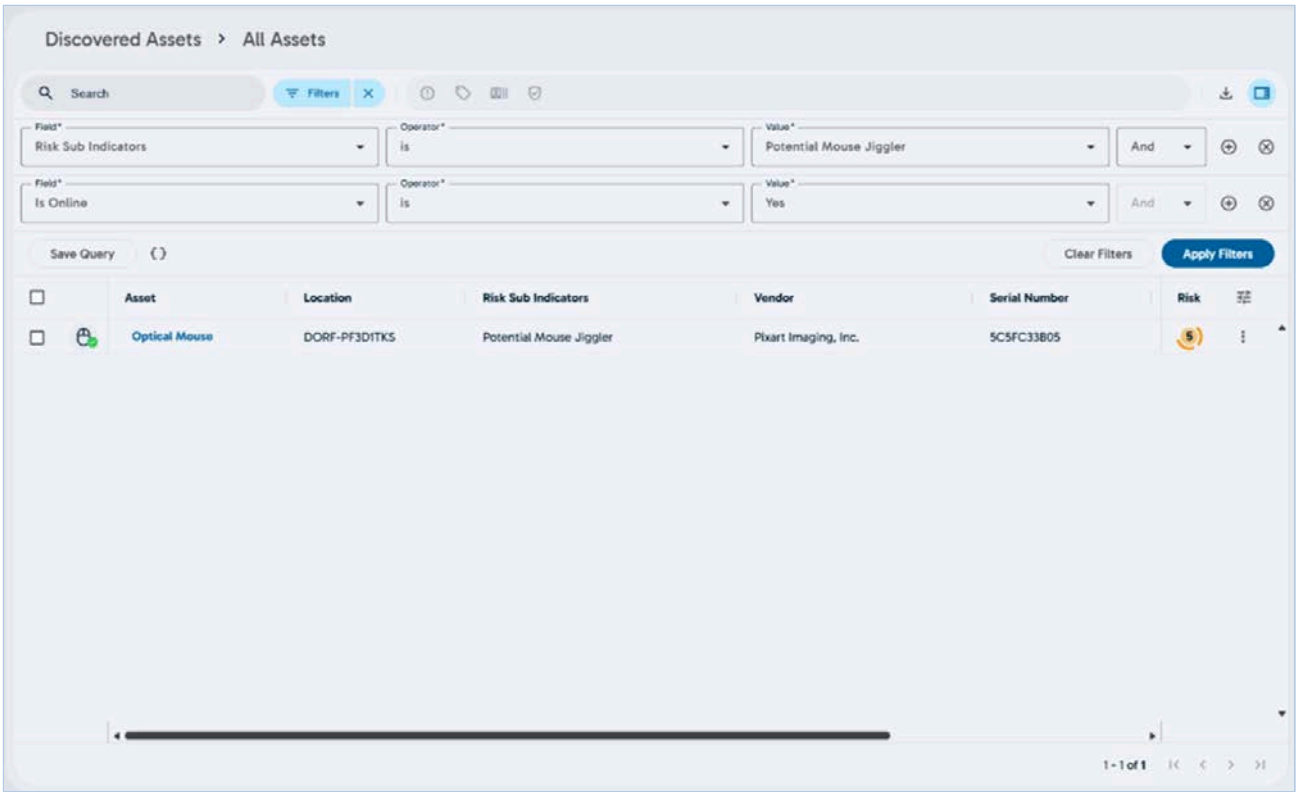
Block Mouse Jiggler

**Note:** Additional information about creating policies can be found in Peripheral Policy Introduction.

## Use Cases

**Query all active mouse jigglers in the organization:**

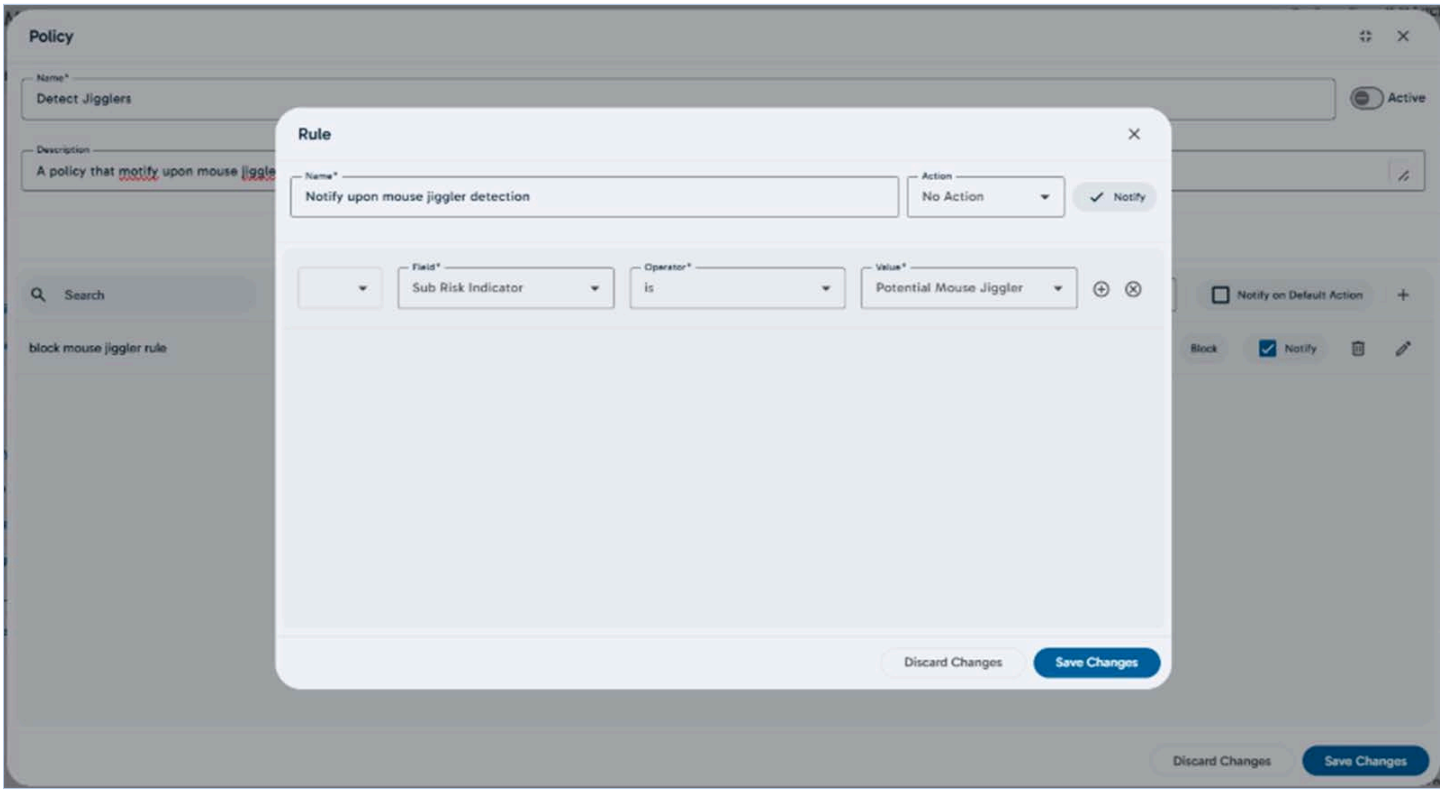
Query based on: “Risk Sub Indicator Is Potential Mouse Jiggler” and “Is Online is Yes”:




Risk Sub Indicator Is Potential Mouse Jiggler

**Get notification upon detection of mouse jiggler:**

Set up a policy with a rule:
“Sub Risk Indicator Is Potential Mouse Jiggler” with a notify action:




Discovered Assets View

## Related Topics

- About Risk Management
  - About Risk Indicators and Risk Scores
  - Risk Indicator Groups
- Risky Assets Statuses
- Risky Device Connected

# About Risk Indicators and Risk Scores

## Risk Indicators

A Risk Indicator is used to assess and measure actions or activities that could harm your organization's assets if vulnerabilities are exploited. A threat is an attack, breach, or negative event, while a Risk Indicator reflects both the probability of the threat and its potential impact.

Risk Indicators together represent an asset's potential risk to your organization.

Sepio's Risk Indicators are organized into groups, some of which contain sub-indicators. Each Risk Indicator (and sub-indicator) is detected, calculated, and displayed separately, so an asset can have multiple active Risk Indicators at the same time.

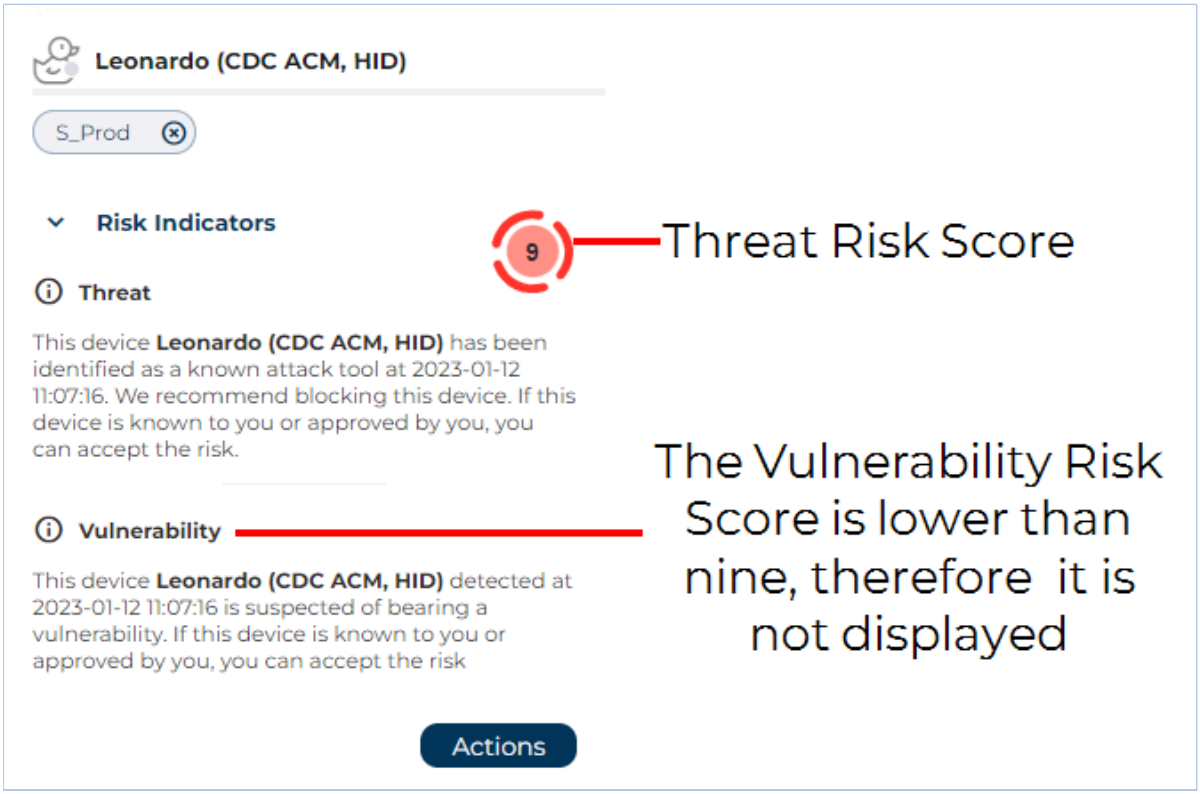
See **Risk Indicator Groups** for detailed information about the groups.

## Risk Scores

A Risk Score is a numeric value ranging from 1 to 9, where 9 indicates extremely high risk and 1 indicates extremely low risk.

| Risk Score Icon | Risk Score | Risk Level | Color |
|---|---|---|---|
|  | 8-9 | High Risk | Red |
|  | 6-7 | Medium Risk | Orange |
|  | 1-5 | Low Risk | Yellow |

An Asset might have multiple Risk Indicators (see example below). Each Risk Indicator has a Risk Score, the platform only displays the highest Risk score.




Asset Risk Indicators

# Risk Indicator Groups

## Overview

The following section lists the Risk Indicator families and their sub-indicators. Each sub-indicator can be turned on or off based on your organization's risk management priorities. The Risk Score for each indicator is predefined by Sepio. The Flag specifies the attribute required to enable the indicator.

Each sub indicator can be turned on/off based on your organization's risk management processes and priorities. The Risk Score is predefined by Sepio.

## Unsupervised Device

Unsupervised devices are not actively monitored by Sepio.Their activity, and that of any connected devices, cannot be properly tracked or analyzed. This creates blind spots in the network, compromises Full Visibility, and makes it harder to enforce security policies or detect threats.

| Risk Sub-Indicator | Description | Asset Type | Risk Score |
|---|---|---|---|
| Unsupervised Network Infrastructure | If a network element is not scanned by Sepio, its connected assets will not have their correct location and Risk Sub-Indicators compromising Full Visibility.<br>Flag to turn on/off: `RI_UNSUPERVISED_NET_INFRA` | Network Infrastructure and Network Elements that can be managed by Sepio | 6 |
| Unsupervised Host | If a host is not supervised by Sepio, all its connected peripherals will not be scanned, making them a liability in the Network and compromising Full Visibility.<br>Flag to turn on/off: `RI_UNSUPERVISED_HOST` | Hosts and Peripherals | 6 |

## Threat

Assets may be malicious or compromised based on Sepio's proprietary DNA fingerprinting. Threats can be active or dormant and may be present in infrastructure or peripheral devices. These indicators highlight potential Rogue Devices or unauthorized equipment.

| Risk Sub-Indicator | Description | Asset Type | Risk Score |
|---|---|---|---|
| Active Network Threat | A core detection capability of Sepio: If an asset's DNA matches that of a Rogue Device and cannot be verified as legitimate, it is flagged as a potential threat to the organization.<br>Flag to turn on/off: `RI_ACTIVE_NETWORK_THREAT` | Network Infrastructure and Elements | 9 |
| Inactive Network Threat | Similar to the Active Network Threat, but applied to assets that are dormant or idle. Since they are not communicating with the network, the risk is lower.<br>Flag to turn on/off: `RI_INACTIVE_NETWORK_THREAT` | Network Infrastructure and Elements | 6 |
| Peripheral Threat | Equivalent to the Active Network Threat but applied to hosts and peripherals.<br>Flag to turn on/off: `RI_PERIPHERAL_THREAT` | Hosts and Peripherals | 9 |

## Vulnerability

This category captures weaknesses in devices or configurations that could be exploited by attackers. It includes documented software or hardware vulnerabilities, suspicious behaviors (such as keylogging), and configurations that indicate the presence of unmanaged hardware.

| Risk Sub-Indicator | Description | Asset Type | Risk Score |
|---|---|---|---|
| Peripheral Vulnerability | Vulnerabilities in peripheral hardware and software are frequently documented and made public through various sources. These vulnerabilities can be exploited by attackers, making them highly relevant for risk assessment.<br>Flag to turn on/off: `RI_PERIPHERAL_VULNERABILITY` | Host and Peripherals | 5 |
| Potential WiFi Keylogger | Keyloggers don't interfere with the connection between the keyboard and the computer, they simply listen, which poses a security risk. A host can detect the presence of a potential Wi-Fi keylogger in the area, and Sepio leverages this capability.<br>Flag to turn on/off: `RI_WIFI_KEYLOGGER` | Host and Peripherals | 7 |

| Risk Sub-Indicator | Description | Asset Type | Risk Score |
|---|---|---|---|
| Common Vulnerabilities and Exposures (CVE) | Publicly disclosed weaknesses identified by the National Vulnerability Database (NVD), applicable to hardware or software components. These vulnerabilities are scored individually based on their severity.<br>Flag to turn on/off: `RI_COMMON_VULNERABILITIES` | Network Infrastructure and Elements | Depending on the base score of the CVE |
| Potential Unmanaged Switch | Indicates the possible presence of an unmanaged switch when multiple devices are connected to a port that shouldn't logically support them.<br>If the number of assets on the port is reduced to one, but the port's AssetDNA is not changed, thus the connection was not changed, the risk indicator will remain.<br>Flag to turn on/off:<br>`RI_POTENTIAL_UNMANAGED_NET_INFRA` | Network Infrastructure and Elements | 7 |

## Anomaly

Anomalies are deviations from expected behavior or configurations. While they may not represent immediate threats, they can signal deeper issues such as impersonation attempts, policy violations, or stealth devices. These indicators help detect subtle, suspicious patterns.

| Risk Sub-Indicator | Description | Asset Type | Risk Score |
|---|---|---|---|
| Asset DNA Anomaly | Devices with DNA that does not match Sepio's Trusted Collection may indicate impersonation, faulty hardware, or rogue configurations.<br>Flag to turn on/off: `RI_DNA_ANOMALY` | Network Infrastructure and Elements | 8 |
| Low Speed on High-Speed Port | Detects low-speed devices (e.g., 10/100 Mbps) connected to high-speed ports (e.g., 10 Gbps), which may suggest unauthorized or outdated equipment.<br>Flag to turn on/off: `RI_LOW_SPEED_HIGH_SPEED_PORT` | Network Infrastructure and Elements | 6 |

| Risk Sub-Indicator | Description | Asset Type | Risk Score |
|---|---|---|---|
| Rare Device | In a large enterprise network, it is expected that many devices share the same type and vendor. Rare occurrences of a specific device type or vendor are unusual and may indicate a liability within the network.<br>Flag to turn on/off: `RI_RARE_DEVICE` | Network Infrastructure and Elements | 5 |
| Communication Anomaly | Unusual connection speeds (auto-negotiated lower than expected) may indicate tampering or misconfigured hardware.<br>Flag to turn on/off: `RI_COMMUNICATION_ANOMALY` | Network Infrastructure and Elements | 5 |
| Extended Idleness | While some devices enter sleep mode to conserve energy, prolonged idleness may suggest passive sniffing or a lack of legitimate use.<br>Flag to turn on/off: `RI_EXTENDED_IDLENESS` | Network Infrastructure and Elements | 5 |

## Compliance

Compliance indicators flag deviations from security best practices or organizational policies. While they may not represent direct technical vulnerabilities, they still pose operational and reputational risks, especially in regulated environments.

| Risk Sub-Indicator | Description | Asset Type | Risk Score |
|---|---|---|---|
| Bad Reputation | Devices from vendors with poor reputations or a history of insecure products may pose inherent risks.<br>Flag to turn on/off: `RI_BAD_REPUTATION` | All Assets | 5 |
| Dual Use | There are devices which are known to serve both legitimate and potentially malicious purposes (e.g., tools that can function as both network analyzers and attack vectors).<br>Flag to turn on/off: `RI_DUAL_USE` | All Assets | 4 |
| Missing EDR | Sepio provides integration with EDR vendors (as of v42 with CrowdStrike), so that if a PC is found in the Network without EDR installed, Sepio can flag them with a missing | Network Infrastructure and Elements | 6 |

| Risk Sub-Indicator | Description | Asset Type | Risk Score |
|---|---|---|---|
| | Endpoint Detection and Response (EDR).<br>Flag to turn on/off: `RI_MISSING_EDR` | | |
| Dormant Device | Devices with prolonged inactivity may either be non-functional endpoints or passive monitoring tools that operate stealthily.<br>Flag to turn on/off: `RI_DORMANT_DEVICE` | Network Infrastructure and Elements | 4 |
| Duplicated MAC Address | Devices which are directly connected to more than one location which should be physically impossible.<br>Flag to turn on/off: `RI_DUPLICATED_MAC` | Network Infrastructure and Elements | 5 |
| Port Compliance Violation | Sepio security administrators can define rules that verify whether the configurations of one or more switch ports comply with organizational policies when devices with defined MAC prefixes are directly connected. If such a policy violation is detected, Sepio raises a dedicated Sub Risk Indicator named Port Compliance Violation.<br>Flag to turn on/off: `RI_PORT_COMPLIANCE_VIOLATION` | All assets | 6 |
| Potential CLI Governance Violation | Switches that contain automation scripts may intercept or alter command results, potentially hiding critical information. | Network Infrastructure | 6 |

# Risky Assets Statuses

## Overview

You can use **statuses** to manage and monitor risky assets in your network. The following tables describe the available asset statuses.

| Action | Status | Description |
|---|---|---|
| Accept Risk | Accepted | Accept the risk. The risky asset/host/peripheral remains in the network. Its Risk Score icon color changes to gray. |
| Remove Accept Risk | – | Remove the accept status from a risky asset/peripheral. The asset/host/peripheral remains in the network, and its Risk Score icon returns to its original color. |
| Block | Blocked | Blocking the risky Asset/Host/Peripheral disconnects it from your network and eliminates the risk. |
| Block (Network Element) | Blocked | Block the network port to which the risky asset is connected. Blocking the port disconnects the risky asset and eliminates the risk. |

## Applicable Only to Hosts

> **Note:** By default, when connecting a host to the platform, its peripherals are set to **Disapproved** and **Enabled**.

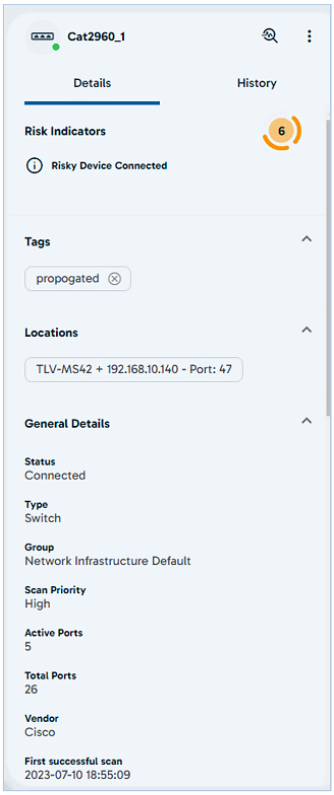
| Action | Status | Description |
|---|---|---|
| Approve Peripheral | Approved | The peripheral won't be blocked if the host mode is set to Armed. |
| Approve All | Host Approved | Approves all peripherals for the host. |
| Disapprove Peripheral | Disapproved | The peripheral will be blocked if the host mode is set to Armed. |
| Enable Peripheral | Enabled | If a peripheral is blocked, you must first approve it and then enable it to make it functional again. |

| Action | Status | Description |
| --- | --- | --- |
| Approve and Enable Peripheral | Approved and Enabled | Approve and enable a blocked peripheral to make it functional again in one step. |

# Risky Device Connected

## Overview

When a device is risky, Sepio highlights this to its parent device, indicating that a risky device is connected. The parent device **inherits the Risk Score of the child.**



Risky Device Connected

| Setting | Description | Default Value |
|---|---|---|
| `RI_RISKY_CHILD_CONNECTED` | Activates or deactivates the Risky Child Connected indicator. When enabled, the parent inherits the child's Risk Score. | True |
| `RISKY_CHILDREN_MIN_RISK` | Defines the minimum Risk Score of a child device that will trigger the "Risky Child" status on the parent. | 3 |

**Note:** Network devices' Risk Scores will be updated after the next successful scan.

# Policy Management

## Overview

Policy Management provides a unified framework for defining, assigning, and enforcing security policies across your environment. Through this interface, administrators can centrally manage peripheral policies and assign them to specific scopes.

This page serves as the entry point for creating and maintaining all policy-related configurations, ensuring consistent and controlled enforcement across the organization.

## Related Topics

- Peripheral Policy Introduction

# Common Use Cases

## Policy Mode as an Improved Version of Armed Mode

In Armed Mode, a new peripheral is automatically blocked until it is **manually approved and enabled**. This manual approval requires the device to be physically connected at least once.

This can create challenges if the organization wants to **pre-approve devices in advance**, before they ever appear on the endpoint.

**Policy Mode solves this.**

You can create a policy with:

- **Default Action = Block**
- **Rules that Allow specific VID/PID/types/vendor etc.**

This enables you to:

- Pre-allow devices before they are connected for the first time
- Ensure that only authorized peripherals are allowed
- Avoid the immediate block behavior seen in Armed mode
  (where the device must first be connected → blocked → manually approved and enabled)

This is a very common use case for organizations transitioning from Armed Mode to Policy Mode.

## Creating a Policy That Behaves Like 'Blocked Known Threats' (BKT) Mode

You can create a policy that mimics 'Blocked Known Threats' (BKT) Mode behavior.

To do this, add a rule with:

- **Action: Block**
- **Rule: Risk Sub-Indicator is Peripheral Threat Detected**

With this rule, any attack tool that is connected to a host will be immediately blocked – similar to 'Blocked Known Threats' (BKT) mode.

This provides automatic threat mitigation **inside Policy Mode**, giving more flexibility and visibility than classic 'Blocked Known Threats' (BKT) mode.

## Identifying Peripherals That Are Blocked but Shouldn't Be Blocked by Policy

A common operational task is to find peripherals currently blocked in the organization that should not be blocked according to the current active policies.

To do that:

- Go to **All Assets**
- Query:
  - **Is Blocked = Yes**
  - **BlockedBy = Empty**

This provides a list of peripherals that are blocked due to:

- Local agent modes (Blocked Known Threats / Block Mass Storage Devices and Known Threats / Armed)
- Older block policies that are no longer active

**Important Note:** If the host is **not running in Policy Mode**, the **Blocked By** attribute will remain empty even if the device should be blocked according to the policy. Hence, it is recommended to first verify that all relevant agents are in Policy Mode.

**Important Note:** Devices blocked by (Blocked Known Threats / Block Mass Storage Devices and Known Threats / Armed) will also show **Blocked By attribute as empty**. Hence, be careful not to unintentionally enable devices that were blocked for legitimate security reasons.

# Peripheral Policy Introduction

## Prerequisites

- **Sepio Platform:** Version 50 or higher
- **Agent Version:** 17.2511.124 or higher

## Overview

The Peripheral Policy feature introduces the capability to enforce and control the use of peripherals across defined scopes. With this feature, Sepio security administrators can centrally define which peripherals are permitted or blocked, apply notification logic, and ensure consistent enforcement aligned with organizational security policies.

To support this capability, a new agent operating mode, **Policy Mode**, has been introduced.

> **Note:** Previous Sepio Agents that are not upgraded will continue to operate and support all other capabilities, except peripheral policies.

## Policy Creation

Under the **Policy Management** section of the user interface, administrators can create and manage peripheral policies.
Each policy defines a combination of rules, a default action, and scope assignments.

## Policy Fields

| Field | Description |
|---|---|
| Name | The Policy name. |
| Description | Free-text field describing the policy's purpose. |
| Status (Active/Inactive) | Policies can be enabled or disabled. Inactive policies are not enforced by the platform. |
| Default Action | Defines the action for any device not matching an explicit rule. Possible values: *Allow all else* or *Block all else*. |

| Field | Description |
| --- | --- |
| Rules | Defines policy actions and logic. Each rule can include multiple matching criteria. |
| Scope Assignment | Specifies one or more scopes to which the policy applies. |

## Rule Definition

Rules can be defined using any combination of the following attributes:

- **Vendor ID (VID)**
- **Product ID (PID)**
- **Peripheral Type**
- **Peripheral Name**
- **Vendor Name**
- **Serial Number**
- **Risk Sub Indicator**

Each rule must include:

- **Action:** Allow, Block, or No action (Notify only).
- **Notify checkbox:** When enabled, it generates a user event whenever the rule is matched.

> **Note:** The Notify checkbox is automatically enabled for Notify Only rules and cannot be disabled.

## Policy Conflict Resolution

- **Rule Conflict:** If a peripheral matches both Block and Allow rules, the agent prioritizes the **Block** rule.
- **Default Action Conflict:** If multiple policies with different default actions apply to the same host, the agent prioritizes **Block All Else**.

## Policy Mode Behavior

When the agent operates in **Policy Mode**, it enforces all assigned policy rules.

> **Note:** Agents that are not operating in Policy Mode will not enforce organizational policies.

## Action Decision Logic

| Condition | Result |
| --- | --- |
| Peripheral matches one or more **Block** rules | Block the peripheral. |
| Peripheral matches one or more **Allow** rules (and no block rules) | Allow the peripheral. |
| No matching rules | Enforce according to the default action. |

## Additional Notes

- **Rule Enforcement:** Blocking or allowing rules are applied regardless of the peripheral's approved status in the user interface.
- **Manual Enablement:** A manually enabled peripheral that matches a block rule will be immediately re-blocked.
- **No Auto-Enable:** Once a peripheral is blocked, it remains blocked unless manually re-enabled and allowed by the policy.

## Notification Logic and User Events

Policies include configurable options to generate event logs when rules are matched, allowing administrators to monitor enforcement and user behavior.

## Notification Behavior

| Condition | User Event Type Generated | Number of Events Generated |
| --- | --- | --- |
| Peripheral matching a rule with no action and **Notify** is enabled | USB Peripheral Policy Notified | One event per matching rule |
| Peripheral matching one or more **Block** rules and **Notify** is enabled | USB Peripheral Policy Blocked | Single event for the first matching rule |
| Peripheral matching one or more **Allow** rules and **Notify** is enabled | USB Peripheral Policy Allowed | Single event for the first matching rule |

| Condition | User Event Type Generated | Number of Events Generated |
|---|---|---|
| Peripheral matching only the **Default Action** rule and **Notify** is enabled | USB Peripheral Policy | Single event |

## Additional Notes: Policy Notifications and Events

- When both **Allow** and **Block** rules match (and both have **Notify** enabled), **Block** takes precedence. Only a USB Peripheral Policy Blocked event is generated.
- If multiple **Notify-only** rules match, a separate USB Peripheral Policy Notified event is created for each rule.
- While in **Policy Mode**, the agent does not generate the following non-policy mode USB Peripheral events:
  - New USB Peripheral Connected
  - USB Peripheral Connected
  - USB Peripheral Disconnected
  - USB Peripheral Disabled

## Bulk Enablement and 'Blocked By' Attribute Introduction

Administrators can enable multiple blocked peripherals across multiple hosts directly from the All-Assets screen.

A new attribute, **Blocked By**, has been introduced to provide visibility into which **policy name** and **rule name** caused a peripheral to be blocked.

**Example:**
Blocked By → Policy A / Rule: Block all keyboards

> **Note:** This attribute allows users to identify the source of enforcement and select specific blocked peripherals for bulk re-enablement operations.

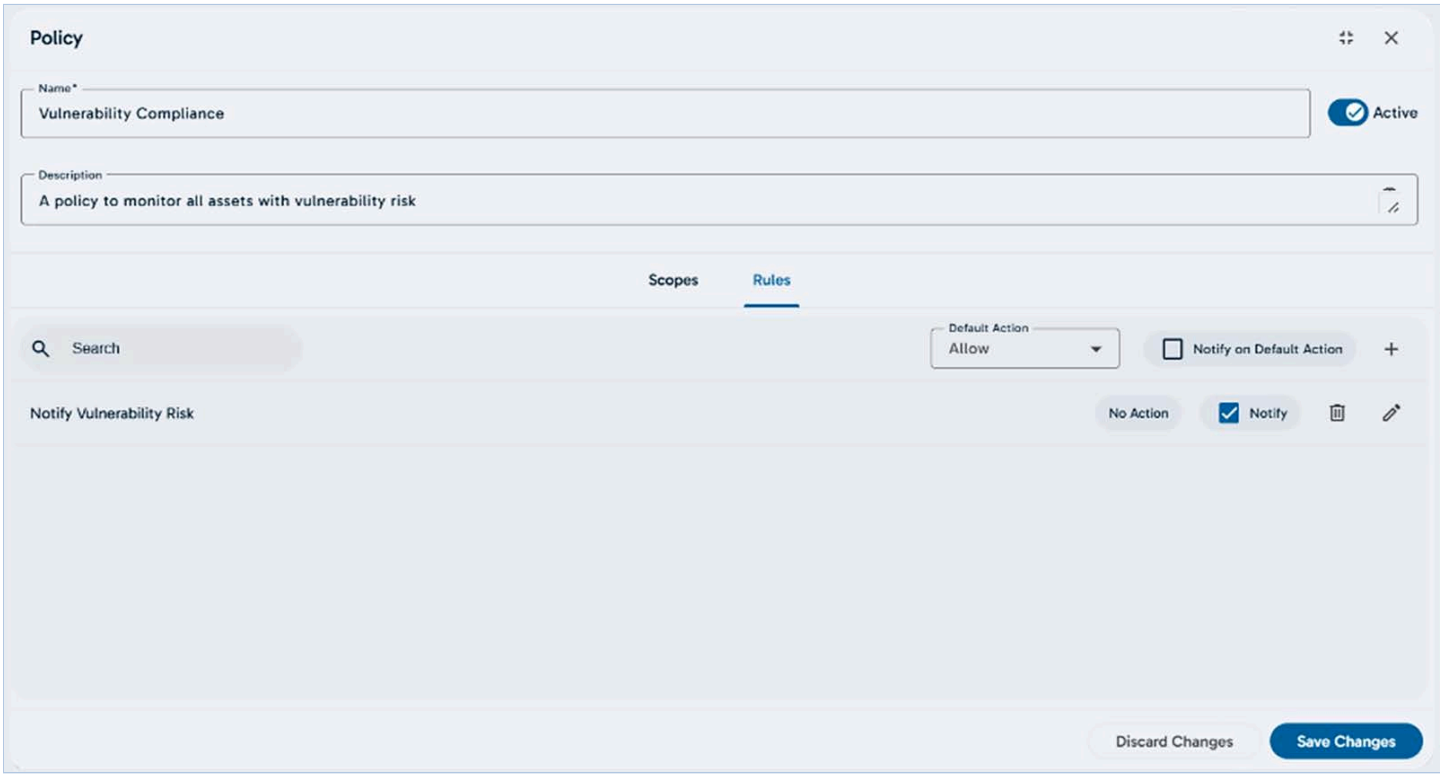
## Policy Enforcement Examples

The purpose of this section is to demonstrate how Sepio Security Administrators can operate and observe Peripheral Policy through the platform.

The following example illustrates how to receive notification and block assets when certain conditions are met (in this case, sending a notification upon vulnerability detection and performing a block action on threat detection).

**Receive notification when a vulnerability is discovered**

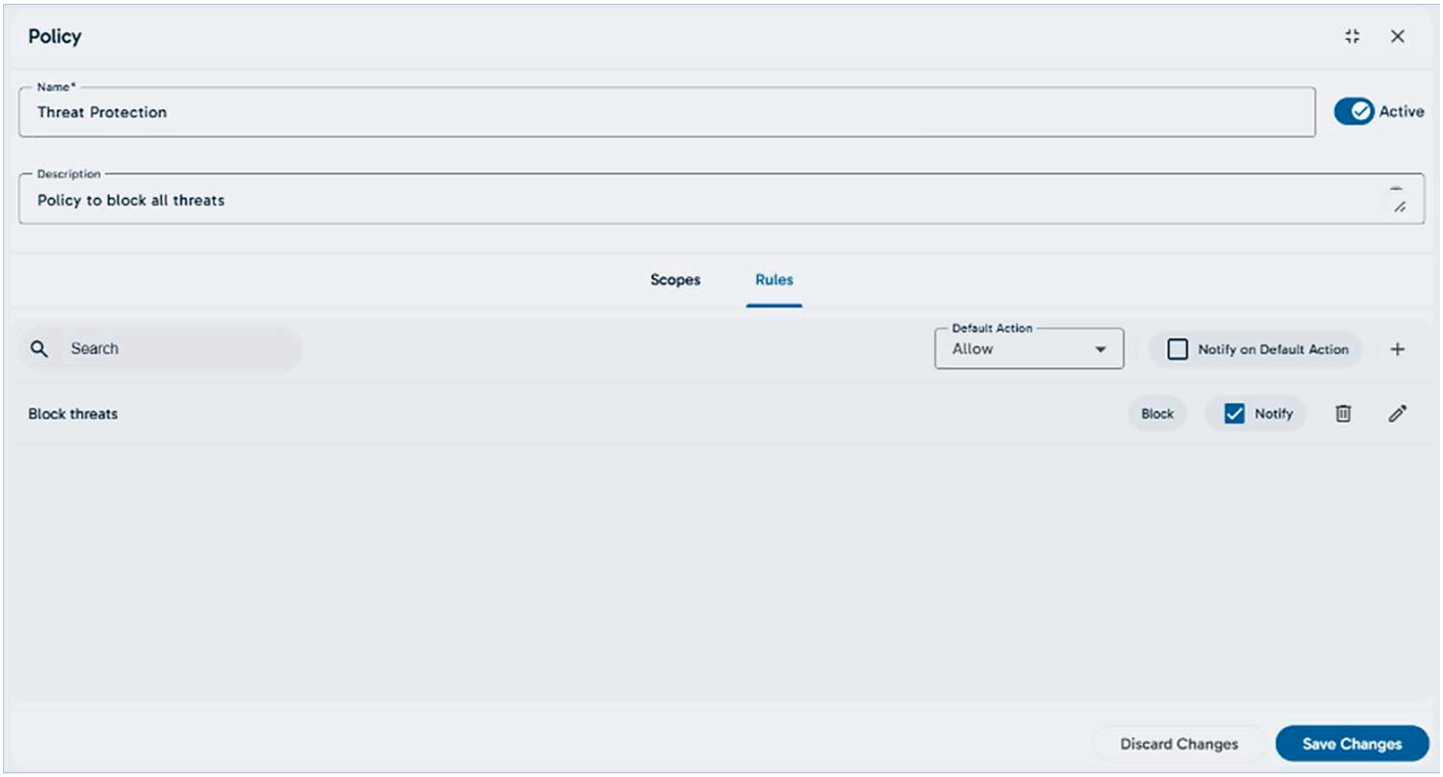
This policy is designed to generate a notification when an asset with a vulnerability is connected to the organization via a host.




Notify Vulnerability Risk

**Threat Protection**

A policy designed to block any asset that is identified as a threat.



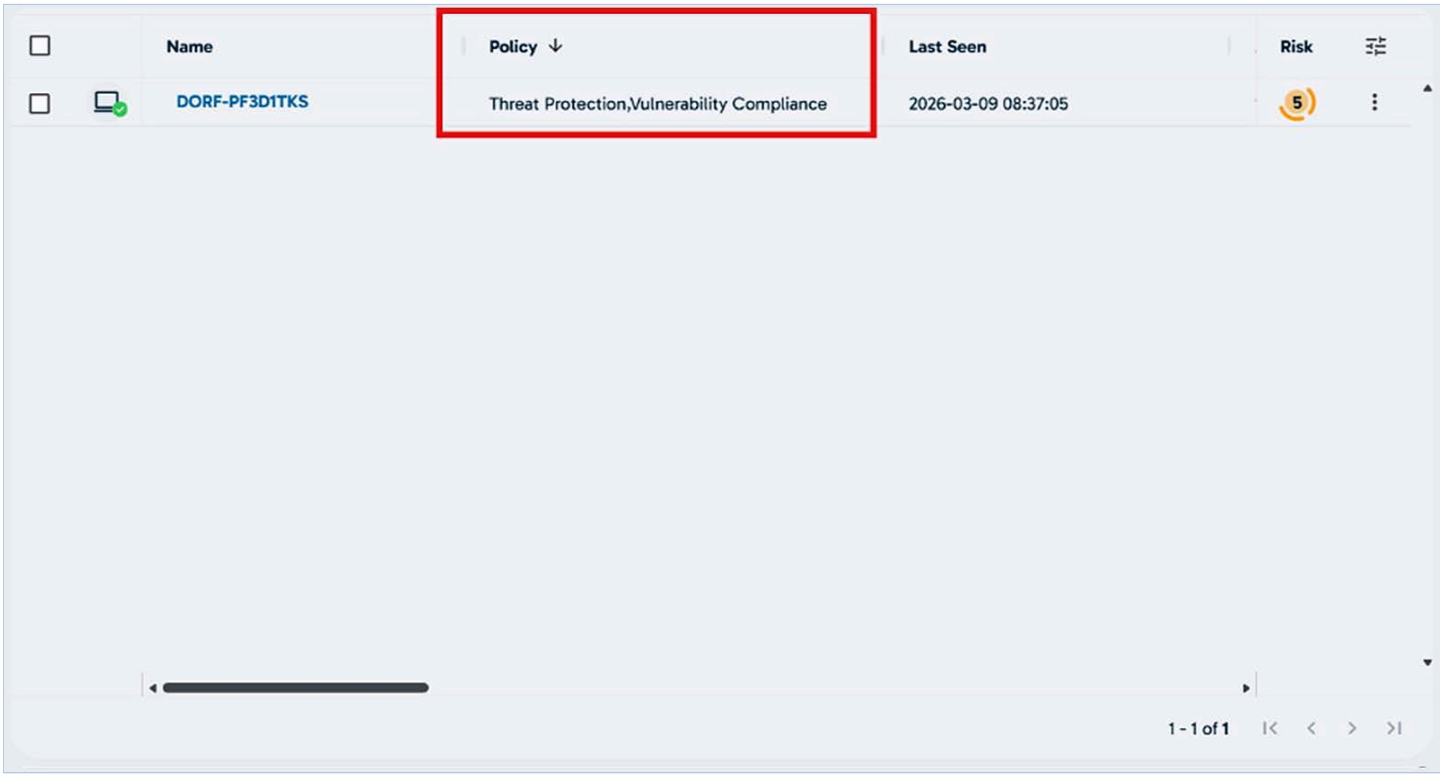

Block Threats

## Policy Verification

Sepio Security Administrators can verify that policies have been successfully assigned to hosts using the following indicators:

**Policy attribute in the Sepio Platform**

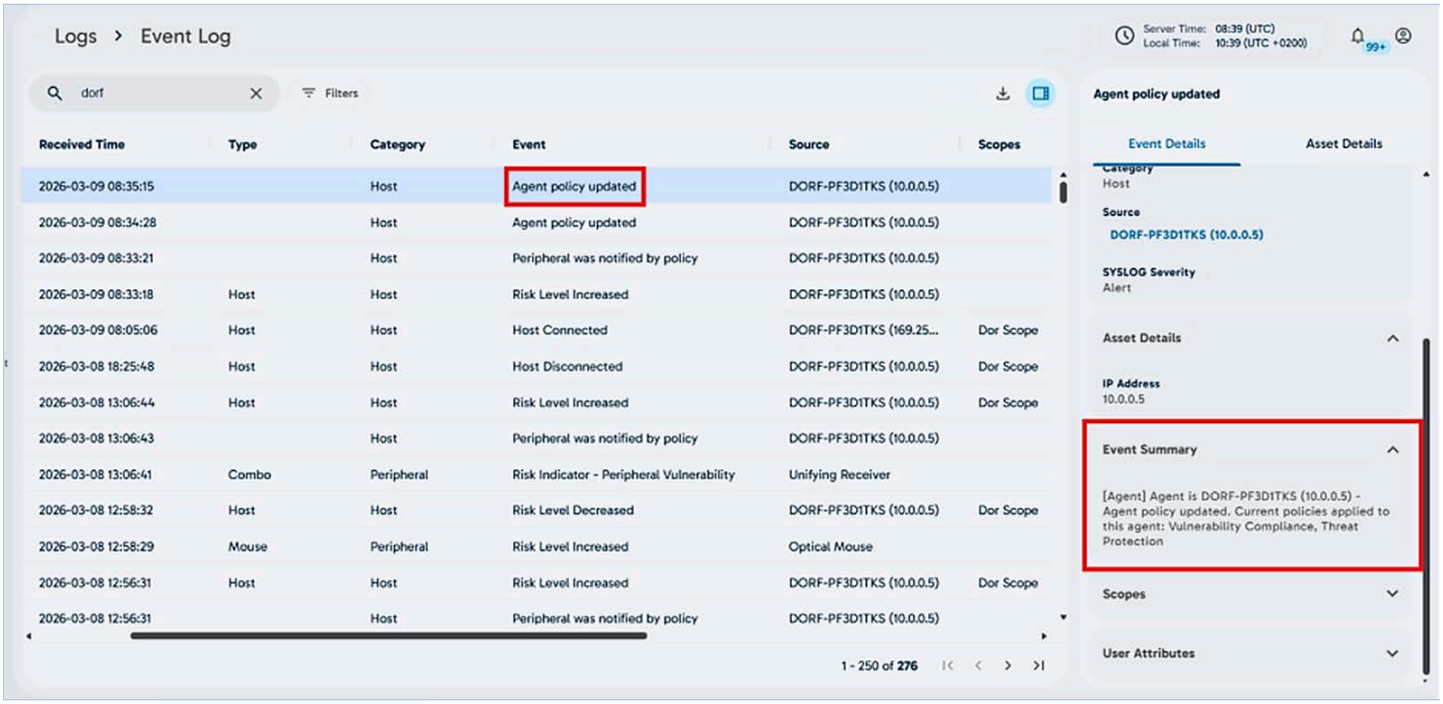
The host page displays the name of the policy that is currently associated with the host agent.




Policy Attribute in the Sepio Platform

### Agent policy update event

When a policy is assigned or updated, the platform generates an "**Agent Policy Update**" event confirming that the host has received the updated policy configuration.



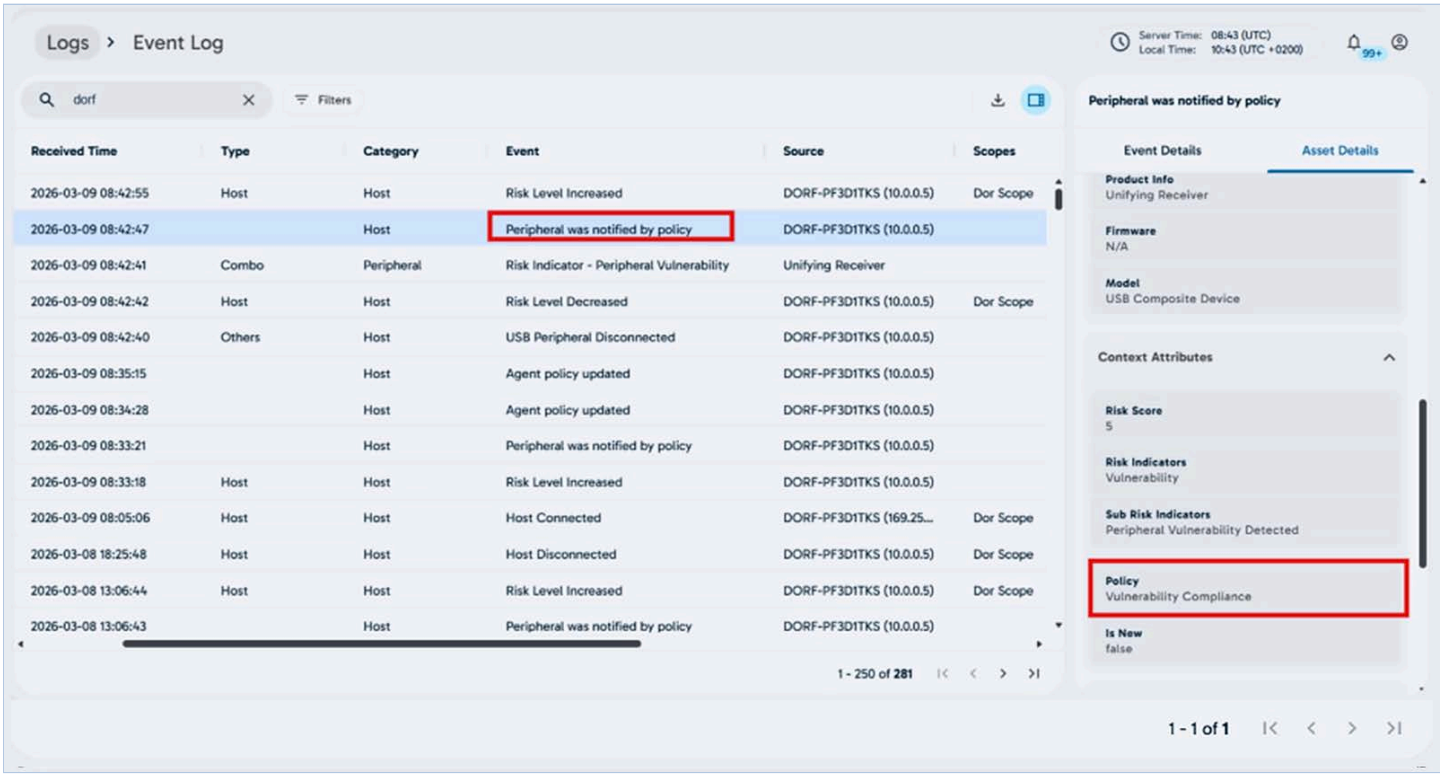

Agent Policy Update Event

Once the agent operates in **Policy Mode**, it begins enforcing the assigned policies.

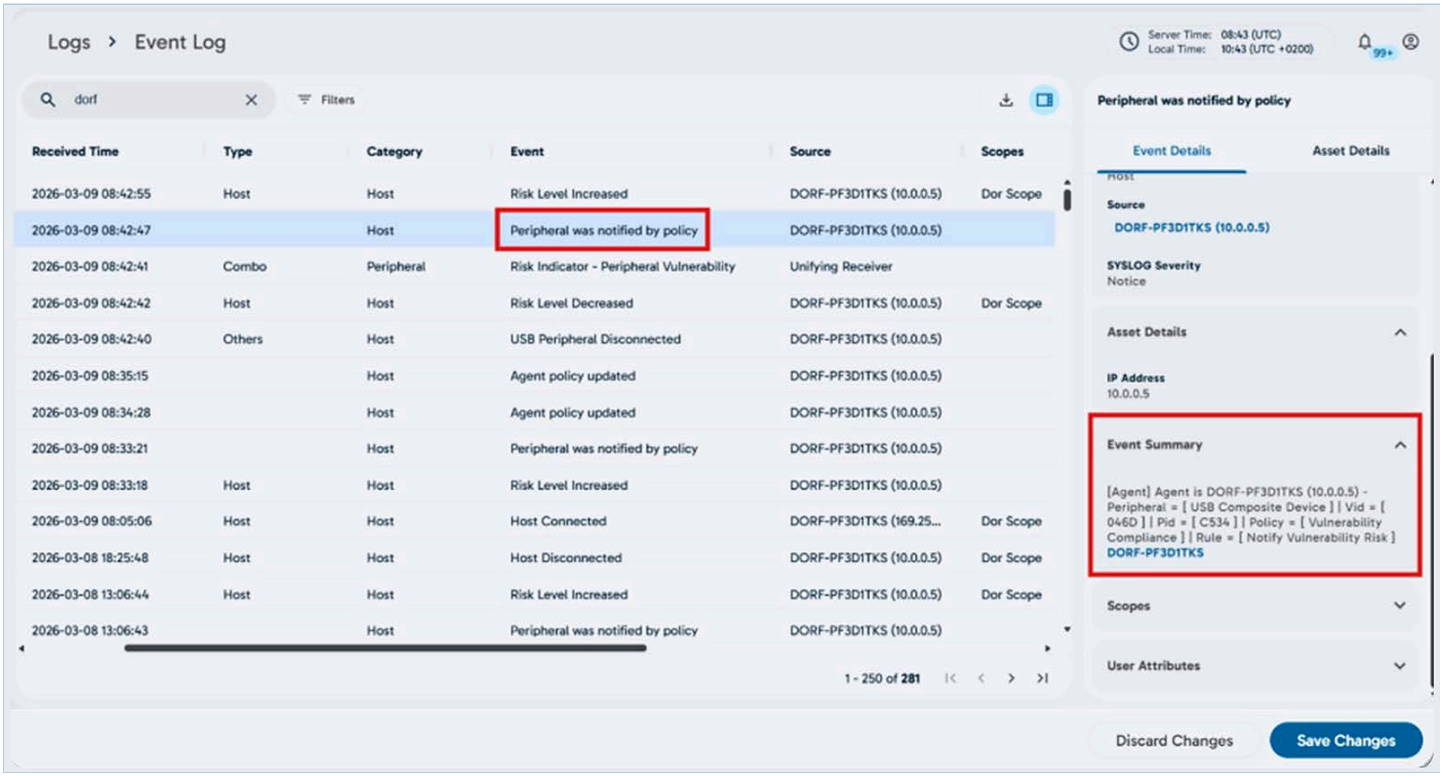
If an asset with a **vulnerability risk** is connected to a host within the defined policy scope, the agent generates a **notification event.**

Sepio Security Administrators can view the policy responsible for the notification in the following ways:

- The **Policy** field within the Event Details
- The **Event Summary**, which includes both the **triggering policy name** and the **triggering rule name**




The Policy field within the Event Details

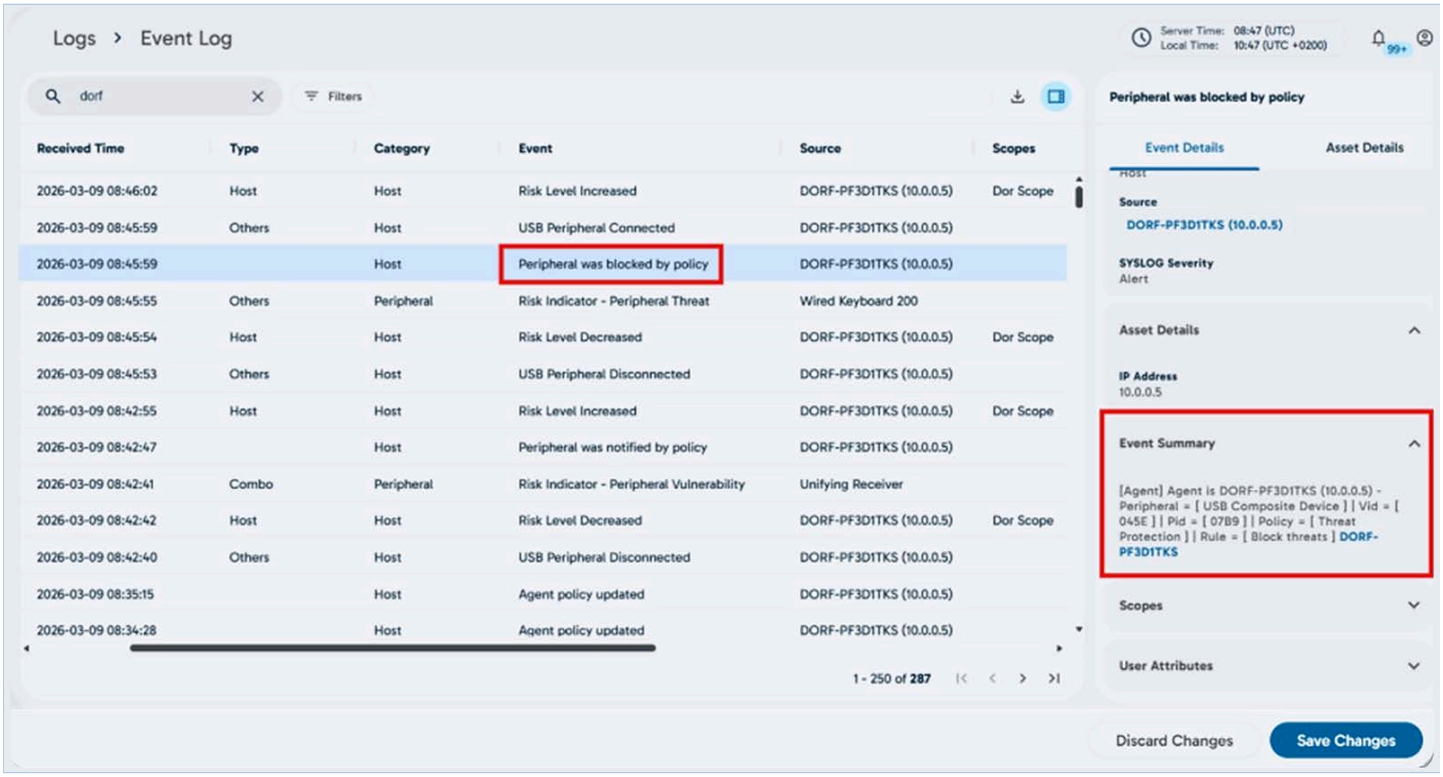



The Event Summary within the Event Details

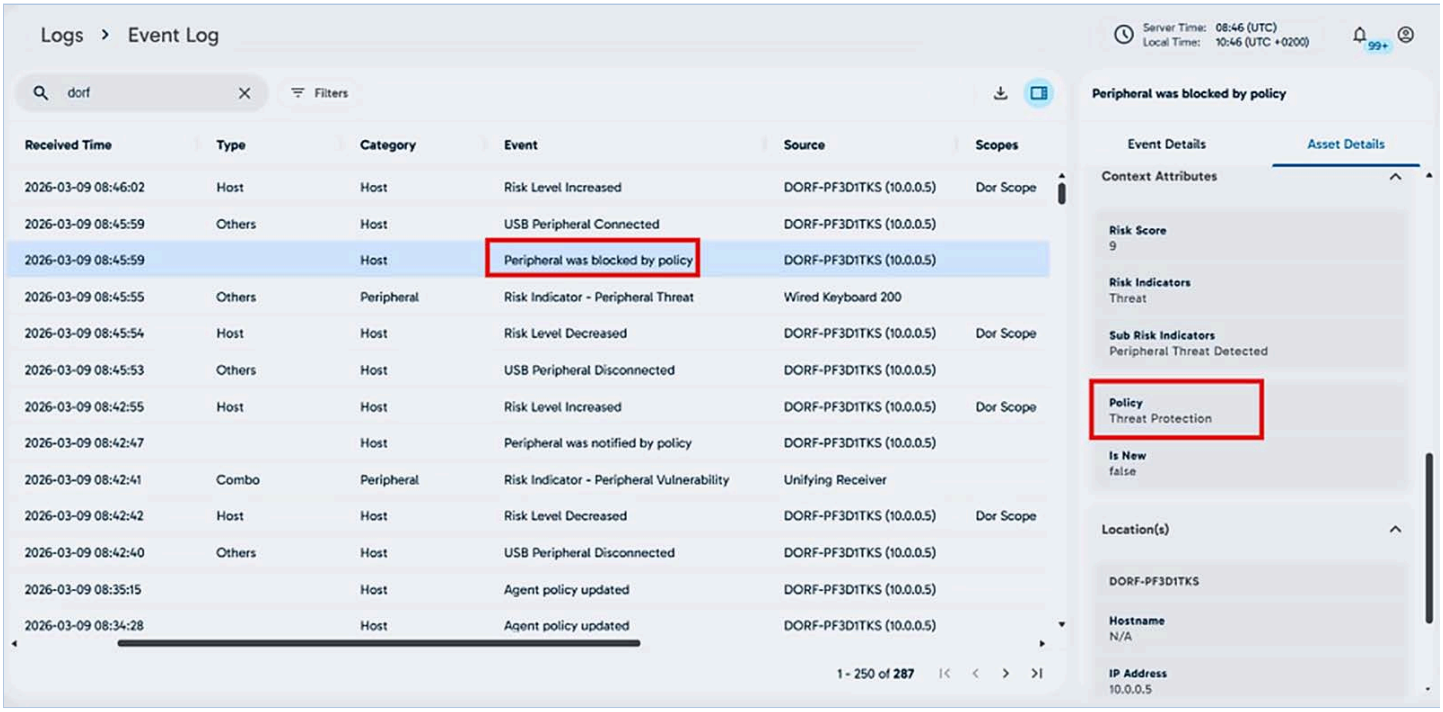
Similarly, when an asset identified as a **threat** is connected to a host within the policy scope, the agent enforces the **Threat Protection** policy and blocks the asset.

A "**Peripheral was blocked by policy**" event is generated to indicate that enforcement has occurred.

As with notification events, administrators can review the **policy name and rule name** that triggered the enforcement directly within the event details.




Peripheral was blocked by policy – Event Details – Event Summary




Peripheral was blocked by policy – Event Details – Policy

# Network Infrastructure Management

## Related Topics

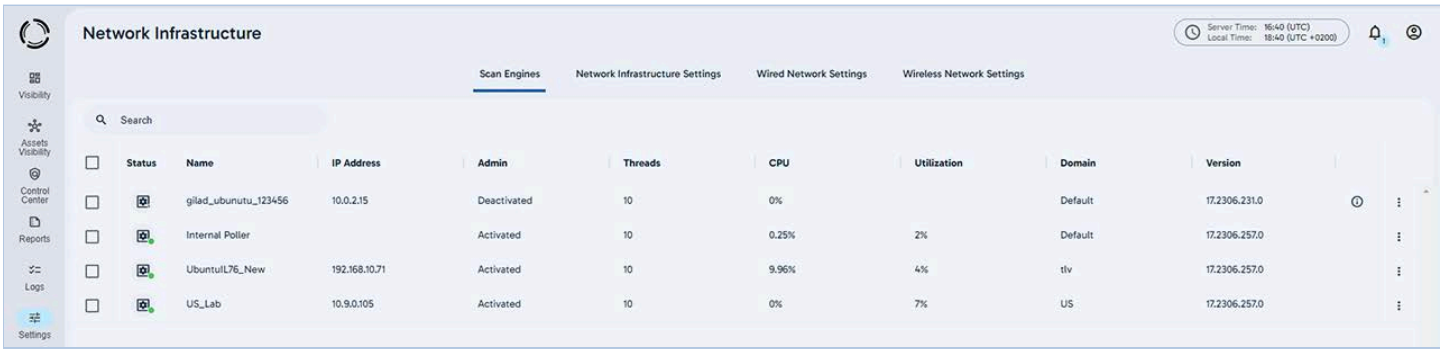
- Network Infrastructure
- Adding and Editing Network Elements
  - Adding and Configuring a Switch
  - Editing a Switch Configuration
  - Adding and Configuring a Meraki Switch
  - Adding and Editing Switch Lists in Bulk
  - Configuring Port Blocking for Cisco Switches using SNMP
- Managing Scan Engines
  - About Scan Engines
  - Event Based Scan Engine
  - Adding a Domain
  - Activating and Deactivating a Scan Engine
  - Assigning Domains and Viewing the Domain of a Scan Engine or NE
  - Changing Scan Priority Intervals
  - Switch Scanning Status Explanations
- Wireless Network Management
- Wired Network Management
- Network Asset Ageing

# Network Infrastructure

## Overview

A **network infrastructure** is a collection of network elements that work together to operate an IT network. Within Sepio, this includes network elements such as switches, controlled access points, and assets that can be connected or disconnected from switch ports, among others.
A controlled access point acts as a client to the Wireless LAN Controller (WLC) and is technically referred to as a Lightweight Access Point (LWAP). LWAPs do not make forwarding decisions; instead, when they receive a frame from a connected device, they forward it to the WLC. The WLC, based on security configurations, decides whether the received frame should be forwarded or discarded. If forwarding is required, the WLC sends the frame back to the LWAP connected to the destination device, which then transmits it to the destination.

You can review, edit and manage your Network Infrastructure settings from the **Settings** -> **Network Infrastructure** screen.
In this screen you can define and review settings in each tab for Scan Engines, Wireless and Wired Networks as well as general settings.



Network Infrastructure screen

## Related Topics

- Scan Engines
- Changing Scan Priority Intervals

# Adding and Editing Network Elements

# Switches

# Adding and Configuring a Switch

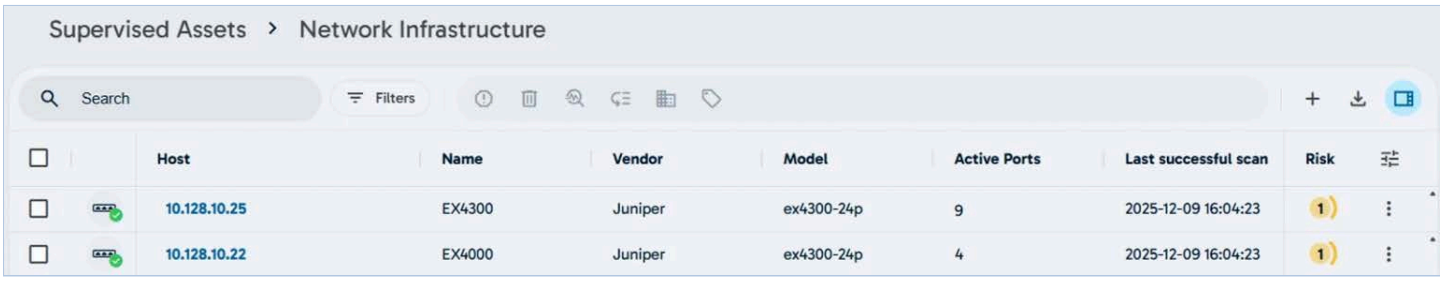
## Overview

In the Add Infrastructure view, you can add and configure a switch to be scanned by Sepio within your network infrastructure.

> **Note:** All Switches are added and configured according to the below procedure except for the Meraki Switch. For adding and configuring the Meraki Switch see Meraki.

## To Add and Configure a Switch

1. Open the Network Infrastructure Visibility view.
2. Click the Add Switch icon.




Network Infrastructure Visibility view

3. Enter the required information as described in the Parameters Table below.



Add Infrastructure

## Parameters Table

| Field | Description | Options |
|---|---|---|
| Product Category | Sepio internal category | • Network Switch<br>• Wireless Controller |
| Protocol | The protocol the network element uses to communicate with Sepio | • SSH<br>• Telnet |
| Host | IP Address of the switch | – |
| Username | Username of the switch | – |
| Password | Password of the switch | – |
| Enable Password | Secures the privileged mode on Cisco switches, which is necessary for executing any commands that modify the router's configuration. By configuring the enable password, you prevent users with general access from making unauthorized changes to the router's settings. | – |

| Field | Description | Options |
| --- | --- | --- |
| Scan Priority | Sepio's scan engine scanning intervals. | • Critical, scans every 1 minute<br>• High, scans every 30 minutes<br>• Normal, scans every 2 hours<br>• Low, scans every 8 hours<br>• Occasional, scans every 24 hours<br>• Manual, scans upon request |
| Domain Name | A domain is a logical organization of switches defined for scanning purposes, typically a geographical domain. | – |

**SNMP Configuration**

| Field | Description | Options |
| --- | --- | --- |
| SNMP Version | SNMP version of the switch | • NoSNMP<br>• SNMPV2C<br>• SNMPV3 |
| SNMPv2 | This SNMP version is only recommended for testing and troubleshooting, as it is encrypted.<br>Read/Write Community string -is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the Networking Node or NE (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent. Allows a remote NE to read information from a NE and to modify settings on that NE. | – |
| SNMPv3 | Recommended SNMP version, as it is encrypted.<br>• User – SNMP username configured on a switch | Authentication Protocol:<br>• None |

| Field | Description | Options |
| --- | --- | --- |
| | • Authentication Protocol – the authentication protocol used to authenticate the source of traffic from SNMP V3 users.<br>• Authentication Passpharse – The SNMP authentication protocol passphrase<br>• Privacy Protocol – the SNMP privacy protocol configured on the switch for SNMPv<br>• Privacy Passpharse – the passphrase used to encrypt the SNMP data. | • Md5<br>• Sha1<br>• Sha256<br>• Sha384<br>• Sha512<br><br>Privacy Protocol:<br>• None<br>• DES<br>• 3DES<br>• Aes128<br>• Aes192<br>• Aes256<br>• Aes128Ext<br>• Aes192Ext<br>• Aes256Ext |

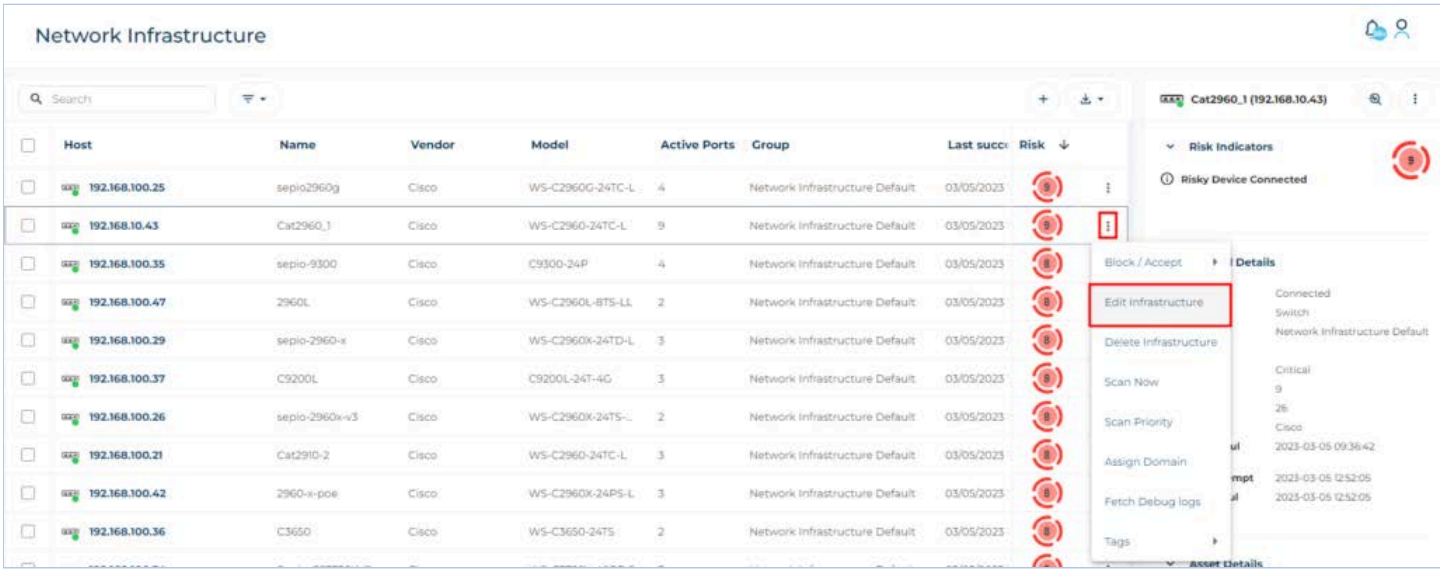
4. Click **Save.**

# Editing a Switch Configuration

## Edit a Switch Configuration

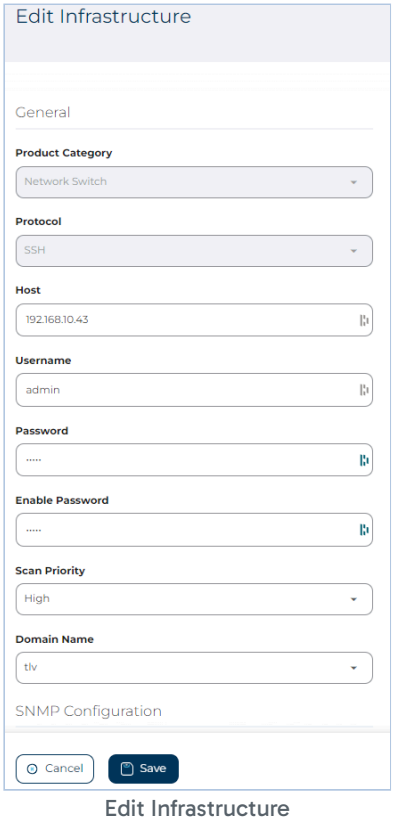
You edit a Switch configuration in the 'Edit Infrastructure' view.

1. Open the Network Infrastructure Visibility view
2. Select the row containing the Switch which configuration you want to edit, then click ⋮




Network Infrastructure Visibility view

3. Edit required parameters, as described in the following table.




Edit Infrastructure

## Parameters Table

| Field | Description | Options |
|---|---|---|
| Host | IP Address of the switch | – |
| Username | Username of the switch | – |
| Password | Password of the switch | – |
| Enable Password | Secures the privileged mode for Cisco switches. The privileged mode is required for all commands that change the router's configuration. Configuring enable password therefore keeps people with general access to your router from changing the router's configuration. | – |
| Scan Priority | Sepio's scan engine scanning intervals. | • 1 – Critical – scans every 1 minute<br>• 2 – High – scans every 30 minutes<br>• 3 – Normal – scans every 2 hours<br>• 4 – Low – scans every 8 hours<br>• 5 – Occasional – scans every 24 hours |
| Domain Name | A domain is a logical organization of switches defined for scanning purposes, typically a geographical domain. | – |

## SNMP Configuration

| Field | Description | Options |
|---|---|---|
| SNMP Version | SNMP version of the switch | • NoSNMP<br>• SNMPV2C<br>• SNMPV3 |
| SNMPv2 | This SNMP version is only recommended for testing and troubleshooting, as it is encrypted.<br><br>Read/Write Community string -is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the Networking Node or NE (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.<br><br>Allows a remote NE to read information from a NE and to modify settings on that NE. | – |

| Field | Description | Options |
| --- | --- | --- |
| SNMPv3 | Recommended SNMP version, as it is encrypted.<br>• User – SNMP username configured on a switch<br>• Authentication Protocol – the authentication protocol used to authenticate the source of traffic from SNMP V3 users.<br>• Authentication Passpharse – The SNMP authentication protocol passphrase<br>• Privacy Protocol – the SNMP privacy protocol configured on the switch for SNMPv<br>• Privacy Passpharse -the passphrase used to encrypt the SNMP data. | Authentication Protocol:<br>• None<br>• Md5<br>• Sha1<br>• Sha256<br>• Sha384<br>• Sha512<br>Privacy Protocol:<br>• None<br>• DES<br>• 3DES<br>• Aes128<br>• Aes192<br>• Aes256<br>• Aes128Ext<br>• Aes192Ext<br>• Aes256Ext |

4. Click **Save**.

# Adding and Configuring a Meraki Switch

- Please, go to Meraki.

# Adding and Editing Switch Lists in Bulk

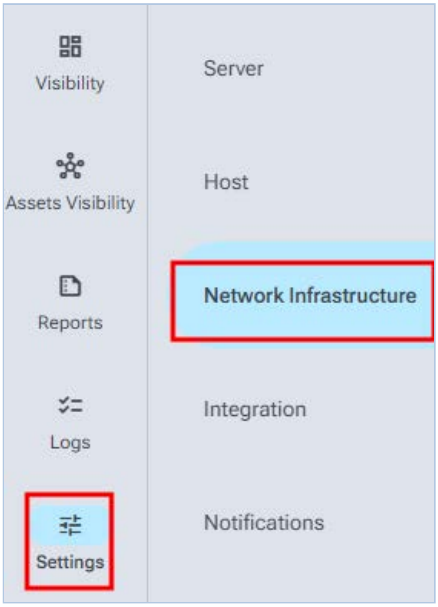
## Overview

The bulk feature enables you to add, configure and modify a list of switches easily and quickly using a CSV file.

> **Note:** It is recommended to configure port blocking for Cisco Switches using SNMP, after adding switches.

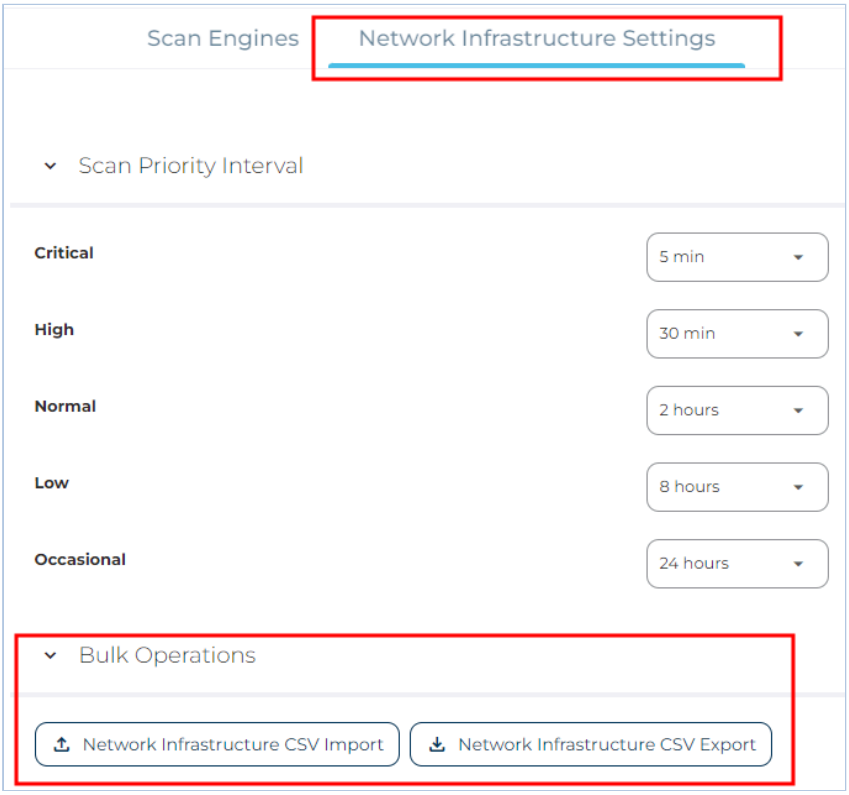
## To add a list of switches and configure them in bulk

1. From Sepio menu (navigation bar) select, **Settings** -> **Network Infrastructure**



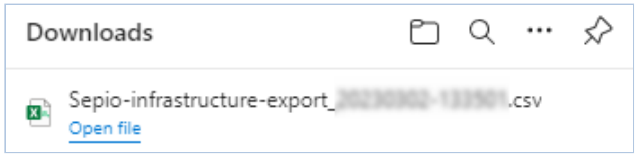

Sepio menu (navigation bar)

2. Navigate to **Network Infrastructure** -> **Network Infrastructure Settings** -> **Bulk Operations**




Network Infrastructure Settings -> Bulk Operations

3. If you are adding and configuring switches for the first time, click "**Network Infrastructure CSV Export**" to download the file.
4. The 'Sepio Systems Infrastructures List Export' Excel file is downloaded and appears in your 'Downloads' folder.

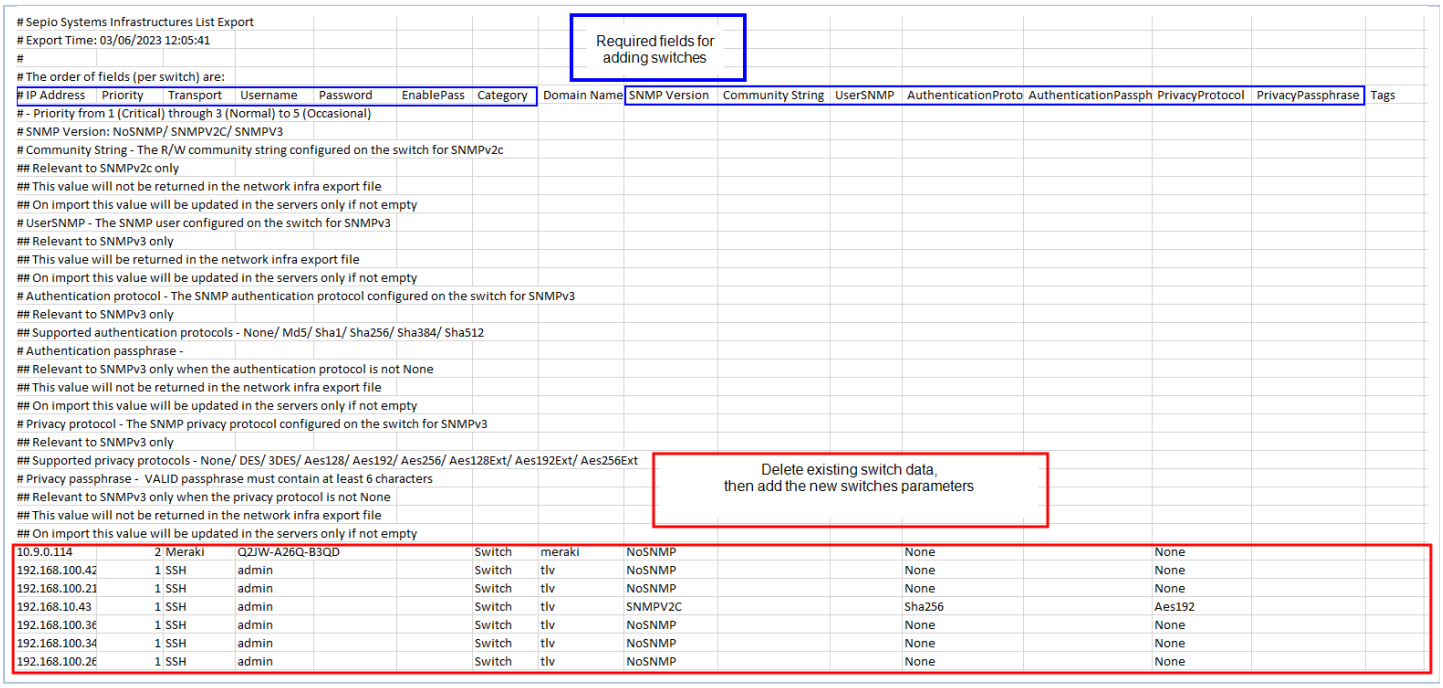



Sepio Systems Infrastructures List Export

**Note:** It is recommended to save the 'Sepio Systems Infrastructures List Export' Excel file (as an Excel, or as a CSV file) after downloading it for the first time, for future use.

**Note:** You can use a CSV file for adding and configuring switches.

5. Open and save the **Sepio Systems Infrastructures List Export** Excel file (see example below).



# Sepio Systems Infrastructures List Export
# Export Time: 03/06/2023 12:05:41
#
# The order of fields (per switch) are:

Required fields for adding switches

| # IP Address | Priority | Transport | Username | Password | EnablePass | Category | Domain Name | SNMP Version | Community String | UserSNMP | AuthenticationProto | AuthenticationPassph | PrivacyProtocol | PrivacyPassphrase | Tags |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # - Priority from 1 (Critical) through 3 (Normal) to 5 (Occasional) | | | | | | | | | | | | | | | |
| # SNMP Version: NoSNMP/ SNMPV2C/ SNMPV3 | | | | | | | | | | | | | | | |
| # Community String - The R/W community string configured on the switch for SNMPv2c | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv2c only | | | | | | | | | | | | | | | |
| ## This value will not be returned in the network infra export file | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | |
| # UserSNMP - The SNMP user configured on the switch for SNMPv3 | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | |
| ## This value will be returned in the network infra export file | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | |
| # Authentication protocol - The SNMP authentication protocol configured on the switch for SNMPv3 | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | |
| ## Supported authentication protocols - None/ Md5/ Sha1/ Sha256/ Sha384/ Sha512 | | | | | | | | | | | | | | | |
| # Authentication passphrase - | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only when the authentication protocol is not None | | | | | | | | | | | | | | | |
| ## This value will not be returned in the network infra export file | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | |
| # Privacy protocol - The SNMP privacy protocol configured on the switch for SNMPv3 | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | |
| ## Supported privacy protocols - None/ DES/ 3DES/ Aes128/ Aes192/ Aes256/ Aes128Ext/ Aes192Ext/ Aes256Ext | | | | | | | | | | | | | | | |
| # Privacy passphrase - VALID passphrase must contain at least 6 characters | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only when the privacy protocol is not None | | | | | | | | | | | | | | | |
| ## This value will not be returned in the network infra export file | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | |
| 10.9.0.114 | 2 | Meraki | Q2JW-A26Q-B3QD | | | Switch | meraki | NoSNMP | | | None | | None | | |
| 192.168.100.42 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.100.21 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.10.43 | 1 | SSH | admin | | | Switch | tlv | SNMPV2C | | | Sha256 | | Aes192 | | |
| 192.168.100.36 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.100.34 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.100.26 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |

Delete existing switch data, then add the new switches parameters

Sepio Systems Infrastructures List Export

6. Delete the existing switch data and add the following parameters for each switch to be added to Sepio:

| Parameter | Description | Required |
|---|---|---|
| IP Address | IP address of the Switch | Yes |
| Priority | Sepio's scan engine scanning intervals (i.e. define how frequently the scan engine collects data from a switch ports)<br>1. Critical – scans every 1 minute<br>2. High – scans every 30 minutes<br>3. Normal – scans every 2 hours<br>4. Low – scans every 8 hours<br>5. Occasional – scans every 24 hours<br><br>Note: If required you can modify the above set scanning intervals. | Yes |
| Transport | Data transporting method | Yes |
| Username | Username of the Switch | Yes |
| Password | Password of the Switch | Yes |
| EnablePass | Secures the privileged mode for Cisco switches. The privileged mode is required for all commands that change the router's configuration. Configuring enable password therefore keeps people with general access to your router from changing the router's configuration. | Yes |

| Parameter | Description | Required |
|---|---|---|
| Category | Network element category | Yes |
| Domain Name | A domain is the logical organization of switches defined for scanning purposes, typically a geographical domain. | No |
| SNMP Version | SNMP version of the switch<br>• No SNMP<br>• SNMPv2C<br>• SNMPv3 | Yes |
| Community String | The R/W community string configured on the switch for SNMPv2c Read/Write Community string -is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the Networking Node or device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent. Allows a remote device to read information from a device and to modify settings on that device.<br><br>**Notes:**<br>• This string is only relevant to SNMPv2c<br>• This value will not be returned to the network infra export file<br>• On import this value will be updated in the servers only if not empty | Yes |
| User SNMP | The SNMP username configured on a switch.<br><br>**Notes:**<br>• Relevant to SNMPv3 only<br>• This value will not be returned to the network infra export file<br>• On import this value will be updated in the servers only if not empty | Yes |

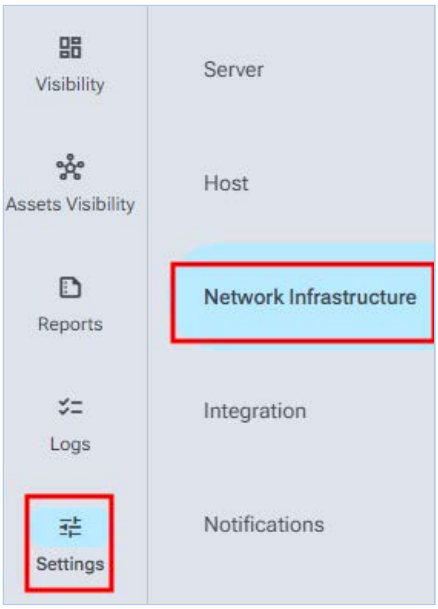
| Parameter | Description | Required |
|---|---|---|
| Authentication Protocol | The authentication protocol is used to authenticate the source of traffic from SNMP V3 users.<br><br>**Notes:**<br>• Relevant to SNMPv3 only<br>• Supported authentication protocols:<br>None/ Md5/ Sha1/ Sha256/ Sha384/ Sha512 | Yes |
| Authentication passphrase | The SNMP authentication protocol passphrase<br><br>**Notes:**<br>• Relevant to SNMPv3 only when the authentication protocol is not None<br>• This value will not be returned to the network infra export file<br>• On import this value will be updated in the servers only if not empty | Yes |
| Privacy Protocol | The SNMP privacy protocol configured on the switch for SNMPv3<br><br>**Note:** Relevant to SNMPv3 only | Yes |
| Tags | Sepio tags | No |

7. Save the modified Excel or CSV file.
8. Click **Network Infrastructure CSV Import** to upload the file to Sepio.

The switches are added to the list in the Network Infrastructure Visibility view.
By default, risk score 1 is assigned to the newly added switches. The switches risk score might change after being scanned by Sepio scan engine.

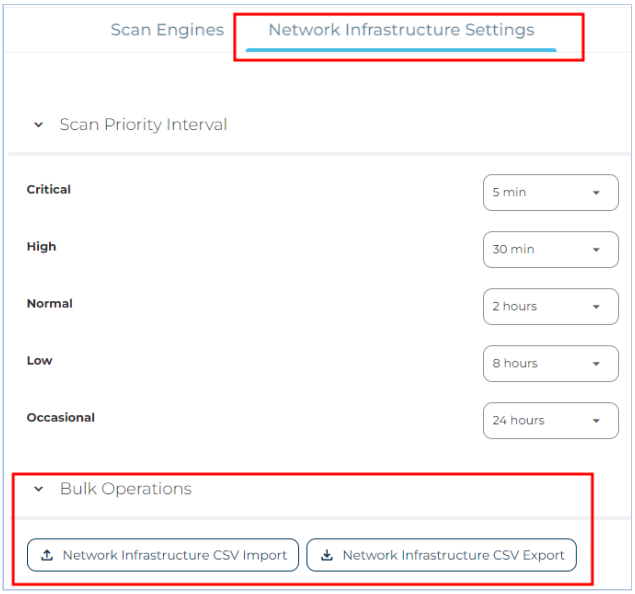
## To edit switches configuration in bulk:

1. From Sepio menu select **Settings** -> **Network Infrastructure**



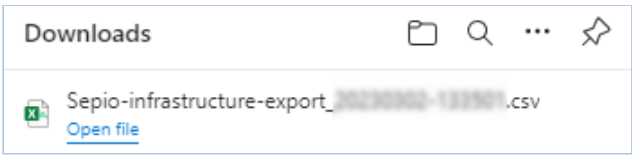
Sepio menu (navigation bar)

2. In the **Network Infrastructure** -> **Network Infrastructure Settings** -> **Bulk Operations**



Network Infrastructure Settings -> Bulk Operations

3. Click **Network Infrastructure CSV Export** to download the current list of switches you wish to edit. The **Sepio Systems Infrastructures List Export** Excel file will be downloaded to your **Downloads** folder.



Sepio Systems Infrastructures List Export

4. Open and save the **Sepio Systems Infrastructures List Export** Excel file.
5. Edit the switch parameters as needed and save the file.

# Sepio Systems Infrastructures List Export
# Export Time: 03/07/2023 09:38:09
#
# The order of fields (per switch) are:

| # IP Address | Priority | Transport | Username | Password | EnablePass | Category | Domain Name | SNMP Version | Community String | UserSNMP | AuthenticationProtocol | AuthenticationPassphrase | PrivacyProtocol | PrivacyPassphrase | Tags |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # - Priority from 1 (Critical) through 3 (Normal) to 5 (Occasional) | | | | | | | | | | | | | | | |
| # SNMP Version: NoSNMP/ SNMPV2C/ SNMPV3 | | | | | | | | | | | | | | | |
| # Community String - The R/W community string configured on the switch for SNMPv2c | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv2c only | | | | | | | | | | | | | | | |
| ## This value will not be returned in the network infra export file | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | |
| # UserSNMP - The SNMP user configured on the switch for SNMPv3 | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | |
| ## This value will be returned in the network infra export file | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | |
| # Authentication protocol - The SNMP authentication protocol configured on the switch for SNMPv3 | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | |
| ## Supported authentication protocols - None/ Md5/ Sha1/ Sha256/ Sha384/ Sha512 | | | | | | | | | | | | | | | |
| # Authentication passphrase - | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only when the authentication protocol is not None | | | | | | | | | | | | | | | |
| ## This value will not be returned in the network infra export file | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | |
| # Privacy protocol - The SNMP privacy protocol configured on the switch for SNMPv3 | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | |
| ## Supported privacy protocols - None/ DES/ 3DES/ Aes128/ Aes192/ Aes256/ Aes128Ext/ Aes192Ext/ Aes256Ext | | | | | | | | | | | | | | | |
| # Privacy passphrase - VALID passphrase must contain at least 6 characters | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only when the privacy protocol is not None | | | | | | | | | | | | | | | |
| ## This value will not be returned in the network infra export file | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | |
| 192.168.100.26 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.100.21 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.100.25 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.100.29 | 1 | ssh | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.100.42 | 1 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |
| 192.168.10.43 | 1 | SSH | admin | | | Switch | tlv | SNMPV2C | | | Sha256 | | Aes192 | | |
| 192.168.100.28 | 3 | SSH | admin | | | Switch | tlv | NoSNMP | | | None | | None | | |

Edit switches parameters

Edit switches parameters

6. Click **Network Infrastructure CSV Import** to upload the file to Sepio.

## Tips

- The edited switches parameters are modified, you can see them in the Network Infrastructure Visibility view.
- When changing an existing switch domain, a new switch will be created with this newly defined domain. The logic here is that the same switch IP address and name can be used in multiple network segments of your infrastructure (for example, in a virtualized environment, or internal labs).
- When creating a new Switch, it is possible to define multiple tags for the same switch. Use the numbers sign (“#”) to separate the different tags.
- Fields are case-sensitive.

| #IP Address | Priority | Transport | Username | Password | EnablePass | Category | Domain Name | SNMP Version | R/W Community String | Read Community String | UserSNMI | Authentic | Authentic | Privacy Pr | Privacy Pa | Tags |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.9.0.2 | 1 | SSH | | | | Switch | US | NoSNMP | | | | | | | | IT_LAB |
| 192.168.100.42 | 1 | SSH | | | | Switch | tlv | NoSNMP | | | | | | | | Boston#Prod#Amit#BYDO#BKT |
| 192.168.100.37 | 2 | SSH | | | | Switch | tlv | SNMPV2C | | | | | | | | IT_LAB |
| 192.168.100.23 | 3 | Telnet | | | | Switch | Lisbon | NoSNMP | | | | | | | | IT_LAB |
| 172.17.101.160 | 2 | Meraki | | | | Switch | tlv | NoSNMP | | | | | | | | Office |
| 10.7.0.27 | 2 | SSH | | | | Switch | US | NoSNMP | | | | | | | | IT_LAB |
| 192.168.100.40 | 3 | SNMP | | | | Switch | US | SNMPV2C | | | | | | | | Office |
| Meraki | 1 | Meraki | | | | Switch | tlv | NoSNMP | | | | | | | | Office |
| 192.168.10.254 | 3 | SSH | | | | WLC | | | | | | | | | | |

Use the numbers sign (“#”) to separate the different tags.

# Configuring Port Blocking for Cisco Switches using SNMP

## Overview

Sepio allows blocking a physical port of a Cisco switch using SNMP, when detecting risky devices (or a risky device) are connected to it. To enable this option, configure the SNMP connection on the switch and on Sepio.

Sepio uses the default SNMP port (UDP port 161) . To change the default port number contact support@sepiocyber.com

**Note:** It is recommended using SNMPv3 for security reasons, as it is encrypted (SNMPv2 is recommended for testing and troubleshooting).

**Note:** If a warming is displayed after configuring the Cisco switch and the Sepio SNMP connection, ensure that the firewall rules allow the use of SNMP between the Scan Engines and the network switches.

## To Configure Port Blocking on a Cisco Switch

1. Access the switch CLI.

2. Configure the SNMP group and user names.

**Note:**

- In this example, 'sepio' is both the group and user names.
- You can use any values for a user name and group name.
- Ensure that you use the same values (names) in both the switch and Sepio SNMP configuration.

Enter `snmp-server group sepio v3 priv write v1default` to assign the group write permissions.

Enter `snmp-server user sepio sepio v3 auth sha authentication_password priv aes 256 privacy_passwordnter`

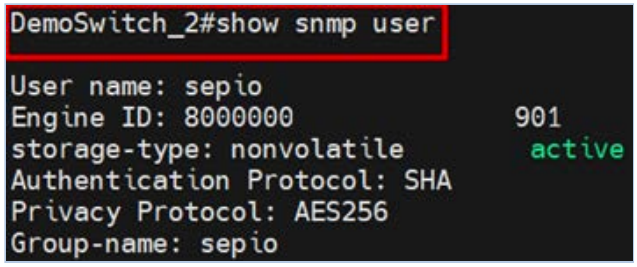
to enable the SNMPv3 user to work with the created group.

Enter the show SNMP group command to verify the group configuration




SNMP group command to verify the group configuration

Enter the show SNMP user command (as shown below) to verify the user configuration.




SNMP user command to verify the user configuration

**Note:** Ensure you enter the same Username, Authentication Protocol and Privacy Protocol in both the switch and Sepio configurations.

**Note:** Rebooting the switch without saving the configuration does not preserve the changes.

## To configure port blocking in Sepio

You can either configure the SNMP connection settings while adding a Switch configuration, or editing a Switch configuration.

1. Go to **Assets Visibility** -> **Network Infrastructure** -> click +. The Add Infrastructure view appears.

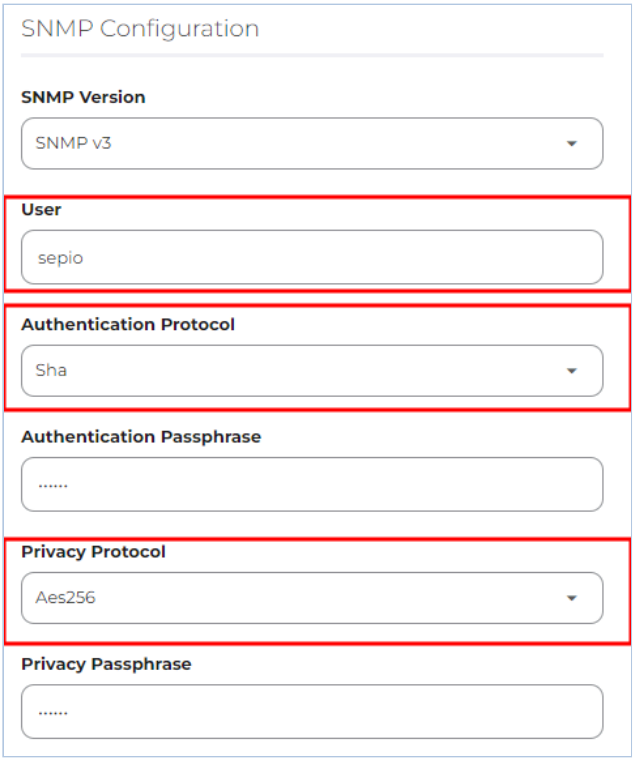



Network Infrastructure

Or, go to **Assets Visibility** ->**Network Infrastructure** -> click next to the Asset you are configuring -> **Edit Infrastructure**. The Edit Infrastructure view appears.

2. In the Add or Edit Infrastructure view, enter information in the required fields as explained in the following table.

**Note:** Ensure you enter the same User name, Authentication Protocol and Privacy Protocol in both the switch and Sepio configurations.



SNMP Configuration

| Field | SNMP Configuration | Options |
|---|---|---|
| SNMP Version | SNMP version of the switch. For configuring Port Blocking it is recommended to use SNMPv3. | ◦ NoSNMP<br>◦ SNMPV2C<br>◦ SNMPV3 |
| SNMPv2 | This SNMP version is only recommended for testing and troubleshooting, as it is not encrypted.<br>Read/Write Community string -is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the Networking Node or device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent. Allows a remote device to read information from a device and to modify settings on that device. | – |
| SNMPv3 | Recommended SNMP version for configuring Port Blocking, as it is encrypted.<br>◦ User – SNMP user name configured on a switch | Authentication Protocol:<br>◦ None<br>◦ Md5 |

| Field | SNMP Configuration | Options |
| --- | --- | --- |
| | ◦ Authentication Protocol – the authentication protocol used to authenticate the source of traffic from SNMP V3 users.<br>◦ Authentication Passpharse – The SNMP authentication protocol passphrase<br>◦ Privacy Protocol – the SNMP privacy protocol configured on the switch for SNMP<br>◦ Privacy Passpharse -the passphrase used to encrypt the SNMP data. | ◦ Sha1<br>◦ Sha256<br>◦ Sha384<br>◦ Sha512<br><br>Privacy Protocol:<br><br>– None<br><br>◦ DES<br>◦ 3DES<br>◦ Aes128<br>◦ Aes192<br>◦ Aes256<br>◦ Aes128Ext<br>◦ Aes192Ext<br>◦ Aes256Ext |

# Managing Scan Engines

## Related Topics

- About Scan Engines
- Event Based Scan Engine
- Adding a Domain
- Activating and Deactivating a Scan Engine
- Assigning Domains of a Scan Engine or Network Element
- Changing Scan Priority Intervals
- Switch Scanning Status Explanations

# Event Based Scan Engine

## Event Based Scanning

### Introduction

Starting from Sepio Platform **V49**, scan engines now support event-based scanning for network-supervised switches.
With this enhancement, Sepio Security Administrators can configure their network switches to send **trap events** directly to the Sepio Scan Engine.

Upon receiving a **Link-Up** or **Link-Down** trap event, the Scan Engine immediately performs a targeted scan on the relevant port. This enables faster, more efficient, event-driven scanning with real-time visibility into network changes.

A single Scan Engine can now support both **periodic** and **event-based** scanning methods.

### Prerequisites

- **Sepio Platform version:** V49 or higher
- **Switch configuration:** Must be set to send **Link-Up** and **Link-Down** trap events (supported for SNMP v2 and v3)

### Comparison Between Event Based and Scheduled Scanning

The following table highlights the key differences and similarities between the available scanning modes, along with recommended use cases.

| Scanning Method | When to Use – Use Cases | Advantages | Disadvantages |
|---|---|---|---|
| **Scheduled** | Asset management and discovery, device identity, application discovery | Reliable | Time gap between switch scans |
| **Event-based + Scheduled** | Asset management and discovery, device identity, application discovery, near real-time attack detection | Reliable and provides real-time detection | Requires additional switch configuration |
| **Event-based only** | Not Supported | | |

### Installation

To enable **event-based scanning**, ensure the following configurations are properly set and completed.

1. **Sepio Management Server Configuration**

   Set the following parameters to `true`:

   `ENABLE_EVENT_BASED_SCANNER=true`

   `PORT_STREAM_CONSUMER=true`

2. **Scan Engine configuration**

   Edit the `config.env` file of the poller (config.env file location can be found here).

   `ENABLE_TRAP_RECEIVER=true`

   `NETPOLLER_TRAP_RECEIVER_LEVEL=4`

   If the switch is configured with **SNMP v3**, also define the following parameters:

   `NETPOLLER_TRAPS_SNMP_V3_USER=<USER_NAME>`

   `NETPOLLER_TRAPS_SNMP_V3_AUTH_PROTOCOL=<AUTH_PROTOCOL>`

   `NETPOLLER_TRAPS_SNMP_V3_AUTH_PASS=<AUTH_PASS>`

   `NETPOLLER_TRAPS_SNMP_V3_PRIVACY_PROTOCOL=<PRIVACY_PROTOCOL>`

   `NETPOLLER_TRAPS_SNMP_V3_PRIVACY_PASS=<PRIVACY_PASSWORD>`

3. **Switch configuration**

   To configure traps for **SNMP V2:**

   **Note:** The following example applies to Juniper switches. Please refer to your specific switch vendor's documentation for accurate commands.

   ```
   cli
   configure
   set snmp community public authorization read-only
   set snmp trap-group <TRAP_GROUP_NAME> version v2
   set snmp trap-group <TRAP_GROUP_NAME> targets <TARGET_MACHINE_IP>
   set snmp trap-group <TRAP_GROUP_NAME> categories link
   commit
   exit
   ```

   **To configure traps for SNMP V3:**

   ```
   cli
   configure
   set snmp v3 usm local-engine user <USER_NAME> <AUTHENTICATION_PROTOCOL> authentication-password <AUTH_PATH>
   set snmp v3 usm local-engine user <USER_NAME> <PRIVACY_PROTOCOL> privacy-password <PRIVACY_PASSWORD>
   set snmp v3 vacm security-to-group security-model usm security-name <SECURITY_GROUP_NAME> group <GROUP_NAME>
   set snmp v3 vacm access group <GROUP_NAME> default-context-prefix security-model any security-level privacy read-view ALL
   set snmp v3 vacm access group <GROUP_NAME> default-context-prefix security-model any
   ```

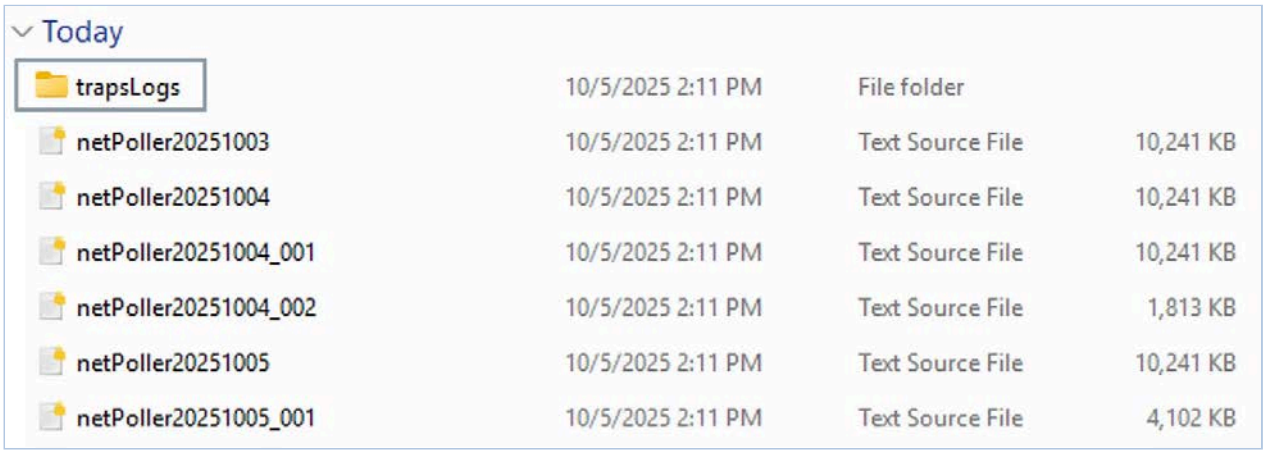
```
security-level privacy write-view ALL
set snmp v3 vacm access group <GROUP_NAME> default-context-prefix security-model any
security-level privacy notify-view ALL
set snmp v3 target-address <TARGET_NAME> address <TARGET_IP>
set snmp v3 target-address <TARGET_NAME> tag-list <TAG_LIST_NAME>
set snmp v3 target-address <TARGET_NAME> target-parameters <TARGET_PARAMS_NAME>
set snmp v3 target-parameters <TARGET_PARAMS_NAME> parameters message-processing-model v3
set snmp v3 target-parameters <TARGET_PARAMS_NAME> parameters security-model usm
set snmp v3 target-parameters <TARGET_PARAMS_NAME> parameters security-level privacy
set snmp v3 target-parameters <TARGET_PARAMS_NAME> parameters security-name <USER_NAME>
set snmp v3 target-parameters <TARGET_PARAMS_NAME> notify-filter ALL
set snmp v3 notify NOTIFY_ALL type trap
set snmp v3 notify NOTIFY_ALL tag <TAG_LIST_NAME>
set snmp v3 notify-filter ALL oid .1 include
set snmp trap-options source-address <SOURCE_IP>
commit
exit
```

### Validation

To verify a successful setup and operation of event-based scanning, follow the steps below:

1. **Trigger a Trap Event:**
   Connect a device to a switch port to generate a Link-Up trap event.
2. **Collect Logs:**
   Export the Scan Engine logs from the Sepio Platform.
3. **Verify Trap Reception:**
   - In the exported log directory, open the folder named `trapsLogs`.
   - Inspect the most recent log file.
   - You should find entries similar to the following:

     ```
     Received trap SNMP message switch SNMP version
     Link state changed on port : UP
     ```




Folder named trapsLogs

4. **Confirm Scan Results in Platform:**
    - Open the **switch's page** in the Sepio Platform.
    - The port associated with the trap event should display the detected device(s).
    - The following attributes will also be updated with the latest scan details:
        - Last Successful Port Scan
        - Last Port Scan Attempt




Switch's page in the Sepio Platform

### Further Configurations (Optional)

The Scan Engine includes a set of configuration parameters designed to optimize the trap-to-scan response time based on business logic and operational requirements.

> **Note:** It is highly recommended to consult the Sepio Support team before modifying the default values.

| Configuration Name | Default Value | Description |
| --- | --- | --- |
| NETPOLLER_EVENT_BASED_SCANNER_MIN_TIME_TO_SCAN_SEC | 5 seconds | Defines the minimum delay between receiving a trap event and initiating a port scan. This short waiting period ensures the link state has stabilized before scanning begins. (Recommended: greater than 5 seconds) |
| NETPOLLER_EVENT_BASED_SCANNER_MAX_TIME_TO_SCAN_SEC | 30 seconds | Specifies the maximum time the Scan Engine waits for additional traps before starting the scan. This allows grouping of multiple trap events within the same switch, that occur in close succession. |
| NETPOLLER_EVENT_BASED_SCANNER_MAX_PORTS_TO_SCAN | 5 seconds | When multiple trap events are received from the same switch within the defined time window, the Scan Engine aggregates them into a single scan to improve efficiency. This parameter controls |

| Configuration Name | Default Value | Description |
| --- | --- | --- |
| | | the maximum number of ports included in one combined scan. |

# About Scan Engines

## Overview

Sepio Scan Engines (previously known as the Netpoller) collect data from Network Elements (NEs). Sepio installation includes an internal Scan Engine. Additional Scan Engines can be added as needed. For more information, refer to the section on Installing and Activating a Sepio Scan Engine.

## Communication with Network Elements

Scan Engines communicate with Network Elements (such as switches and WLAN controllers) over SSH, Telnet, or SNMP. For an illustration go to Sepio Architecture.

### Logical Domains and Scan Priority

Sepio uses logical domains to define which Network Elements are scanned by a specific Scan Engine and provides configurable scan priority levels to determine how frequently a Scan Engine collects data from a Network Element. The Scan Engine installed during the initial setup will scan any Network Elements that have not been assigned to a Domain.
You can assign a Domain to each Scan Engine. A Scan Engine can be assigned to multiple Domains, including the Default Domain.

## Related Topics

- Installing and Activating a Scan Engine
- Adding a Domain
- Assigning Domains and Viewing the Domain of a Scan Engine or NE
- Activating and Deactivating a Scan Engine
- Assigning a Scan Priority to a NE(Switch)
- Changing Scan Priority Intervals
- Scan Engine Architecture and Performance

# Adding a Domain

## Overview

Sepio uses Domains for defining which Network Elements are scanned by a specific Scan Engine. For more information, see About Scan Engines.

## To Add a Domain

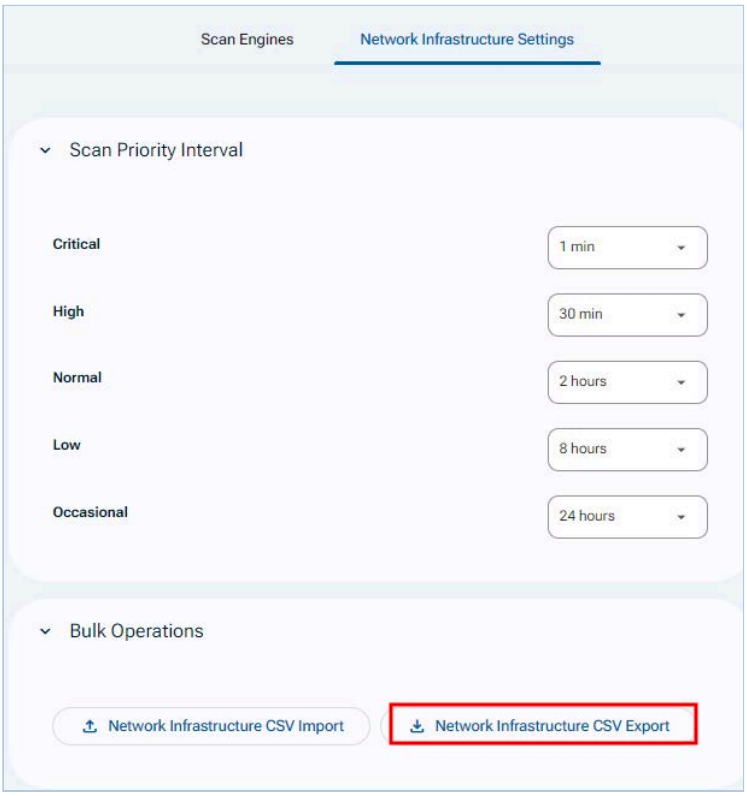
1. Add and configure a Switch.



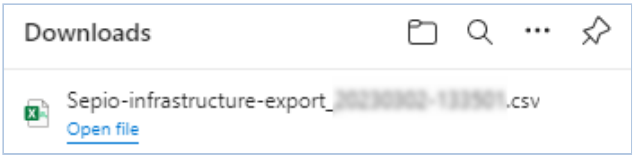

Network Infrastructure

2. From the Sepio menu select:
**Settings** -> **Network Infrastructure** -> **Network Infrastructure Settings** -> **Bulk Operations.**

3. Click **Network Infrastructure CSV Export.**
The 'Sepio Infrastructures List Export' Excel file is downloaded and saved to your '**Downloads' folder.**




Network Infrastructure CSV Export




Downloads folder

4. Open the **'Sepio Infrastructures List Export'** Excel file and save it. (See example below.)

| # UserSNMP - The SNMP user configured on the switch for SNMPv3 | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | | |
| ## This value will be returned in the network infra export file | | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | | |
| # Authentication protocol - The SNMP authentication protocol configured on the switch for SNMPv3 | | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | | |
| ## Supported authentication protocols - None/ Md5/ Sha1/ Sha256/ Sha384/ Sha512 | | | | | | | | | | | | | | | | |
| # Authentication passphrase - | | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only when the authentication protocol is not None | | | | | | | | | | | | | | | | |
| ## This value will not be returned in the network infra export file | | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | | |
| # Privacy protocol - The SNMP privacy protocol configured on the switch for SNMPv3 | | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only | | | | | | | | | | | | | | | | |
| ## Supported privacy protocols - None/ DES/ 3DES/ Aes128/ Aes192/ Aes256/ Aes128Ext/ Aes192Ext/ Aes256Ext | | | | | | | | | | | | | | | | |
| # Privacy passphrase - VALID passphrase must contain at least 6 characters | | | | | | | | | | | | | | | | |
| ## Relevant to SNMPv3 only when the privacy protocol is not None | | | | | | | | | | | | | | | | |
| ## This value will not be returned in the network infra export file | | | | | | | | | | | | | | | | |
| ## On import this value will be updated in the servers only if not empty | | | | | | | | | | | | | | | | |
| # IP Address | Priority | Transport | Username | Password | EnablePa | Category | Domain Name | SNMP Ve | R/W Com | Read Com | UserSNM | Authentic | Authentic | PrivacyPr | PrivacyPa | Tags |
| 192.168.100.45 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 190.169.110.47 | 3 | SSH | admin | | | Switch | Default | NoSNMP | | | Sha256 | | Aes192 | | | |
| 192.168.100.21 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.26 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.20 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.35 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.29 | 1 | ssh | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.33 | 1 | Telnet | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.25 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.32 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.42 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.36 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.24 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.34 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.30 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.47 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.48 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.37 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |
| 192.168.100.41 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None | | | |

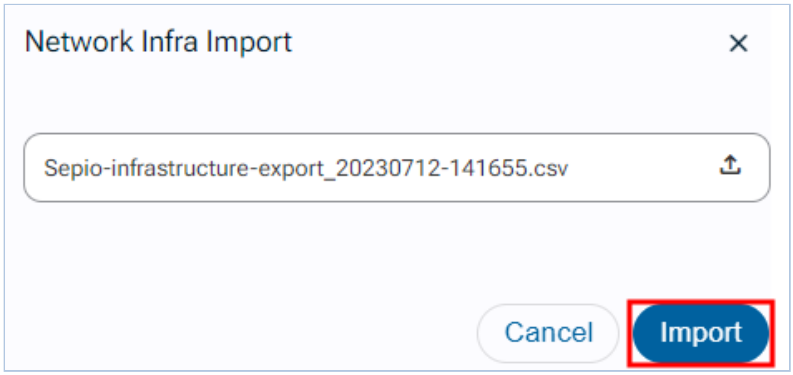
Sepio Infrastructures List Export

5. In the **Switch Domain** column, change **'Default'** to the name of the Domain you want to add (as shown below).

| |
|---|
| ## Supported authentication protocols - None/ Md5/ Sha1/ Sha256/ Sha384/ Sha512 |
| # Authentication passphrase - |
| ## Relevant to SNMPv3 only when the authentication protocol is not None |
| ## This value will not be returned in the network infra export file |
| ## On import this value will be updated in the servers only if not empty |
| # Privacy protocol - The SNMP privacy protocol configured on the switch for SNMPv3 |
| ## Relevant to SNMPv3 only |
| ## Supported privacy protocols - None/ DES/ 3DES/ Aes128/ Aes192/ Aes256/ Aes128Ext/ Aes192Ext/ Aes256Ext |
| # Privacy passphrase - VALID passphrase must contain at least 6 characters |
| ## Relevant to SNMPv3 only when the privacy protocol is not None |
| ## This value will not be returned in the network infra export file |
| ## On import this value will be updated in the servers only if not empty |

| # IP Address | Priority | Transport | Username | Password | EnablePa | Category | Domain Name | SNMP Ve | R/W Com | Read Con | UserSNM | Authentic | Authentic |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.100.45 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 190.169.110.47 | 3 | SSH | admin | | | Switch | TLV | NoSNMP | | | Sha256 | | Aes192 |
| 192.168.100.21 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.26 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.20 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.35 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.29 | 1 | ssh | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.33 | 1 | Telnet | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.25 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.32 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.42 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.36 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.24 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.34 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.30 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.47 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.48 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.37 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.41 | 1 | SSH | admin | | | Switch | ISR | NoSNMP | | | None | | None |
| 192.168.100.23 | 1 | Telnet | admin | | | Switch | ISR | NoSNMP | | | None | | None |

6. Click **Network Infrastructure CSV Import**, choose the Excel (CSV) file to upload, and then click **Import.**
The Domain name is added to Sepio.



Network Infrastructure CSV Import

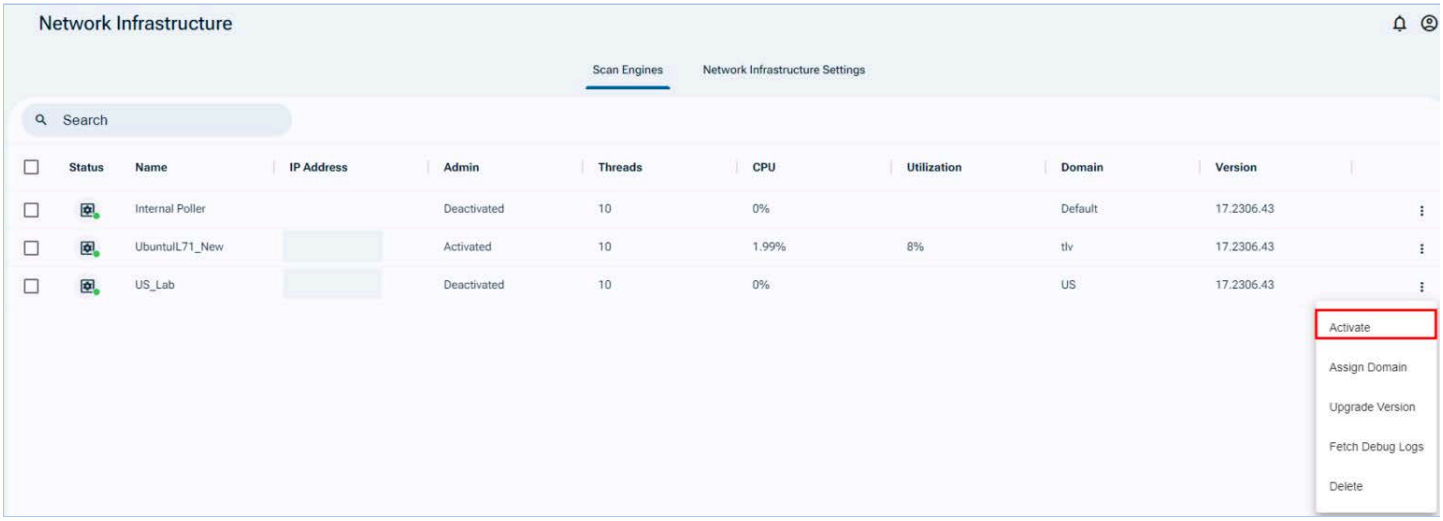
7. Assign a Domain to a Scan Engine or NE.

# Activating and Deactivating a Scan Engine

## To Activate the Scan Engine

To start scanning your network infrastructure, you must activate a Scan Engine.

1. On the Sepio menu, select: **Settings** -> **Network Infrastructure** -> **Scan Engines.**

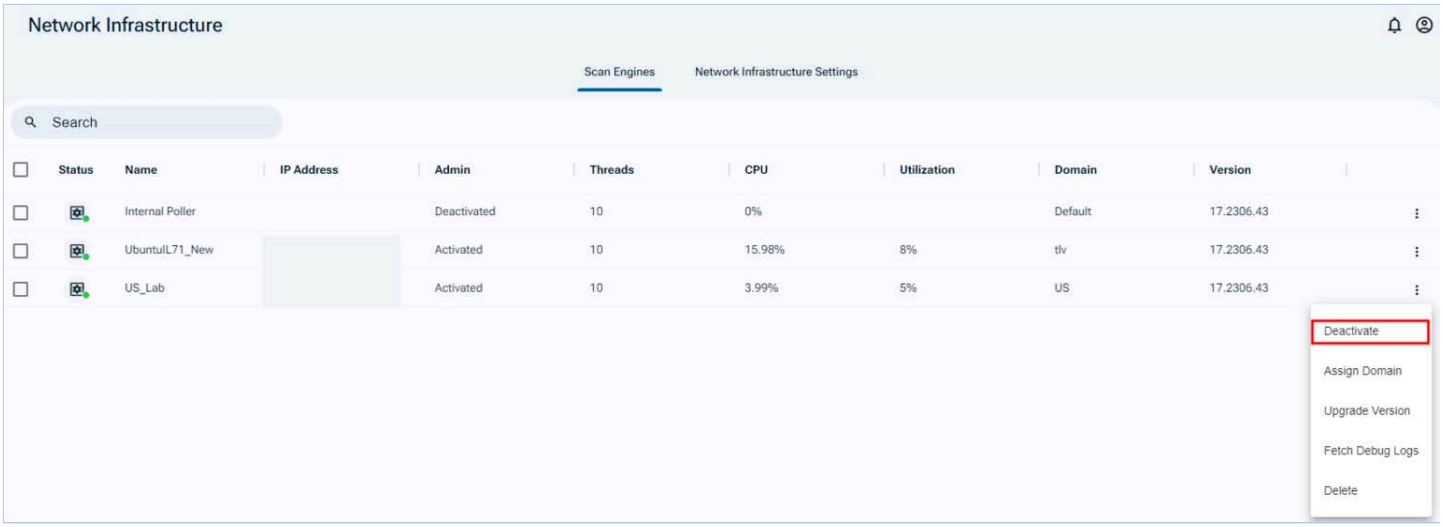



Network Infrastructure – Activate Scan Engine

2. In the **Scan Engines** list, click the icon next to the Scan Engine you want to activate, then select **Activate.**
3. If required, adjust the Scan Engine priority intervals.

## To Deactivate a Scan Engine

1. On the Sepio menu, select: **Settings** -> **Network Infrastructure** -> **Scan Engines.**




Network Infrastructure – Deactivate Scan Engine

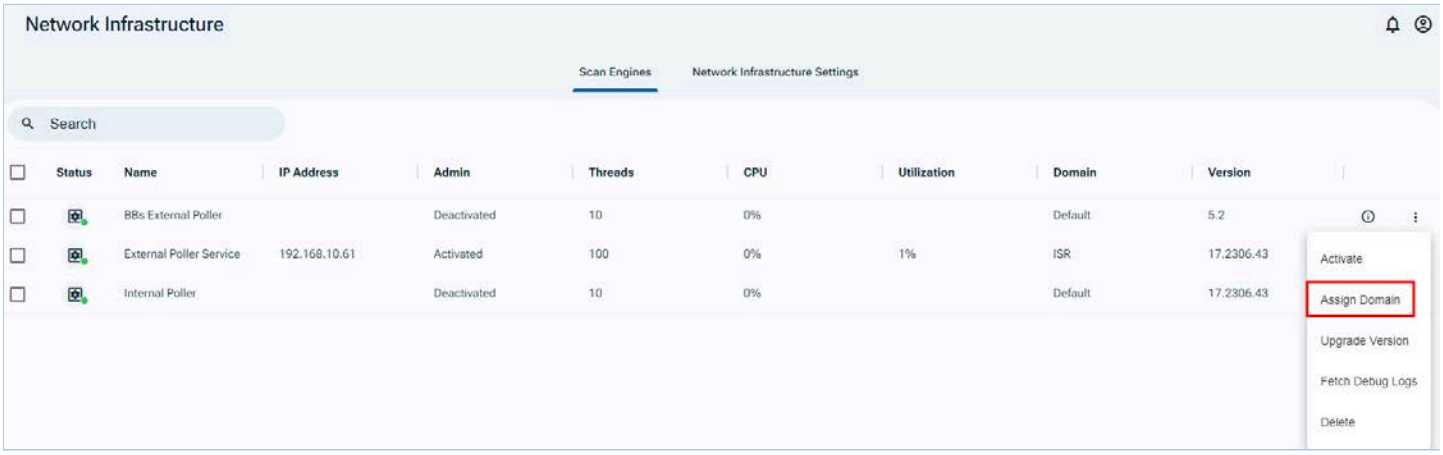
2. In the **Scan Engines** list, click the icon next to the Scan Engine you want to deactivate, then select **Deactivate**.

# Assigning Domains of a Scan Engine or Network Element

## To Assign a Domain to a Scan Engine

You assign a Domain to a Scan Engine or to a NE.

- From the Sepio menu select **Settings** ->**Network Infrastructure** ->**Scan Engines**
- Click ⋮ next to the Scan Engine to assign a Domain and select **Assign Domain**

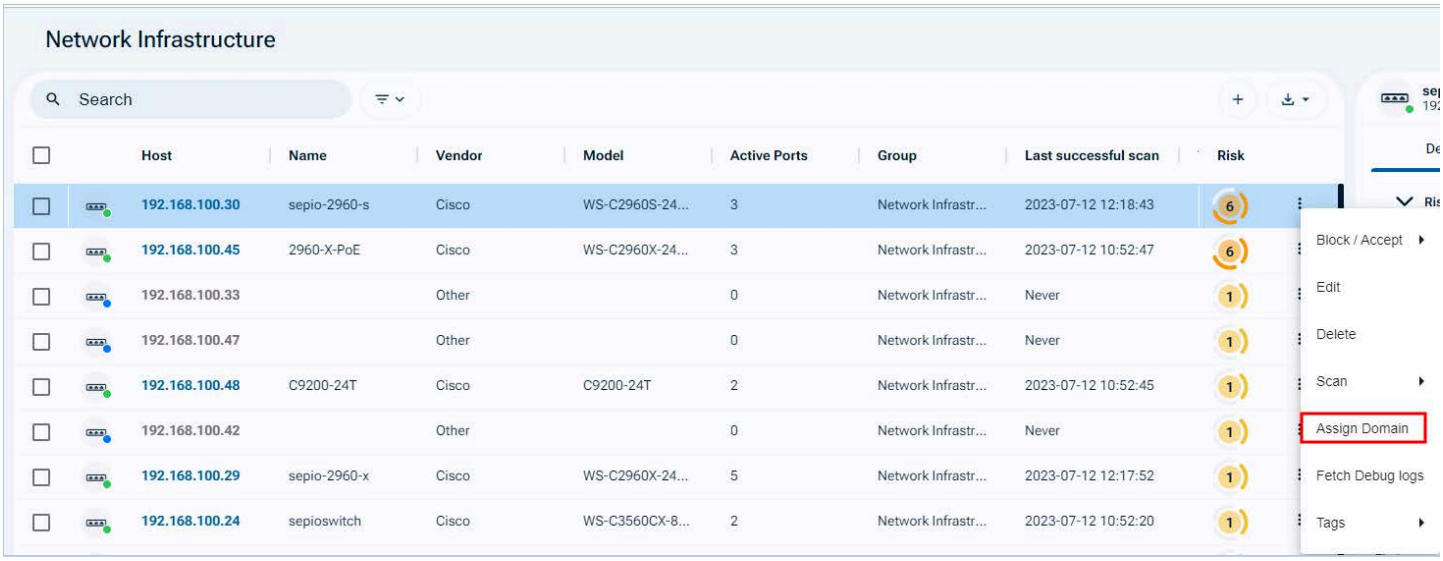



Select Assign Domain

- Select the required Domain from the list and click **Save**

## To Assign a Domain to an Network Element (Switch)

- From the Sepio menu select **Assets Visibility** ->**Network Infrastructure**




Select Assign Domain

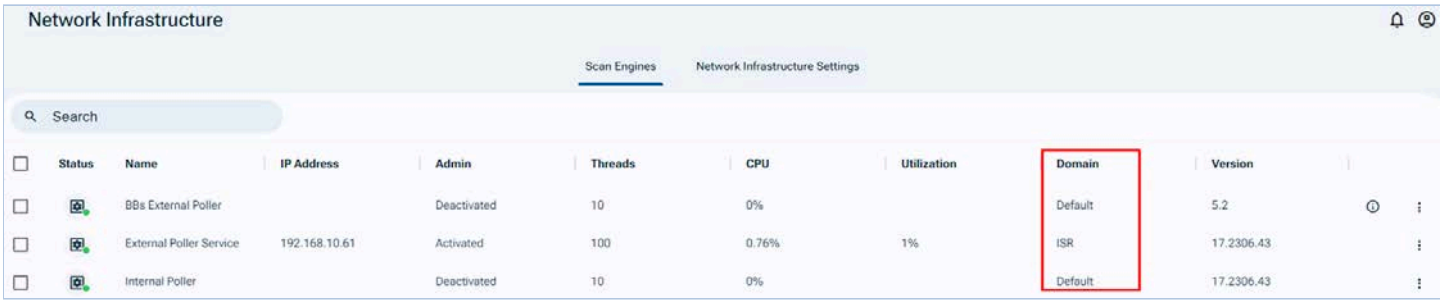
- Click ⋮ next to the NE to assign a Domain and select **Assign Domain**
- Select the required Domain from the list and click **Save.**




Assign Domain

## To View a Domain of a Scan Engine

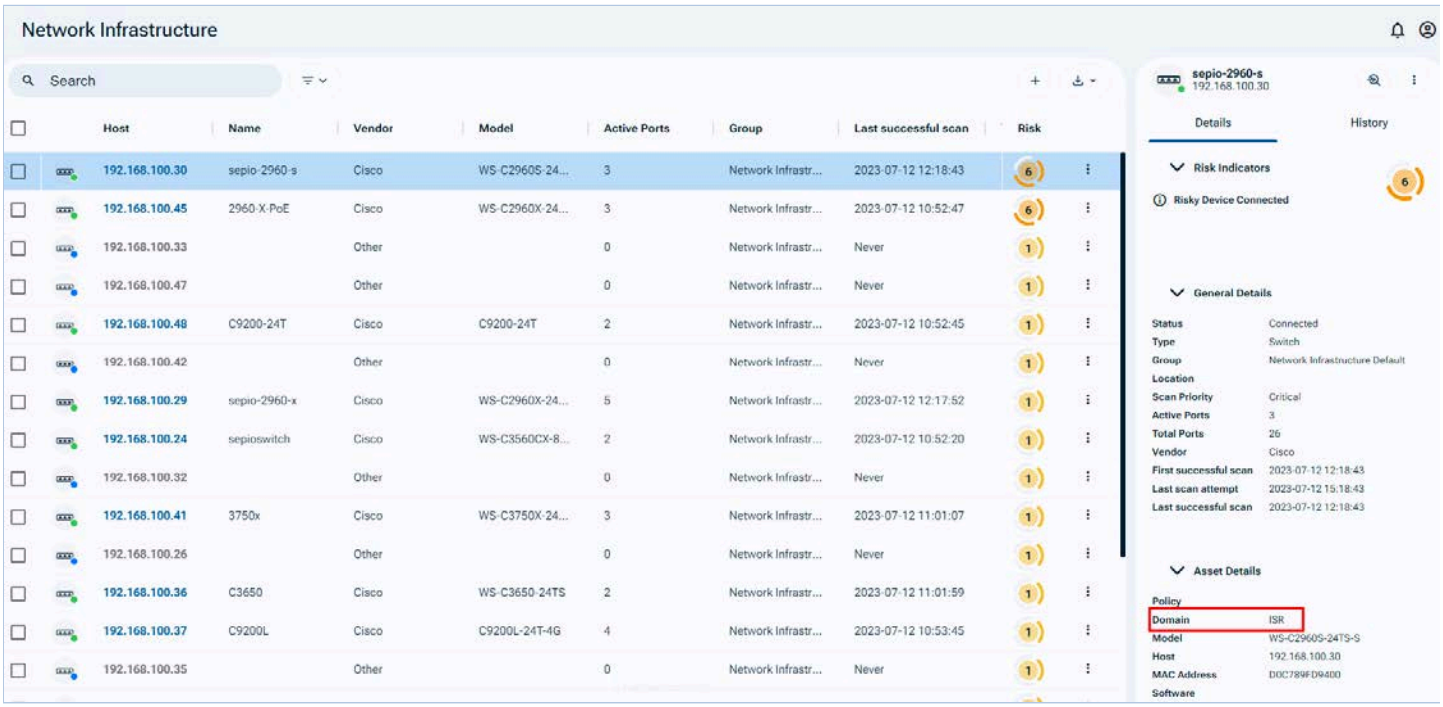
From the Sepio menu select **Settings** -> **Network Infrastructure** -> **Scan Engines**




Scan Engines

## To View a Domain of an Network Element (Switch)

From the Sepio menu select **Assets Visibility** -> **Network Infrastructure**




Asset Details – Domain

# Changing Scan Priority Intervals

## Overview

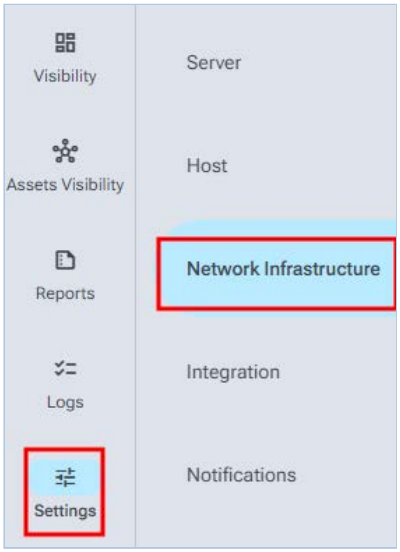
The Scan Engines are configured with the following default scanning intervals, which determine how often a Scan Engine collects data from a Network Element:

- **Critical:** scans every 1 minute
- **High:** scans every 30 minutes
- **Normal:** scans every 2 hours
- **Low:** scans every 8 hours
- **Occasional:** scans every 24 hours
- **Manual Only:** scans upon request

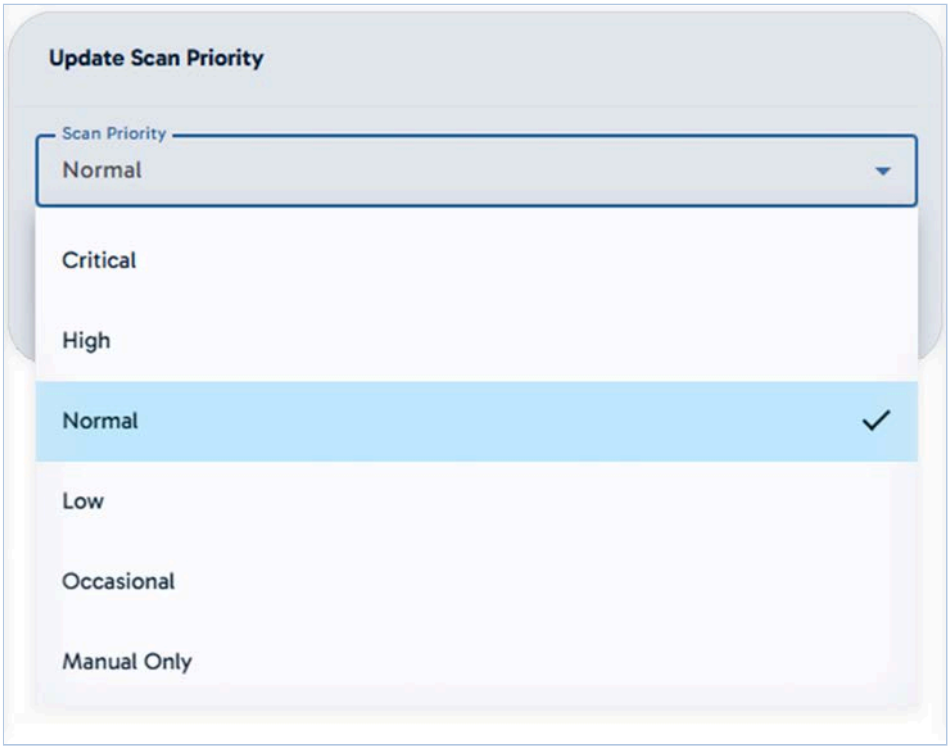
If required, you can change these intervals by following the procedure below.

## Modify the Scan Priority Intervals

1. On the Sepio menu, select: **Settings** -> **Network Infrastructure**




2. Navigate to: **Network Infrastructure** -> **Network Infrastructure Settings** -> **Update Scan Priority**




Network Infrastructure Settings – Update Scan Priority

3. Adjust the scan priority intervals as required.

**Note:** You can define a manual scan for any number of network infrastructure elements, which overrides any previously defined scan intervals for a specific device. When the manual scan option is selected, run the **Scan Now** command to initiate the scan.

## Related Topics

- About Scan Engines
- Adding a Domain
- Activating and Deactivating a Scan Engine
- Assigning Domains of a Scan Engine or Network Element
- Switch Scanning Status Explanations

# Switch Scanning Status Explanations

## Overview of the Scanning Process

When the Scan Engine establishes an SSH connection with a switch, it sends a series of commands categorized by importance. The success or failure of these commands determines the progression of the scanning process and the final scanning status.

## Key Initial Command

The first command executed is:

```
Terminal length 0
```

This command disables the default prompt behavior for the Scan Engine's SSH session, allowing the entire output to be displayed without interruptions. It is a critical command and must execute successfully.

- **Command Variability:** While some vendors support this command as-is, others require a different syntax. Sepio automatically determines the correct command based on the switch's initial response.

If this command is parsed successfully, the Scan Engine proceeds with executing the subsequent commands.

## Command Execution and Data Collection

Following the response, other commands are executed, and data is collected by the Scan Engine for processing.  Some commands might fail due to lack of execution permissions, specific device configuration or other hardware or software issues. Some commands are critical for the entire data collection process while others are related to network topology, configuration and additional data that Sepio uses for its operation.

- **If all the commands are executed successfully**, the switch Status will show "**connected**".
- **If a critical command fails** (e.g., extracting the switch model), the scanning process will be aborted. In case that the switch is supported by Sepio, the scan status result will be "**Internal Error**". If it is unsupported, the status will be "**Unsupported**".
- **If a non-critical command fails** (e.g., extracting AssetDNA data), the scanning process will continue. However, the resulting scan status will be "**Connected**" with a partial scanning indication.
- **If a non-impactful command fails** (e.g., reviewing the ARP table), the scanning process remains unaffected. The status will remain "**Connected**", and details about the failed commands can be reviewed in the debug logs.

## Switch Scanning Status Table

This categorization ensures clarity in identifying and addressing issues during the scanning process. The following table provides a summary of the Switch Scanning Status results:

| Scan Status | Description | Possible Reason |
|---|---|---|
| Connected | Scan completed successfully. | All critical commands were executed successfully. |
| Connected (Partial) | Scan completed with some limitations. | Non-critical commands failed (e.g., extracting AssetDNA data). |
| Internal Error | Scan failed due to an internal error within the Sepio system. | Critical command failed (e.g., extracting switch model) and the switch is supported by Sepio. |
| Unsupported | Switch models are not supported by Sepio. | Critical command failed (e.g., extracting switch model) and the switch is not supported by Sepio. |
| Unable to connect | Scan Engine cannot establish SSH connection to the switch. | There is a temporary issue, probably a networking or routing problem that is preventing the Scan Engine from reaching the switch and establishing the SSH session. It is also possible that the device's response time exceeds Sepio's default timeout of 10 seconds. |
| Authentication failed | The Scan Engine cannot log-in to the switch. | There is a temporary issue, probably Radius/Tacacs problem that is preventing the Scan Engine from successfully login to the switch. |
| Initializing | The Scan Engine was able to import the switch information but is unable to complete the first scan. | The first scan is not completed. In some cases, when the scan was interrupted and was not completed successfully the switch will remain in this state. |

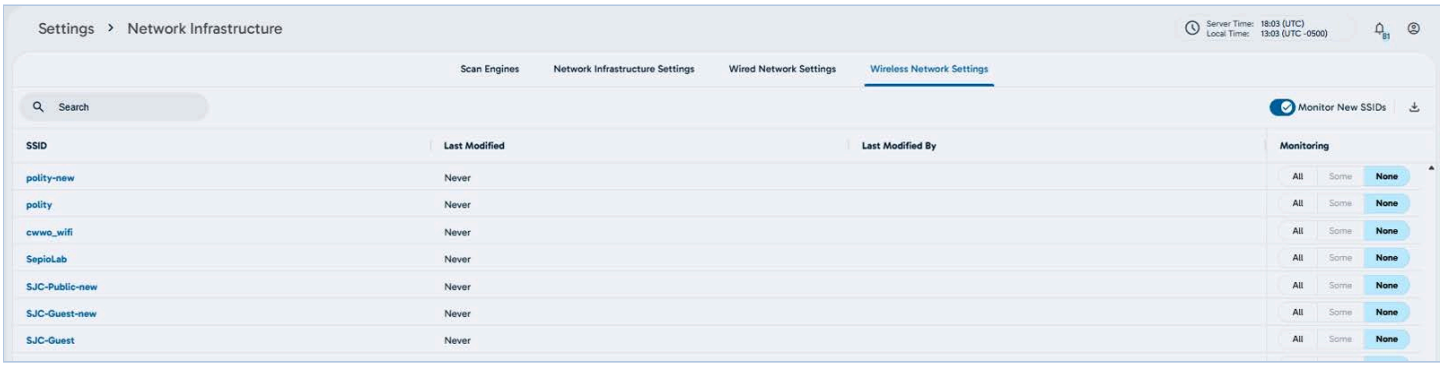
**Note:** The specific commands considered critical or non-critical may vary depending on the switch hardware and operating system / firmware version.

# Wireless Network Management

## Overview

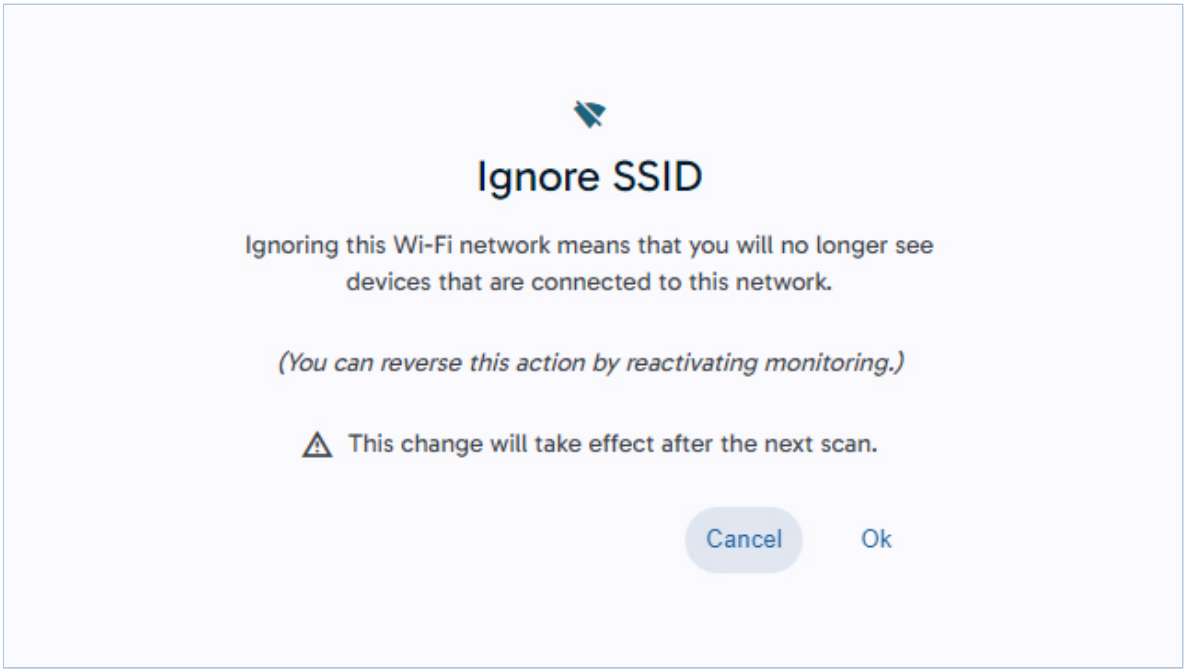
Sepio identifies network assets across both wired and wireless networks. There are use cases in which devices on certain wireless networks should not be discovered, monitored, or managed by Sepio. For example, when a wireless network provides guest access, some organizations are required not to monitor its devices. Security administrators can define which networks should be monitored with Sepio.

The wireless network names (based on SSID) are collected automatically from managed access points and will appear in the UI. To select which networks should be monitored, use the monitoring options: All, Some, or None.



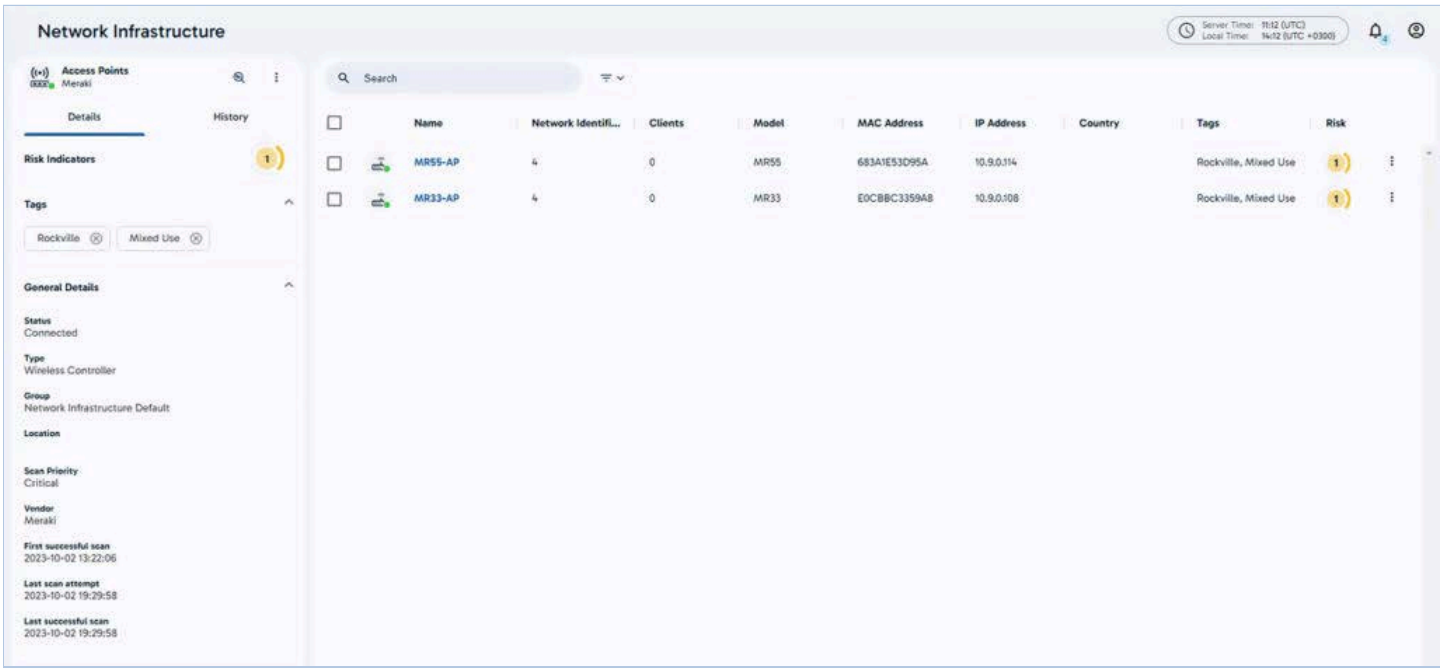

Network Infrastructure > Wireless Network Settings

In order for the ignore operation to become effective, you should approve the action:




Ignore SSID

Additional information regarding the SSID and the access points they are associated with is available for every device. For example, there are two access points connected with this Meraki device.




Network Infrastructure > Additional information regarding the SSID

## Clicking on the access point will provide detailed information.




Access Point Details

# Wired Network Management

## Overview

Sepio identifies network assets across both wired and wireless environments. In certain use cases, such as when a network is designated for testing, devices within specific networks may need to be excluded from discovery, monitoring, or management. While it is possible to exclude an entire switch from monitoring by adjusting its scanning interval, Sepio enables security administrators to define more granular settings using VLAN information, adding important business context.

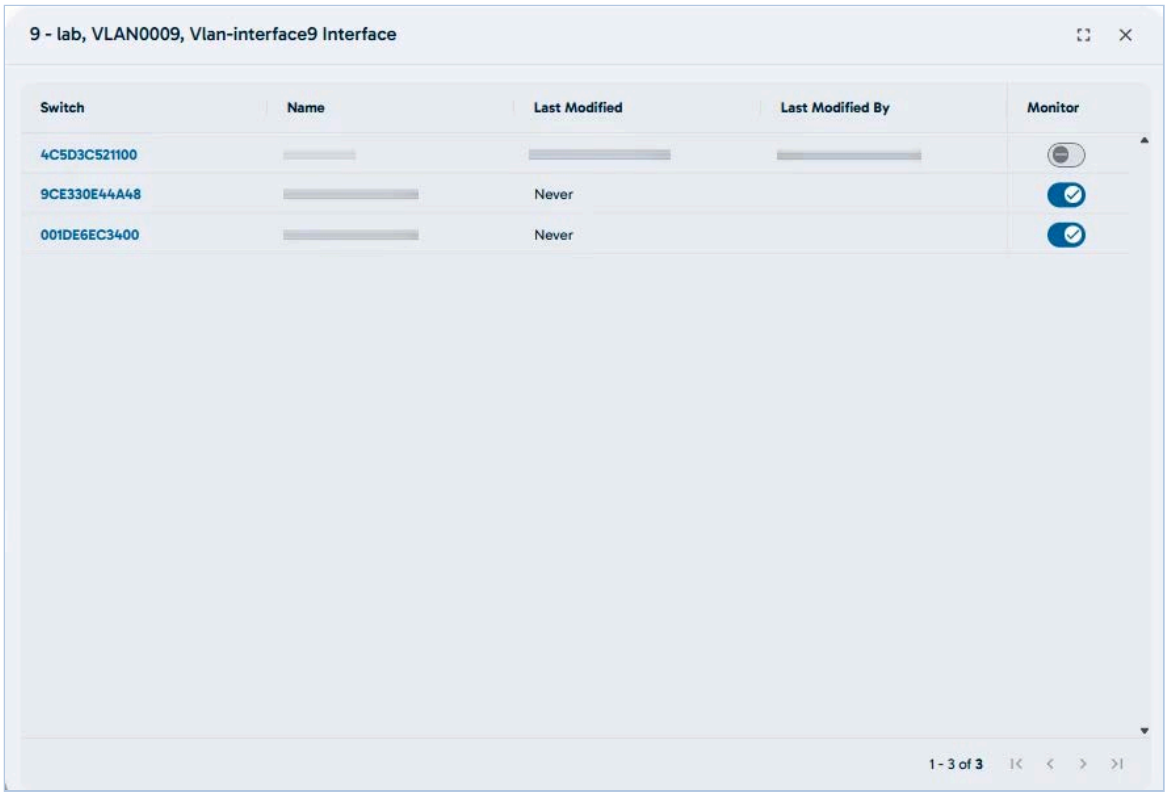
VLANs from managed switches are automatically collected and displayed in the UI. To exclude a network from monitoring, toggle the action button (Monitor on/off).
If an asset is linked to a VLAN that is later excluded from monitoring, the asset will be removed.

To configure VLAN monitoring, go to: **Settings** -> **Network Infrastructure** -> **Wired Network Settings**.



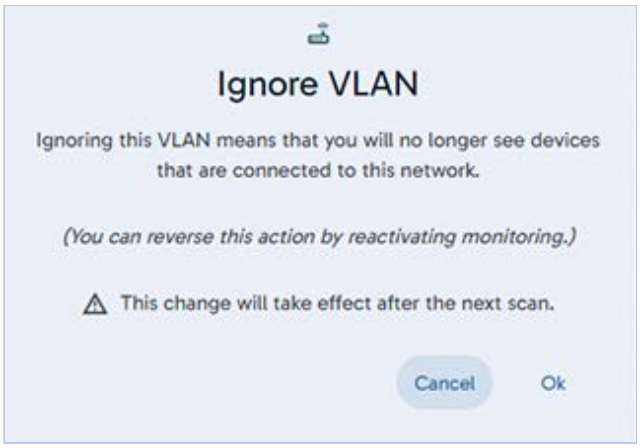

Wired Network Settings

VLAN exclusion is granular: you can exclude a VLAN across all switches or limit the exclusion to specific switches.




Granular VLAN exclusion – excluding specific switches

## When a VLAN is excluded from monitoring, the following message appears:




VLAN is excluded from monitoring

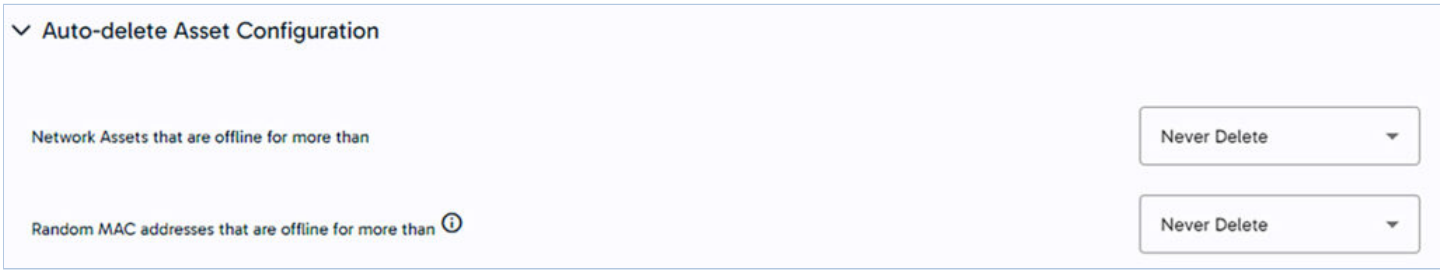
# Network Asset Ageing

Sepio Administrators can manage the ageing of network devices. When a device reaches the defined age without being seen during this duration, it will be automatically deleted from the assets database.

There are different ageing configuration options for regular assets and assets that use random MAC addresses.

> **Note:** Random MAC addresses ageing defines override settings of regular network assets.

To define asset ageing and automatic deletion edit the configuration options form the UI **Settings** -> **Server** -> **Server settings**




Auto Delete Asset Configuration

Use the drop-down menu to set the values.

Possible ageing values are pre-defined and can be set to one of the following: Never, one day, three days, one week, two weeks, one month, three months, six months and one year. The ageing of Random MAC addresses can be also set to just one hour.

# User Management

## Related Topics

- Creating Users
- User Types
- Authentication and Authorization
- Static API Keys for Machine Identities
    - API Key Management

# Static API Keys for Machine Identities

## Related Topics

- API Key Management

# API Key Management

## Overview

API Keys allow your organization to authenticate automated systems, scripts, and third-party integrations with Sepio without requiring an interactive user login. They are long-lived credentials designed for **machine-to-machine communication**.

## Key Features

> **Note:** Available starting Sepio Platform v58 .

- Create named API keys with a descriptive label and application identifier so you can track which integration uses which key.
- Assign a permission level (**Administrator, Manager, or User**) to control what each key can access.
- Set an optional expiration date or let keys remain valid indefinitely.
- Revoke keys instantly when they are no longer needed or may have been compromised.
- Track usage to see when each key was last used, who created it, and when.

## How to Use

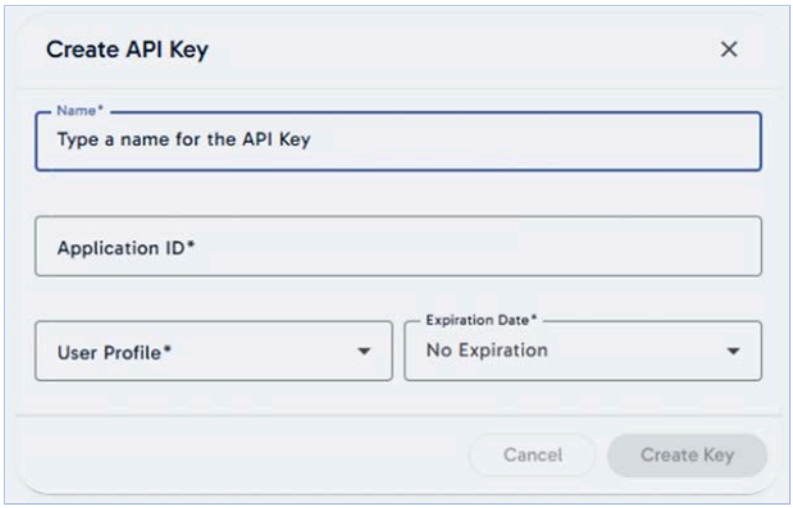
The `ENABLE_API_KEY` flag must be enabled to create API keys.

### Creating a Key

1. Navigate to the API Key management section on the **Settings** -> **Server** page (Administrator privileges required).
2. Provide a **name** (e.g. “SIEM Integration”), an **application identifier** (e.g. “splunk-connector”), and a **permission level**.
3. Optionally, set an expiration date.
4. The full API key is displayed **only once after creation**. Copy and store it in a secure location, **as it cannot be retrieved later**.




Settings -> Server -> API Keys



Create API Key

## Authenticating with a Key

Include the key in your API requests using either of the following methods:

| Method | Header |
| --- | --- |
| Dedicated header | `X-API-Key: sepio_...` |
| Bearer token | `Authorization: Bearer sepio_...` |

## Revoking a Key

Select the key from the list and revoke it. The key is **immediately and permanently** disabled. Any system using the revoked key will no longer be able to authenticate. To restore access, create a new key.

## Security

- API keys are **never stored in plain text**. Only a secure hash is kept.
- The full key is shown **only once at creation** and cannot be recovered afterward.
- Revocation is **instant and irreversible**, ensuring compromised keys can be deactivated immediately.
- All key lifecycle events (creation, usage, revocation) are **audited** with timestamps and usernames.

## Permissions

Only **Administrators** can create, view, and revoke API keys. The permission level assigned to a key determines what the bearer of that key can access. It works the same as user role permissions throughout the application.

**Note:** if `ENABLE_API_KEY` is disabled, all API keys will stop working. If re-enabled, they will start working again — they will not be revoked.

## API Usage

Below is an example of how a customer can use Sepio's API key capabilities to create internal integrations.

### Endpoint & JSON Request Format

#### POST

`https://<SEPIO_HOST>/sepio-data`

#### Headers

`Content-Type: application/json`

The request body is a JSON object with the following structure:

```
{
  "operationName": "YourOperationName",
  "variables": {},
  "query": "query YourOperationName { ... }"
}
```

| Field | Type | Description |
|---|---|---|
| `operationName` | String | A name for the operation (can be any descriptive name) |
| `variables` | Object | GraphQL variables (can be empty {}) |
| `query` | String | The GraphQL query string |

### Extract GraphQL from Sepio Management Platform

The Sepio Management Platform provides the ability to use its filtering system and extract queries in GraphQL format, which can then be used for internal integrations.



GraphQL Format

### Querying All Assets

The main query for fetching assets is **conditionalTable**. It accepts the following parameters:

- **query** - an object containing:
  - filters
  - systemFilters
  - globalSearch
- **pagination:**
  - pageSize
  - pageNumber
  - sortBy

Example: Basic Query – First Page of Assets (No Filters)

```
{
"operationName": "GetAssets",
"variables": {},
"query": "query GetAssets { conditionalTable(query: { filters: [], systemFilters: [],
globalSearch: \"\" }, pagination: { pageSize: 100, pageNumber: 0, sortBy: \"riskLevel_desc\"
}) { data { id assetDisplayName ipAddress vendor mac riskLevel isOnline statusDescription
typeDescription } recordsFiltered recordsTotal } }"
}
```

**cURL Example:**

```
curl -X POST https:///sepio-data \
-H "Content-Type: application/json" \
-H "X-API-Key: sepio_your_api_key_here" \
-d '{
"operationName": "GetAssets",
"variables": {},
"query": "query GetAssets { conditionalTable(query: { filters: [], systemFilters: [],
globalSearch: \"\" }, pagination: { pageSize: 100, pageNumber: 0, sortBy: \"riskLevel_desc\"
}) { data { id assetDisplayName ipAddress vendor mac riskLevel isOnline statusDescription
```

```
typeDescription } recordsFiltered recordsTotal } }"
}'
```

### Filtering

Filters are passed as an array of filter objects inside `query.filters`. Each filter object has the following fields:

| Field | Type | Description |
|---|---|---|
| index | Int | Position index of the filter (0, 1, 2...) |
| field | String | The asset field to filter on (e.g., "`riskLevel`", "`isOnline`") |
| expression | String | The filter expression (see table below) |
| value | String | The filter value |
| op | String | Logical operator: "`AND`" or "`OR`" |
| conditionTypeValue | String | "`freetext`" for free-text values, "`multiple`" for multi-select |
| is_userattribute | Boolean | `true` if filtering a custom/dynamic field (prefix z_), otherwise `false` |

### Response Structure

```
{
  "data": {
    "conditionalTable": {
      "data": ,
      "recordsFiltered": 1,
      "recordsTotal": 500
    }
  }
}
```

### Response Field

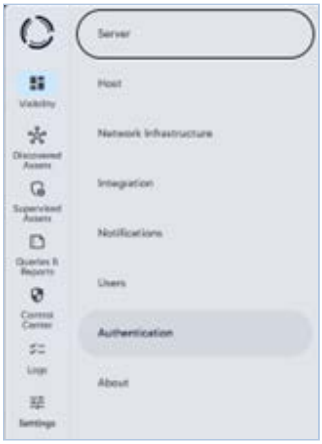
- recordsTotal - total assets in the system (before filter)
- recordsFiltered - assets matching the filter

### Error Responses

| HTTP Status | Meaning |
| --- | --- |
| 200 | Success (check data/errors in JSON body) |
| 401 | Invalid or missing API key |
| 403 | Valid API key but insufficient permissions |

# Authentication and Authorization

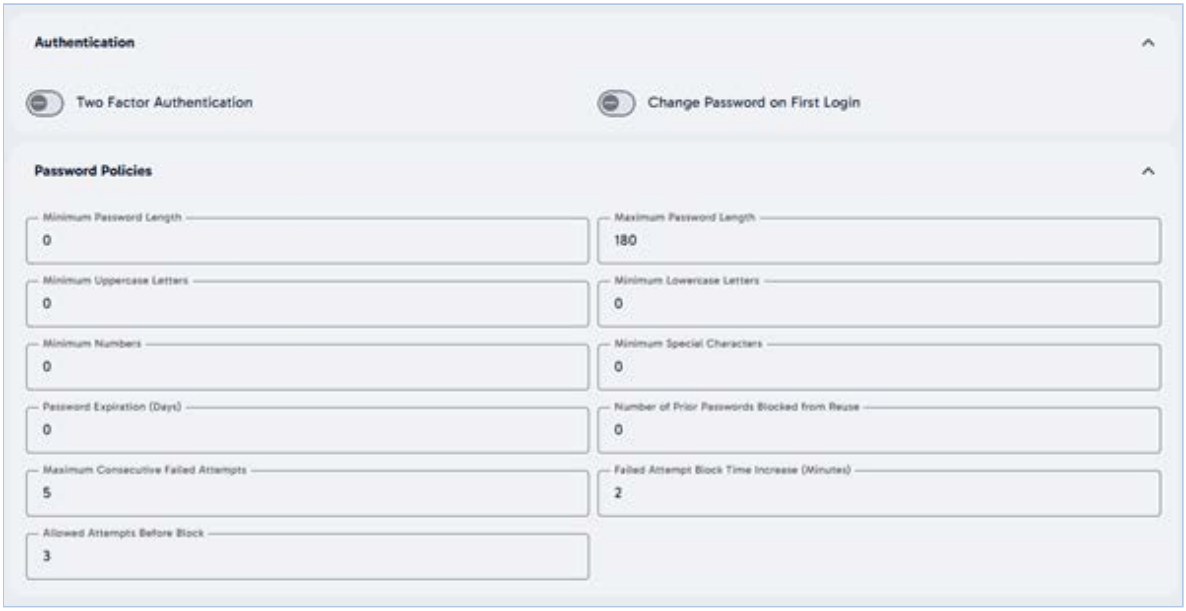
In order to configure password policies and authorization strategies, use the authentication page (under the Settings menu).



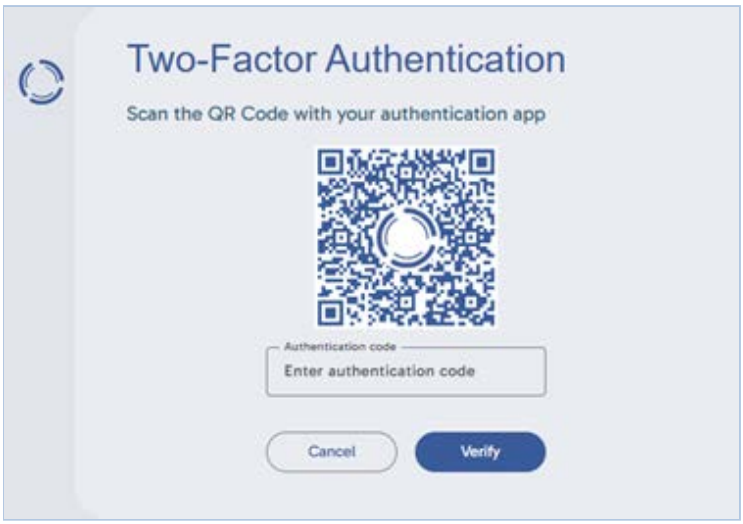

Settings menu

In this page, it is possible to define global password policy requirements, including minimum length, the use of uppercase and lowercase letters, numbers, and special characters.

In addtion, one can enable two-factor authentication (2FA) using QR codes compatible with apps such as Google Authenticator or Microsoft Authenticator, and enforce password changes upon a user's first login.

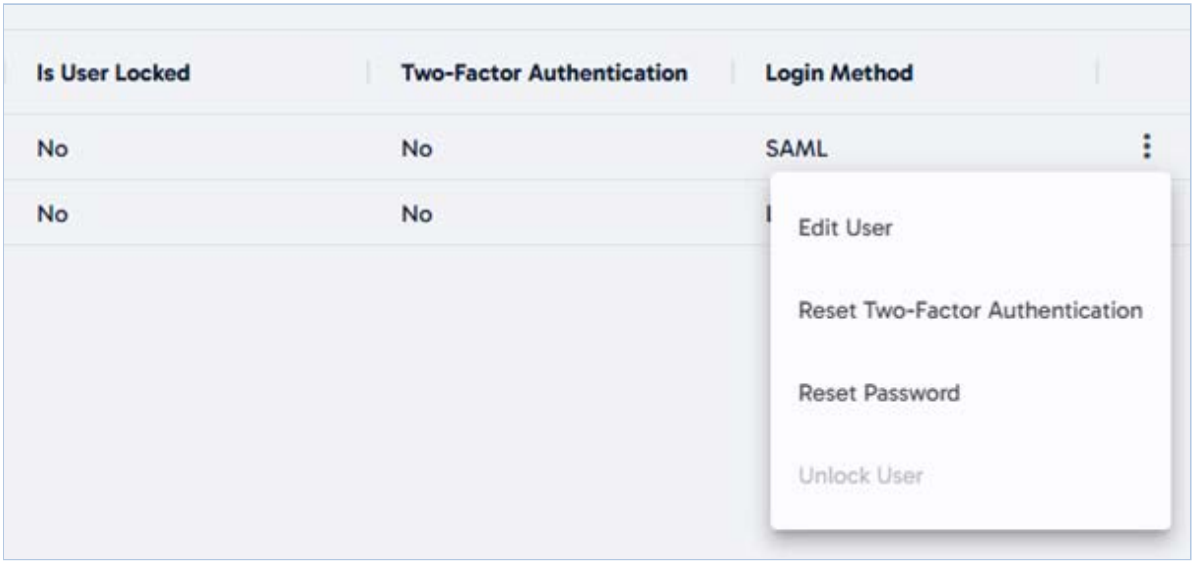



Authentication – Password Policies




Two-Factor Authentication – QR Code

**Note:** Reset passwords and unlock user accounts directly from the User Settings page.




User management and support

# Creating Users

## Overview

Profiles define how users access views and data, and what they can do within the Platform. When you create a user, you assign a profile to each one.

After logging in to Sepio for the first time you can create a user profile for each new user.

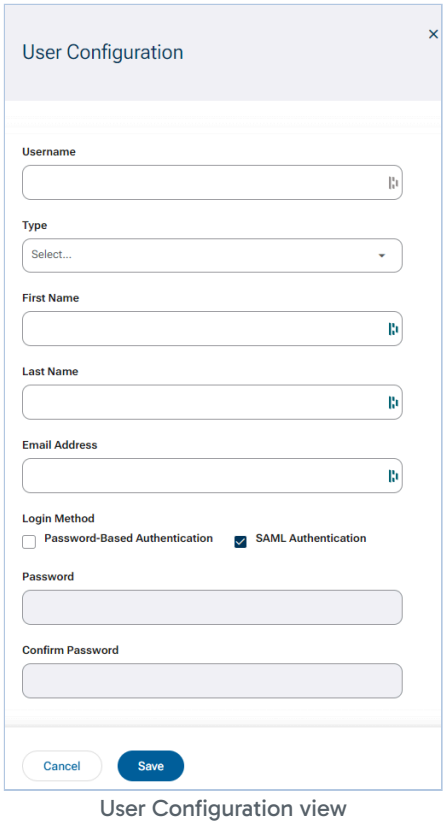
## To Create a User Profile

1. Log in to Sepio as an Administrator.
2. On Sepio main menu go to **Settings** -> **Users**
3. Click Create




Create a user profile

4. In the User Configuration view, enter information as described in the following table.




User Configuration view

## User Configuration Table

| Field | Description | Options |
|---|---|---|
| Username | A unique name given to a user to identify them on a computer network. | – |
| Type | User permission type, read write and execute. | • Administrator<br>• Manager<br>• User |
| First Name | User's first name | – |
| Last Name | User's last name (surname) | – |
| Email address | User's email address | – |
| Login Method | User authentication method | • Password – Based Authentication<br>• SAML – Authentication.<br><br>**Note:** Configure and enable SAML before selecting this option |
| Password | User's password | – |
| Confirm Password | User's password confirmation | – |

5. Click Save

**Note:** Authentication and Authorization policies are global and thus user actions must adhere to the system's policies.

# User Types

## Sepio Platform User Roles

Sepio platform supports 3 roles: Administrator, Manager and User.
Sepio Platform users with Administrator permissions are super-users and can perform any action within the platform. Managers have similar capabilities, but they are not allowed to create other platform managers while “users” have limited capabilities.

## Sepio Platform User Roles Capabilities

The table below shows the different capabilities for each user type.

| | User | Manager | Administrator |
|---|---|---|---|
| Create, modify, add users | – | – | + |
| Change self-password | + | + | + |
| Change other self attributes | – | – | + |
| Change scan engine settings | – | + | + |
| Change scan priorities | – | + | + |
| Import switches – bulk operations | – | + | + |
| Change Wi-Fi networks | + | + | + |
| View the audit | – | + | + |
| View the event log | + | + | + |
| View reports | – | + | + |
| Create policies | – | – | + |
| View asset visibility | + | + | + |
| Perform actions on Network infrastructure | – | + | + |
| Accept risk | + | + | + |
| Add / delete tags | + | + | + |

| | User | Manager | Administrator |
|---|---|---|---|
| Run Queries | – | + | + |
| View settings/host | + | + | + |
| Edit settings/host | – | + | + |
| View and Edit Integration | – | + | + |
| View and Edit notifications | – | + | + |

## Supported Network Elements

Sepio collects information from supervised infrastructure elements using its Scan Engines and employs two asset-discovery methods in its Asset Risk Management Platform.

There are two different software attributes that define how Sepio supports a managed network device:

1. Network infrastructure hardware and its Internal Operating System (IOS)
2. Supported connectivity protocols and relevant encryption algorithms for SSH, secure SNMP, and TLS/SSL for API communication.

# Supported Network Elements Using Asset DNA

## Overview

Sepio uses two Asset discovery methods in its Asset Risk Management Platform:

## Universal Discovery

This method uses SNMP version 2c or SNMP version 3 for asset detection (assets include network elements, devices, and their peripherals). The Platform supports any asset that generates an SNMP engine ID.

## Asset DNA

This is Sepio's proprietary discovery method. It establishes trust in each asset's identity by analyzing the asset's unique characteristics that cannot be altered or spoofed by attackers, ensuring reliable device monitoring and detection of unauthorized or rogue devices.

## Switches and IOS

The following Switches and IOS are supported:

- Arista
- Aruba
- Cisco
- HP
- Huawei
- Juniper
- Meraki
- Rockwell Automation
- Ruijie Networks

## Supported Switches and IOS Link List

The following Switches and IOS are supported:

- Arista
- Aruba
- Cisco
- HP
- Huawei
- Juniper
- Meraki
- Rockwell Automation
- Ruijie Networks

# Arista

## Arista Switches

The following switches are supported.

- DCS-7050T-36
- DCS-7050T-52
- DCS-7050T-64
- DCS-7050SX3
- DCS-7150S-52
- 7050SX3-48YC8
- 7050SX3-48C8
- CCS-758-CH-F
- CCS-758-25-BND
- CCS-720XP-96ZC2-F
- CCS-720XP-96ZC2-4F

**Note:** DNA collection is currently not available for the next Arista switches:

- 7050SX3-48YC8
- 7050SX3-48C8
- CCS-758-CH-F
- CCS-758-25-BND
- CCS-720XP-96ZC2-F
- CCS-720XP-96ZC2-4F

## Arista EOS Software Versions

The following versions are supported.

- 4.12.7.1

# Aruba

## Aruba Switches

The following switches are supported.

- 2930F-24G-PoE+-4SFP
- 2930F-48G-740W-PoE+-4SFP
- 3810M-16SFP+-2-slot
- 3810M-24G-1-slot
- 3810M-24G-PoE+-1-slot
- 3810M-48G-PoE+-1-slot
- 6100 24G CL4 4SFP+
- 6200M 36G 12SR5 PoE 4SFP+
- 6300M 48G CL4 PoE 4SFP56
- 2530 Series
- 2540 Series
- 2920 Series
- 2930F Series
- 2930M Series
- 3810 Series
- 5400R Series

**Note:** DNA collection is currently not available for the next Aruba switches:

- 2530 Series
- 2540 Series
- 2920 Series
- 2930F Series
- 2930M Series
- 3810 Series
- 5400R Series

# Cisco

## Cisco Switches

The following switches are supported.

- **Cisco Catalyst 1000 Series**
- **Cisco Catalyst 2960 Series**
- **Cisco Catalyst 3560 Series**
- **Cisco Catalyst 3650 Series**
- **Cisco Catalyst 3750 Series**
- **Cisco Catalyst 3850 Series**
- **Cisco Catalyst 4500 Series**
- **Cisco Catalyst 4900 Series**
- **Cisco Catalyst 9200 Series**
- **Cisco Catalyst 9300 Series**

**Cisco Catalyst 9400 Series**

**Cisco Catalyst 9500 Series**

**Cisco Nexus Series**

**Cisco IE – 2000**

**Cisco IE – 3000**

**Cisco IE – 3200**

**Cisco IE – 4000**

**Cisco IE – 5000**

## Cisco Catalyst Micro Switches

- CMICR-4PT
- CMICR-4PS
- CMICR-4PC

**Note:** DNA collection is currently not available for the following Cisco switches:

- Catalyst Micro Switch (CMICR-4PT)
- Nexus 9000 (N9K)
- Nexus 3172 (C3172)
- Catalyst IE3200 (IE-3200)

## IOS Versions

Other versions are supported as well, but the minimum set of tested and verified versions are:

**Cisco IOS Versions 3**

**Cisco IOS Versions 9**

**Cisco IOS Versions 12**

**Cisco IOS Versions 15**

**Cisco IOS Versions 16-17**

# HP

## HP Switches

The following switches are supported.

- HPE 4800G
- HPE 5130
- HPE 5139
- HPE 5120
- HPE 7902
- HPE 5950
- HPE 5940
- H3C S5500-52C-EI (3Com 4800)
- HP 3600 v2 series with Comware 3 OS

**Note:** DNA collection is currently not available for the next HPE switches:

- HP 3600 v2 series with Comware 3 OS

## HP Comware Version

The following switches are supported.

- 5.x
- 7.x

# Huawei

## Huawei Switches

The following switches are supported.

- S5735-L48T4X-A1
- S5735-L48P4X-A
- S5735-L24T4S-A1
- S5735-L24P4S-A
- S5731-S48P4X
- S5731-S24P4X
- S5720-52P-PWR-LI-AC

# Juniper

## Juniper Switches

The following switches are supported. It is likely that other models will work as well.

- ex4200-48p
- ex4300-24t
- ex4300-32f
- ex4300-48mp
- ex4300-48p
- ex4300-48t
- mx480
- qfx5100-48s-6q
- qfx5100-96s-8q

**Note:** DNA collection is currently not available for the next Juniper switches:

- ex4200
- ex4300-32f
- qfx5120

## Junos Software Versions

The following versions are supported.

#### Junos 13

- 13.2X51-D26.2
- 13.2X51-D32.1
- 13.2X51-D35.3
- 13.2X51-D38

#### Junos 14

- 14.1X53-D30.7
- 14.1X53-D42.3
- 14.1X53-D46.7
- 14.1X53-D46.7

#### Junos 15

- 15.1R3.6
- 15.1R4-S6.2

- 15.1R7-S6.3
- 15.1R7.8

**Junos 16**

- 16.12.02
- 16.12.1
- 16.12.3a
- 16.12.4
- 16.6.2
- 16.6.3
- 16.6.4
- 16.6.5
- 16.6.6
- 16.9.2
- 16.9.3
- 16.9.4

**Junos 17-19**

- 17.03.03
- 17.3R3-S7.2
- 18.4R3.3
- 19.3R2-S1.5
- 19.3R2.9
- 19.4R3-S3.3

# Meraki

## Meraki Switches

The following switches are supported. It is likely that other models will work as well.

**Note:** DNA collection is currently not available for Meraki due to the API limitations.

- MS120-48FP
- MS120-48LP
- MS120-8
- MS120-8FP
- MS125-24
- MS125-24P
- MS125-48LP
- MS130-8
- MS130-8P-I
- MS130-24P
- MS130-48P
- MS210-24P
- MS210-48FP
- MS220-24P
- MS220-48FP
- MS220-8P
- MS225-24P
- MS225-48FP
- MS250-24
- MS250-48
- MS320-24P
- MS355-24X2
- MS355-48X2
- MS390-24
- MS390-24P
- MS390-48
- MS390-48U
- MS410-16
- MS425-16
- MS425-32

## Cisco Switches with Meraki Firmware

- C9300-24U

- C9300-48UXM

# Rockwell Automation

## Rockwell Automation Switches

The following switches are supported.

- Stratix 5400
- Stratix 5410
- Stratix 5700
- Stratix 5800

# Ruijie Networks

## Ruijie Networks Switches

The following switches are supported. It is likely that other models will work as well.

**Note:** DNA collection is currently not available for Ruijie Networks due to the API limitations.

- RG-NBS3100 Series

## Wireless LAN Controllers (WLC)

The following Wireless LAN Controllers are supported:

- Cisco WLC
- Meraki WLC

# Cisco

## Cisco WLC

The following Wireless LAN Controllers (WLC) are supported.

- AIR-CT2504
- AIR-CT2504-K9
- AIR-CT3504
- AIR-CT3504-K9
- AIR-CT5208
- AIR-CT5220
- AIR-CT5508-K9
- AIR-CT5520-K9
- AIR-CT8510
- AIR-CT8510-K9
- AIR-CT8540
- C9800-80-K9-FAN
- C9800-L-C-K9
- C9800-L-F-K9-FAN
- C9800-L-F-K9-FAN

# Meraki

## Meraki WLC

The following Wireless LAN Controllers (WLC) are supported.

- MR20
- MR46
- MR78
- MR86
- MR55
- MR33

# Meraki Cloud-Managed Wi-Fi Access Points

- Meraki WAP

# Wireless Access Points (WAP)

The following Wireless Access Points (WAP) are supported.

- Meraki

# Meraki

## Meraki WAP

The following Wireless Access Points (WAP) are supported.

- MR20
- MR46
- MR78
- MR86
- MR55
- MR33

# Supported Encryption Algorithms

This page lists the different encryption algorithms and methods that are supported by Sepio platform starting from V29.

## Encryption Methods

The following encryption methods are supported:

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm
- aes256-gcm
- aes128-cbc
- aes192-cbc
- aes256-cbc
- 3des-cbc
- blowfish-cbc
- twofish-cbc
- twofish192-cbc
- twofish128-cbc
- twofish256-cbc
- arcfour
- arcfour128
- arcfour256
- cast128-cbc

## Key Exchange Methods

The following key exchange methods are supported:

- curve25519-sha256
- curve25519-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group16-sha512
- diffie-hellman-group14-sha256

- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1

## Public Key Authentication

The following private key formats are supported:

- RSA in OpenSSL PEM (“BEGIN RSA PRIVATE KEY”) and ssh.com (“BEGIN SSH2 ENCRYPTED PRIVATE KEY”) format
- DSA in OpenSSL PEM (“BEGIN DSA PRIVATE KEY”) and ssh.com (“BEGIN SSH2 ENCRYPTED PRIVATE KEY”) format
- ECDSA 256/384/521 in OpenSSL PEM format (“BEGIN EC PRIVATE KEY”)
- ECDSA 256/384/521, ED25519 and RSA in OpenSSH key format (“BEGIN OPENSSH PRIVATE KEY”)

Private keys can be encrypted using one of the following cipher methods:

- DES-EDE3-CBC
- DES-EDE3-CFB
- DES-CBC
- AES-128-CBC
- AES-192-CBC
- AES-256-CBC

## Host Key Algorithms

The following host key algorithms are supported:

- ssh-ed25519
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- rsa-sha2-512
- rsa-sha2-256
- ssh-rsa
- ssh-dss

## Message Authentication Code

The following MAC algorithms are supported:

- hmac-sha2-256
- hmac-sha2-512

- hmac-sha2-512-96
- hmac-sha2-256-96
- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-md5-etm
- hmac-md5-96-etm

# Supported Operating Systems for Sepio Host Agent

The following are all supported operating systems for Sepio Agent. Check the Release Notes for any restrictions.

## Apple (macOS)

- macOS 14 and above
- Supported Devices: MacBook Pro with M-series processors

## Linux

- **RHEL:** Versions 7, 8, 9, and above
  - Note: Restrictions in Audit Mode. Please see Release Notes for details.
- **Ubuntu:** Version 16.04 and above
- **Debian:** Version 9 and above

## Windows

### Windows 7

- Enterprise (32-bit and 64-bit)
- Professional (32-bit and 64-bit)

### Windows 8.1

- Pro (64-bit)

### Windows 10

- Pro, Pro N, Pro Education, Pro for Workstations (64-bit)
- Enterprise, Enterprise N, Enterprise LTSC, Enterprise 2016 LTSB (64-bit)
- Education, Education N (64-bit)
- IoT Enterprise (64-bit)

### Windows 11

- Pro, Pro N, Pro Education, Pro for Workstations (64-bit)
- Pro Education ARM (64-bit Processor)
- Enterprise, Enterprise N, Enterprise Multi-session (64-bit)
- Business (64-bit)
- IoT Enterprise (64-bit)

**Windows Server**

- 2012 R2 Standard (64-bit)
- 2016 Standard, Datacenter (64-bit)
- 2019 Standard, Datacenter (64-bit)
- 2022 Standard, Datacenter (64-bit)

# Platform Operations

Platform Operations encompasses the ongoing management, monitoring, and operational administration of cybersecurity systems to ensure optimal performance, visibility, and security posture. In the context of enterprise security, platform operations involve the configuration, maintenance, and day-to-day operational tasks required to keep security infrastructure running effectively while providing actionable intelligence to security teams.

## Platform Operations Philosophy

Sepio's approach to platform operations is built on three core principles:

1. **Visibility:** Comprehensive monitoring and logging provide transparency into platform performance, asset inventory, and security events.
2. **Operational Efficiency:** Streamlined workflows and automation capabilities enable security teams to manage hardware risk at scale while reducing operational overhead
3. **Integration:** Seamless connectivity with enterprise security infrastructure through standard protocols (standard syslog, CEF) and purpose-built integrations (ServiceNow, SIEM platforms, Rest API and GraphQL)

This section of the documentation guides security administrators through the operational capabilities of the Sepio Platform, providing instructions for configuration, monitoring, and day-to-day management.

## Platform Operations in Sepio

The Sepio Platform provides comprehensive operational capabilities designed to manage and optimize your hardware risk management and Cyber-Physical Systems (CPS) security strategy. Sepio's platform operations framework enables security administrators to maintain full visibility and control over their network and endpoint infrastructure through a robust set of tools and operational workflows.

## Core Operational Capabilities

The documentation covers the following key areas:

#### Monitoring and Observability

- Comprehensive logging of event and audit messages for security analysis and compliance.
- Platform monitoring through Grafana dashboards for real-time visibility into the Sepio Management Platform's health and performance.
- Queries and Reports for generating custom security intelligence and compliance outputs.
- Licensing management for platform entitlements and usage tracking.

**Advanced Operations and Control**

- Operational Scenarios covering real-world use cases including Governance, Endpoint and Network Security, and deployment of allowed peripherals at scale.
- Managing Tags for organizing and categorizing assets across your infrastructure.
- ServiceNow CMDB Operations for synchronizing asset data with Configuration Management Databases.
- Shadow IT detection and management capabilities.
- Control Center for centralized platform management, including Scopes and Agent Mode configuration.

**Event Management and Integration**

- CEF Operations for exporting security events in Common Event Format, including both Network CEF Operations and Agent CEF Operations.
- Events API for programmatic access to platform events and security data.
- Integration with external SIEM platforms through syslog, Splunk add-ons, and vendor-specific connectors.

# Auto-Tagging and Tags

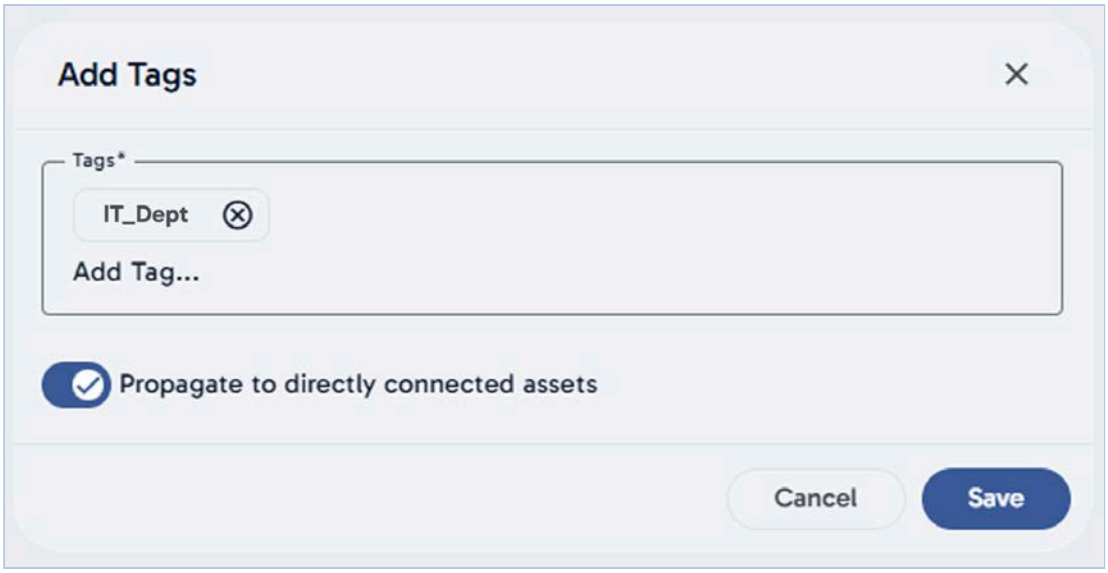
## Overview

Auto-Tagging rules can be used to automatically assign tags to assets based on their attributes.

## Methods for Creating Auto-Tagging Rules

### Propagation Rules

When manually adding a tag to host or switch, you can select "**Propagate to directly connected assets.**" This option automatically creates an Auto-Tagging rule. When an asset or device connects to the parent host or switch, the specified tag is automatically applied.




Add Tags – Propagate to directly connected assets

For example, if you tag a switch with "**IT_Dept**" and select "**Propagate to directly connected assets**", any asset connected to that switch will automatically receive the "**IT_Dept**" tag.

### Manually Created Auto-Tag Rules

Users can create custom auto-tagging rules based on collected asset attributes, including:

- **IP Address** (i.e. IP Addresses beginning with `10.10.1.`)
- **Hostname** (i.e. Asset Name begins with `ABC`)
- **Location** (i.e. the Switch or Host the asset is connected to)
- **Asset Type** (i.e. all WLC's)

## Creating Propagation Rules

- Locate the asset for which you want to create a propagation rule (host or switch).
- Click the **Tag** icon.
- Create your tag name and select "**Propagate to directly connected assets**".
- The tag will be applied to the selected host or switch, as well as all directly connected assets.
- To view the newly created rule, navigate to: **Control Center** -> **Auto-Tagging and Tags**.
    - The new rule will follow the format: `Propagate-<asset_name>`

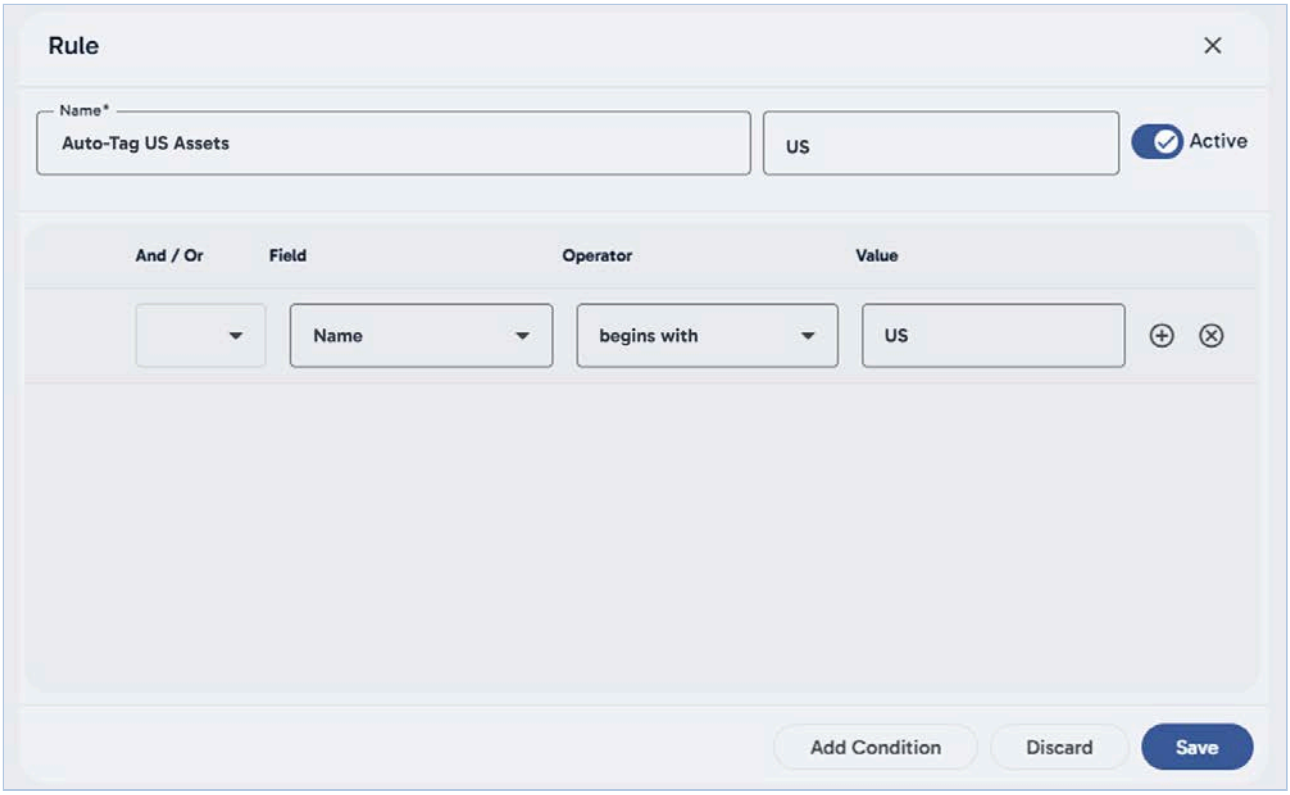
## Create Auto-Tagging Rules

1. Navigate to **Control Center** -> **Auto-Tagging and Tags**
2. Click the '**+**' icon in the top right corner.
3. Enter a rule name and description.
4. Click the '**+**' icon to add a new rule.
5. Name the Rule.
6. Create a tag value (this is the tag that will be applied)
7. Select the field, operator, and value pertaining to the assets you want to automatically tag

For example, If your endpoints follow a naming convention such as `USxxxx`, `UKxxxx`, `CAxxxx`, you can automatically tag them by location.

**Example Configuration**:

- **Name:** Auto-Tag US Assets
- **Tag Value:** US
- **Field:** Name
- **Operator:** begins with
- **Value:** US



Auto-Tagging Rule

## Additional Information

- Auto-tagging based on network segments
- Using tags with bulk operations

# Enhanced Event and Logging System

## Overview

The Enhanced Sepio Event and Logging System provides structured, contextual, and actionable security events that enable organizations to monitor their environments, respond to risks in real time, and maintain accurate records for compliance, audit, and forensic investigations.

The system is designed to deliver clear, enriched logs that combine event details, asset context, risk information, and network visibility in a single, standardized format. This approach ensures that security analysts, SOC teams, and administrators can quickly understand what happened, why it matters, and how to respond, without requiring additional correlation or data lookups.

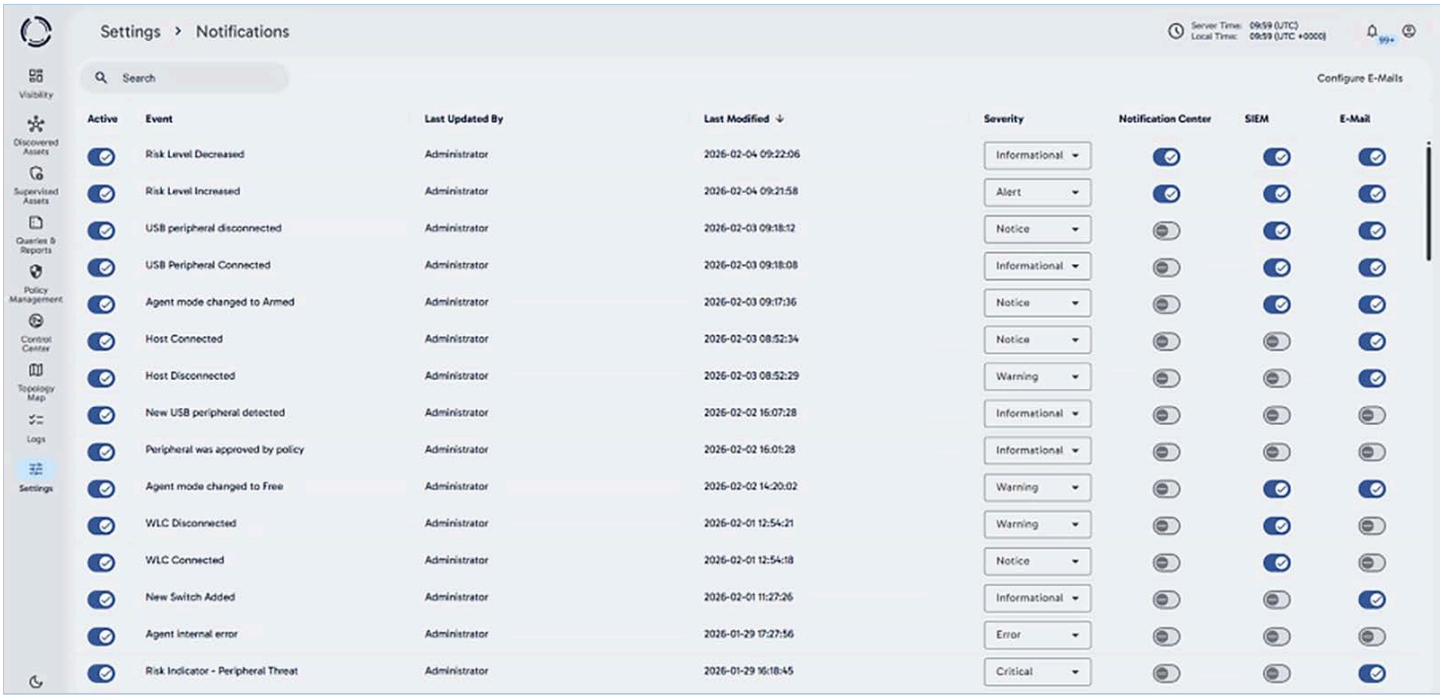
Key capabilities of the Event and Logging System include configurable event delivery and severity, enriched asset and network context, standardized log structures for seamless SIEM and SOAR integration, and consolidated event records that preserve full investigative context.

## Configurable Event and Log Management

Administrators can control which events are generated and how they are delivered from the Sepio platform. This includes enabling or disabling specific events, customizing severity levels, and selecting delivery channels such as SIEM integrations, email notifications, and the Sepio Notification Center.

These controls allow organizations to align logging behavior with their operational processes and governance policies, ensuring that teams receive relevant, actionable signals without unnecessary noise.

Event configuration is managed through the **Settings** -> **Notifications** page, where individual events can be activated, deactivated, assigned a severity level, and mapped to one or more delivery channels. Email notifications are aggregated and sent in defined intervals to reduce alert fatigue.



Settings -> Notifications

## Event Aggregation

A core enhancement of the new Event and Logging System is its ability to **aggregate multiple related events into a single, high-fidelity event record**.

Traditionally, a single real-world activity could generate multiple independent events. For example, when an asset connects to the network, the system might separately generate events for asset detection, risk indicator assignments, and risk score changes. While accurate, this model can overwhelm analysts and external SIEM platforms with high event volumes.

With the enhanced aggregation model, all events that occur at the same time and relate to the same asset are merged into a single consolidated event. Instead of emitting multiple fragmented records, the system creates one enriched event that captures the full sequence of changes and their combined impact.

### Example

Previously, when an asset connects to the network and two risk indicators are assigned, increasing its overall risk, it would result in four separate events:

1. Asset connected
2. Risk Indicator assigned (Indicator 1)
3. Risk Indicator assigned (Indicator 2)
4. Risk score increased

With the new event system, **a single event is generated** that includes:

- The asset connection activity
- All assigned risk indicators
- The updated risk score and contributing factors

This significantly reduces the number of events sent to external systems, helping prevent SIEM message overflow while preserving full analytical value.

#### Priority-Based Event Identity

Within an aggregated event:

- The **event header and event code** are determined using a priority model, ensuring that the most critical aspect of the activity is clearly represented.
- The **summary field concatenates the summaries of all underlying activities**, providing a readable, end-to-end description of what occurred at a single glance.

> **Note:** Note: Events sent by the Sepio Agent that occurred while the Agent was offline will still be transmitted and processed once the Agent reconnects.

## Enriched Event Context

All events generated by the Sepio platform include enriched contextual data to support faster investigation and more effective response. Each log contains comprehensive information about the event itself, the affected asset, and its surrounding network context.

> **Known limitation:** For older versions of Sepio Agent, events that are produced while the agent is offline won't be enriched.

#### Event Metadata

Events include standardized identifiers and timestamps, such as creation and receipt times, type, category, source, event code, summary, severity, and recorded changes.

#### Asset Identification

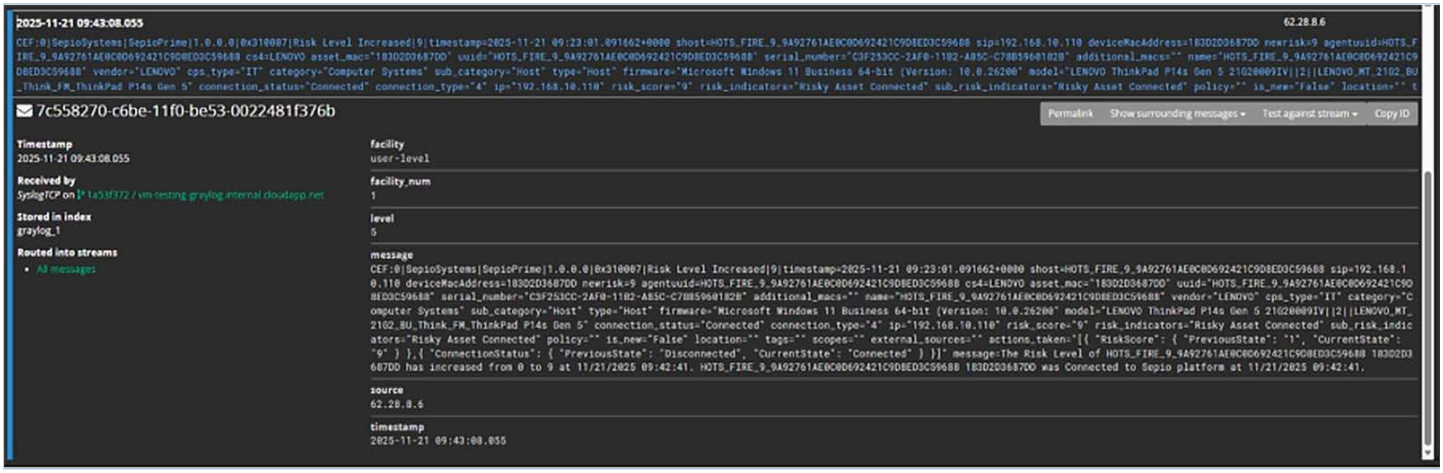
Logs provide detailed asset identifiers, including MAC addresses, VID/PID information, UUIDs of supervised hosts, serial numbers, vendor and product details, firmware and model information, and asset classification attributes.

### Asset and Network Context

To support rapid understanding and correlation, events include network location data, IP addresses, hostnames, VLAN or SSID information, connected ports or access points, user-defined attributes, tags, scopes, and policy context. Risk-related data, such as risk scores, indicators, and sub-indicators, is also included, along with relevant external data points when available.

## Standardized Log Structure and Integrations

All event data is structured using a consistent key-value format to support easy parsing and reliable integration with SIEMs, SOAR platforms, and other security workflows. This standardization reduces integration effort and enables faster correlation across systems, improving analyst efficiency and response accuracy.

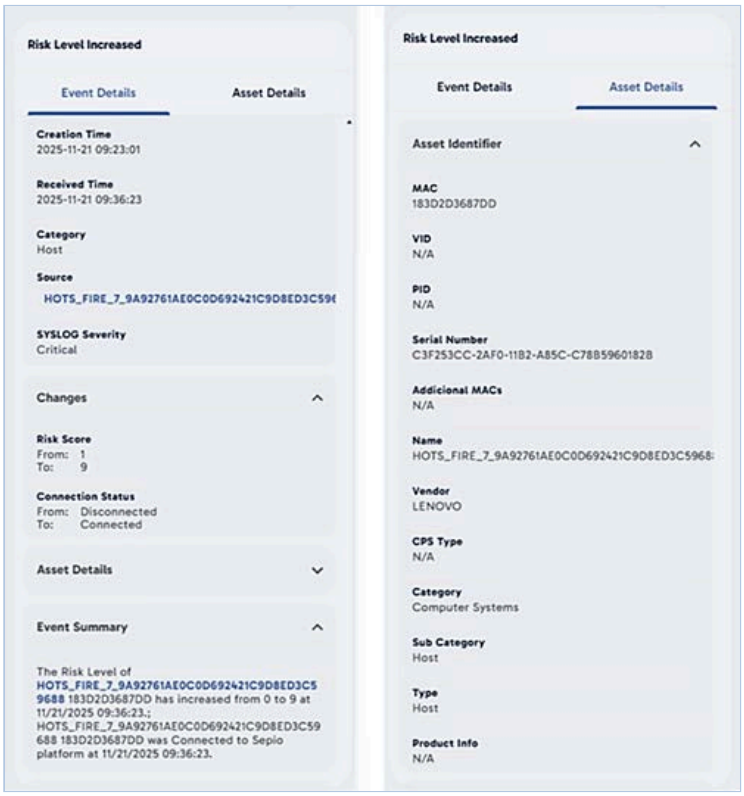



Standardized Log Structure

## Consolidated and High-Integrity Event Records

Each event is recorded as a single, comprehensive log entry that contains all relevant details and context. By avoiding fragmented or multi-record events, the logging system ensures a complete and accurate view of each occurrence.

For example, when a vulnerable asset connects to the network for the first time, the resulting log indicates the detection of the new asset and clearly associates it with the identified risk and vulnerability details. This consolidated approach preserves investigative context and simplifies auditing, reporting, and forensic analysis.



High-Integrity Event Records

## CEF Logging – Extended Asset Context

SepioPrime events are exported using **CEF (Common Event Format)**.
Starting with Sepio Platform v56, the new logging system CEF messages now include **extended asset, risk, and network context**, while maintaining backward compatibility with existing parsers.

### CEF Header

All events continue to use the standard CEF header:

```
CEF:0|SepioSystems|SepioPrime|1.0.0.0|{EventCode}|{EventDescription}|{CEFSeverity}|
```

### Legacy Fields (Still Included)

The following fields remain in the CEF payload for backward compatibility:

| Field | Description |
|---|---|
| `timestamp` | Event trigger time |
| `asset_id` | Unique asset identifier |
| `shost` | Asset name (host name for peripherals) |
| `sip` | Asset IP address |

| Field | Description |
| --- | --- |
| `deviceMacAddress` | Primary asset MAC address |
| `newrisk` | Risk score |
| `agentuuid` | Host UUID |
| `vid` | Vendor ID |
| `pid` | Product ID |
| `cs4` | Vendor name |
| `portNumber` | Port number (if connected to a port) |
| `portId` | Port ID (if connected to a port) |
| `location` | Asset location |
| `scopes` | List of scopes |
| `tags` | List of tags |
| `user_att` | User-defined attributes |

## New Extended Fields

Starting with Sepio Platform v56, the new logging system adds normalized, enriched asset metadata to each event.

> **Note:** The flag `EVENTS_AGGREGATION_PROCCESS_ENABLED` need to be enabled.

### Asset Identity & Hardware

| Field | Description |
| --- | --- |
| `asset_mac` | Primary asset MAC address |
| `additional_macs` | Additional MAC addresses |
| `uuid` | Host UUID |

| Field | Description |
| --- | --- |
| `serial_number` | Asset serial number |
| `vendor` | Vendor name |
| `model` | Asset model |
| `product_info` | Product information |
| `firmware` | Firmware / OS version |
| `hardware_version` | Hardware version (Supervised Network Infrastructure only) |
| `Asset Classification` | Asset classification details |

### Asset Classification

| Field | Description |
| --- | --- |
| `cps_type` | CPS type (IT, IoT, OT) |
| `category` | Classification category |
| `sub_category` | Classification subcategory |
| `type` | Asset type |

### Network & Connectivity

| Field | Description |
| --- | --- |
| `connection_status` | Connection state |
| `connection_type` | Connection type |
| `ip` | Asset IP address |
| `hostname` | Host name |
| `ssid` | Connected SSIDs |
| `vlans` | Connected VLANs |
| `connected_access_point` | Connected access points |

| Field | Description |
| --- | --- |
| connected_port | Connected switch port |
| directly_connected | Indicates direct connectivity |
| snmp_location | SNMP-reported location |

### Risk & Policy

| Field | Description |
| --- | --- |
| risk_score | Risk score |
| risk_indicators | List of risk indicators |
| sub_risk_indicators | List of sub-risk indicators |
| policy | Applied policies |
| is_new | Indicates whether the asset is newly discovered |

### Supervised Network Infrastructure Fields

These fields are **only populated for supervised network infrastructure assets.**

| Field | Description |
| --- | --- |
| boot_info | Boot information |
| is_stack | Indicates stack switch |
| version_id | Switch IOS version |
| image | Switch image |
| cpu_env | CPU environment |
| active_port_count | Number of active ports |
| max_access_points | Maximum supported APs |
| scan_priority_id | Scan priority ID |
| scan_priority_human_readable_name | Scan priority (readable) |

| Field | Description |
| --- | --- |
| domain_id | Scan engine domain ID |
| domain_human_readable_name | Domain name (readable) |
| snmp_version_id | SNMP version |
| snmp_community_name | SNMP community |
| snmp_user | SNMP user |
| authentication_protocol_id | Authentication protocol |
| privacy_protocol_id | Privacy protocol |
| used_protocol_name | Protocol name |
| ssh_user | SSH user |
| meraki_organization_id | Meraki organization ID |

### Locations Object

**Locations** is a structured array describing where the asset is observed. Example:

### Metadata & Enrichment

| Field | Description |
| --- | --- |
| tags | List of tags |
| scopes | List of scopes |
| custom_attributes | User-defined attributes |
| external_sources | External source enrichment |

### Actions & Event Details

| Field | Description |
| --- | --- |
| actions_taken | List of attribute changes (previous vs. current state) |
| message | Human-readable event details |

### Example of CEF legacy message:

```
CEF:0|SepioSystems|SepioPrime|1.0.0.0|0x100002|Host Connected|3|timestamp=2026-02-25
11:17:49.747494+0000 asset_id=66AFDC03D05B518EDC03B717F9CB1F94 shost=SERGIO-FWHXKN3
sip=10.128.2.7 deviceMacAddress=C8CB9EA782E4 agentuuid=66AFDC03D05B518EDC03B717F9CB1F94
cs4=Dell Inc. scopes="Global"
```

### Example of enriched CEF Message:

```
CEF:0|SepioSystems|SepioPrime|1.0.0.0|0x100002|Host Connected|3|timestamp=2026-02-25
11:17:49.747494+0000 asset_id=66AFDC03D05B518EDC03B717F9CB1F94 shost=SERGIO-FWHXKN3
sip=10.128.2.7 deviceMacAddress=C8CB9EA782E4 agentuuid=66AFDC03D05B518EDC03B717F9CB1F94
cs4=Dell Inc. scopes="Global" asset_mac="C8CB9EA782E4" uuid="66AFDC03D05B518EDC03B717F9CB1F94"
serial_number="FWHXKN3" additional_macs="" name="SERGIO-FWHXKN3" vendor="Dell Inc."
cps_type="IT" category="Computer Systems" sub_category="Host" type="Host" firmware="Microsoft
Windows 11 Business 64-bit (Version: 10.0.26200" model="Dell Inc. Latitude Latitude
7420||2||0A36" connection_status="Connected" connection_type="4" ip="10.128.2.7"
risk_score="1" risk_indicators="" sub_risk_indicators="" policy="" is_new="False" locations=[]
connected_port="()-" tags="" scopes="Global" external_sources="" actions_taken=""
```

### The same enrichment is done on SYSLOG messages (not using CEF) as seen on the example:

```
SepioPrime EventsService:Network Element Disconnected, Device Virtual Machine 00505683B0E4
disconnected from the Network at 02/25/2026
10:39:00. AssetIdentifier= AssetContext= ActionsTaken=
```

# Data Extractions

## Extracting Non-identifiable Data file from the Sepio Platform

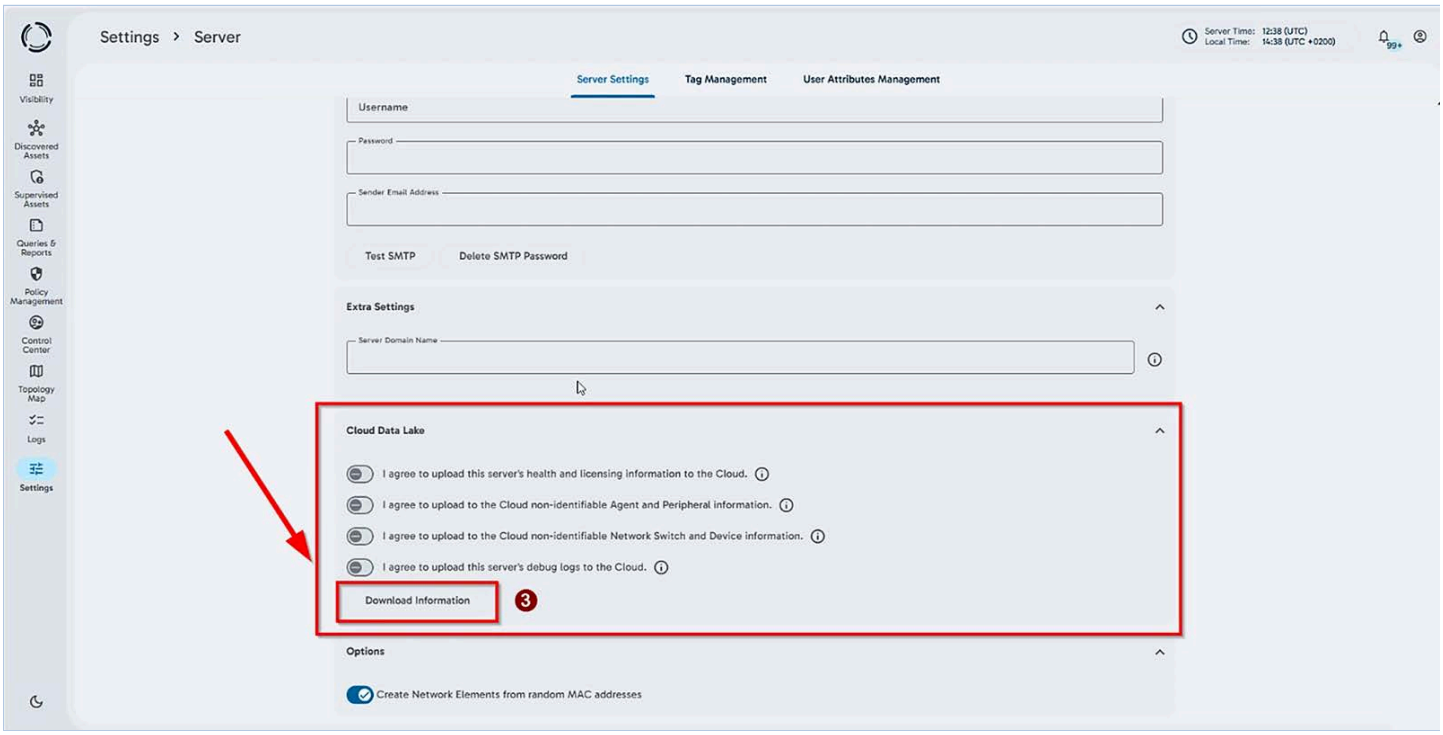
To download anonymized data and update the Sepio data lake repository, you'll need to extract the Non-identifiable Data file. First, click on the Settings (1) button and select Server (2).




Settings -> Server

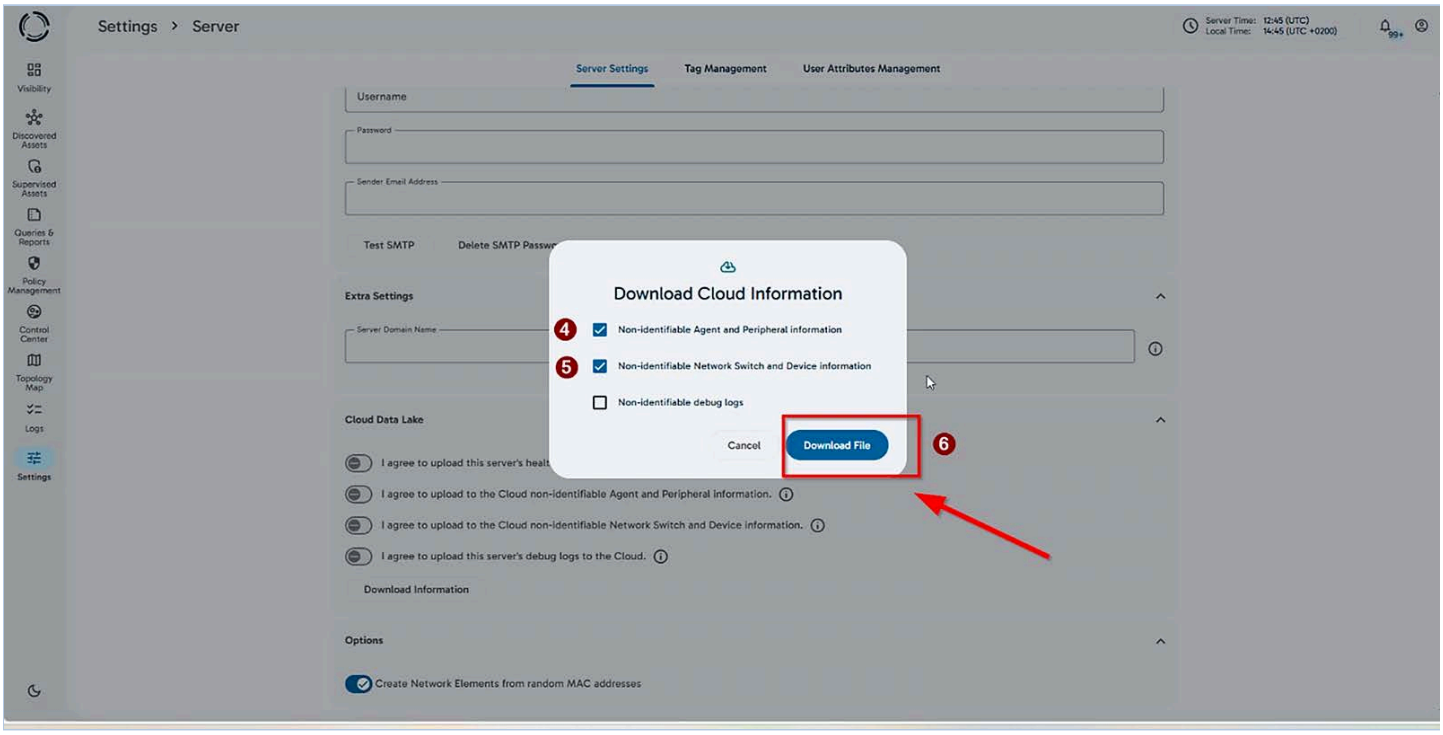
Scroll down the Data Lake section and click on Download Information (3)

> **Note:** If required by corporate governance policies, accept the terms. However, it is possible to download content as long as you press the "Download Information" button.




Download Information

Ensure that only “Non-identifiable Agent and Peripheral Information” (4) and “Non-identifiable Network Switch and Device Information” (5) are selected. Then click the Download File button (6).




Download File

Save the file (7).

# Platform Monitoring

## Monitoring

This guide explains how to log in to Grafana and view monitoring data for the Sepio Management Platform.

### Prerequisites

- Sepio Platform version v51 or higher

### Initial Setup

During the first installation, run the following command to generate the default Grafana credentials:

```
sepioctl monitoring
```

This will create a username and password for accessing the monitoring dashboard.

### Resetting Credentials

Before resetting credentials, verify that the monitoring component is active:

```
sepioctl monitoring --check
```

If the check succeeds, it means credentials already exist.
If needed, reset them using:

```
sepioctl monitoring --password
```

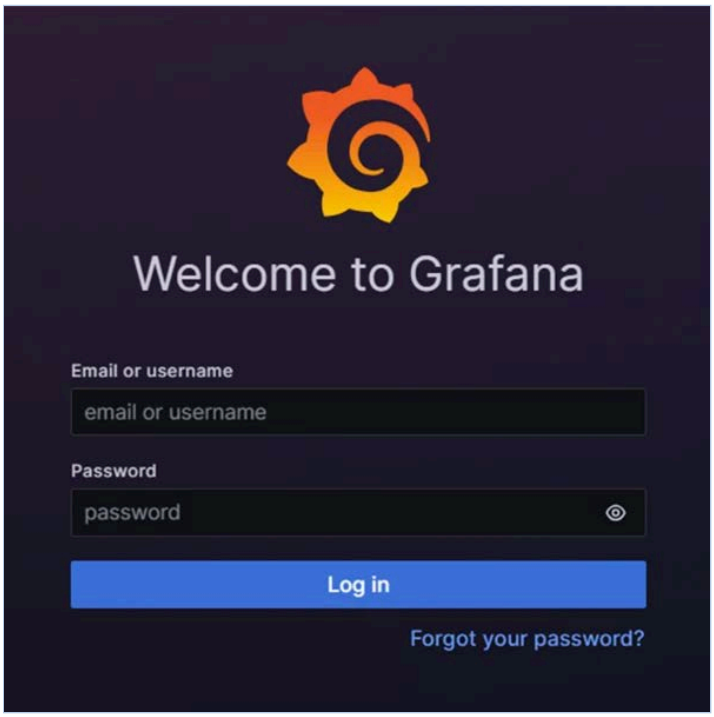
### Accessing the Monitoring Dashboard

After generating or resetting the credentials, open Grafana in your browser:

<IP / Domain / Hostname>/grafana

Examples:

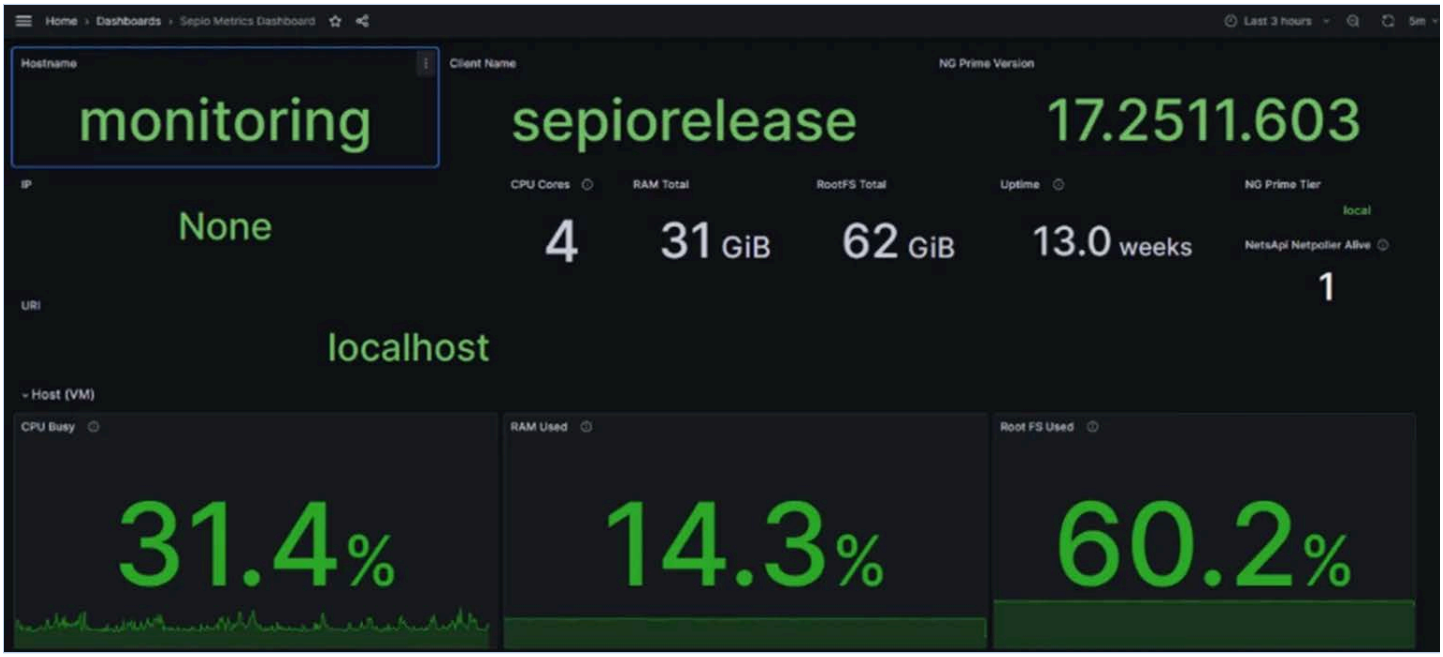
- 10.101.1.200/grafana
- sepio.example.com/grafana



Welcome to Grafana

### Grafana Dashboard Overview

Once logged in, you will see the built-in dashboard that monitors the Sepio Management Platform.



Sepio Metrics Dashboard

# Control Center

## Related Topics

- Scopes and Agent Mode in Sepio Platform
- Port Compliance

# Port Compliance

## Overview

Port Compliance introduces a configuration validation capability that enables organizations to enforce port-level configuration security, compliance, and governance standards based on the characteristics of connected devices.

Armed with this powerful feature, Sepio security administrators can define rules that verify whether the configuration of one or more switch ports complies with organizational policies when devices with defined MAC prefixes are directly connected.

If such a policy violation is detected, Sepio raises a dedicated **Sub Risk Indicator** named **Port Compliance Violation** on the relevant asset.

> **Note:** The following prerequisites must be met before proceeding. Ensure that both `RI_PORT_COMPLIANCE_VIOLATION` and `PORT_VERIFICATION` are enabled.



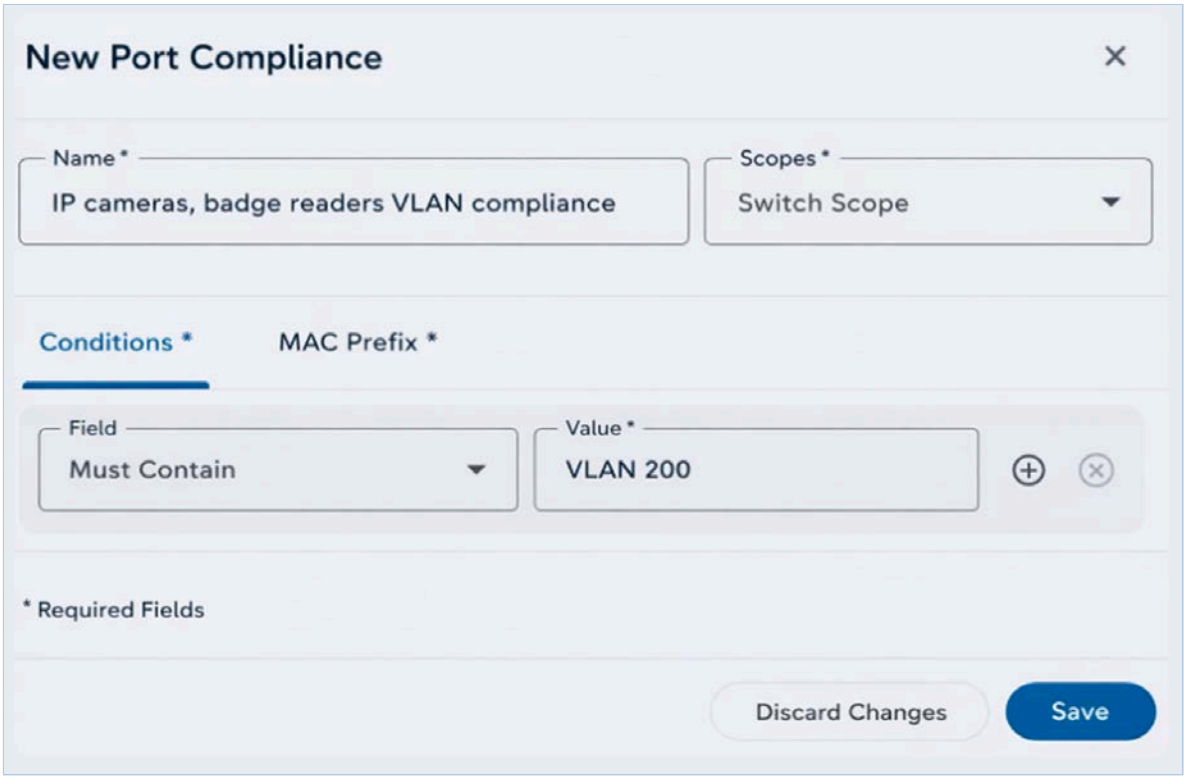

Port Compliance Violation

## Configuration

A template can be configured from **Control Center** -> **Port Compliance**.

Port Compliance is configured using the following parameters:

| Field | Description |
| --- | --- |
| MAC Prefix | MAC prefix defined by the user |
| Switch Scope | Selected scope of switches to monitor |
| Configuration Condition | Defines whether a specific configuration must or must not be present on the port |



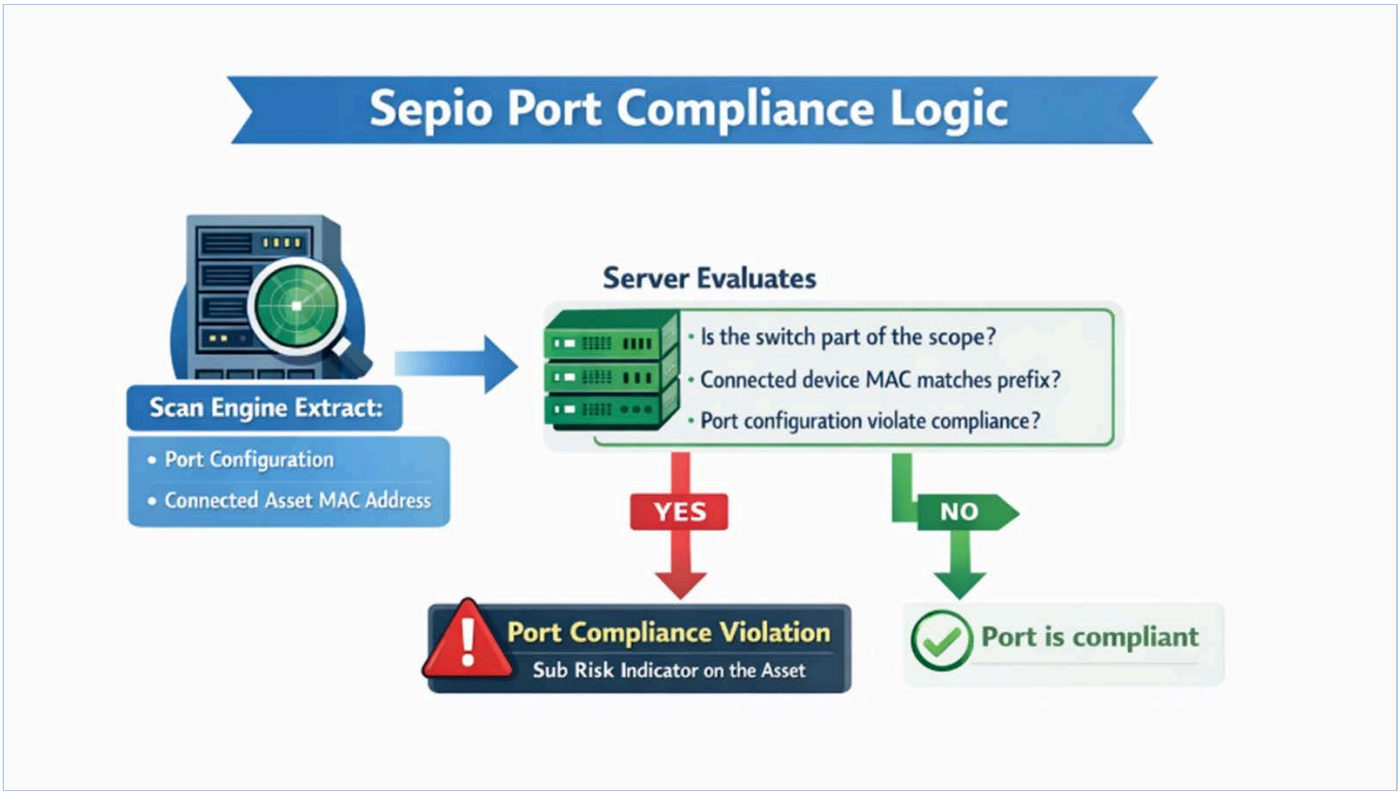
New Port Compliance

## Compliance Validation Logic

Port Compliance is calculated during every scan cycle.

### Evaluation Flow

1. Scan Engine retrieves:
    - Switch port configuration
    - Connected device MAC addresses
2. Server evaluates:
    - Is the switch part of the selected scope?
    - Is a connected device MAC matching the configured prefix?
    - Does the port configuration violate any of the defined conditions?
3. If all conditions are met:
    - A Sub Risk Indicator is raised on the connected asset.




Sepio Port Compliance Logic

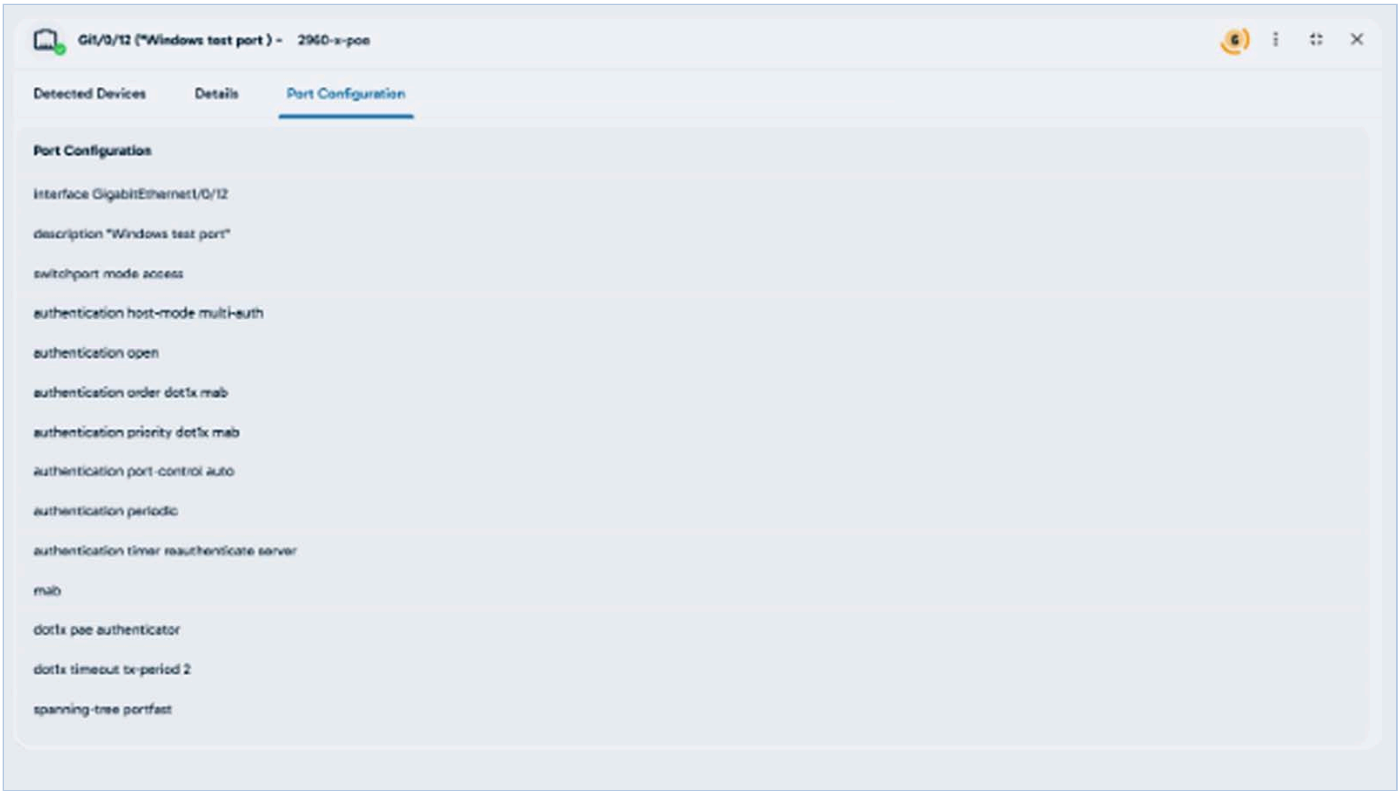
## View Port Configuration

Sepio introduces the ability to view switch port configurations directly from the port screen.

This allows administrators to easily investigate and understand why a Port Compliance Violation was raised on a connected asset.

By accessing the port configuration, users can:

- Review the exact configuration retrieved from the switch
- Validate whether the configuration meets the defined compliance conditions
- Identify missing or unexpected configuration elements




View Port Configuration

## Sample Use Cases

Here are several use cases that Sepio security administrators use to validate compliance, security, and governance policies.

### Enforcing Least Privilege for IoT Devices

#### The Issue

IoT devices such as IP cameras, printers, and badge readers are often over-privileged and mistakenly connected to production ports without proper segmentation or port security.

#### How Port Compliance Solves It

Define a rule stating that devices with specific MAC prefixes must be connected to ports configured with:

- A dedicated VLAN
- Port Security enabled

If the configuration does not match, a **Port Compliance Violation** is raised.

### Detecting Unauthorized Network Extensions

#### The Issue

Employees might connect unmanaged switches or unauthorized access points, bypassing corporate port-level controls and creating security risks.

**How Port Compliance Solves It**

Monitor ports where corporate laptops (based on approved MAC prefixes) are connected.
If the port is configured as Trunk Mode or has STP disabled instead of being in Access Mode, a violation is triggered.

**Ensuring VoIP Configuration Consistency**

**The Issue**

IP phones require specific Voice VLAN and QoS settings. Missing configuration can lead to degraded call quality.

**How Port Compliance Solves It**

Define a rule for VoIP MAC prefixes.
If the port does not include the required Voice VLAN configuration, a violation is raised.

**Supporting Regulatory Compliance (e.g., POS Systems)**

**The Issue**

Regulatory frameworks require strict isolation and authentication controls for devices handling sensitive data.

**How Port Compliance Solves It**

Define a rule requiring POS terminals to be connected only to ports where 802.1X authentication is enforced.
If the configuration is missing, a violation is raised, enabling real-time compliance validation.

## Best Practices

Port Compliance evaluates a port's configuration by directly comparing it, as text, to the configuration retrieved from the switch.

The compliance verification logic checks whether the defined configuration string:

- **Exists** in the port configuration (Must Contain), or
- **Does not exist** in the port configuration (Must Not Contain)

Naming conventions can vary across vendors, models, or software versions, as configuration parameters may be represented differently.

**Example**

A security configuration may appear as:

- ACL
- Access Control List

- IP access-group
- other vendor-specific syntax

Port Compliance performs an exact text match on the configured value. Administrators should ensure that the defined configuration string exactly matches the syntax displayed in the actual port configuration output.

**Recommended Approach**

If an organization operates multiple switch vendors, models, or OS versions where configuration syntax differs:

- **Group switches into separate scopes** based on vendor, model, version.
- Create dedicated Port Compliance configurations per scope.
- Define the configuration string exactly as it appears in each switch type.

This approach ensures accurate validation and avoids unintended false-positive or false-negative detections.

# Scopes and Agent Mode in Sepio Platform

## Introduction

Starting with Sepio Platform **V49**, the concept of **Scopes** has been significantly expanded. Scopes allow administrators to dynamically group assets based on queries and enforce consistent operational behavior across agents.

A major enhancement introduced in this version is the ability to control **Agent Mode** through scopes. This ensures that organizations can centrally define and enforce agent modes, eliminating manual misconfigurations and inconsistencies.

## Scopes

A **Scope** is a group of assets that is automatically and continuously updated based on a defined query. Assets are dynamically added to or removed from the scope as they match (or stop matching) the query criteria.

### Purpose

Scopes provide a way to:

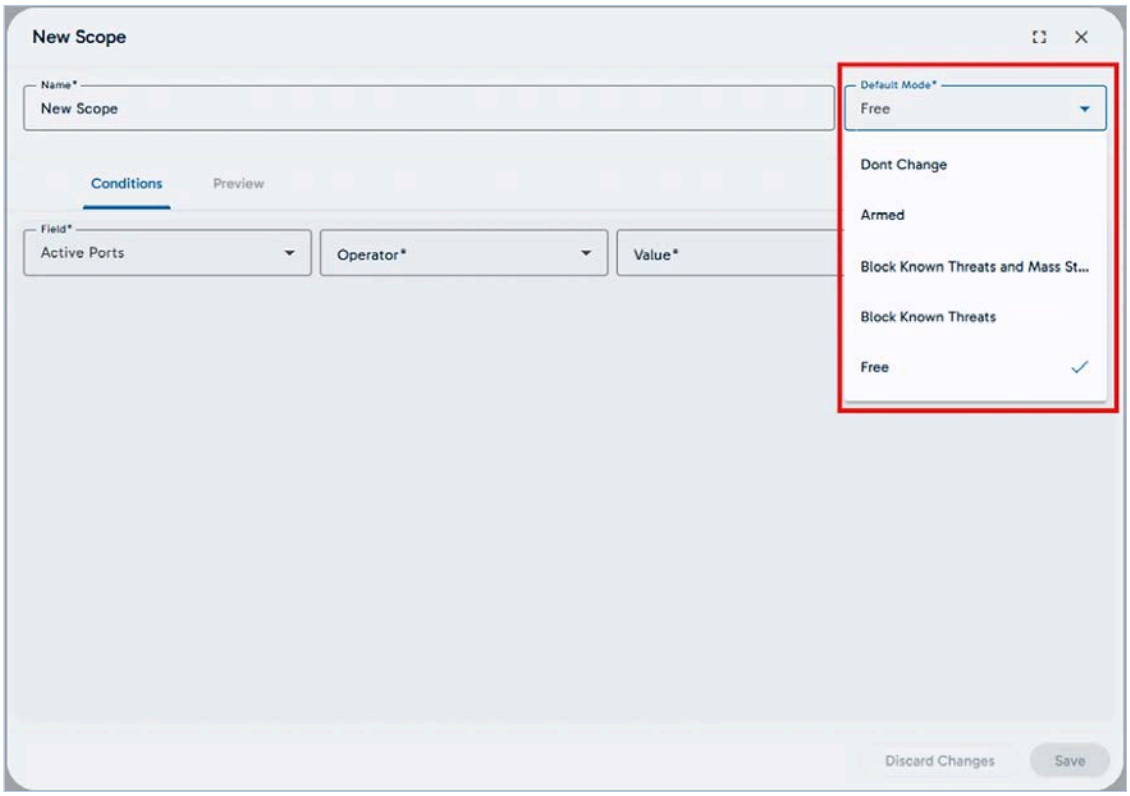
- Organize assets logically (for example, by location or asset type).
- Filter and analyze assets more effectively using queries and reports.
- Reduce administrative overhead by automating asset grouping and agent behavior enforcement.

## Agent Mode

### Default Mode in Scopes

When creating a scope, there is now a mandatory field called **Default Mode**:

- Any agent that belongs to the scope will inherit and operate according to the scope's Default Mode.
- Manual agent mode changes are not allowed while the agent is part of the scope.
- To allow manual agent mode changes (so the scope does not override the agent's mode), select **Default Mode = Don't Change.**




Default Mode = Don't Change

### Conflict Resolution Between Multiple Scopes

If an agent is associated with multiple scopes that specify different **Default Mode** values, the system resolves conflicts using the following priority order:

**Don't Change > Policy > Arm > BST > BKT > Free**

This priority order ensures a deterministic and predictable outcome when scopes overlap.

### Scope Attribute

Agents associated with a scope display the scope name in a dedicated **Scopes** attribute. This gives administrators clear visibility into which scope controls the agent's operating mode.




Attribute Scopes

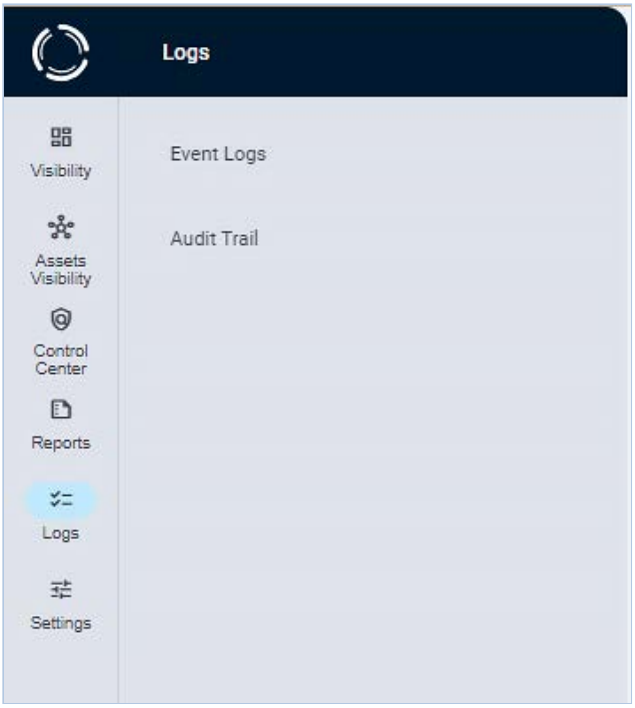
## Behavior Summary

The table below summarizes the expected behavior when agents are associated with scopes:

| Agent Mode (Before Scope Association) | Scope Default Mode | Manual Changes Allowed? | Agent Mode (After Scope Association) |
|---|---|---|---|
| Free | Free | No | Free |
| Free | BKT | No | BKT |
| Free | BST | No | BST |
| Free | Arm | No | Arm |
| Free | Don't Change | Yes | Free |
| BKT | Free | No | Free |
| BKT | BKT | No | BKT |
| BKT | BST | No | BST |
| BKT | Arm | No | Arm |
| BKT | Don't Change | Yes | BKT |
| BST | Free | No | Free |
| BST | BKT | No | BKT |
| BST | BST | No | BST |
| BST | Arm | No | Arm |
| BST | Don't Change | Yes | BST |
| Arm | Free | No | Free |
| Arm | BKT | No | BKT |
| Arm | BST | No | BST |
| Arm | Arm | No | Arm |
| Arm | Don't Change | Yes | Arm |

## Logging

The Sepio Platform logs relevant event and audit messages to two separate running lists for each type that appear under the Logs top-menu item. The same messages can be viewed locally and in addition can be exported via various integrations including generic, RFC based syslog, Splunk add-on, vendor specific syslog and API.




Logs menu

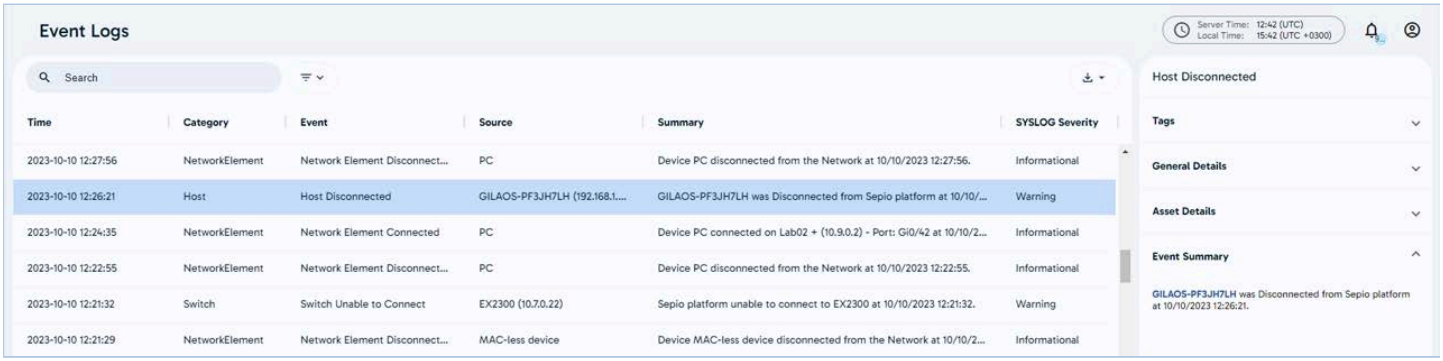
Sepio security administrators can manage the event messages and decide what should be viewed in the UI and exports.

## Sepio Events

Each event in Sepio has a similar structure that includes the following elements:

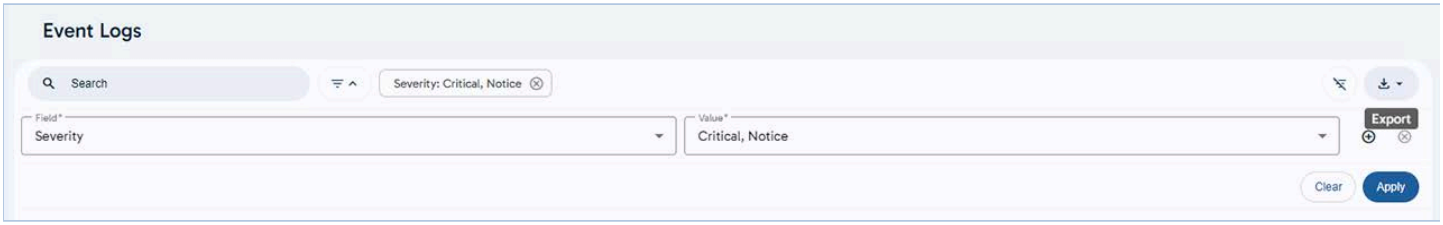
| Logging element | Content |
|---|---|
| Date | Date of the event |
| Severity | Syslog-like severity definition. There are 8 filtering options. |
| Category | High level event classification |
| Source | Subsystem or source of the log |
| Description | Event description |
| Type | Detailed classification |

| Logging element | Content |
| --- | --- |
| Details | Detailed information |



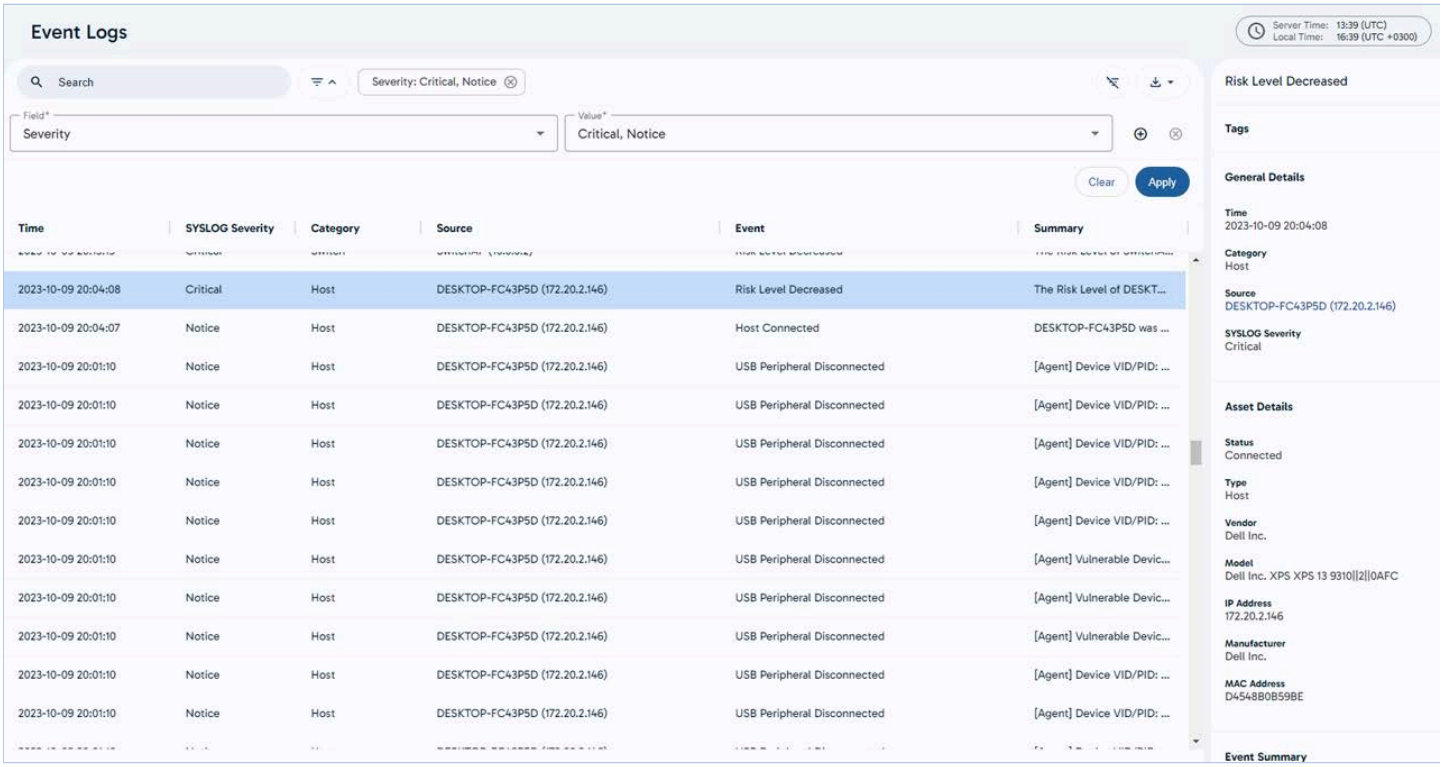

Event logs

It is possible to use filters and export the events to CSV or PDF files.
Use the "**export**" button on the top right side of the UI to generate and download the CSV or PDF files based on the filters that you created.




Export button on the top right side of the UI.

The right-hand panel will display the event information.




The right-hand panel displays the event information.

## Sepio Events and External SIEM/Syslog

Sepio events can be exported to external SIEM using API, Applications (for example, the Splunk Application) or syslog. Please see the Integrations section for additional information.

### Events Creation

The events themselves are created using a well-defined structure based on a matching criterion. Sepio provides an option to follow the logic of event creation which allows to expand the supported use cases based on customer requirements.
There are multiple criteria options. It is enough to have a single match to generate an event. Every parameter of an asset including timers (for example: last seen, first seen etc.) can be used as a criterion for event creation. The Sepio management includes an event definition file **event_messages.json** which includes all the default messages.
Events can be matched based on parameters such as asset type, OS version, Asset Vendor, peripheral type, asset manageability, location, policy, risk score, risk acceptance and many other attributes.

Once there's a match, events will be created using the following fields:

| Field | Content | Comment |
|---|---|---|
| Indicator | Type of the risk Indicator | |
| Indicator Sub Type | Additional filtering for sub Risk Indicators | |
| Risk Level | Sepio's risk score | |
| Severity | Syslog like severity level | Mandatory field |
| Event Code | Numeric code useful for external syslog filtering | Mandatory field, defined by Sepio |
| Event Description | Description fields | Mandatory field |
| Event Message | Syslog message | Mandatory field |
| Ui Message | UI message, can include hyperlink references to assets | Mandatory field |

Each message has a decimal Severity level indicator. Sepio uses the standard syslog severity model as defined by the syslog Protocol RFC (5424). The severity and their values are described in the following table. Severity values MUST be in the range of 0 to 7 inclusive. Sepio Security Administrators can override Sepio's severity recommendations (see more below).

| Severity | Value |
|---|---|
| Emergency | 0 |
| Alert | 1 |
| Critical | 2 |
| Error | 3 |
| Warning | 4 |
| Notice | 5 |
| Informational | 6 |
| Debug | 7 |

There are six types of asset types for which messages are created:

- Switch
- Port
- WLC
- Network Elements
- Peripheral
- Host

A message can include new information or state change if there was a previous status message. In addition, there are events codes which are not exposed via the UI but are available for syslog export. Messages will have one of the following event descriptions with additional information per type.

- New Switch Added
- Switch Connected
- Switch Unable to Connect
- Switch Disconnected
- Switch Authentication Failed
- Port Link Up
- Port Link Down
- New WLC Added
- WLC Connected
- WLC Unable to Connect
- WLC Disconnected
- WLC Authentication Failed
- Network Element Connected
- Network Element Disconnected

- New Network Element Detected
- Host Connected
- Host Disconnected
- Sleeping Device
- Risk Indicator – Network Threat
- Risk Indicator – Peripheral Threat
- Risk Indicator – Wi-Fi Keylogger
- Risk Indicator – Unsupervised Network Infrastructure
- Risk Indicator – Unsupervised Host
- Risk Indicator – Peripheral Vulnerability
- Risk Indicator – Rare Device
- Risk Indicator – Asset DNA Anomaly
- Risk Level Increased
- Risk Level Decreased

## Event Definition

As mentioned above,the **event_messages.json** includes all the default messages. Here's an example for two separate messages: a "New Switch Added" and "Switch Connected"

```
 () added to Sepio platform at ",
            "uiMessage": "Switch  () added to Sepio platform at "
        }
    },
    {
        "criteria": {
            "asset_type": "Switch",
            "connection_status": "Connected"
        },
        "eventValues": {
            "severity": 5,
            "eventCode": "0x200002",
            "eventDescription": "Switch Connected",
            "eventMessage": "Sepio platform successfully connected to  at ",
            "uiMessage": "Sepio platform successfully connected to  at "
        }
    }
]
```

### Changing Events

To override some event or even disable it, one should use the **event_messages_override.json** file.




event_messages_override.json

**Note:** Please contact Sepio before changing event messages.

To override an event, you will need to add it with the same criteria as the one in the original **event_messages.json** file.
For example, let's say you want to override the following event to change the severity value and the messages:

```
{
    "criteria": {
        "asset_type": "Peripheral",
        "connection_status": "|and|Connected"
    },
    "eventValues": {
        "severity": 4,
        "eventCode": "0x110001",
        "eventDescription": "New USB peripheral detected",
        "eventMessage": "Device  Connected. VID/PID: / ()",
        "uiMessage": "Device  Connected. VID/PID: / (). "
    }
}
```

You will need to copy the entire object and replace the values you need. Let's say you want to lower severity to 5 and change the message to remove all VID/PID information, you will add this object to the **event_messages_override.json** file:

```
    ...{other events} ,
    {
        "criteria": {
            "asset_type": "Peripheral",
            "connection_status": "|and|Connected"
        },
        "eventValues": {
            "severity": 5,
            "eventCode": "0x110001",
            "eventDescription": "New USB peripheral detected",
            "eventMessage": "Device  Connected.",
            "uiMessage": "Device  Connected."
        }
    }
]
```

**The “criteria” acts as a Key and the event will be overridden by the new values.**

### Disabling an Event

If you want to disable an event, you will need to add a new property: “**disabled**” and keep all the other information from criteria the same. For example, if you just want to disable the above event, you will add to the **event_messages_override.json** file as follows:

```
    ...{other events} ,
    {
        "disabled": true,
        "criteria": {
            "asset_type": "Peripheral",
            "connection_status": "|and|Connected"
        },
        "eventValues": {
            "severity": 4,
            "eventCode": "0x110001",
            "eventDescription": "New USB peripheral detected",
            "eventMessage": "Device  Connected. VID/PID: / ()",
            "uiMessage": "Device  Connected. VID/PID: / (). "
        }
    }
]
```

**Note:** changes will be effective as soon as the Json file is saved. There’s no need to restart services.

**Editing the event_messages_override.json File**

1. SSH to the Sepio Platform.
2. Connect to the event producer container using the following command.

```
docker exec -it sepioprime-eventproducerworker-1 ash
```

> **Note:** The parameter ash in the command `docker exec -it sepioprime-eventproducerworker-1 ash` specifies the shell to be used inside the container. By default, Docker uses the /bin/sh shell. However, the ash shell is a smaller and faster shell that is often used in embedded systems and containers.

3. Edit the /app/event_file/event_messages_override.json .

Please pay attention to the file structure:

1. The text block starts with the left square bracket and ends with the right square bracket. (“”).
2. Use a comma at the end of logical text blocks inside the file.
3. You all set. Verify the changes in the Sepio event logs section.

> **Tip:** Use a JSON validation tool to ensure there are no errors. We recommend using https://jsonlint.com. Copy and paste the changes you made, then press the “Validate JSON” button to verify that the JSON is valid.

> **Note:** Changes will take effect as soon as the JSON file is saved. There’s no need to restart services.

## Event and Audit Log Retention

Security best practices, regulatory requirements, and corporate governance policies require clearly defined retention policies for event and audit records.

Logs stored on the system have a capacity of **300,000 entries** and are automatically rotated, with entries older than the defined retention period being removed. We recommend forwarding event and audit log records to a **syslog server** for long-term storage, monitoring, and other corporate functions, enabling you to retain data for the required periods.

| Attribute | Description | Default value |
| --- | --- | --- |
| **AUDIT_TRAIL_ROW_LIMIT** | Maximum number of entries in the Audit Trail table. | 300000 |
| **EVENT_ROW_LIMIT** | Maximum number of entries in the Event History table. | 300000 |
| **DAYS_REPORT_LOGS** | Sets the number of days to keep logs (Events and Audit). | 180 |

# CEF Operations

## Introduction

Syslog is a common protocol for sending event logs from devices and applications to a central server. While it offers a basic way to collect logs, it lacks structure and standardization for security events. This is where Common Event Format (CEF) comes in.

CEF is an industry-standard format that sits on top of Syslog, providing a structured way to represent security events. It defines a specific set of fields for things like device information, timestamps, event types, and user data. This standardized format allows Security Information and Event Management (SIEM) systems to easily ingest and understand logs from various security devices and applications, regardless of the vendor.

CEF became the industry standard for SIEM integration using Syslog due to the following benefits.

- **Standardization:** CEF provides a common language for security events, enabling SIEM systems to process logs from diverse sources without needing individual configurations for each device type.
- **Richer Data:** CEF allows for more detailed information to be captured in logs compared to plain Syslog messages. This richer data helps SIEM systems perform better analysis and identify security threats more effectively.
- **Interoperability:** By using CEF, organizations can integrate security devices and applications from different vendors with their SIEM system, promoting a more holistic view of their security posture.

> **Note:** See Sepio's Syslog integration options in configuring Syslog.

## Sepio CEF Messages

All CEF messages follow the same format that includes the received **timestamp, source,** and the **message** itself**.**
The message has a fixed structure that has a header, starting with CEF:0, the message and the details.

For example, see the following two messages:

| Timestamp | Source | Message |
|---|---|---|
| 2024-03-21T10:30:19.876Z | 104.211.45.142 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100002\|Host Connected\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 deviceMacAddress=04CF4B76E92C cs4=LENOVO |

| Timestamp | Source | Message |
|---|---|---|
| | | agentuuid=E30A31B35B85D19684660702ECD323EF message=SHARON-PF415E8W 04CF4B76E92C was Connected to Sepio platform at 03/21/2024 10:30:19. |
| 2024-03-21T10:30:25.881Z | 104.211.45.142 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x110002\|USB Peripheral Connected\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 vid=30C9 pid=0063 agentuuid=E30A31B35B85D19684660702ECD323EF message= Device VID/PID: 30C9/0063 (Luxvisions Innotech Limited Integrated Camera) |

## Important Sepio CEF Message Parameters

| Parameter | Example and meaning |
|---|---|
| sip= | Agent's Source IP address: sip=192.168.86.169 |
| shost= | Source HOST name: shost=SHARON-PF415E8W |
| newrisk= | HOST's new risk score (1...9): Newrisk=9 |
| agentuuid= | Agent's unique identifier: agentuuid=E30A31B35B85D19684660702ECD323EF |
| message= | The message details: message= Rogue Device VID/PID: 2341/8037 (Arduino Leonardo (CDC ACM, HID)) |
| deviceMacAddress= | HOST's MAC address: deviceMacAddress=04CF4B76E92C |
| vid= | Peripherial Vendor ID: vid=18D1 |
| pid= | Peripherial Product ID: pid=4EE1 |

The current version of the Sepio Platform allows the security administrator to tune platform and network messages that are exported via Syslog as explained in logging. However, the Agent messages cannot be changed in the field.

**Note:** For more detailed information, see Agent CEF Operations Messages and Network CEF Operations Messages.

## Network CEF Operations

The following table shows the main CEF messages for network events, their explanation and suggested actions that organizations should take when such messages appear:

| CEF Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| New Network Element Detected | 0x400001 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x400001\|New Network Element Detected\|1\|SIP=192.168.100.28, SHOST=SepioN3K(FOC1725R0CY), deviceMacAddress=001F6CD2447F, location=C3650 + 192.168.100.36 – Port: Gi1/0/24 cs4=Cisco Systems, Inc, cn1=1 | Sepio discover networked dev listed it. Action should a risk is identif Administrators look for “risk Ir messages. **Suggested act** |
| Network Element Connected | 0x400002 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x400002\|Network Element Connected\|1\|SIP=192.168.100.28, SHOST=SepioN3K(FOC1725R0CY), deviceMacAddress=001F6CD2447F, cs4=Cisco Systems, Inc, cn1=6 location=C3650 + 192.168.100.36 – Port: Gi1/0/24 | A previously d asset that was disconnected connected. **Suggested act Suggested SO Playbook:** Loo frequent connected/dis messages. It m indicate a netv |
| Network Element Disconnected | 0x400003 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x400003\|Network Element Disconnected\|1\|SIP=192.168.100.28, SHOST=SepioN3K(FOC1725R0CY), deviceMacAddress=001F6CD2447F, cs4=Cisco Systems, Inc, cn1=6 location=C3650 + 192.168.100.36 – Port: Gi1/0/24 | A previously d asset that was connected is r disconnected. **Suggested act Suggested SO Playbook:** Loo frequent connected/dis messages. It m indicate a netv |

| CEF Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| Port Link Down | 0x210002 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x210002\|Port Link Down\|5\|shost=Gi1/0/24, sip=10.128.10.20, deviceMacAddress=64F69D806098, portNumber=24, portId=Gi1/0/24, location=C3750X-48P-S message=Port 24, Gi1/0/24 on Switch 10.128.10.20, C3750X-48P-S is disconnected at 08/19/2024 13:33:02. | A switch port i disconnected changed its st "down". **Suggested act Suggested SO Playbook:** Loo frequent up/d messages. It m indicate a netv |
| Port Link Up | 0x210013 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x210013\|Port Link Up\|5\|shost=Gi1/0/24, sip=10.128.10.20, deviceMacAddress=64F69D806098, portNumber=24, portId=Gi1/0/24, location=C3750X-48P-S message=Port 24, Gi1/0/24 on Switch 10.128.10.20, C3750X-48P-S is connected at 08/19/2024 13:45:48. | A switch port i connected and changed its st "up". **Suggested act Suggested SO Playbook:** Loo frequent up/d messages. It m indicate a netv |
| Failure in disabling a port | 0x980022 | CEF:0\|SepioSystems\|SepioPrime\|\|0x980022\|Failure in disabling a port\|8\|Failure in disabling a port shost=C9200-24T sport= Gi1/0/24 SIP=192.168.100.48 suser=sharonb@sepiocyber.com | The Sepio Plat unable to bloc switch's netwo order to mitig security conce issue. **Suggested act Investigate th** |
| Accepted risk on Asset | 0x310027 | CEF:0\|SepioSystems\|SepioPrime\|\|0x310027\|Accepted risk on Asset\|9\| SHOST=2960-x-poe SIP=192.168.100.13 sport= Gi1/0/24 Suser=sharonb@sepiocyber.com | The listed adm accepted a rep **Suggested act** |
| Risk Level Decreased | 0x310008 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x310008\|Risk Level Decreased\|1\|sip=192.168.100.28 shost=SepioN3K(FOC1725R0CY) deviceMacAddress= | The risk level networked dev decreased. Th score indicate |

| CEF Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| | | XXXXXXXX newrisk=1 cs4=Other agentuuid=00FCBA7A9380_FDO2209Q1XZ | level. **Suggested act Suggested SO Playbook: non** |
| Risk Level Increased | 0x310007 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x310007\|Risk Level Increased\|7\| sip=10.128.10.20 shost=Gi1/0/24Gi1/0/24 portId= deviceMacAddress=64F69D806098 newrisk=7 cs4= agentuuid=64F69D806080_FDO1850H1AJ, location=C3750X-48P-S | The risk level networked dev increased and The new risk s indicated the **Suggested act Investigate. C additional log detailed inforr Suggested SO Playbook:** Aut ticket creation investigation. |

**Note:** For more information, see CEF Operations.

# Agent CEF Operations

The following tables list the different agent-related Common Event Format (CEF) messages, their explanations, and the recommended actions organizations should take when such messages appear:

## Administrative CEF Messages

| Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| Host Connected | 0x100002 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100002\|Host Connected\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 deviceMacAddress=04CF4B76E92C cs4=LENOVO agentuuid=E30A31B35B85D19684660702ECD323EF message=SHARON-PF415E8W 04CF4B76E92C was Connected to Sepio platform at 03/21/2024 10:30:19 | The endpoint with the installed Sepio Agent (aka "HOST") is connected to the Sepio Platform which manages it. **Suggested action: none.** |
| Host Disconnected | 0x100003 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100003\|Host Disconnected\|5\|shost=SHARON-PF415E8W sip=192.168.86.169 deviceMacAddress=04CF4B76E92C cs4=LENOVO agentuuid=E30A31B35B85D19684660702ECD323EF message=SHARON-PF415E8W 04CF4B76E92C was Disconnected from Sepio platform at 08/26/2025 15:34:38 | The endpoint with the installed Sepio Agent (aka "HOST") is disconnected from the Sepio Platform which manages it. **Suggested action: none.** |
| Agent Startup | 0x100007 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100007\|Agent Startup\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 agentuuid=E30A31B35B85D19684660702ECD323EF | The Sepio platform is notified that |

| Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| | | message= Workstation uptime: 4d 11h 28m 40s, Agent Version: 17.2306.292 | an Agent that was previously uninstalled or in a non-running state has started. **Suggested action: none.** |
| Agent mode changed to Free | 0x100004 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100004\|Agent mode changed to Free\|5\|shost=SHARON-PF415E8W sip=192.168.86.169 agentuuid=E30A31B35B85D19684660702ECD323EF message= Agent: SHARON-PF415E8W (192.168.86.169). Agent mode was changed from (BlockKnownThreatsAndMassStorage) to (Free) | The Sepio Platform is notified that the Agent activity mode command was received and executed. **Suggested action: verify. Check that indeed this configuration was made on purpose** (for example, it has a valid Change Request ticket ID). |
| Agent mode changed to Armed | 0x100005 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100005\| Agent mode changed to Armed\|5\|shost=SHARON-PF415E8W sip=192.168.86.169 agentuuid=E30A31B35B85D19684660702ECD323EF message= Agent: SHARON-PF415E8W (192.168.86.169). Agent mode was changed from (Free) to (Armed) | The Sepio Platform is notified that the Agent activity mode command was received and executed. **Suggested action: verify.** |

| Message | Code | Example | Meaning and suggestions |
| --- | --- | --- | --- |
| | | | **Check that indeed this configuration was made on purpose** (for example, it has a valid Change Request ticket ID)**.** |
| Agent set to Block known threats | 0x100021 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100021\|Agent set to Block known threats\|5\|shost=SHARON-PF415E8W sip=192.168.86.169 agentuuid=E30A31B35B85D19684660702ECD323EF message= Agent: SHARON-PF415E8W (192.168.86.169) Agent mode was changed from (Free) to (BlockKnownThreats) | The Sepio Platform is notified that the Agent activity mode command was received and executed. **Suggested action: verify. Check that indeed this configuration was made on purpose** (for example, it has a valid Change Request ticket ID)**.** |
| Agent Upgrade | 0x140001 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x140001\|Agent Upgrade\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 agentuuid=E30A31B35B85D19684660702ECD323EF message=Agent is SHARON-PF415E8W (192.168.86.169) – Version download completed, Agent is being upgraded by file: SepioAgent_Win_64_17.2306.352.msi | The Agent was upgraded. **Suggested action: none.** |

## Asset CEF Messages

| Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| New USB Peripheral Connected | 0x110001 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x110001\|New USB Peripheral\|5\|shost=SHARON-PF415E8W sip=192.168.86.169 vid=27C6 pid=6594 agentuuid=E30A31B35B85D19684660702ECD323EF message= Device VID/PID: 27C6/6594 (Shenzhen Goodix Technology Co.,Ltd. Goodix Moc Fingerprint) | The Agent detected a new peripheral and listed it. Action would be taken (and reported separately) based on the HOSTS configuration. **Suggested action: none.** |
| USB Peripheral Connected | 0x110002 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x110002\|USB Peripheral Connected\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 vid=30C9 pid=0063 agentuuid=E30A31B35B85D19684660702ECD323EF message= Device VID/PID: 30C9/0063 (Luxvisions Innotech Limited Integrated Camera) | A previously seen peripheral is now connected. This is a similar message to “New USB Peripheral Connected”. Action would be taken (and reported separately) based on the HOST’S configuration. **Suggested action: none.** |
| USB Peripheral Disconnected | 0x110003 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x110003\|USB Peripheral Disconnected\|1\|shost=SHARON-PF415E8W sip=10.100.102.134 vid=2341 pid=8037 agentuuid=E30A31B35B85D19684660702ECD323EF | A previously connected peripheral is now disconnected. |

| Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| | | message= Rogue Device VID/PID: 2341/8037 (Arduino Leonardo (CDC ACM, HID)) | **Suggested action: none.** |
| USB Peripheral Enabled | 0x110006 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x110006\|USB Peripheral Enabled\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 vid=18D1 pid=4EE1 agentuuid=E30A31B35B85D19684660702ECD323EF message= Device VID/PID: 18D1/4EE1 (Google Inc. Nexus/Pixel Device (MTP)) | A previously disabled peripheral is now enabled. This can take place when a device that is blocked or disabled due to the HOST's policy received a new message. **Suggested action: verify. Check that indeed this configuration was made on purpose** (for example, it has a valid Change Request ticket ID)**.** |
| USB Peripheral Disabled | 0x110007 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x110007\|USB Peripheral Disabled\|9\|shost=SHARON-PF415E8W sip=192.168.86.169 vid=18D1 pid=4EE1 agentuuid=E30A31B35B85D19684660702ECD323EF message= Device VID/PID: 18D1/4EE1 (Google Inc. Nexus/Pixel Device (MTP)) | A connected peripheral state was changed to "disabled". **Suggested action: verify. Check that indeed this configuration was made on purpose** (for example, due to a |

| Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| | | | policy decision on the endpoint). |
| HID block | 0x100009 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100009\|HID release\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 vid=18D1 pid=4EE1 agentuuid=E30A31B35B85D19684660702ECD323EF message= Apply wide HID block (all HID devices are blocked) | A connected HID peripheral state was changed to “disabled”. All the HID devices on the machines have been blocked. **Suggested action: verify. Check that indeed this configuration was made on purpose** (for example, due to a policy decision on the endpoint). |
| HID release | 0x100010 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100010\|HID block\|1\|shost=SHARON-PF415E8W sip=192.168.86.169 vid=18D1 pid=4EE1 agentuuid=E30A31B35B85D19684660702ECD323EF message= Release wide HID block (all approved HID devices are active) | A disabled HID peripheral was disconnected. All connected blocked HID devices have been released. **Suggested action: verify. Check that indeed this configuration was made on purpose** (for example, due to a |

| Message | Code | Example | Meaning and suggestions |
| --- | --- | --- | --- |
| | | | policy decision on the endpoint). |

## Risk and Incidents CEF Messages

| Message | Code | Example | Meaning and suggestions |
| --- | --- | --- | --- |
| Risk level increased | 0x310007 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x310007\|Risk Level Increased\|9\|sip=10.100.102.203 shost=SHARON-PF415E8W deviceMacAddress=04CF4B76E92C newrisk=9 cs4=LENOVO agentuuid=E30A31B35B85D19684660702ECD323EF message=The Risk Level of SHARON-PF415E8W 04CF4B76E92C has increased from 1 to 9 at 08/26/2025 16:19:11 | The risk level of the HOST has increased and is higher. The new risk indicated the risk level. **Suggested action: Investigate. Check additional logs for more detailed information** (For example, search for the Peripheral threat or Peripheral vulnerability messages). |
| Risk level decreased | 0x310008 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x310008\|Risk Level Decreased\|1\|sip=10.100.102.134 shost=SHARON-PF415E8W deviceMacAddress=04CF4B76E92C newrisk=1 cs4=LENOVO agentuuid=E30A31B35B85D19684660702ECD323EF message=The Risk Level of SHARON-PF415E8W | The risk level of the HOST has decreased. The new risk indicated the risk level. |

| Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| | | 04CF4B76E92C has decreased from 9 to 1 at 08/26/2025 16:56:43 | **Suggested action: none.** |
| Risk level increased | 0x310007 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x310007\|Risk Level Increased\|9\|sip=10.100.102.203 vid=046D pid=C52B shost=GALB-6QTKXT2 newrisk=5 cs4=Logitech, Inc. agentuuid=6E42D0D7CE16001BB80094213A1CE58D message=The Risk Level of Unifying Receiver on GALB-6QTKXT2 has increased from 1 to 5 at 08/26/2025 18:51:01 | The risk level of the Peripheral has increased and is higher. The new risk indicated the risk level. **Suggested action: Investigate. Check additional logs for more detailed information.** |

## Attack Tools CEF Messages

Because IP addresses are not stable identifiers and can change (e.g., via DHCP), and MAC addresses can be spoofed, CEF messages related to attack tools activity include the Agent UUID, a persistent identifier derived from the endpoint's CPU and BIOS identifiers. See the Agent deep dive for more details.

| Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| Peripheral Threat | 0x100019 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100019\|Risk Indicator – Peripheral Threat\|9\|shost= ANDRE-PF40BC6P agentuuid=73C2ECF8CF669DFEF2CBBF3BF68ACD6E vid=046D pid=C31C cs4=HAK5 Rubber Ducky spoofing Logitech, Inc. message=This peripheral has been identified as a HAK5 Rubber Ducky spoofing Keyboard K120 on ANDRE-PF40BC6P at 03/22/2024 16:59:24 | **Suggested action: Investigate. Check additional logs for more detailed information.** |

| Message | Code | Example | Meaning and suggestions |
|---|---|---|---|
| Peripheral Vulnerability | 0x110011 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x110011\|Risk Indicator – Peripheral Vulnerability\|9\|shost= ANDRE-PF40BC6P agentuuid=73C2ECF8CF669DFEF2CBBF3BF68ACD6E vid=046D pid=C52B cs4=Logitech, Inc., message=This device Unifying Receiver detected at 03/22/2024 16:59:24 on ANDRE-PF40BC6P is suspected of bearing a vulnerability | **Suggested action: Investigate.** |
| Bad Reputation | 0x310031 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x310031\|Risk Indicator – Bad Reputation\|9\|shost=GALB-6QTKXT2 agentuuid=6E42D0D7CE16001BB80094213A1CE58D vid=0603 pid=1010 cs4=Novatek Microelectronics Corp., message=The asset USB Mouse (connected on GALB-6QTKXT2 at 08/26/2025 19:37:00) is known by Sepio to have a bad reputation | **Suggested action: Investigate. Check additional logs for more detailed information.** |
| WiFi Keylogger detected | 0x100019 | CEF:0\|SepioSystems\|SepioPrime\|1.0.0.0\|0x100019\| WiFi Keylogger detected \|9\|sip=10.0.0.68 shost=GALB-6QTKXT2 agentuuid=6E42D0D7CE16001BB80094213A1CE58D message=Agent is GALB-6QTKXT2 (10.0.0.68) – Host has detected a potential WiFi keylogger in proximity, Network AIR_6863D9 (5202916863D9) | **Suggested action: Investigate.** |

**Note:** For more information, see CEF Operations.

## Events API

The Sepio Platform web-based API can be used to export events in a variety of formats, including JSON, CSV, and XML. This makes it easy to integrate Sepio data with other systems and use it for a variety of purposes, such as: Security analytics, Threat intelligence, Compliance reporting and can provide Operational insights.

Here are some specific examples of how the Sepio Platform web-based API can be used to export events and use it for a variety of use cases:

- A security analyst can use the Sepio Platform web-based API to export events to a security analytics tool such as Splunk or Sumo Logic. This will allow the analyst to identify trends and patterns in attacks, as well as to investigate specific incidents.
- A threat intelligence analyst can use the Sepio Platform web-based API to export events to a threat intelligence feed such as MISP or ThreatConnect. This will keep the analysts informed of the latest threats and allow them to update their security systems accordingly.
- A compliance officer can use the Sepio Platform web-based API to export events to a compliance reporting tool such as ArcSight or LogRhythm. This will allow the officer to generate reports that demonstrate compliance with security regulations.
- A security operations manager can use the Sepio Platform web-based API to export events to a data visualization tool such as Tableau or Power BI. This will allow the manager to gain insights into how security operations are performing and identify areas for improvement.

Overall, the Sepio Platform web-based API provides a flexible and powerful way to export events and use them for a variety of purposes.

## View the Events API

You can view the API by examining the Sepio OpenAPI specification (formerly Swagger Specification) which is the API description format for REST APIs.

**View Settings** -> **About** -> **Dev Tools:**




Dev Tools

The **Events API** is described alongside all other events in the specification file:




Events API

You can **try it out** by executing the API call. First, try without editing any parameter, then compare your results after editing some query options.



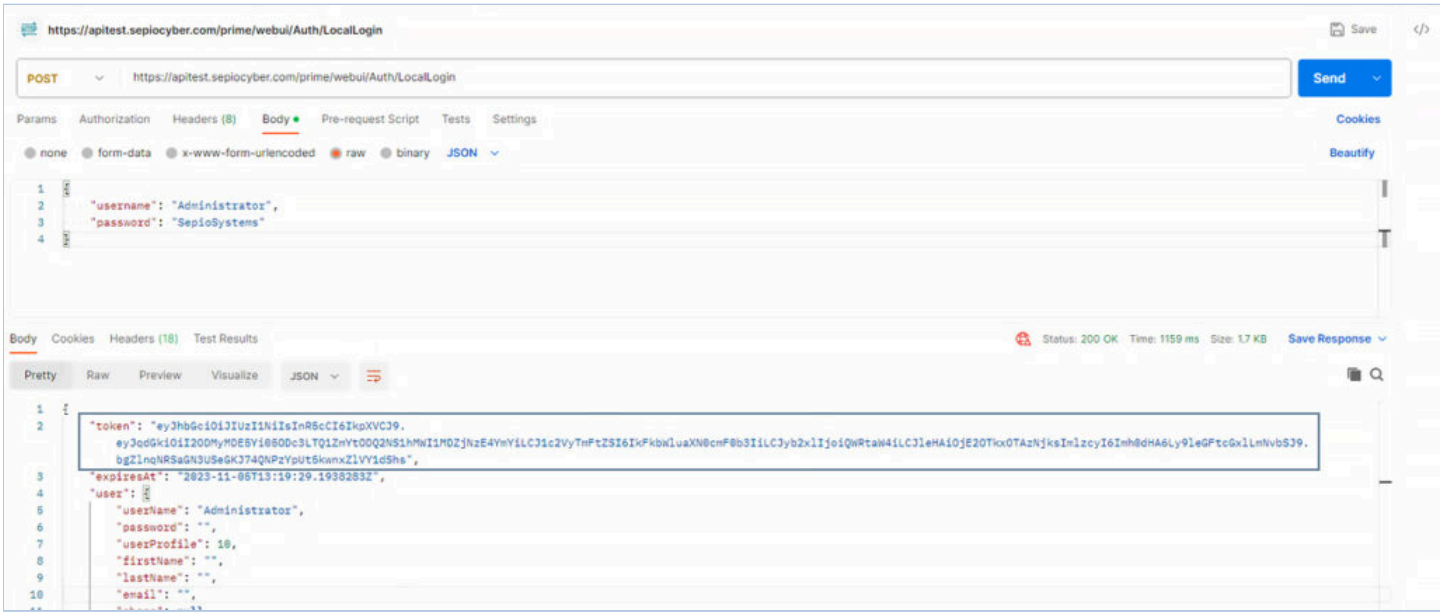

API calls

## Export the Events logs using Postman

In this section will describe how to use the Sepio Platform API to export the Events log file using the popular Postman application (https://www.postman.com/) as the access tool. Other tools can be used.

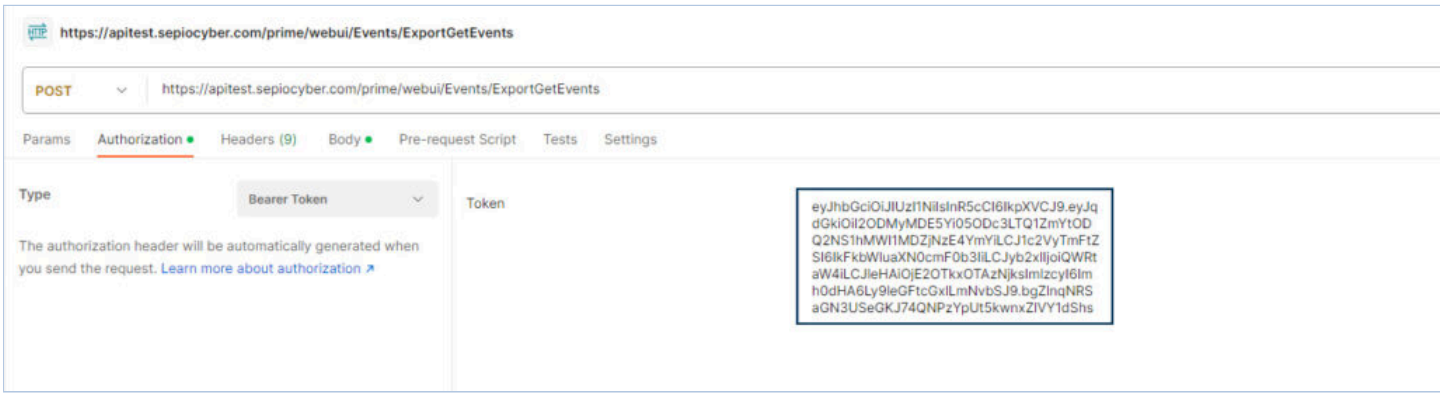
### 1. Login to the platform for getting the auth token.

Upon successful connection please **copy** the **token** as you will need it in the next step.

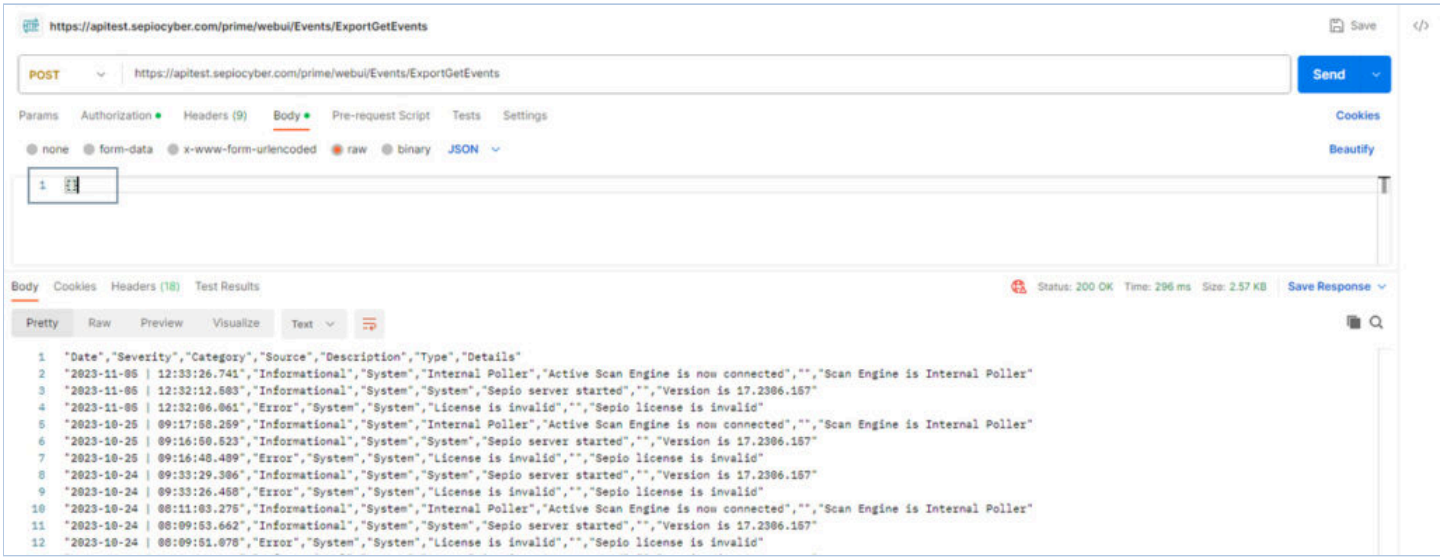



### 2. Export the Events log.

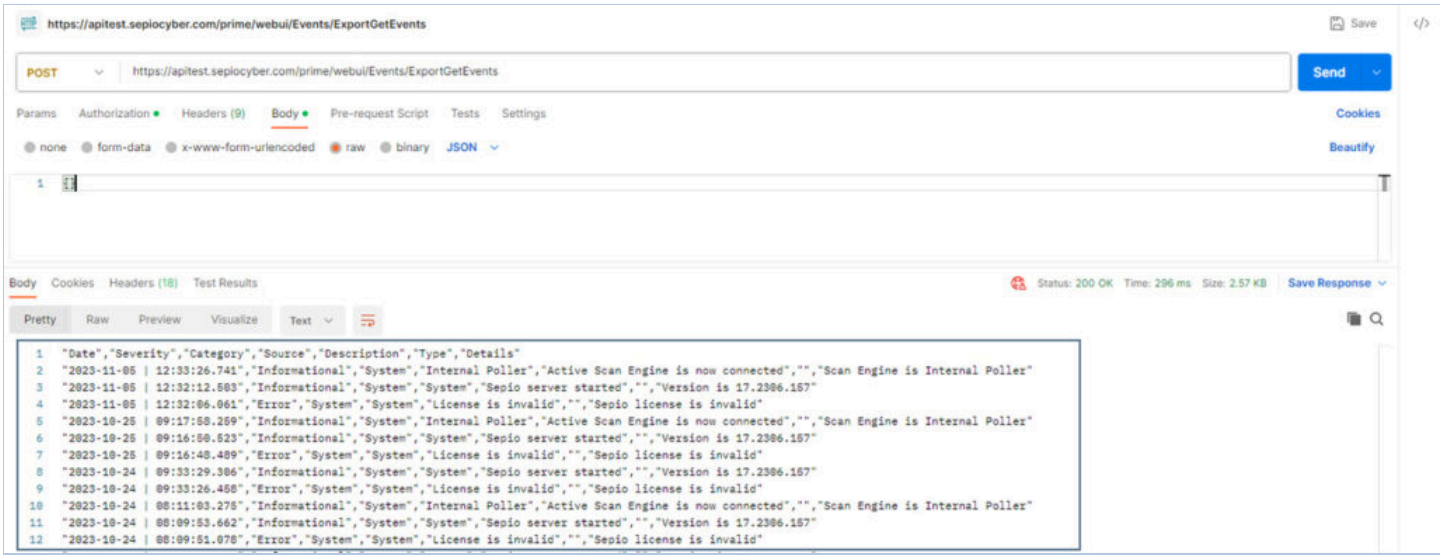
**a)** As the first action you should **add** the **auth token** to the API request.




**b)** Then, add the request **body.** In this example we are sending **empty body**, and the result will be exporting of all content of the **events log.**




**c)** After sending the request we are getting the **events log** entries.




**d)** The output can be **saved to a file.**


Body Cookies Headers (18) Test Results
Status: 200 OK Time: 296 ms Size: 2.57 KB
Save Response
Pretty Raw Preview Visualize Text
Save to a file
"Date","Severity","Category","Source","Description","Type","Details"
"2023-11-05 | 12:33:26.741","Informational","System","Internal Poller","Active Scan Engine is now connected","","Scan Engine is Internal Poller"
"2023-11-05 | 12:32:12.503","Informational","System","System","Sepio server started","","Version is 17.2306.157"
"2023-11-05 | 12:32:06.061","Error","System","System","License is invalid","","Sepio license is invalid"
"2023-10-25 | 09:17:58.259","Informational","System","Internal Poller","Active Scan Engine is now connected","","Scan Engine is Internal Poller"
"2023-10-25 | 09:16:50.523","Informational","System","System","Sepio server started","","Version is 17.2306.157"
"2023-10-25 | 09:16:48.409","Error","System","System","License is invalid","","Sepio license is invalid"
"2023-10-24 | 09:33:29.306","Informational","System","System","Sepio server started","","Version is 17.2306.157"
"2023-10-24 | 09:33:26.458","Error","System","System","License is invalid","","Sepio license is invalid"
"2023-10-24 | 08:11:03.275","Informational","System","Internal Poller","Active Scan Engine is now connected","","Scan Engine is Internal Poller"
"2023-10-24 | 08:09:53.662","Informational","System","System","Sepio server started","","Version is 17.2306.157"
"2023-10-24 | 08:09:51.078","Error","System","System","License is invalid","","Sepio license is invalid"

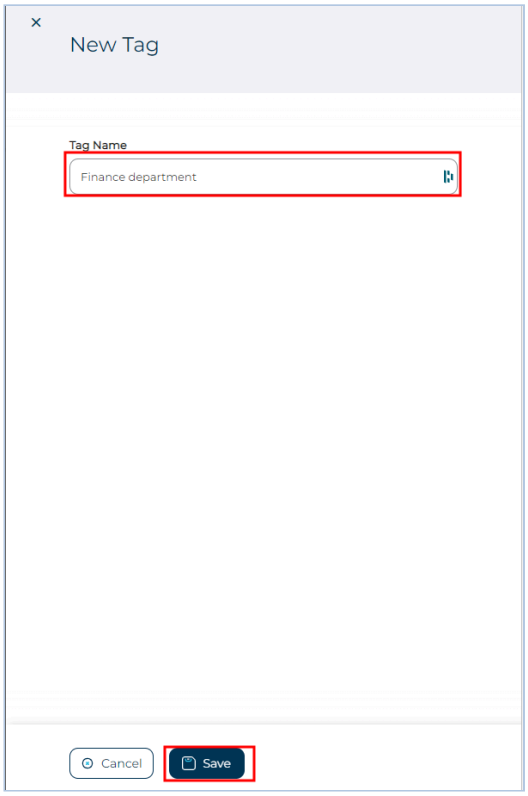
# Managing Tags

Tags enable you to customize the Sepio Platform. You can add, delete, and edit tags for filtering assets in the **Tag Management** tab, as explained in this topic.

## Adding, Deleting and Editing Tags in Sepio Platform

### To Add a Tag in the Sepio Platform

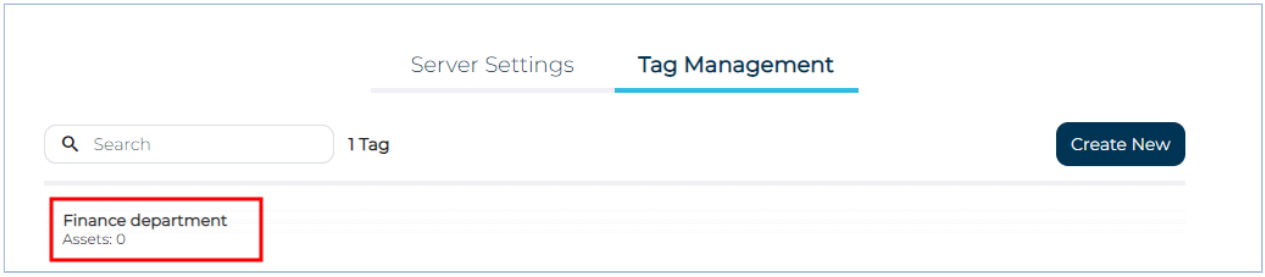
1. Navigate to: **Server** -> **Tag Management** -> **Create New**




New Tag

2. Enter a tag name (e.g., Finance Department).

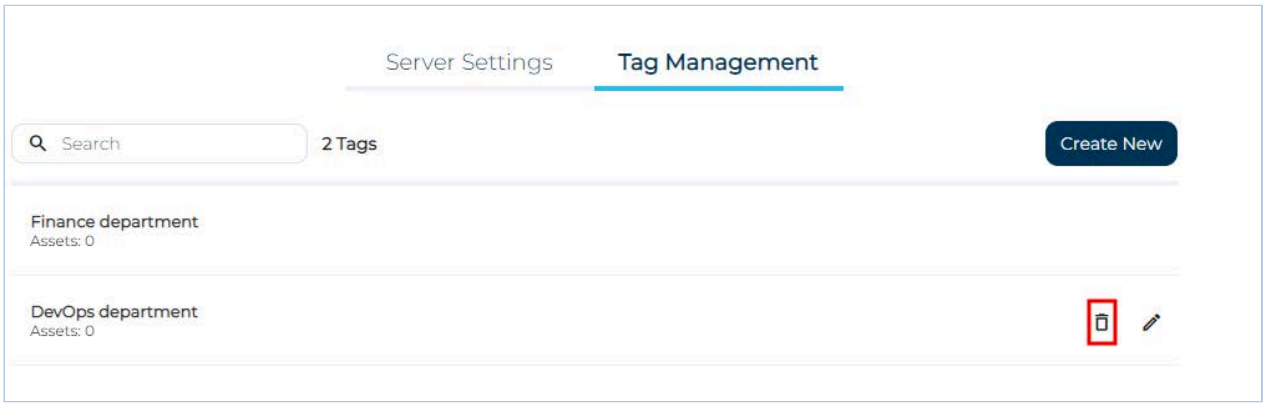
3. Click **Save.**




Tag Management

### To Delete a Tag from the Sepio Platform

1. Navigate to: **Server** -> **Tag Management**




Tag Management

2. Hover over the row containing the tag you want to delete, then click the Delete icon.

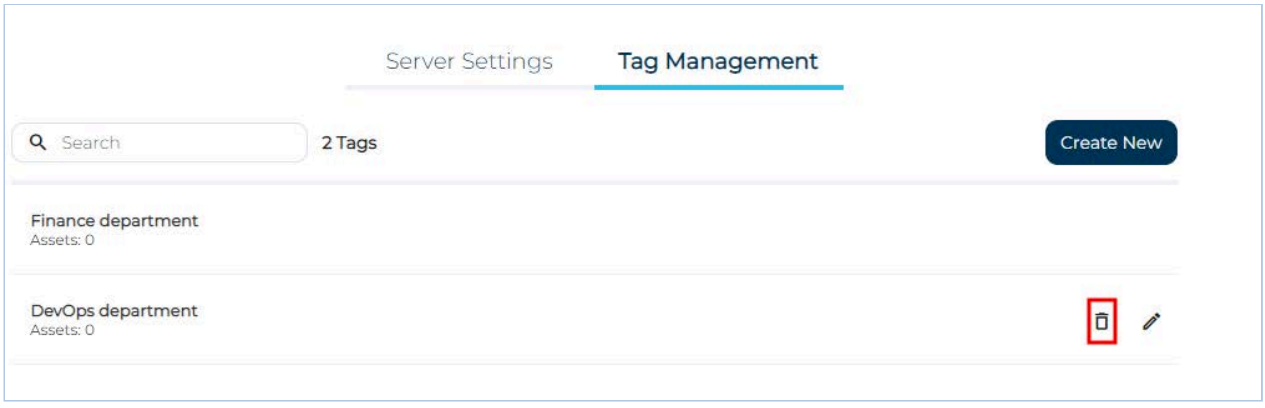



Delete Tag

3. Confirm by clicking **Delete.**

### To Edit a Tag in the Sepio Platform

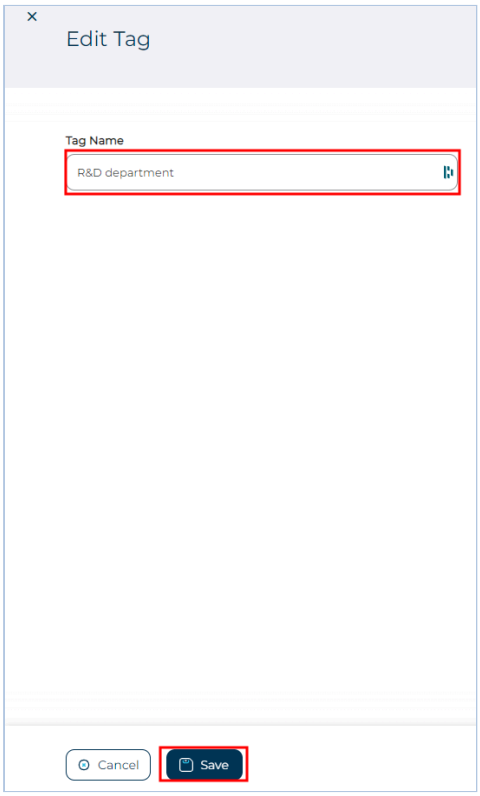
1. Navigate to: **Server** -> **Tag Management**




Tag Management

2. Hover over the row containing the tag you want to edit, then click the **Edit** icon.

3. Update the tag information, then click **Save.**




Edit Tag and Save

# Operational Scenarios

The Sepio Platform offers a set of tools for managing governance, endpoint and network security as part of your hardware risk management and CPS strategy.  This section of the user guide will delve into various operational scenarios that Sepio security administrators encounter during the use of the platform.

## Related Topics

- Governance
- Endpoint and network security
- Deployment of Allowed Peripherals at Scale

## Governance

Sepio provides important governance capabilities for organizations that are concerned about hardware and asset management as part of their risk management process. The following list highlights some of the main tasks that are related to governance in the context of reducing the risk associated with hardware and asset management.

| Governance Requirement | How Sepio assists |
|---|---|
| **Asset State Management** | Asset state management within Sepio's governance framework refers to the continuous monitoring, tracking, and management of the status of physical assets within a cyber-physical system. These assets include industrial control systems (ICS), sensors, actuators, and other components that interact with digital systems.<br><br>**Key aspects of asset state management governance include:**<br>• **Inventory and Classification:** Maintaining a comprehensive inventory of all physical assets, including their location, type, and criticality to operations.<br>• **Monitoring and Data Collection:** Collecting real-time data on asset network presence and conditions.<br>• **Analysis and Anomaly Detection:** Applying DNA detection to identify deviations from normal operating conditions, potential anomalies, or signs of compromise.<br>• **Risk Assessment and Mitigation:** Evaluating the potential risks associated with asset vulnerabilities and implementing appropriate mitigation strategies.<br><br>Every asset discovered and managed by Sepio includes "first seen" and "last seen" dates in its metadata, visible to the user. Since Sepio tracks the precise location of each asset, down to the physical edge port it connects to, detailed reports can be generated to show any changes in asset location and site or switch configuration. This information allows for the creation of a playbook to manage asset state changes effectively. |
| **Configuration Management** | **Configuration management** in the context of Cyber Physical Security (CPS) governance refers to the process of ensuring that the configuration of all physical assets within a cyber-physical system is consistent, accurate, and secure. This includes managing settings, parameters, and software updates to maintain optimal performance and prevent vulnerabilities.<br><br>Sepio, with its ability to gather detailed information about devices, including exact location, network layer 1 and layer 2 information, and using third-party integrations, |

| Governance Requirement | How Sepio assists |
| --- | --- |
| | can significantly assist in configuration management for CPS governance. Here's how:<br>• **Comprehensive Asset Inventory:** Sepio can provide a detailed inventory of all physical assets within a cyber-physical system, including their location, type, and network connectivity. This information is essential for effective configuration management.<br>• **Baseline Configuration Enforcement:** Sepio can help enforce baseline configurations by monitoring the network infrastructure, asset DNA and identify risk then alerting administrators to any deviations. This can help prevent unauthorized changes and maintain system integrity.<br>• **Anomaly Detection:** By analyzing asset DNA and device behavior, Sepio can detect anomalies that may indicate network configuration issues or security threats. This can help identify and address problems before they escalate.<br>• **Integration with Existing Tools:** Sepio can integrate with existing configuration management tools, such as ServiceNow, Intune, Tanium, Ansible or Puppet, to provide additional capabilities and streamline workflows.<br><br>By leveraging Sepio's capabilities, organizations can improve their ability to manage asset configurations, reduce the risk of security breaches, and ensure the reliable and efficient operation of their cyber-physical systems.<br><br>**Note: Patch Management** Automation, an important configuration capability, is not covered by Sepio. |
| **Change Management** | **Change management** in the context of Cyber Physical Security (CPS) governance refers to the process of controlling and managing changes to the configuration of physical assets within a cyber-physical system. This includes reviewing, approving, and implementing changes in a controlled manner to minimize risks and disruptions.<br><br>**Key aspects of change management in CPS governance include:**<br>• **Change Request Process:** Establishing a formal process for submitting, reviewing, and approving change requests.<br>• **Impact Assessment:** Evaluating the potential impact of changes on system operations, security, and performance.<br>• **Testing and Validation:** Conducting thorough testing and validation of changes before implementation.<br>• **Documentation and Auditing:** Maintaining detailed documentation of all changes and conducting regular audits to ensure compliance. |

| Governance Requirement | How Sepio assists |
| --- | --- |
| | • **Incident Response:** Having a plan in place for responding to incidents related to changes, including troubleshooting and rollback procedures.<br><br>## How Sepio Can Assist in Change Management<br><br>Sepio assist in change management for CPS governance. Here's how:<br>• **Change Impact Assessment:** Sepio can help assess the potential impact of changes by analyzing the network physical dependencies between devices and identifying potential risks.<br>• **Configuration Monitoring:** Sepio can monitor asset state to detect unauthorized changes or deviations from the baseline. This can help identify and address issues promptly.<br>• **Integration with Existing Tools:** Sepio can integrate with existing change management tools, such as serviceNow to provide additional capabilities and streamline workflows.<br><br>**Note: Rollback Capability**, which is an important change management governance capability cannot be handled by Sepio.<br><br>By leveraging Sepio's capabilities, organizations can improve their ability to manage changes to their cyber-physical systems, reduce the risk of disruptions, and ensure the security and reliability of their operations. |

# Endpoint and Network Security

The following list provides examples and playbook creation guidelines based on Sepio's capabilities and it can be applied for all the different use cases.

## Endpoint Security

| Scenario | Detection category | Sepio configuration | Next steps |
|---|---|---|---|
| Detection of a USB attack tool, typically able to bypass other endpoint solutions and device controls based on VID/PID detection or broad categories. Using an innocent-looking flash drive to deliver powerful payloads, injecting keystrokes and more. Powerful attack tools, can be purchased online for less than $100 and can bypass most other security controls. | HOST (Sepio Agent). Rubber Ducky used as a difference type of device to bypass other security solutions. | **Detection:** HOST agent in free mode. **Prevention:** HOST agent in BKT or BST modes. **Notifications:** • Peripheral Risk Score 9. • Asset Risk Indicator: risky device connected. • Event log messages. | **Detection only:** isolate the machine. Notify the user. Assume that this machine could be infected. **Blocking:** collect the artifacts for forensics. Check with EDR or other endpoint protection platform which other systems without Sepio agent have this tool's signature. Follow regular procedures for post infection. |
| Detection of a USB implant. Such tools can exploit the target with payloads that trigger when keywords of interest are typed. Emulating trusted devices like serial, storage, HID and Ethernet, it opens multiple attack vectors – from keystroke injection to network hijacking. | HOST (Sepio Agent). Key Croc. | **Detection:** HOST agent in free mode. **Prevention:** HOST agent in BKT or BST. **Notifications:** • Peripheral Risk Score 9. • Asset Risk Indicator: risky device connected. | **Detection only:** isolate the machine. Notify the user. Assume that this machine could be infected. **Blocking:** collect the artifacts for forensics. Check with EDR to see which other systems without Sepio agent have this tool's signature. Follow regular |

| Scenario | Detection category | Sepio configuration | Next steps |
|---|---|---|---|
| | | • Event log messages. | procedures for post infection. |
| Detection of a USB implant hidden inside a regular looking USB cable. It's a cable that looks identical to the other cables users already have. Inside each cable there is an implant that's got a web server, USB communications, and Wi-Fi access. So, it plugs in, powers up, and the attacker can connect to it. | HOST (Sepio Agent).<br>O.MG Cable. | **Detection:** HOST agent in free mode.<br>**Prevention:** HOST agent in BKT or BST modes.<br>**Notifications:**<br>• Peripheral Risk Score 9.<br>• Asset Risk Indicator: risky device connected.<br>• Event log messages. | **Detection only:** isolate the machine. Notify the user. Assume that this machine could be infected.<br>**Blocking:** collect the artifacts for forensics. Check with EDR which other systems without Sepio agent have this tool's signature. Follow regular procedures for post infection. |
| Detection and control of storage device which are used for the most common data theft and exfiltration scenarios. | HOST (Sepio Agent).<br>USB thumb drive. | **Detection:** HOST agent in free mode.<br>**Prevention:** HOST agent in BST modes.<br>**Notifications:**<br>• Asset Risk Indicator: risky device connected.<br>• Event log messages. | **Note:** Sepio can be used to alert about storage violations during non-working hours.<br>In case that the event violates the corporate policy:<br>Notify the user and other parties according to the corporate policy playbook (i.e., the user violates corporate security guidelines).<br>Check with endpoint DLP/EDR the type of data that was copied (as part of corporate policy playbook). |

| Scenario | Detection category | Sepio configuration | Next steps |
|---|---|---|---|
| Detection and control of a mobile phone used as storage device that can be used for more advanced data theft scenario. | HOST (Sepio Agent).<br>Mobile phone. | **Detection:** HOST agent in free mode.<br>**Prevention:** HOST agent in BST mode.<br>**Notifications:**<br>• Asset Risk Indicator: risky device connected.<br>• Event log messages. | **Note:** Sepio can be used to alert on storage violations during non-working hours.<br>Notify the user and other parties according to the corporate policy playbook (i.e., the user violates corporate security guidelines).<br>Check with endpoint DLP/EDR the type of data that was copied (as part of corporate policy playbook). |
| Detection of a Wi-Fi Keylogger, used for capturing keystrokes and sending them wirelessly to a remote location for unauthorized access. | HOST (Sepio Agent).<br>Wi-Fi Keylogger. | **Detection:** HOST agent in any mode.<br>**Notification:**<br>• Event log messages. | **Sample event log:** Agent is () – Host has detected a potential Wi-Fi keylogger in proximity, Network ().<br>**Note:** the same Wi-Fi Keylogger can be detected by multiple host agents positioned in proximity to the device. |

## Network Security

| Scenario | Detection category | Sepio configuration | Next steps |
|---|---|---|---|
| Detection of dual use network devices like Raspberry Pie that can be especially useful inside the network but can also turn against the | Network Security.<br>Raspberry Pie. | Regular Sepio configuration for the desired corporate use case. (i.e., the relevant Risk | **Sample event log:** This device DNA is known to be found in malicious devices at on .<br>**Triage:** |

| Scenario | Detection category | Sepio configuration | Next steps |
| --- | --- | --- | --- |
| company. It is important to find such devices and control them. | | Indicators are enabled).<br>**Notifications:**<br>• Asset Risk Score: 9.<br>• Event log messages.<br><br>Managed switch SNMP credentials for blocking, SIEM Integration. | • Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device.<br><br>**Blocking:** from Sepio (using SNMP) or via network security tools. |
| Detection of an anomaly in regular assets or dual use device that are suspicious. | Network Security. Raspberry Pie spoofed as a legitimate device. | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 8, potentially additional Risk Score are shown (6 or 9).<br>• Event log messages.<br><br>Managed switch SNMP credentials for blocking, SIEM Integration. | **Sample event log:** System detected an anomaly on the DNA of the asset at on . This anomaly may be caused by a MitM or Spoofing attack.<br>**Triage:**<br>• Check if additional RIs are created for this device.<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device.<br><br>**Blocking:** from Sepio (using SNMP) or via network security tools. |
| Unmanaged switches inside a managed network can | Network Security. | Regular Sepio configuration for the | **Sample event logs:** New device Unmanaged Switch |

| Scenario | Detection category | Sepio configuration | Next steps |
| --- | --- | --- | --- |
| indicate the existence of shadow IT.<br>Adding a switch to bypass security is as simple as plugging a cable inside the socket or connecting to an empty port in your IP phone. | Unmanaged switch. | desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 7.<br>• Event log messages.<br><br>Managed switch SNMP credentials for blocking, SIEM Integration. | detected at 05/20/2024 12:37:33 on + + . The Risk Level of Unmanaged Switch has increased from 1 to 7 at 05/16/2024 01:43:12.<br>**Triage:**<br>• Validate if this RI might be a result of excessive configuration (for example, PLC device uses two MAC addresses).<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device. |
| Detection of network tap that can be used for reconnaissance, data theft, launching other attacks.<br>Attackers using a passive switch with a separate USB interface for C&C reduce the possibility of detection by other network security tools. | Network Security and specifically, MITM detection.<br>Plunder Bug or similar tool. | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 9.<br>• Event log messages.<br><br>Managed switch SNMP credentials for blocking, SIEM Integration. | **Sample event log:** New device detected at on .<br>**Triage:**<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device. |

| Scenario | Detection category | Sepio configuration | Next steps |
|---|---|---|---|
| Detection of network HUB that can be used for reconnaissance, data theft, launching other attacks, using a basic and common IT/Networking tools for LOTL and more advanced attacks. | Network Security. Network Hub. | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 8.<br>• Event log messages.<br><br>Managed switch SNMP credentials for blocking, SIEM Integration. | **Sample event logs:** New device detected at on .<br>The system has detected an anomaly on the DNA of the asset at on . This anomaly may be caused by a MitM or Spoofing attack.<br>**Triage:**<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device. |
| Detection of network tap that can be used for reconnaissance, data theft, launching other attack, using a common tool – some are totally passive, and some are active – can be macless. | Network Security. Network Passive Tap. | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 9.<br>• Event log messages.<br><br>Managed switch SNMP credentials for blocking, SIEM Integration. | **Sample event log:** The system has detected an anomaly on the DNA of the asset at on . This anomaly may be caused by a MitM or Spoofing attack.<br>This device on appears to be sleeping at .<br>**Triage:**<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device. |

| Scenario | Detection category | Sepio configuration | Next steps |
|---|---|---|---|
| | | | **Blocking:** from Sepio (using SNMP) or via network security tools. |
| Attacker behind unmanaged switch/network hub present a simple scenario which and attacker finds easy to execute. | Network Security and specifically, MITM detection.<br>Network Hub. | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 5,8,9.<br>• Event log messages.<br><br>Managed switch SNMP credentials for blocking, SIEM Integration. | **Sample event logs:** This device has been identified as a on at .<br>The system has detected an anomaly on the DNA of the asset at on . This anomaly may be caused by a MitM or Spoofing attack.<br>**Triage:**<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device.<br><br>**Blocking:** from Sepio (using SNMP) or via network security tools. |
| Sleeping device in wait mode could represent an attacker but also a tool that is sleeping or unused tool. When this tool, which might be legitimate, will wake up, it might be missing security patches and create a network risk.<br>It is very hard to detect MAC-less and idle devices. It is more difficult to identify | Network Security and specifically, Dormant devices detection.<br>A sleeping PC. | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 6<br>• Event log messages | **Sample event log:** This device has been identified as a on at .<br>**Triage:**<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of |

| Scenario | Detection category | Sepio configuration | Next steps |
| --- | --- | --- | --- |
| devices that are idle for a long time. | | Managed switch SNMP credentials for blocking, SIEM Integration. | notification can be ignored for this device.<br><br>**Blocking:** from Sepio (using SNMP) or via network security tools. |
| Detection of devices behind a legitimate device. Using a simple scenario like using IP phones that are easy to connect and typically have built-in NAC bypass. | Network Security and specifically, MITM detection.<br>IP Phone with built-in switch | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 9.<br>• Event log messages.<br><br>Managed switch SNMP credentials for blocking, SIEM Integration. | **Sample event log:** This device has been identified as a on at .<br>**Triage:**<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device.<br><br>**Blocking:** from Sepio (using SNMP) or via network security tools. |
| Detection of network anomalies. | Network and security best practices.<br>1G device connected to a 100M port. | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 9 (network anomaly).<br>• Event log messages. | **Sample event log:** This device has been identified as a on at .<br>**Triage:**<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device. |

| Scenario | Detection category | Sepio configuration | Next steps |
| --- | --- | --- | --- |
| Detection of rare devices such as consumer grade products. | Network and security best practices.<br>Xbox game console. | Regular Sepio configuration for the desired corporate use case. (i.e. the relevant RI are enabled).<br>**Notifications:**<br>• Asset Risk Score: 5 (rare device).<br>• Event log messages. | **Triage:**<br>• Identify the location of the discovered asset. Is it expected in this facility, switch and VLAN?<br>• Check with the site owner if this type of notification can be ignored for this device. |

# Deployment of Allowed Peripherals at Scale (Armed mode)

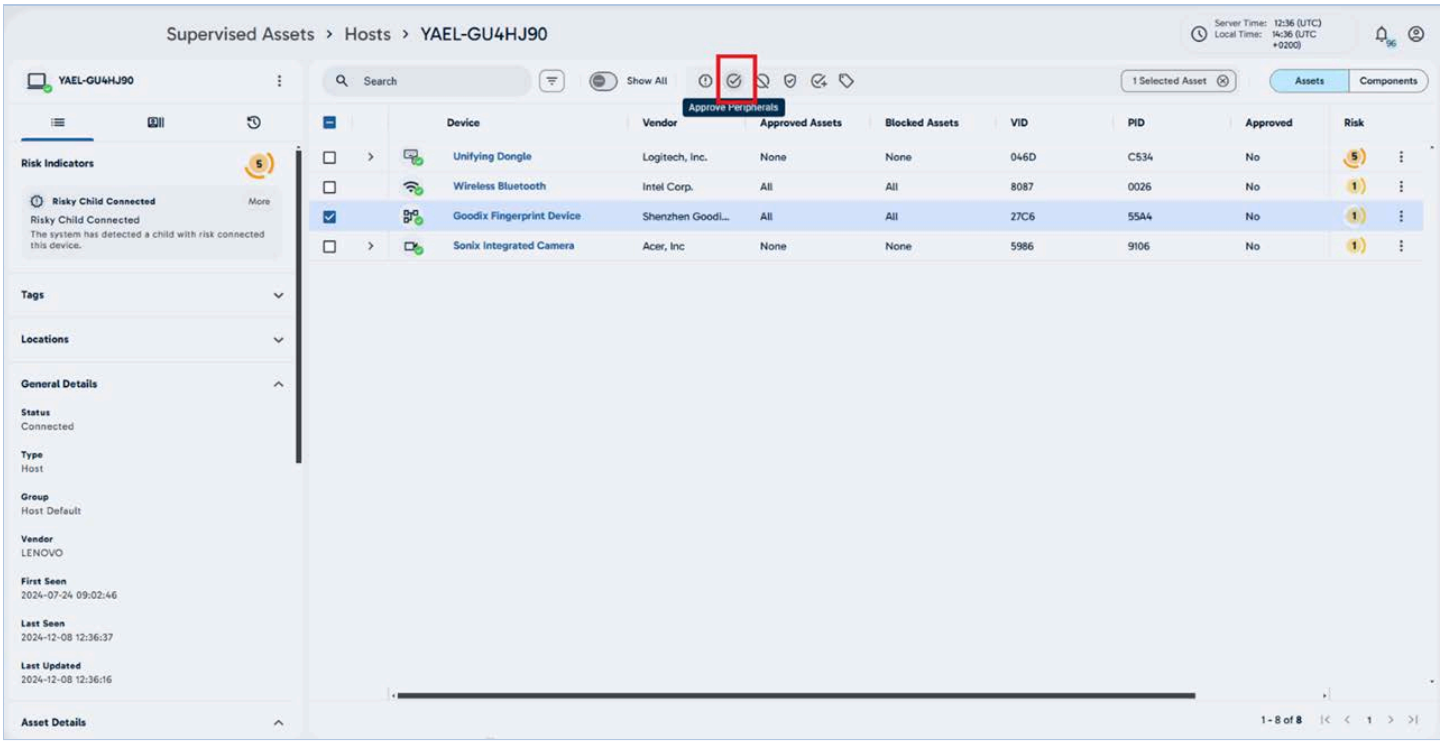
## About Armed Mode

Originally developed to protect ATM, POS terminals, military-grade devices and other special hosts, Armed mode is gaining popularity by organizations that are looking to enforce governance policies for allowed-only peripherals on endpoint devices.

> **Note:** In Armed Mode, the Sepio Agent permits only 'Approved' peripherals to be used within the network. Any peripheral that is not approved or matches the Agent's 'Known Threats' List will be automatically blocked by the platform.

## Approve Peripherals

To enforce an organization-wide policy allowing only specific peripherals, one must first approve those peripherals.
Assets/Peripherals that are not 'Approved' by Sepio will be automatically 'Blocked'. The platform will automatically 'Block' any peripheral that is 'Disapproved,' but it will not block those that are 'Approved'.
The approval task can be performed per specific Host from the host's properties and configuration screen. This screen allows you to select individual peripherals and is designed to provide maximum control and flexibility.



Host's properties and configuration

**Note:** You ‘Approve’ a Host by selecting its ‘Approve All Peripherals’.

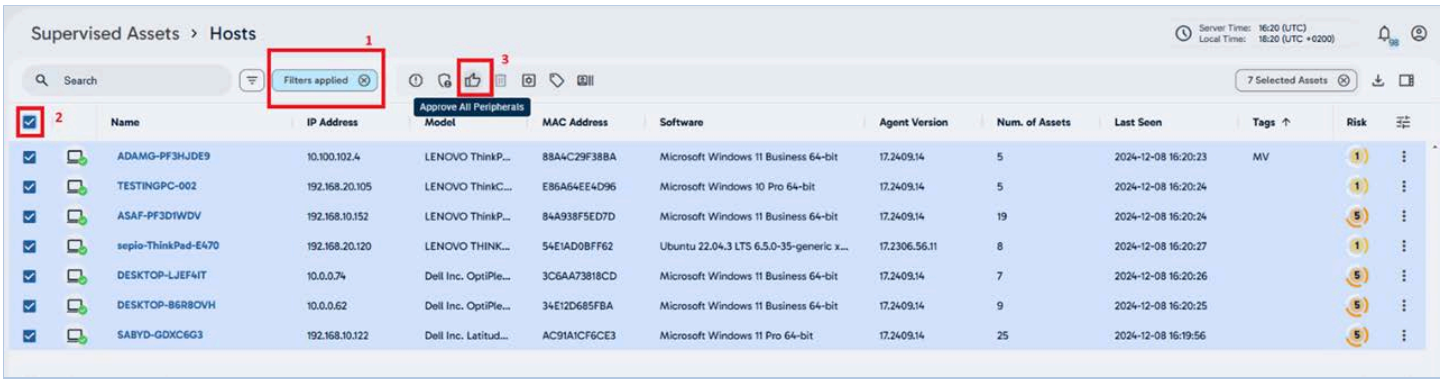
## Peripheral Approval Across Multiple Hosts

When a large number of hosts should be configured, a bulk operation to Approve All Peripherals can be used. The following process can be used:

**Step-by-Step Guide:**

Ensure the hosts to be configured are in **Free Mode**.

1. Create a **query** to identify the hosts with peripherals to approve.
2. Select all the relevant hosts.
3. Execute the **“Approve All Peripherals”** operation.




Approve All Peripherals

**Note:** It is also possible to automate this operation using Sepio’s open API. For detailed instructions or support, contact support@sepiocyber.com.

# ServiceNow CMDB Operations

## Using the Sepio/ServiceNow CMDB Integration

Sepio application for ServiceNow provides device insights for Cyber-Physical Systems (CPS) within the ServiceNow Platform. It enables extending existing processes and workflows already implemented with ServiceNow. Sepio's advanced discovery capabilities feed device information into the configuration management database (CMDB) that is invisible or not available from other sources. It combines ServiceNow's asset mapping and reporting with the ability to reconcile the data found inside the CMDB.

This integration includes automated asset discovery, classification, vulnerability, and risk identification with the seamless extension of current workflows to any environment, leveraging Sepio's asset detection and classification and ServiceNow's Operational Technology Manager (OTM) to improve operational efficiency and security posture.

## Integration Highlights

- Automated discovery of all assets: OT, IT, IoT and any other connected CPS.
- Merging of the discovered inventory in Sepio with the inventory tracked in ServiceNow's CMDB to create a unified, cybersecurity-contextualized, and in-depth inventory of connected assets across all networks and environments.
- Native ServiceNow data model support and reconciliation, feeding asset information directly into ServiceNow, enabling the seamless usage of exported Sepio asset data across various ServiceNow products without any additional manual work.
- Facilitate integration of vulnerability details with Sepio assets for efficient triage, remediation, and security operations extension to all assets.
- Extend existing asset workflows and capabilities.
- More effectively investigate and respond to cybersecurity incidents.

## Sepio ServiceNow Integration Options

It is possible to create new records in CMDB, update existing records only, or perform both actions for different CMDB tables.

Each Configuration Rule can be configured to retrieve single or multiple records, using MAC address as the Identifier key and mapping between Sepio fields and selected ServiceNow CMDB Table fields depending on business requirements.



**Note:** Sepio ServiceNow CMDB integration instructions are listed in Integrating ServiceNow CMDB.

## Sepio ServiceNow Deployment Guidelines

The following guidelines applies to all the different use cases:

- Sepio uses MAC address to match records in CMDB.
- Map between Sepio asset classification and asset type in CMDB. Sepio uses classifications that are like SNOW types but are not identical.
- Create a map between Sepio's asset attribute and the relevant CMDB CI table. For example, Sepio can report VLAN information which may not be present in CMDB for all CI.
- Create reconciliation policy for assets discovered by Sepio (update CMDB / override / add new).
- Create a reconciliation policy for data elements in CI table.
- Decide about the update frequency (scheduling of Sepio app for CMDB).

## Use Case Scenarios with ServiceNow Integration

The following list illustrates the potential of using ServiceNow as part of addressing the different use cases:

| Use Case | Sepio | ServiceNow | Key considerations and Playbooks |
|---|---|---|---|
| Accurate and Complete Asset Inventory | The Sepio platform is tuned for asset discovery | Install Sepio App for ServiceNow CMDB from ServiceNow application store. | 1. Apply the guidelines listed above. |
| Control and reduce the extended asset attack surface | The Sepio platform is tuned for asset discovery with Risk Indicators enabled | Install Sepio App for ServiceNow CMDB from ServiceNow application store.<br>Optional: use ServiceNow SecOps application for integration with Sepio to create tickets within ServiceNow. | 1. Apply the guidelines listed above.<br>2. Decide about the logging strategy for Splunk. Should events that include RI information be exported?<br>3. Add Sepio reports which are exported to SIEM as the input to the attack surface management program.<br>4. Inputs from Sepio are |

| Use Case | Sepio | ServiceNow | Key considerations and Playbooks |
|---|---|---|---|
| | | | added to any risk reduction program. |
| Identify asset vulnerabilities and prioritize by risk | The Sepio platform is tuned for asset discovery, Risk Indicators are enabled, Cisco IOS CVE reports are executed | Install Sepio App for ServiceNow CMDB from ServiceNow application store. | 1. Apply the guidelines listed above.<br>2. Forward risk information notifications from Sepio the SIEM. Create tickets for issues identified by Sepio. |
| Detect & mitigate assets impacted by threats | The Sepio platform is tuned for asset discovery with Risk Indicators enabled. Enable control using SNMP integration for network devices. | Install Sepio App for ServiceNow CMDB from ServiceNow application store.<br>Optional: use ServiceNow SecOps application for integration with Sepio to create tickets within ServiceNow. | 1. Apply the guidelines listed above.<br>2. Forward risk information notifications from Sepio the SIEM. Create tickets for issues identified by Sepio. |

# Shadow IT

Shadow IT refers to information technology (IT) systems and resources used within a company without the approval or knowledge of the central IT department. This can include software, hardware, devices, and cloud services.

## What is Shadow IT in the context of networking?

In the context of networking, Shadow IT refers to any hardware, software, or services used within an organization without the knowledge or approval of the central IT department. This extends beyond just applications to include physical devices that connect to the corporate network, such as personal smartphones, smartwatches, consumer-grade Wi-Fi access points, or even unapproved servers and IoT devices. These assets operate outside established network and security protocols, creating *shadow networks* or blind spots that are invisible to the IT team.

Unauthorized and unsanctioned connections on network devices and infrastructure are a prime example of shadow IT. Here's how it breaks down:

- **Network Devices and Infrastructure:** This includes things like routers, switches, firewalls, and even personal devices plugged into the network.
- **Unauthorized and Unsanctioned Connections:** This refers to any connection made to the network that hasn't been approved or hasn't gone through the proper channels established by the IT department.

## Unauthorized Connections

Here are some ways unauthorized connections can manifest as Shadow IT:

- **Personal Devices:** When an employee plugs in a personal router or storage device to the network, it creates an unauthorized connection. This might be done for file sharing, running personal applications, or bypassing company security protocols.
- **Rogue Access Points:** Setting up a wireless access point without IT's knowledge creates a shadow network connection. This could be the work of a malicious actor attempting to gain access to the network, or simply an employee trying to extend Wi-Fi coverage.
- **Compromised Devices:** If a network device, such as a printer or server, is compromised by malware, it can establish unauthorized connections to external servers for malicious purposes, operating entirely outside IT's control.

The dangers of these unauthorized connections lie in the lack of oversight and security enforcement. IT departments establish specific network configurations and security protocols for a reason. Unauthorized connections bypass these controls, potentially:

- **Introducing Security Vulnerabilities:** Such connections may lack proper firewalls or encryption, creating openings for attackers.
- **Spreading Malware:** Unauthorized devices may carry malware that can spread throughout the network.
- **Data Breaches:** Sensitive data could be accessed or exfiltrated through these unsanctioned connections.

## Shadow IT Scenarios Handled by Sepio

By identifying and addressing unauthorized connections, IT can mitigate the risks of shadow IT and maintain control over the network's security. The table below lists the most common Shadow IT scenarios that are handled by Sepio:

| Scenario | Why is this an issue related to Shadow IT? | Sepio's Fundamental Detection Capabilities | Preparations and Next steps |
|---|---|---|---|
| Unsupervised rogue wireless access point detection. | Access points that are connected to the wired network in a way that is not approved, managed or authorized by corporate, can allow unauthorized access if regular security controls are not implemented. | Access point not associated with Wireless LAN controller. Device is classified as Access Point and has an SSID, which means that it is used as a bridge. | Tag appropriate access point with their parent Wireless LAN controller, then look for access points that are not tagged or that are not managed by such Wireless LAN controller. Create a query filter that can be used to list such access points. |
| Unsupervised rogue wireless access point detection. | Some access point have known vulnerabilities or issues and are not authorized for use. Even if the use of a WIFI network was allowed, it is important to validate and verify that the brand and model of the access point are approved by the corporate. | Unsanctioned access point is being used. Detection of access point which is not found in the authorized asset list. | Tag appropriate access point with their parent Wireless LAN controller, then look for access points that are not tagged or that are not managed by such Wireless LAN controller. Compare detected access point by vendor / type / model / location / business function against, using tags, against the list of |

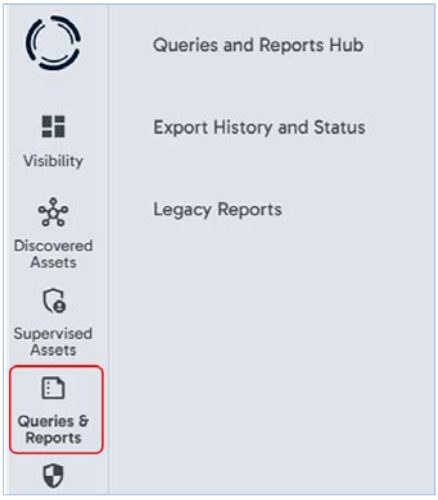
| Scenario | Why is this an issue related to Shadow IT? | Sepio's Fundamental Detection Capabilities | Preparations and Next steps |
|---|---|---|---|
| | | | authorized devices. Create a query filter that can be used to list such access points. |
| Wireless network configuration. | Operational equipment should have fixed IP addresses. Using random MAC addresses violates corporate policies and can indicate a rogue or misconfigured devices that should not be connected to an operational network. | Random MAC address on operational WIFI networks. | Using query filter to identify devices with Random MAC address connected to WIFI that are monitored using production SSID or that are connected to such VLAN that should not have devices with Random Mac address. |
| Wireless network configuration. | Operational equipment should only be connected to operational, monitored and authorized networks. in some cases, guest WIFI networks are configured with lower security requirements. | Operational equipment on guest WIFI networks. | Using query filter to identify devices connected to WIFI that are monitored using non-production SSID or that are connected to such VLAN that should not have guest devices. |
| Wireless network configuration. | BYOD equipment should not be used on operational networks. | BYOD on operational WIFI networks. | Using query filter to identify devices connected to WIFI that are monitored using non-production SSID or that are connected to such VLAN that should not have guest devices. |

| Scenario | Why is this an issue related to Shadow IT? | Sepio's Fundamental Detection Capabilities | Preparations and Next steps |
|---|---|---|---|
| Devices that are not allowed in corporate. | Devices must adhere to corporate policies. Using devices with bad reputation can indicate an issue. In some countries, some types of assets with bad reputation are not allowed to be operated. | Bad reputation. | Create and run scheduled reports to identify devices with bad reputation. |
| Devices that are not allowed in corporate. | Devices that can be used for both legitimate and non-legitimate uses are typically restricted and should be found only in specific locations. | Dual use devices Detection of Gaming / personal use devices. | Create and run scheduled reports to identify devices that belong to such category. |
| Devices that are not allowed in corporate. | Personal use devices can carry vulnerabilities and must be approved by corporate. | Dual use devices in unauthorized locations. | Create and run scheduled reports to identify devices that have dual use. |
| Wired network configuration. | Unmanaged switches extend the boundaries of the network and are often not managed. | Adding an unmanaged switch. | Create and run scheduled reports to report unmanaged switches. |
| Wired network configuration. | Multiple devices that are connected via unmanaged switches or using built-in switches . | Detecting multiple devices on the same port. | Create and run scheduled reports to report unmanaged switches. |
| Wired network configuration. | Switches are expected to be managed and monitored. Using unmanaged switches can extend the boundaries of the network and are often not managed. | Using unsupervised switch. | Create and run scheduled reports to report unsupervised switch. |
| Wired network configuration. | There's a reason for using network segmentation. Violating this principle can indicate wrong configuration, | Using equipment in the wrong VLAN. | Using query filter to identify devices connected to wrong VLANs – for example, ILO interfaces. |

| Scenario | Why is this an issue related to Shadow IT? | Sepio's Fundamental Detection Capabilities | Preparations and Next steps |
|---|---|---|---|
| | security or governance related issues. | | |
| Rogue VM. | VMs should be used on authorized, known and monitored hypervisors only. | Detection of VMs on the wrong VLAN. | Using query filter to identify VM connected to wrong VLANs. |
| Rogue VM. | Using unsanctioned equipment can expose the corporate to security and legal issues. | Detection of unsanctioned Hypervisor vendors. | Using query filter to identify VMs that are not allowed in the network. |

## Queries and Reports

It is possible to use the table viewer to create queries that can be saved as reports. These reports are accessible for immediate use whenever needed or can be scheduled for email delivery.




Queries and Reports

## Query Examples

In this section, we have listed some simple yet very useful queries that can be used as examples:

### New Assets in the Last x Hours

This report displays all newly discovered assets (hosts, peripherals, network devices, etc.) within a configurable time frame. In the example below, the report shows all assets discovered in the last 24 hours.

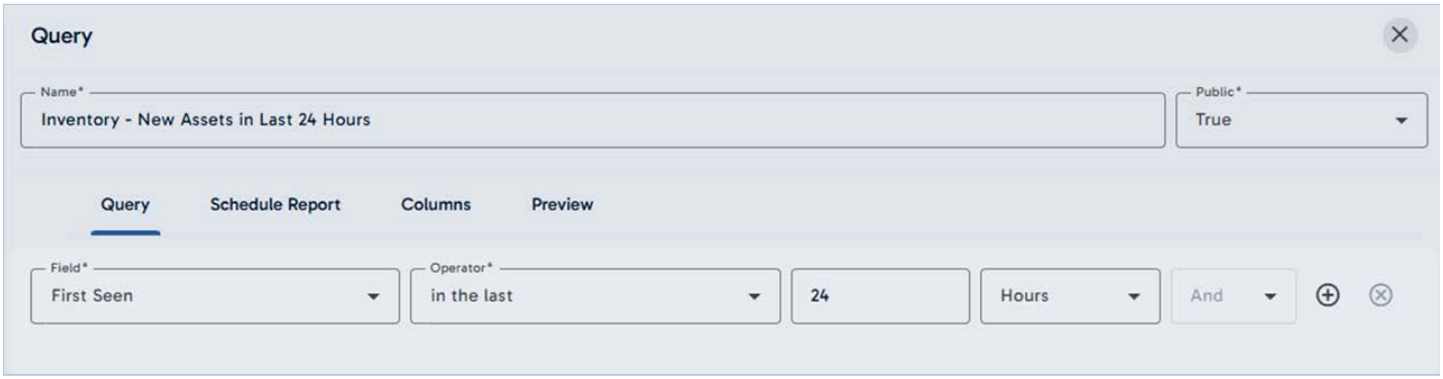
**Use Case:**

- Investigate new assets to detect unexpected changes in the environment, such as unauthorized or unmanaged devices.
- Support continuous asset inventory management.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| First Seen | In the last | 24 hours | |

**Tip:** To report on specific types of new devices within the last 24 hours, add the **Type** field to the query and select the desired device types (e.g., hosts, switches, etc.).




Inventory – New Assets in Last 24 Hours

### New Peripherals

This report displays all newly discovered USB peripherals within a configurable time frame. In this example, we are reporting all peripherals discovered in the last 24 hours.

### Use Case:

- Investigate new USB assets to detect unexpected changes in the environment, such as unauthorized or unmanaged peripherals.
- Support continuous asset inventory management.

### Query Configuration:

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| First Seen | In the last | 24 hours | AND |
| Connection Type | Is | USB | |




Inventory – New Peripherals

### Vulnerable Peripherals

This report identifies all peripherals that contain known vulnerabilities. These hardware vulnerabilities are often exploited through sniffing attacks, such as mousejacking.

**Use Cases:**

- Investigate vulnerable peripherals for potential unauthorized use.
- Support risk management programs by identifying risks associated with USB devices.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Risk Sub Indicator | Is | Peripheral Vulnerability Detected | |

**Tip:** To view **new** vulnerable peripherals, add a **"First Seen in the last x hours/days"** condition to the query.




Security – Vulnerable Peripherals

### Agents Disconnected for More Than x Days

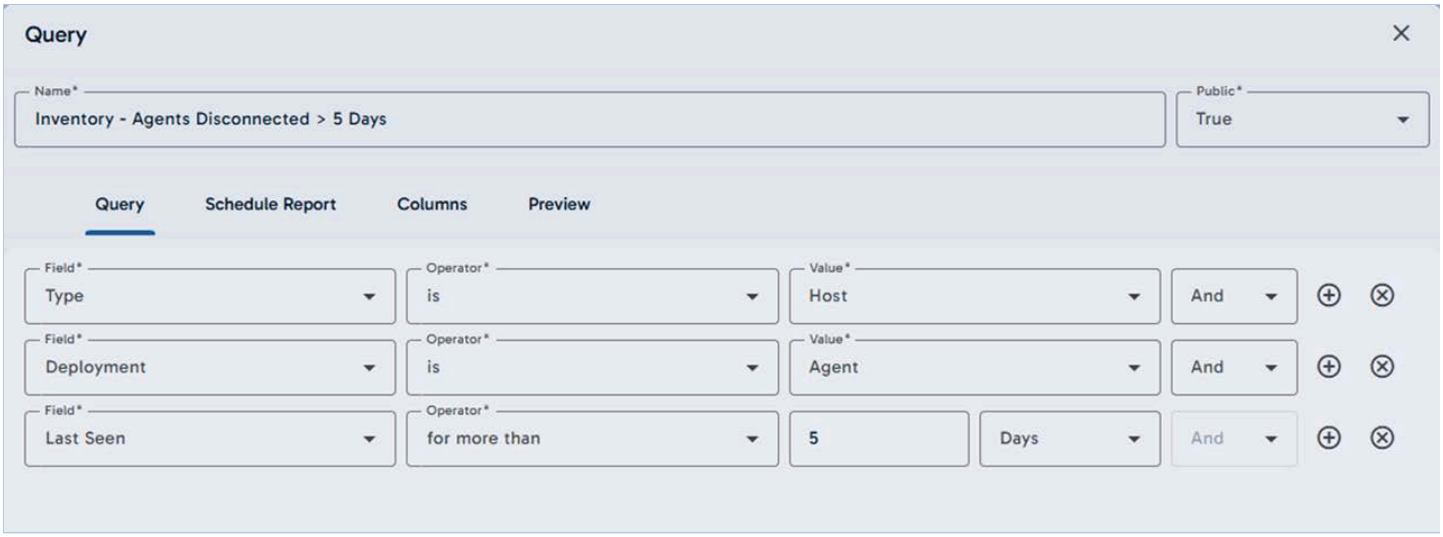
This report identifies any supervised host that has not connected to the platform within a configurable time frame. In this example, the report shows all hosts that have been disconnected for more than 5 days.

**Use Case:**

- Investigate for potential network misconfiguration.
- Identify potential issues with agent connectivity.
- Support continuous asset inventory by tracking online and offline systems.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Type | Is | Host | AND |
| Deployment | Is | Agent | AND |
| Last Seen | For more than | 5 days | |




Inventory – Agents Disconnected More Than 5 Days

### Rare Online Assets

This report identifies any assets from vendors that have a low occurrence within the environment. The occurrence threshold is configurable within the platform and defaults to two. This report shows assets from vendors with two or fewer instances in the environment.

**Use Cases:**

- Investigate unauthorized, suspicious, or rogue assets.
- Validate against the approved vendors list.
- Support vendor risk assessment programs.
- Maintain continuous asset inventory.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Risk Sub Indicator | Is | Rare Device | AND |
| Is Online | Is | Yes | |

**Tip:** The **"Is Online"** condition is optional, use it if you want to display only currently online assets. Omit it to include assets that have connected in the past but are not currently online.




Inventory – Rare online assets

### Bad Reputation Assets

This report identifies assets from vendors flagged with a bad reputation. These vendors are listed in the Sepio Knowledge Base due to prior associations with compromised hardware or involvement in known attacks.

### Use Cases:

- Investigate vendors with a history of poor security practices, known vulnerabilities, or associations with threat actors.
- Identify “Mouse Jigglers”, vendors known for manufacturing USB devices that simulate mouse movement (a specific query for mouse jigglers is provided on the next page).
- Support your risk management program by documenting devices that pose potential risks based on vendor reputation.

### Query Configuration:

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Risk Sub Indicator | Is | Bad Reputation | |




Security – Bad Reputation

### Mouse Jigglers

This report lists devices that are potential mouse jigglers. These devices often use chipsets also found in inexpensive USB keyboards and mice. Any device identified in this report should be investigated to determine its legitimacy and potential risk.

**Use Cases:**

- Investigate potential mouse jiggler use, including:
  - Misuse or abuse of corporate assets.
  - Timecard fraud.
  - Security risks related to bypassing lock screen activation.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Risk Sub Indicator | Is | Bad Reputation | AND |
| Connection Type | Is | USB | |




Security – Mouse Jigglers

### Section 889 Compliance

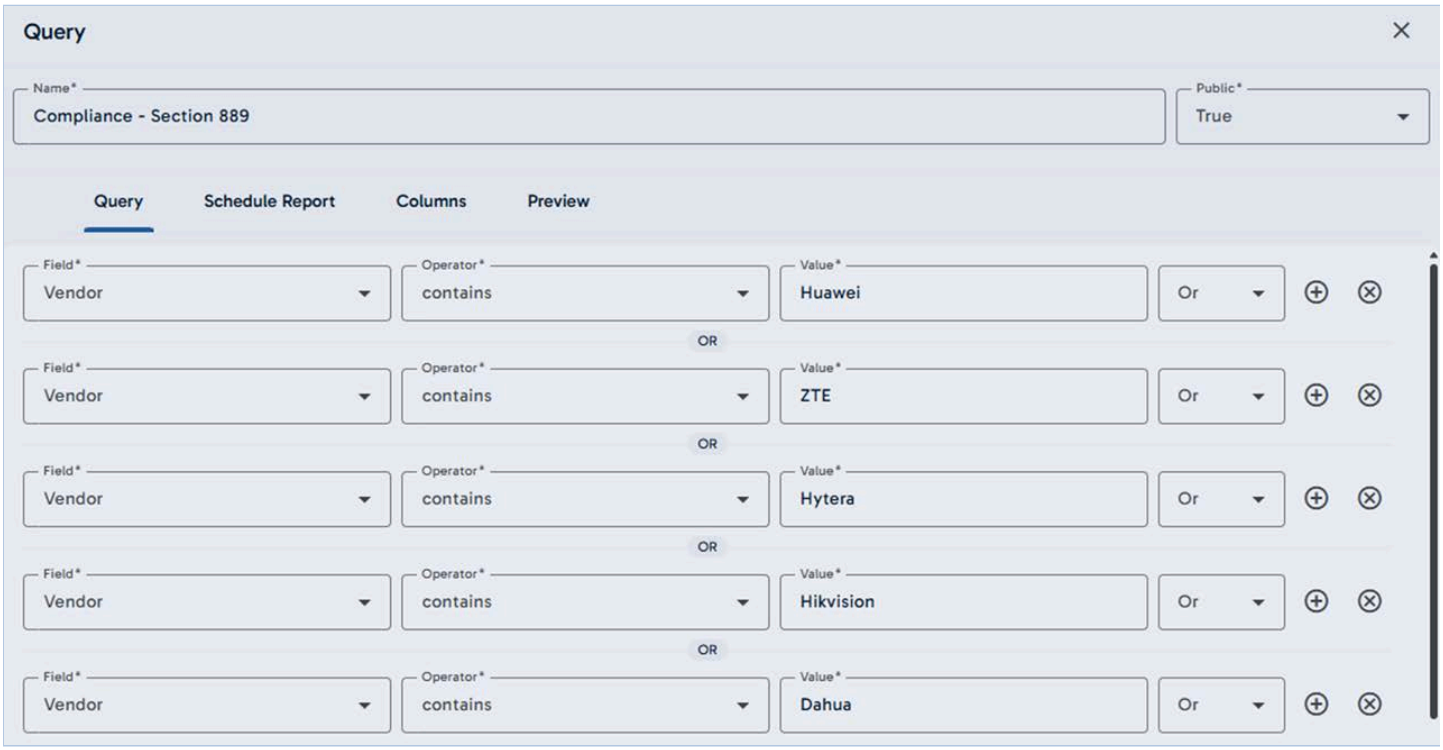
This report displays a list of assets associated with vendors disallowed under Section 889 of the National Defense Authorization Act (NDAA). Disallowed vendors include Huawei, ZTE, Hytera, Hangzhou Hikvision, and Dahua.

**Use Case:**

- Ensure Section 889 compliance.
- Investigate the presence of potentially disallowed vendors.
- Cross-check against the organization's approved vendors list.
- Support vendor risk assessment initiatives.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Vendor | contains | Huawei | OR |
| Vendor | contains | ZTE | OR |
| Vendor | contains | Hytera | OR |
| Vendor | contains | Hikvision | OR |
| Vendor | contains | Dahua | |



Compliance – Section 889

**Unmanaged Switches**

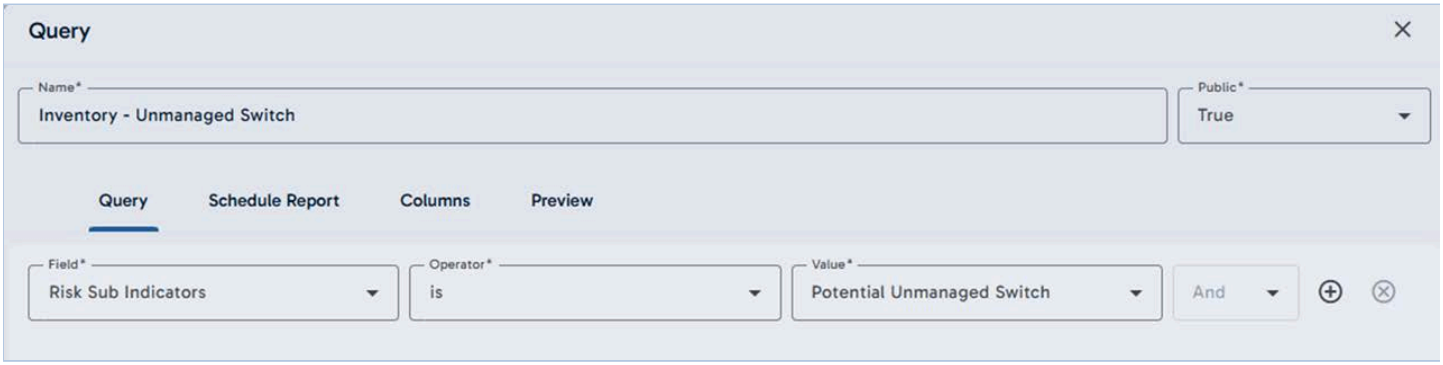
This report identifies any potentially unmanaged switches detected as being connected to supervised network switches.

**Use Case:**

- Investigate shadow IT and unauthorized unmanaged switches.
- Investigate devices connected to those unmanaged switches.
    - Viewable by clicking on the port where the unmanaged switch is connected.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Risk Sub Indicator | Is | Potencial Unmanaged Switch | |




Inventory – Unmanaged Switch

### Unsupervised Switches

This report identifies switches that have been detected in the environment but are not configured to be polled by the Sepio platform.

### Use Cases:

- Identify switches potentially missing from the network inventory.
- Prioritize onboarding of these switches to the Sepio platform for complete coverage and asset visibility.

### Query Configuration:

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Risk Sub Indicator | Is | Unsupervised Network Infrastructure | |




Inventory – Unsupervised Switches

### Unsupervised Hosts

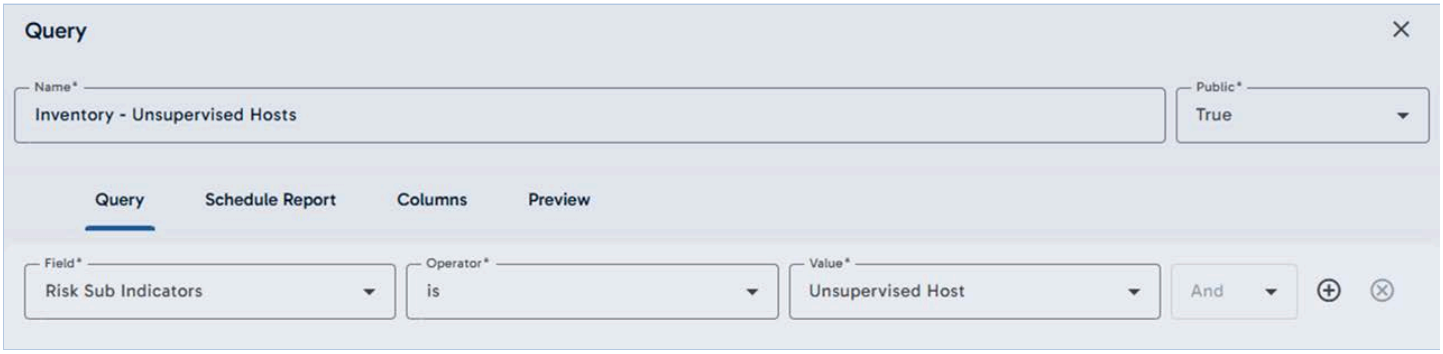
This report identifies discovered hosts on the network that do not have the Sepio Agent installed.

**Use Case:**

- Prioritize hosts for agent installation.
- Full coverage of hosts for full asset visibility.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Risk Sub Indicator | Is | Unsupervised Host | |




Inventory – Unsupervised Hosts

**Switches with Open CVEs**

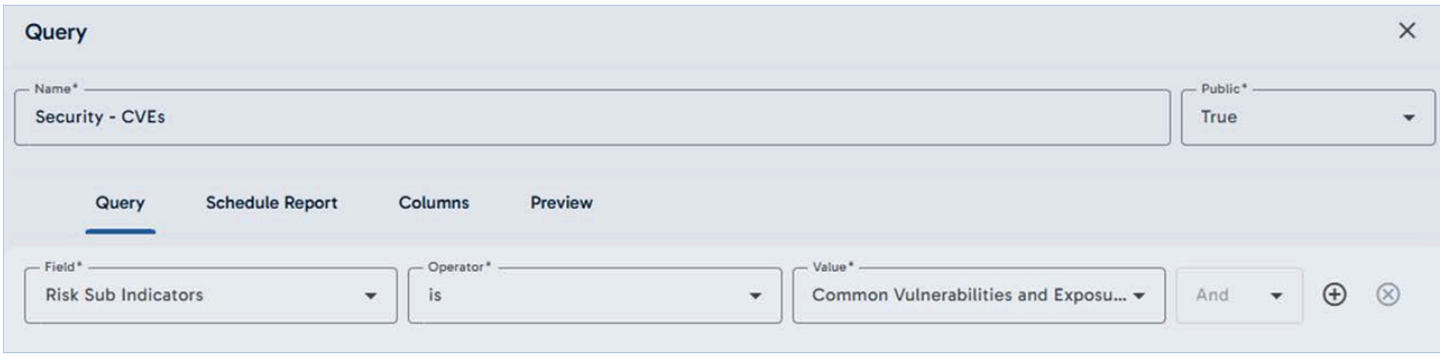
This report identifies switches that have open Common Vulnerabilities and Exposures (CVEs) associated with them. CVEs are identified based on the firmware and service versions of the enabled components on the switch.

**Use Case:**

- Identify switches with vulnerabilities.
- Prioritize vulnerability mitigation efforts.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Risk Sub Indicator | Is | Common Vulnerabilities and Exposures (CVE) | |




Security – CVEs

### Inventory by VLAN

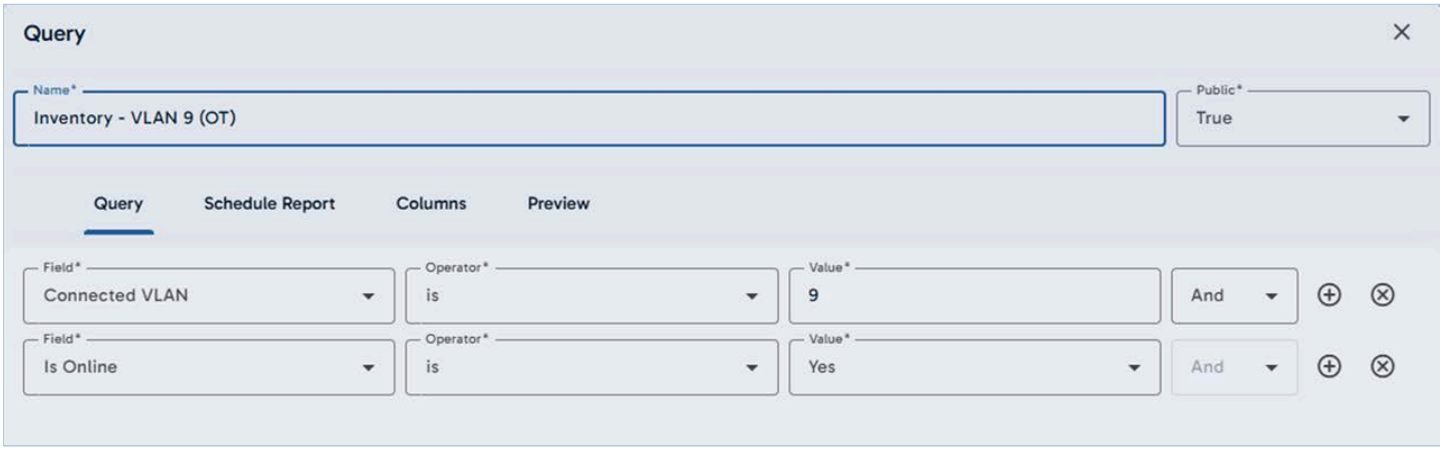
This report identifies all assets connected to a specified VLAN.

### Use Cases:

- Gain visibility into assets connected to sensitive or dedicated VLANs.
- Identify unauthorized devices connected to sensitive VLANs.
- Monitor network segmentation configuration for security and compliance.

### Query Configuration:

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Connected VLAN | Is | | |




Inventory – VLAN 9 (OT)

### Inventory by Tag or User Attribute

This report identifies devices that are tagged with specific user attributes. Tags and user attributes are used to provide additional business context to assets, such as criticality, location, responsibility, etc.

### Use Cases:

- Perform continuous asset inventory based on a location tag or attribute (e.g., All assets in Building ABC).
- Track asset inventory by department.
- Maintain an inventory of sensitive assets.
- Ensure compliance by maintaining inventory information with location details.

**Query Configuration:**

| Field | Operator | Value | Logic Operator |
|---|---|---|---|
| Tag | 'is' or 'contains' | | AND or OR |
| User Attribute/Attribute | 'is or 'contains' | | |




Inventory – Critical Assets in Building 20

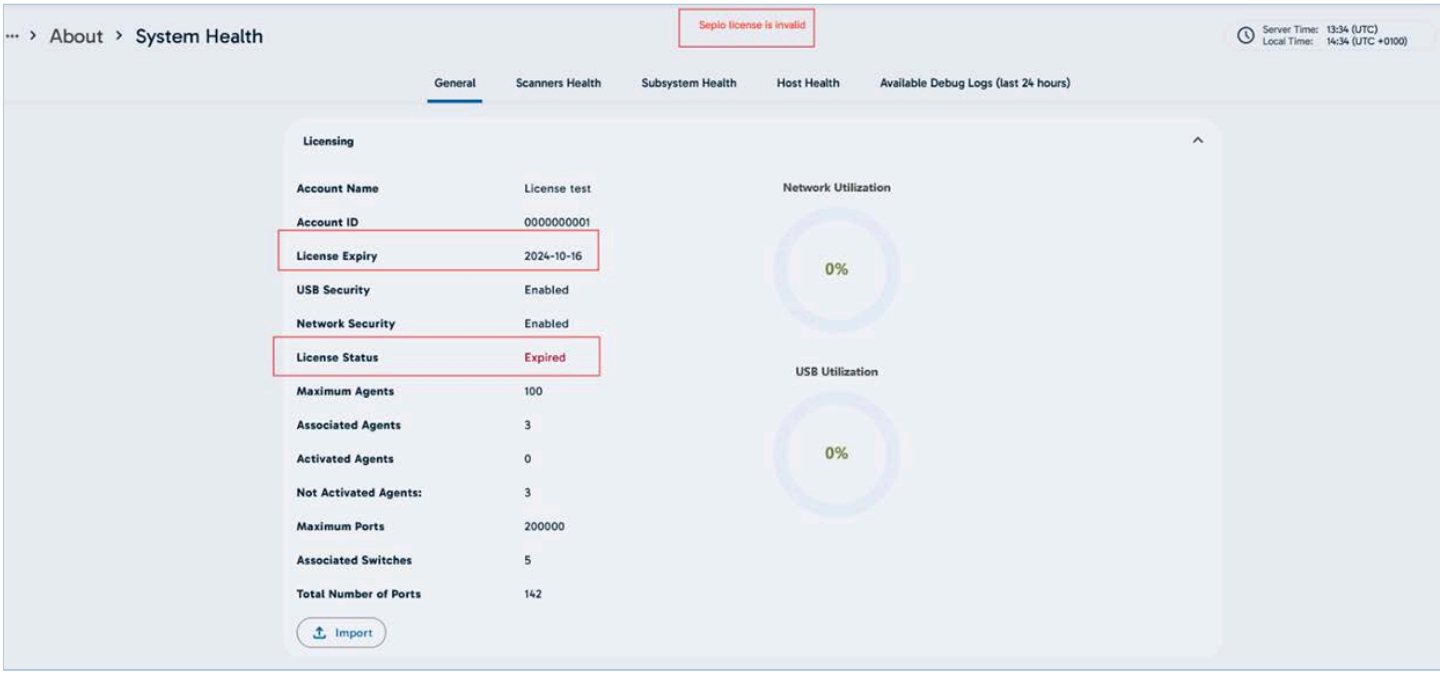
# Licensing

## Overview

A Sepio License covers the number of supervised hosts (hosts with Sepio Agents) and the number of monitored switch ports for the duration of the subscription. You must install the License before using the platform for the first time, as described in “Logging in to Sepio for the first time.”

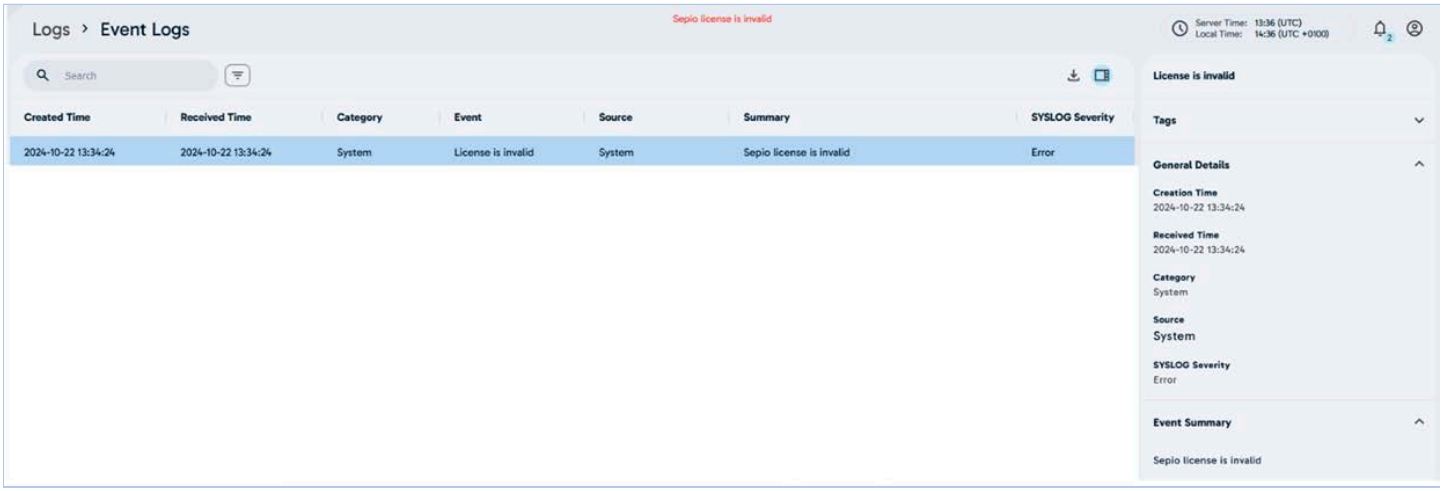
## When the License Has Expired

You can verify the License status on the System page:
**Settings -> About -> System Health -> General**




License Status: Expired

A message will also appear in **Logs ->Event Logs:**
“Sepio License is invalid”




Sepio License is invalid

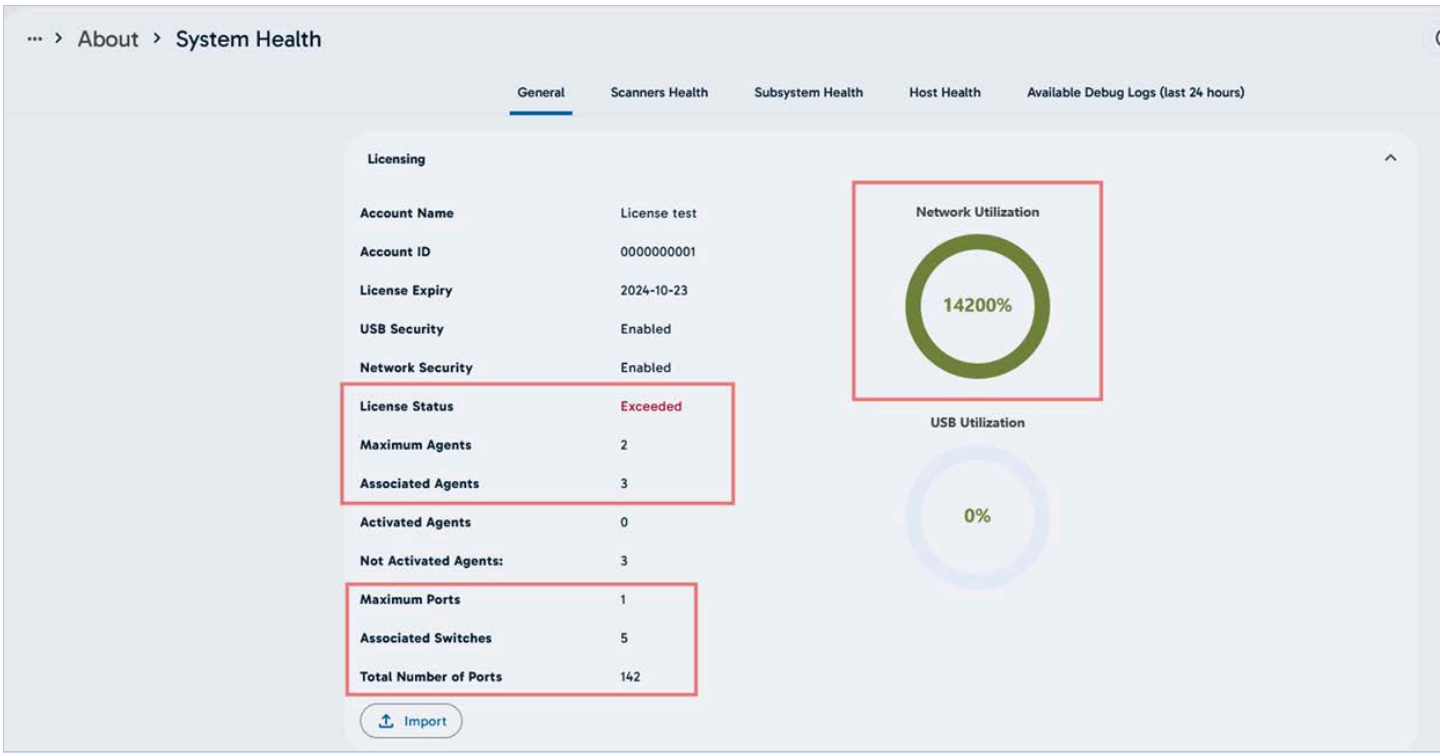
## Symptoms of Expired License

- Hosts will be disconnected from the UI. The following error message may appear in the agent logs (C:\Program Files\Cyber Sepio Systems\SepioAgent\AgentFiles\Logs):
  `https://<the host fqdn>/prime/agentsapi/v2/heartbeat, internetConnection: True, with Result: []. Exceptions Messages: System.Net.Http.HttpRequestException: Response status code does not indicate success: 500 (Internal Server Error)`
- New hosts cannot be added; they will not appear in the Console, and a "**500 (Internal Server Error)**" message may appear in the agent logs.
- Network visibility is not impacted; existing switches will continue to be scanned.
- New switches can be added manually, they will appear in Sepio Console Management and be scanned.
- Network infrastructure can still be added using CSV import even when the License has expired. All imported switches will appear in Sepio Console Management.

## When the License Limit Is Exceeded

You can verify the License status on the System page:

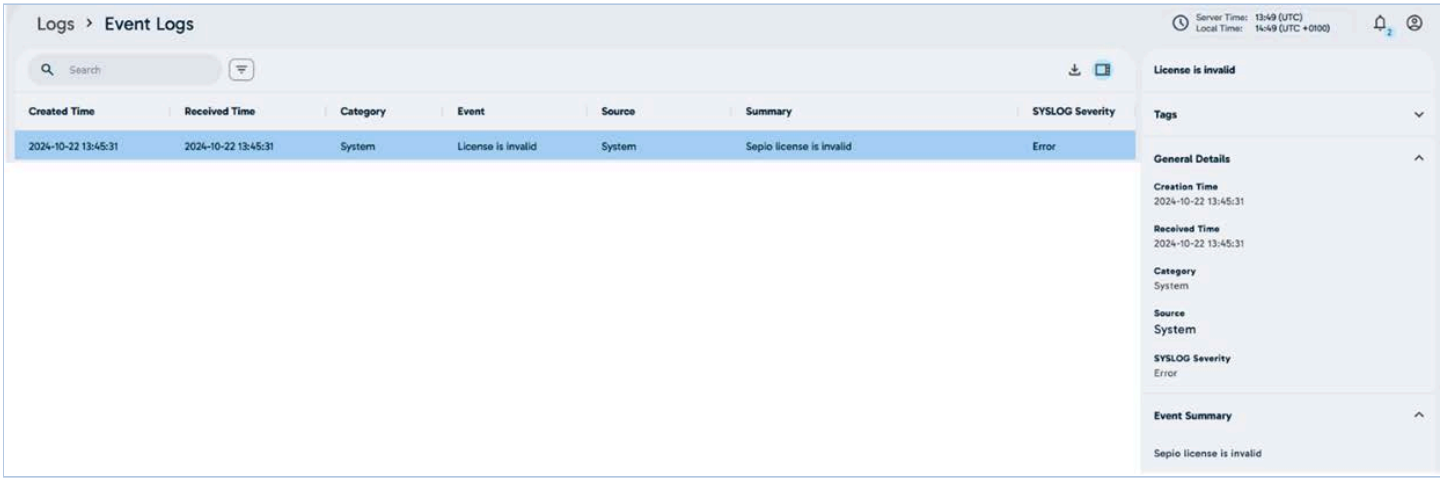
**Settings** -> **About** -> **System Health** -> **General**




License Status: Exceeded

A message will also appear in **Logs** -> **Event Logs:**

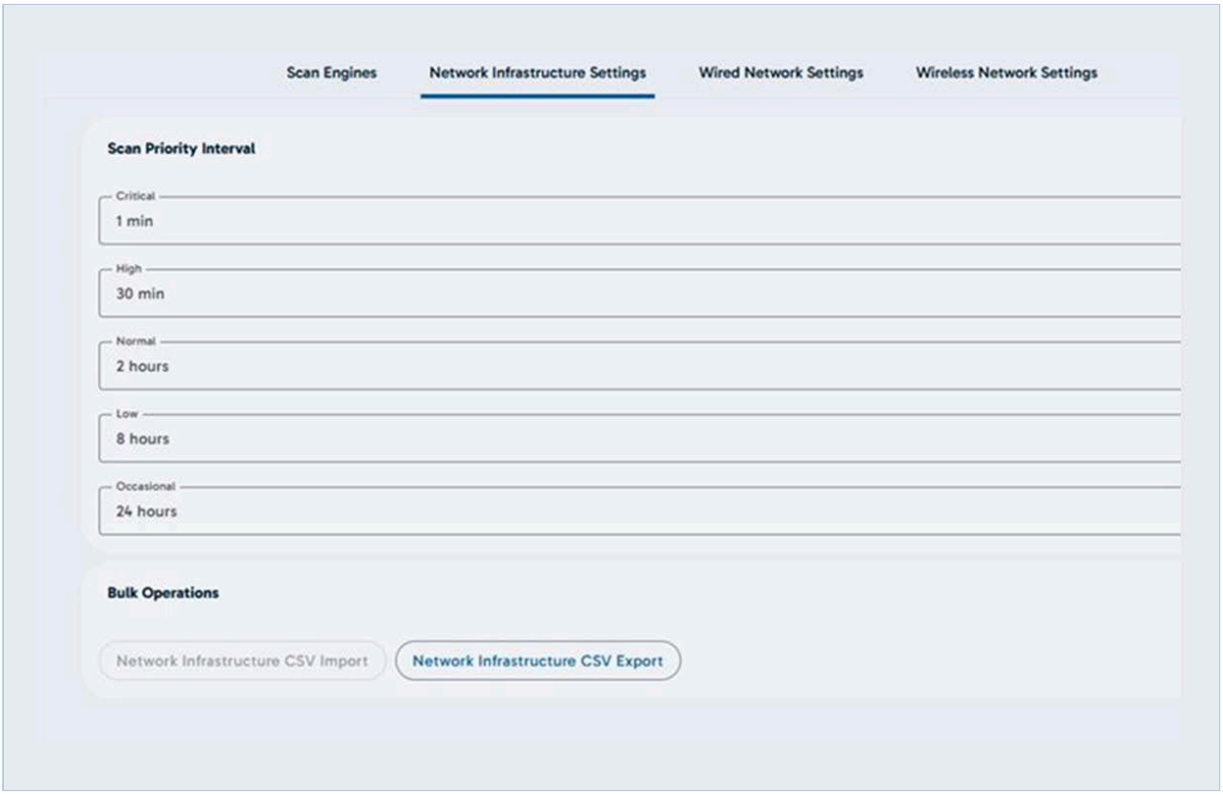
“Sepio License is invalid – Exceeded”




Sepio License is invalid – Exceeded

## Symptoms of Exceeded License Limit

- New hosts cannot be added once the “Maximum Agents” limit is exceeded. They will not appear in the Console, and a “**500 (Internal Server Error)**” message may appear in the agent logs.
- You cannot manually add network assets because the “+” button will be disabled.
- Network Infrastructure cannot be added using CSV import; the “Network Infrastructure CSV Import” button will not be available.




Network Infrastructure CSV Import will not be available

## Installing and Applying a License

The Sepio License file is provided as a password-protected ZIP file. The following instructions apply for both production and evaluation environments.

> **Note:** There is no need to extract the zip file. The License ZIP file is loaded **as is.**

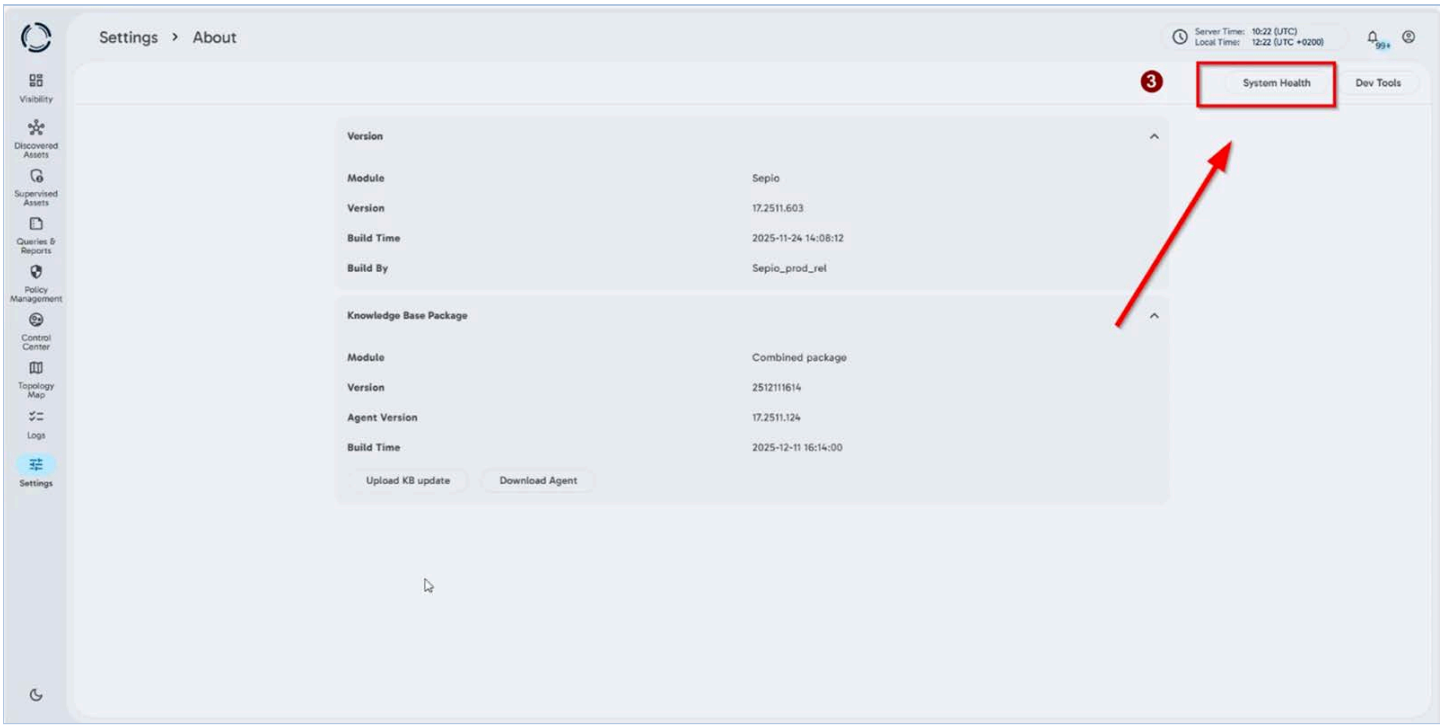
**Steps to apply the License:**

1. From the **Settings** menu, select -> **About**



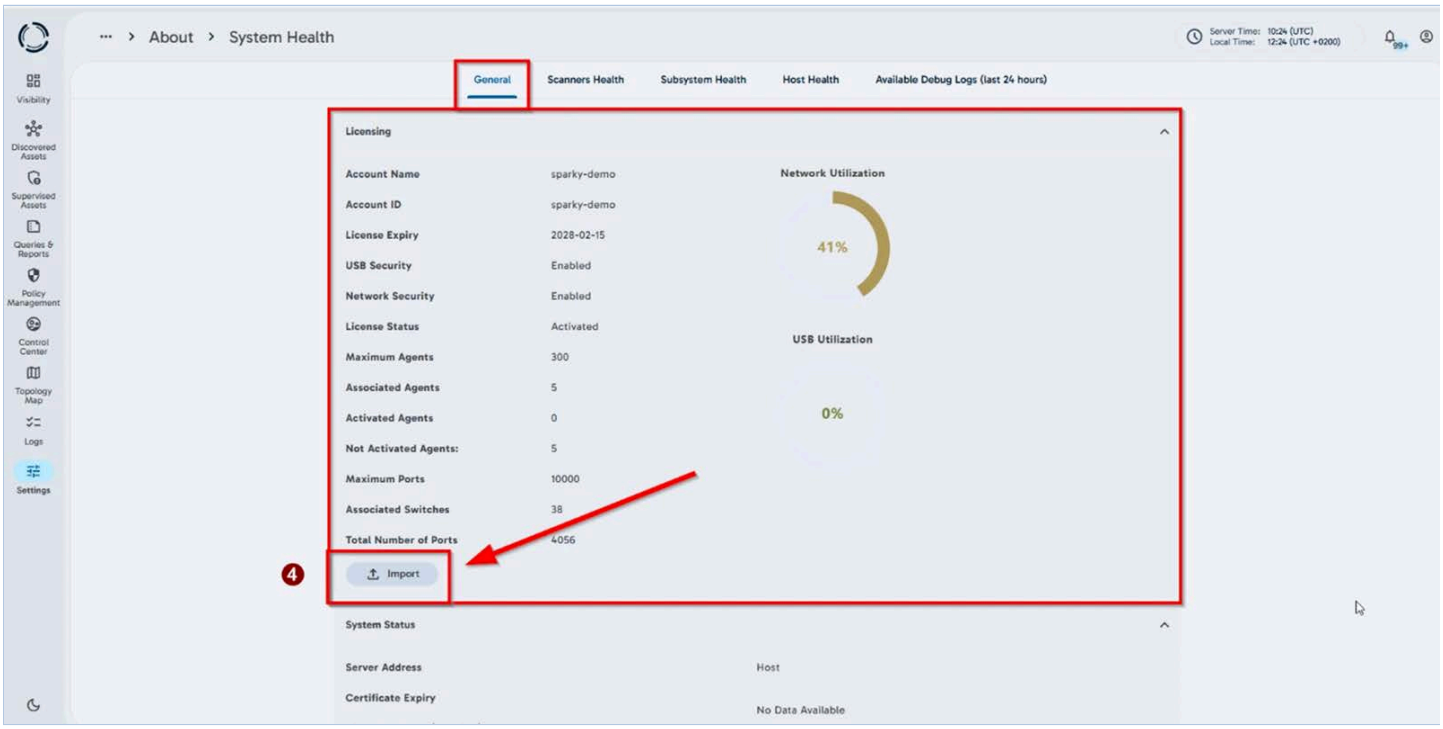

Select About

2. Click **System Health.**



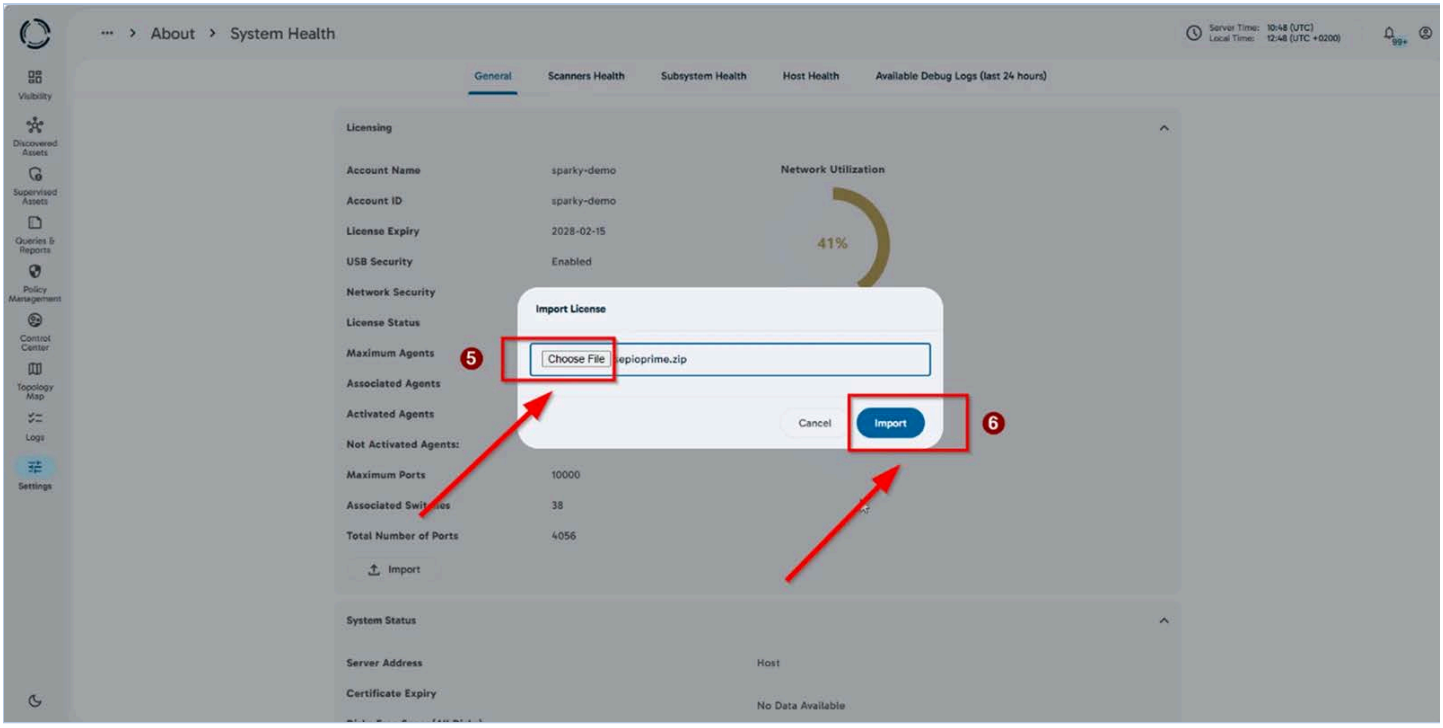

Click System Health

3. Click **Import.**




Click Import

4. Choose the License file (usually named sepioprime.zip) and click **Import.**




Click Import

5. **Finally**, verify that the License is applied correctly and that the number of Agents and monitored Ports matches your subscription.

# Integrations

Integrations allow you to connect the Sepio Platform with other security solutions.

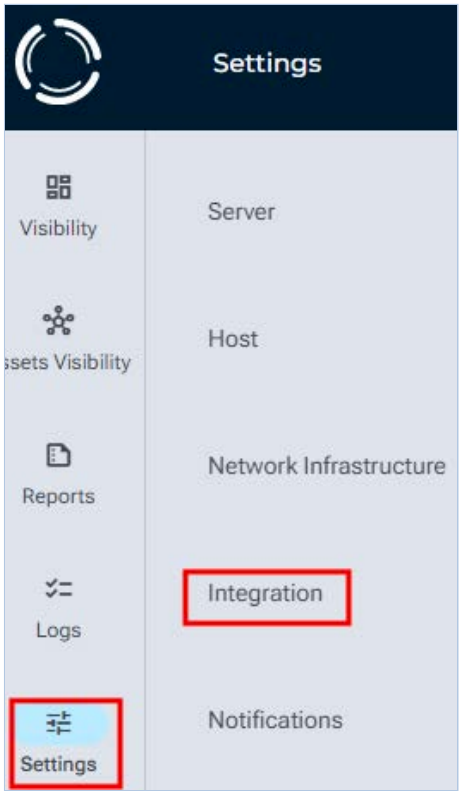
## Related Topics

- Opening the Integration View
- Configuring and Editing Integration Settings
  - Configuration Settings
    - Adding and Configuring a Meraki Switch
    - Axonius Integration
    - CrowdStrike Falcon Integration
    - Cisco Identity Services Engine (ISE) integration
    - Configuring Forescout (legacy)
    - Sepio Connector App for Forescout
    - Configuring Guardicore
    - Configuring SAML
    - Configuring Syslog
    - Integrating ServiceNow CMDB
    - Integrating ServiceNow Queries
    - Integrating ServiceNow SecOps
    - Lightweight Directory Access Protocol (LDAP)
    - Microsoft Intune
    - Network HTTP Proxy
    - Splunk Integration
- Enabling and Disabling Integrations

# Opening the Integration View

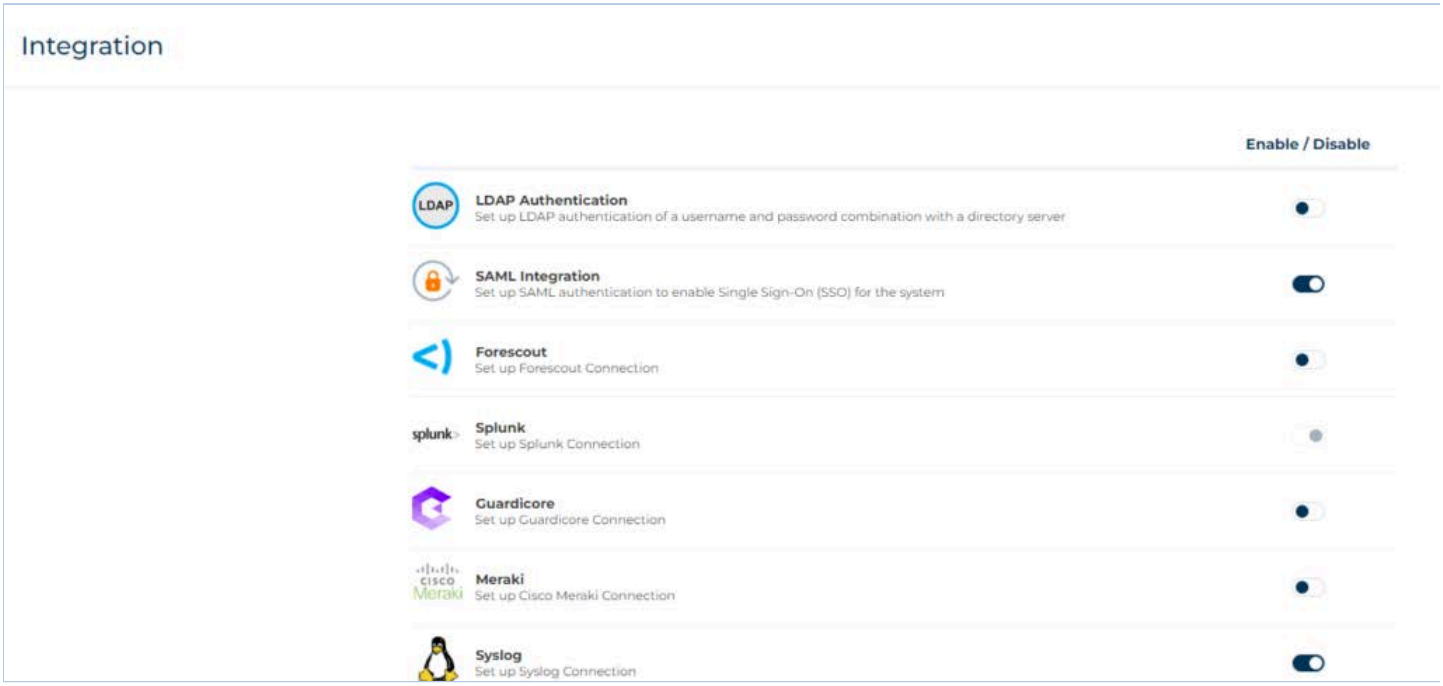
## Integration View

1. On the **Sepio menu**, select **Settings** -> **Integration.**




Integration

2. The **Integration** view window will open.
    - From here, you can **enable or disable integrations** as needed.




Enable or disable integrations

# Configuring and Editing Integration Settings

## Related Topics

- Configuring and Editing Integration Settings
  - Configuring Integrations
    - Adding and Configuring a Meraki Switch
    - Axonius Integration
    - CrowdStrike Falcon Integration
    - Cisco Identity Services Engine (ISE) integration
    - Configuring Forescout (legacy)
    - Sepio Connector App for Forescout
    - Configuring Guardicore
    - Configuring SAML
    - Configuring Syslog
    - Integrating ServiceNow CMDB
    - Integrating ServiceNow Queries
    - Integrating ServiceNow SecOps
    - Lightweight Directory Access Protocol (LDAP)
    - Microsoft Intune
    - Network HTTP Proxy
    - Splunk Integration

# Configuring Integrations

## Related Topics

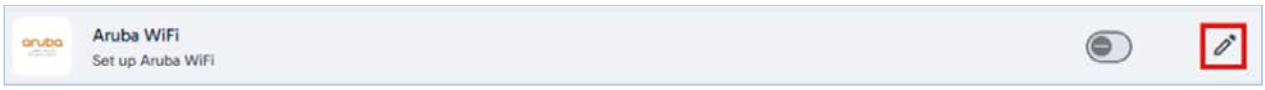
- Adding and Configuring a Meraki Switch
- Aruba Central Integration
- Axonius Integration
- Cisco ISE integration
- Configuring Forescout (legacy)
- Configuring Guardicore
- Configuring SAML
- Configuring Syslog
- CrowdStrike Falcon Integration
- Integrating ServiceNow CMDB
- Integrating ServiceNow Queries
- Integrating ServiceNow SecOps
- Lightweight Directory Access Protocol (LDAP)
- Microsoft Intune
- Network HTTP Proxy
- Sepio Connector App for Forescout
- Splunk Integratio

# Configuring Aruba Devices Through Aruba Central

Aruba Switches and Access Points are cloud-managed and should be integrated into the Sepio Platform through the Aruba Central interface.

## Adding an Aruba Device

1. In the Sepio menu select **Settings** -> **Integration.**
2. Click **Edit.**

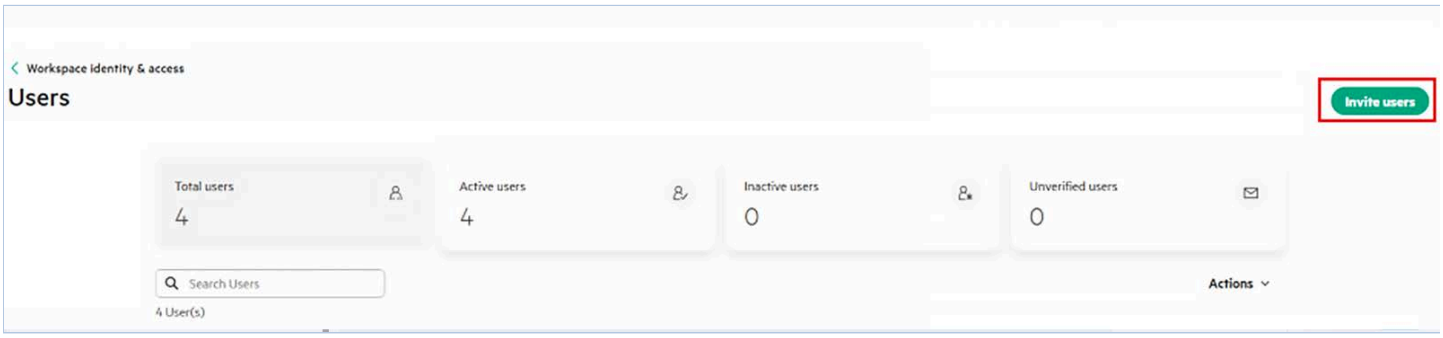



Set up Aruba Wi-Fi

3. Enter the six parameters:
    - **Base URL**
    - **Username**
    - **Password**
    - **Client ID**
    - **Client Secret**
    - **Customer ID**
4. Select a **Scan Priority.**
5. Select a  **Domain.**
6. Click **Test Connection**, to test the connection between Sepio Platform and Aruba Central.

### Creating Username and Password for Sepio

1. Launch **HPE GreenLake Console** -> **User Management** -> **Invite users.**
    - **Email:** Enter a valid email address. This will be the **Username.**
    - **HPE GreenLake Role:** Select **Workspace Observer.**



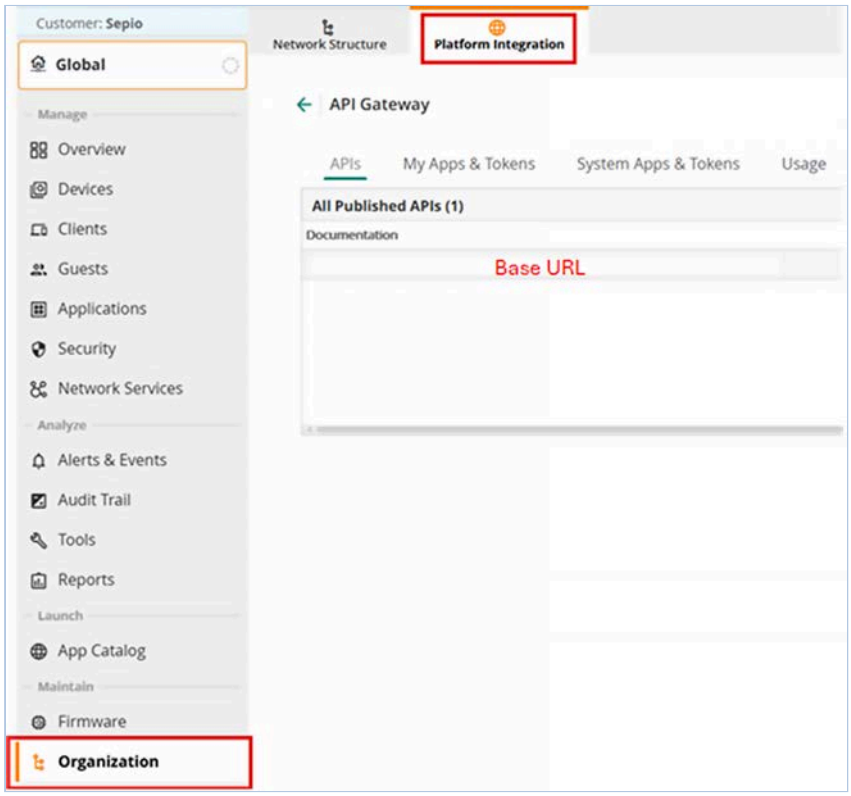

Invite users

2. Open the invitation email and verify the account. (During this process, you will choose the **Password.**)
3. Under the new Sepio account, select **Assign Role:**

- **Service:** HPE Aruba Networking Central
- **Role:** Aruba Central View Only

### Base URL

1. Launch **HPE Aruba Networking Central.**

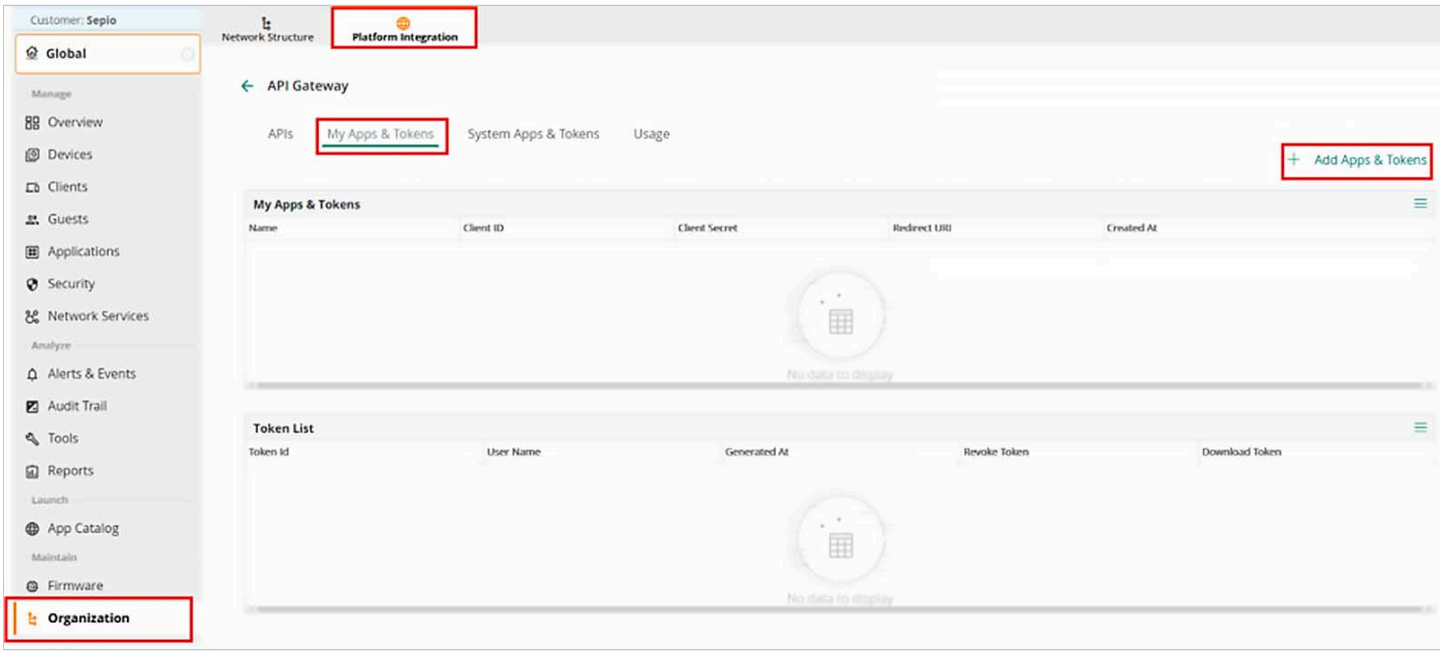



Platform Integration – Base URL

2. Go to **Organization -> Platform Integration -> Rest API.**
3. Locate the URL under the title **Documentation.**
4. The **Base URL** includes everything from 'https' through '.com' (inclusive).
   - Example: `https://something.central.arubanetworks.com`

### Client ID and Client Secret

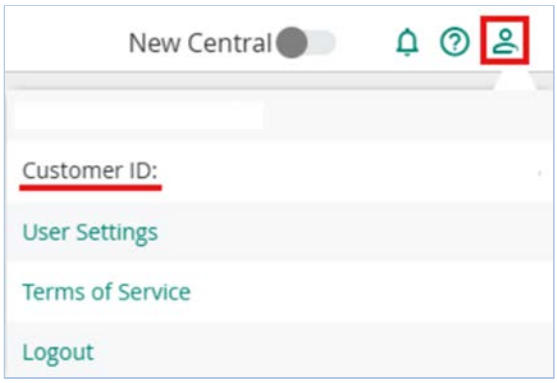
1. Launch **HPE Aruba Networking Central.**
2. Navigate to **Organization** -> **Platform Integration** -> **Rest API** -> **My Apps & Tokens.**
3. Click **Add Apps & Tokens.**
4. Press **Generate.**
5. Copy the **Client ID** and **Client Secret.**




Platform Integration – Rest API – My Apps & Tokens

## Customer ID

1. In the top-right corner, click the **user icon.**
2. Copy the **Customer ID.**




Customer ID

# Adding and Configuring a Meraki Switch

## Overview

Meraki switches and access points are cloud-managed and must be integrated into the Sepio Platform using the Meraki Dashboard API. Adding a Meraki API key automatically discovers Meraki network elements. After adding the key, you select a scan priority and domain, test the connection, and enable the integration.

## Preparing to Add a Meraki Switch

To access the Meraki Dashboard API, you must enable API access for your organization.

- Log in to the Cisco Meraki Dashboard.
- Navigate to **Organization** -> **Configure** -> **API & Webhooks**.
- Enable Dashboard API access, as described in the Cisco Meraki Dashboard API documentation.

## To Add the Meraki API Key

1. From the Sepio menu, select **Settings** -> **Integration**.
2. Click **Add Meraki Integration**.
3. Enter the **Meraki API Key**.




Add Meraki Integration

**Notes:**

- The Meraki API key provides access to the Meraki Dashboard API. Sepio uses the following API endpoints with read-only access (GET):

  `GET /devices/`

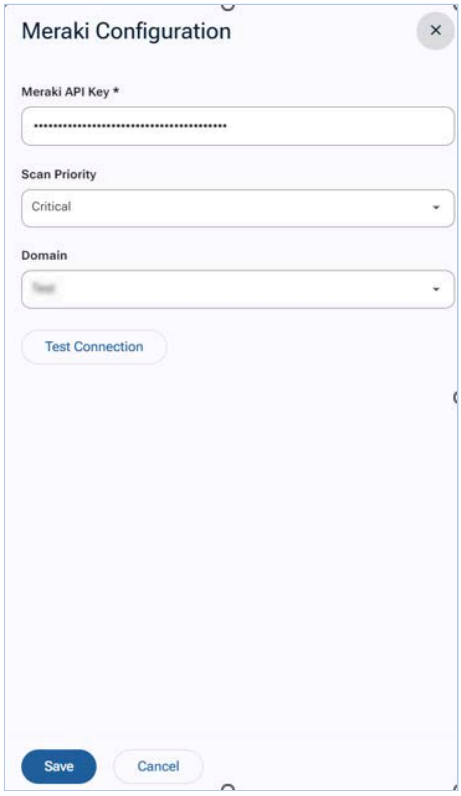
  `GET /networks/`

  `GET /organizations/`

- Sepio also integrates using the (PUT) method with write access when a Sepio administrator explicitly initiates a block port action.

  `PUT /devices/{serial}/switch/ports/{portId}`

4. Select a **Scan Priority**.
5. Select a **Domain**.
6. Click **Test Connection** to verify connectivity between the Sepio Platform and the added switch.



Test Connection

7. Click **Save**.
8. Enable the integration.

## Configure the Meraki API URL

If required, you can configure a custom Meraki API URL for the netpoller service (Sepio Scan Engine).

- Open the NetPoller configuration file.
- Add the following environment variable:
  `Environment="NETPOLLER_MERAKI_URL="`
- Example:
  `Environment="NETPOLLER_MERAKI_URL=api.gov-meraki.com"`

## ALT MGMT LAN IP Configuration

The Meraki cloud provides two sources of IP addresses:

- LAN IP
- ALT MGMT LAN IP

By default, Sepio uses the LAN IP.

If required, it is possible to extract the ALT MGMT LAN IP instead:

- Open the NetPoller configuration file.
- Add the following environment variable:

  ```
  Environment="NETPOLLER_MERAKI_USE_ALT_MGMT_IP=true"
  ```

> **Note:** If the ALT MGMT LAN IP is missing, Sepio will use the LAN IP.

# Axonius Integration

Axonius is a unified cybersecurity asset management platform that helps organizations gain visibility into all their assets, identify and remediate security risks, and automate security workflows. It collects asset information using integrations with various data sources such as Sepio using Data Adapters. Together, the integrated solution can be used for a variety of use cases, including asset inventory, vulnerability management and incident response.

Asset information is provided by Sepio to the Axonius platform in “pull mode”, meaning that Axonius will fetch asset information from Sepio. The Integration with Axonius requires definition of a Sepio user account and ensuring that connectivity between Axonius management and the Sepio Platform can be established. Additional configuration options are available from Axonius adapter page.

This integration is supported from Axonius version 5.0.

# CrowdStrike Falcon Integration

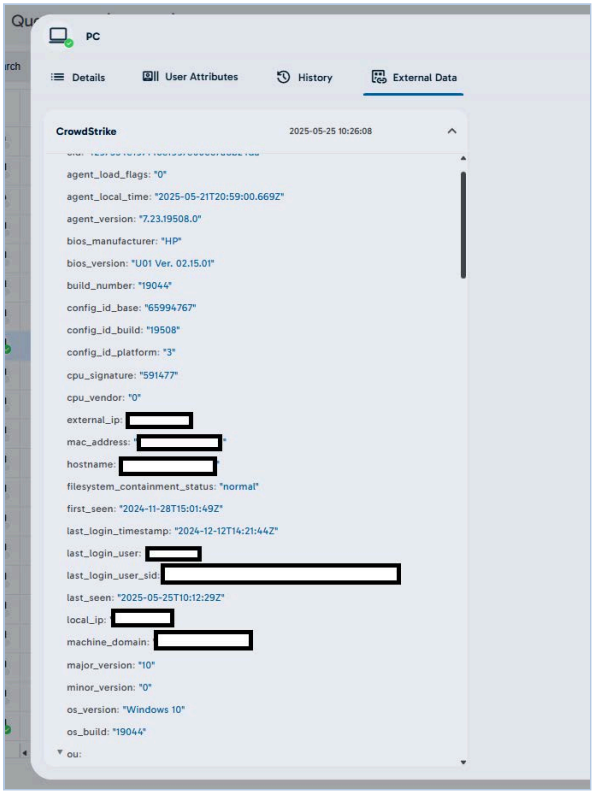
This integration enhances Sepio's capabilities by enriching existing asset data with information from CrowdStrike Falcon, strengthening overall security posture.

## Overview

This integration connects Sepio with CrowdStrike Falcon, enriching asset data by leveraging Falcon's endpoint detection and response (EDR) capabilities. It provides deeper insight into the status of network-connected assets by retrieving information for both online and offline Sepio assets. The integration identifies assets using their MAC address, as found in Falcon's management interface, and presents the enriched data within Sepio's External Data tab.

### CrowdStrike Data Panel

The External Data tab displays detailed insights from CrowdStrike Falcon, including endpoint status, hostname, operating system, agent version, and last seen timestamp. By correlating MAC addresses between Sepio and Falcon, this integration delivers a unified view that combines hardware-level visibility with endpoint-level intelligence, supporting more effective asset monitoring, risk assessment, and threat response.



Sepio External Data tab

**Note:** The initial configuration should be performed by Sepio Customer Support team.

## Requirements

To configure the CrowdStrike integration, the following details are required:

1. **Endpoint:** The CrowdStrike API endpoint URL.
2. **Client ID:** The CrowdStrike API client ID.
3. **Client Secret:** The CrowdStrike API client secret.

> **Note:** To generate the Client ID and Client Secret, ensure the following permissions are granted within CrowdStrike: **HOSTS**, **HOST GROUPS**.

Sepio uses the following CrowdStrike APIs:

- devices/queries/devices-scroll/v1
- devices/entities/devices/v2

## Additional Configuration Parameters

- **Time Interval Frequency:** How often API calls are made.
- **Call Limit:** The number of API calls that can be made.

## Other Sepio Settings

This integration utilizes the Sepio External Source Enrichment API. Ensure the following settings are configured:

- **Condition Active:** Set to **True**.
- **Source Name:** Set to **"CrowdStrike"**.
- **ENRICHMENT_API_ACTIVE:** Set to **"True"**.
- **CrowdStrike Integration Toggle:** Ensure this setting is **enabled**.

## Common Use Case

### Identifying PCs Without the CrowdStrike Agent Installed

A common operational use case is identifying PCs connected to the network that do not appear to have the CrowdStrike Falcon agent installed. This is typically done by searching for host assets that do not have CrowdStrike data populated in the Sepio External Data attribute.

To support this use accurately and avoid false alerts, Sepio recommends using the following filters:

- **Type** = Host
- **External Sources** = is empty
- **Connection Type** = Network
- **Is Online** = Yes
- **First Seen** = more than 7 days ago
- **First Seen** = in the last 14 days

**Why these time-based filters are important**

It may be tempting to use a simple filter such as "**First Seen in the last 24 hours**" to quickly identify new PCs without CrowdStrike. However, this approach can generate **false alarms** due to how CrowdStrike reports MAC addresses for endpoints with multiple network interfaces (NICs).

In environments where PCs have multiple NICs:

- Sepio may detect multiple MAC addresses and create multiple host assets.
- CrowdStrike may not report all MAC addresses for the same PC immediately.
- As a result, a newly detected Sepio host may temporarily appear without CrowdStrike enrichment, even though the CrowdStrike agent is installed and functioning.

The recommended filters address this behavior:

- **First Seen > 7 days** ensures the asset has existed long enough for CrowdStrike to report all associated MAC addresses.
- **First Seen in the last 14 days** keeps the focus on recently introduced PCs while avoiding long-standing exceptions.

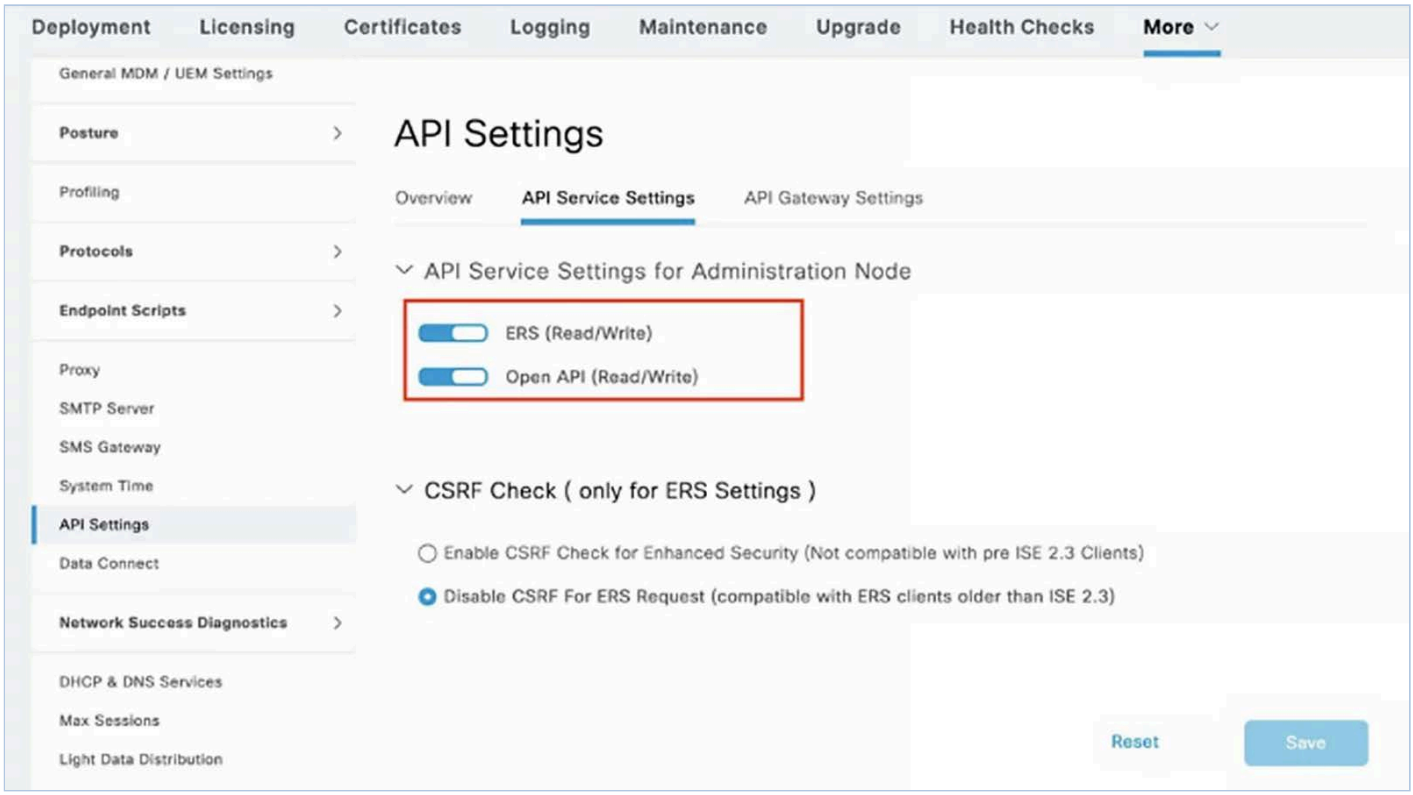
Together, these filters strike a balance between **early detection** and **data stability**, reducing false positives while still highlighting PCs that are genuinely missing CrowdStrike protection.

# Sepio and Cisco Identity Services Engine (ISE) NAC Integration

The Sepio integration with Cisco Identity Services Engine (ISE) enables data transfer from the Sepio Management Platform (SMP) to Cisco Identity Services Engine (ISE). The integration provides information on assets that either have a Risk Indicator or lack MAC address and cannot be identified or detected by Cisco ISE otherwise.

## Requirements

- Create a **dedicated user** in the Sepio Management Platform with **User** permissions (or higher).
- Create a **dedicated user** in Cisco ISE with **ERS Admin** permissions (or higher).
- In Cisco ISE, enable **ERS (Read / Write)** and **Open API (Read / Write)**, in the API Settings section.



API Settings

- **Cisco ISE endpoint name attribute must be set to the device MAC address.**

> **Note:** This integration is verified and validated for Cisco ISE version 3.3

## Installation Process

- Download the **integration package (ZIP file)** provided by **Sepio Customer Support.**
- Copy the ZIP file to the **target server** where the integration will be deployed.
- Unzip the package.

- Update the **integration configuration file** (.yml) with the required settings for your environment (Sepio connection, Cisco ISE connection, logging level, and integration behavior parameters).
- Build the Docker image using `docker build`.
- Start the integration container using `docker start`.

> **Note:** It is recommended to configure the YAML configuration file **before** building and starting the Docker container. Depending on the deployment method, configuration changes may require **rebuilding the Docker image** or **restarting the container** for the updates to take effect.

### Configuration Parameters

The integration is configured using a **YAML configuration file**. Configuration changes are automatically applied on each execution cycle. There is no need to restart the service.

#### Sepio_Connection

```
Hostname: <Sepio URL>
Username: <Sepio username>
Password: <Sepio password>
Ssl_verify: true | false
```

#### CiscoISE_Connection

```
Hostname: <Cisco ISE URL>
Username: <Cisco ISE username>
Password: <Cisco ISE password>
Ssl_verify: true | false
```

#### Sepio_Sub_Indicator_Configuration

This section controls which Sepio assets are pushed to Cisco ISE, based on their **assigned Risk Indicators**.
Supported Risk Indicators include:

- Potential Unmanaged Switch
- Active Network Threat
- Inactive Network Threat
- Communication Anomaly
- Asset DNA Anomaly
- Bad Reputation
- Common Vulnerabilities and Exposures (CVE)
- Extended Idleness
- Low Speed On High Speed Port

- Rare Device
- Risky Child Connected
- Unexpected Speed
- Unsupervised Host
- Unsupervised Network Infrastructure
- Dormant Device

Each Sepio sub-risk indicator can be configured independently using the following parameters:

- **enabled**
  Controls whether the sub-indicator is allowed to update assets in Cisco ISE
- **create**
  Controls whether the integration is allowed to create a new endpoint in Cisco ISE if the asset does not already exist.
- **online_only**
  Controls whether the asset must be online in Sepio to be pushed to Cisco ISE.

**Host_Discovery**

- **Discovery_Frequency_(minutes):** `15`
  This parameter controls the time interval between connections
- **Records_per_Page:** `500`
  This parameter controls the number of assets that are retrieved per API call from Sepio
- **Delay_Between_Pages_(milliseconds):** `100`
  This parameter controls the delay between API requests from Sepio

**Logging**

- Level: `DEBUG | INFO | WARNING | ERROR`

**Condition**

- **Condition_active:** `true | false`
  This parameter allows administrators to **temporarily disable the integration** without stopping the running process.

## General Precedence Rules

When multiple **Sepio sub-risk indicators** apply to the same asset, the following precedence rules are used:

1. **online_only precedence**
   - If **any** sub-indicator is configured with `online_only: true`, the asset **must be online** to be pushed.

    - If the asset is offline, it will be skipped.
2. **create precedence**
    - If **any** sub-indicator is configured with `create: true`, the asset will be created or updated in Cisco ISE.

**Examples**

**Example 1**
Configuration:

- Potential Unmanaged Switch -> `enabled: true` `online_only: true`
- Active Network Threat -> `enabled: true` `online_only: false`

Asset state:

- Sub-indicators:
- `is_online: false`

Result:

- Asset is **not pushed to Cisco ISE**, because at least one sub-indicator requires the asset to be online.

**Example 2**
Configuration:

- Potential Unmanaged Switch -> `enabled: true, create: true`
- Active Network Threat -> `enabled: true, create: false`

Result:

- Asset is **created or updated** in Cisco ISE.

## Dormant Device Precedence Rules

Dormant Devices are handled **separately** and do not follow the standard precedence rules.
Dormant Devices are pushed **regardless of online status**, even if other sub-indicators are configured with `online_only: true`.

**Examples**

**Example 1**

- Sub-indicators:
- `is_online: false`

Result:

- Asset is **pushed to Cisco ISE.**

Dormant Device creation is controlled **only** by the Dormant Device configuration.

**Example 2**

- Potential Unmanaged Switch -> `create: true`
- Dormant Device -> `create: false`

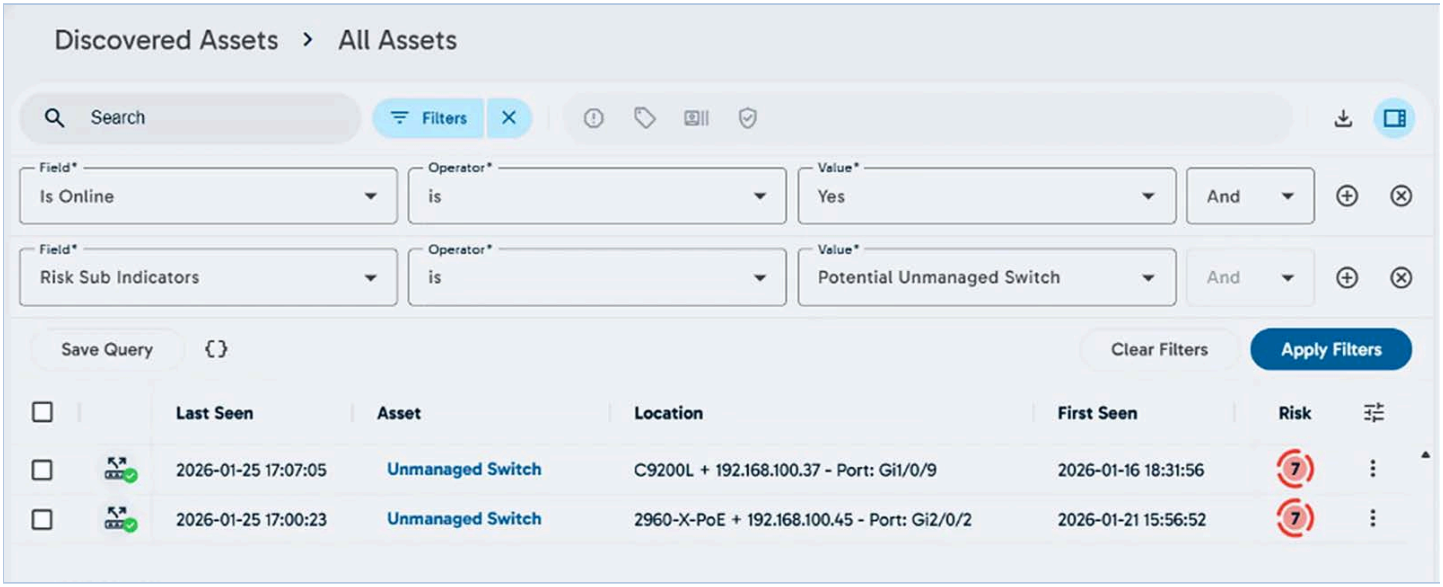
Result:

- Asset is **not created** in Cisco ISE, even though another sub-indicator allows creation.

## Integration Workflow (Example)

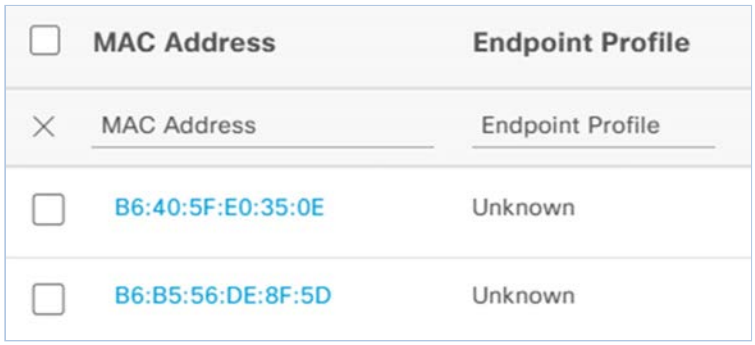
In this example, the integration is configured to create or update all online assets that have the sub-risk indicator Potential Unmanaged Switch in Cisco ISE using the following configuration:
`Potential Unmanaged Switch { enabled:true, create:true, online_only:true }`

First, the assets are displayed in the Sepio Management Platform, showing all connected assets with sub risk indicator of Potential Unmanaged Switch:




Sepio Management Platform – All Assets

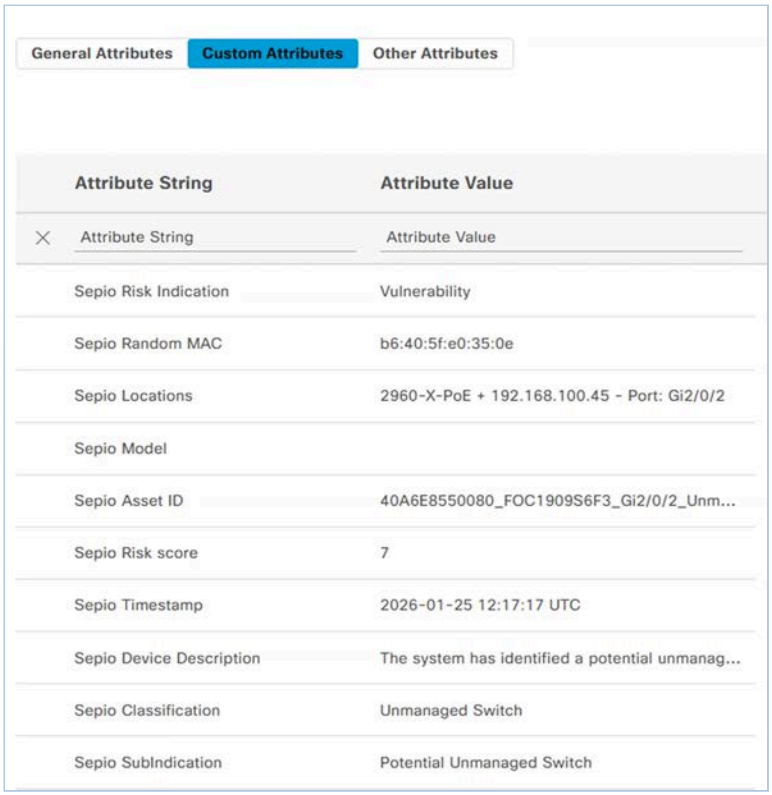
Next, after the integration completes its execution cycle, the same assets appear in Cisco ISE as endpoints. Since unmanaged switches do not have a MAC address, Sepio creates these endpoints in Cisco ISE using a synthetic (random) MAC address.



| MAC Address | Endpoint Profile |
|---|---|
| B6:40:5F:E0:35:0E | Unknown |
| B6:B5:56:DE:8F:5D | Unknown |

Unmanaged Switches in Cisco ISE

Finally, the Cisco ISE endpoint view shows the additional **Sepio custom attributes** that were added to each asset, providing enriched context and enabling enforcement based on Sepio's Layer 1 detection.



General Attributes | Custom Attributes | Other Attributes

| Attribute String | Attribute Value |
|---|---|
| Sepio Risk Indication | Vulnerability |
| Sepio Random MAC | b6:40:5f:e0:35:0e |
| Sepio Locations | 2960-X-PoE + 192.168.100.45 - Port: Gi2/0/2 |
| Sepio Model | |
| Sepio Asset ID | 40A6E8550080_FOC1909S6F3_Gi2/0/2_Unm... |
| Sepio Risk score | 7 |
| Sepio Timestamp | 2026-01-25 12:17:17 UTC |
| Sepio Device Description | The system has identified a potential unmanag... |
| Sepio Classification | Unmanaged Switch |
| Sepio SubIndication | Potential Unmanaged Switch |

Sepio Custom Attributes in Cisco ISE

## Logging and Troubleshooting

It is recommended to run the integration with the logging level set to INFO.
The INFO logging level provides sufficient information to troubleshoot most issues and understand the integration flow.

### INFO Logging Overview

When running with INFO level logging, each iteration will provide the following logs:

`INFO - Active indicators are: []` # Validates the active integration configuration
`INFO - Response status: 200, Page: 1, Page Size: 500` # Confirms a successful response from the

Sepio API (HTTP 200)

```
INFO - Response status: 200, Page: 2, Page Size: 500
INFO - No assets found on page 2. Ending pagination.
INFO - Total assets processed: 2
INFO - Sync complete: Created 0, Updated 2
```

# Summarizes the number of assets created or updated in Cisco ISE

Using the **INFO** logging level makes it easy to determine whether an issue originates from:

- Retrieving assets from the **Sepio API**
- Pushing assets to **Cisco ISE**

If the available information is not sufficient to diagnose the issue, the logging level can be changed to **DEBUG** in the integration configuration file to obtain more detailed execution traces.

## Common Use Cases

### Correlation of MAC-less Devices Between Sepio and Cisco ISE

Some assets discovered by Sepio (such as unmanaged switches) do not have a MAC address and therefore lack a standard unique identifier. Since the MAC address is typically used as the primary correlation key in Cisco ISE, this creates a challenge when mapping MAC-less assets between systems.

To address this limitation, Sepio recommends the following correlation methods:

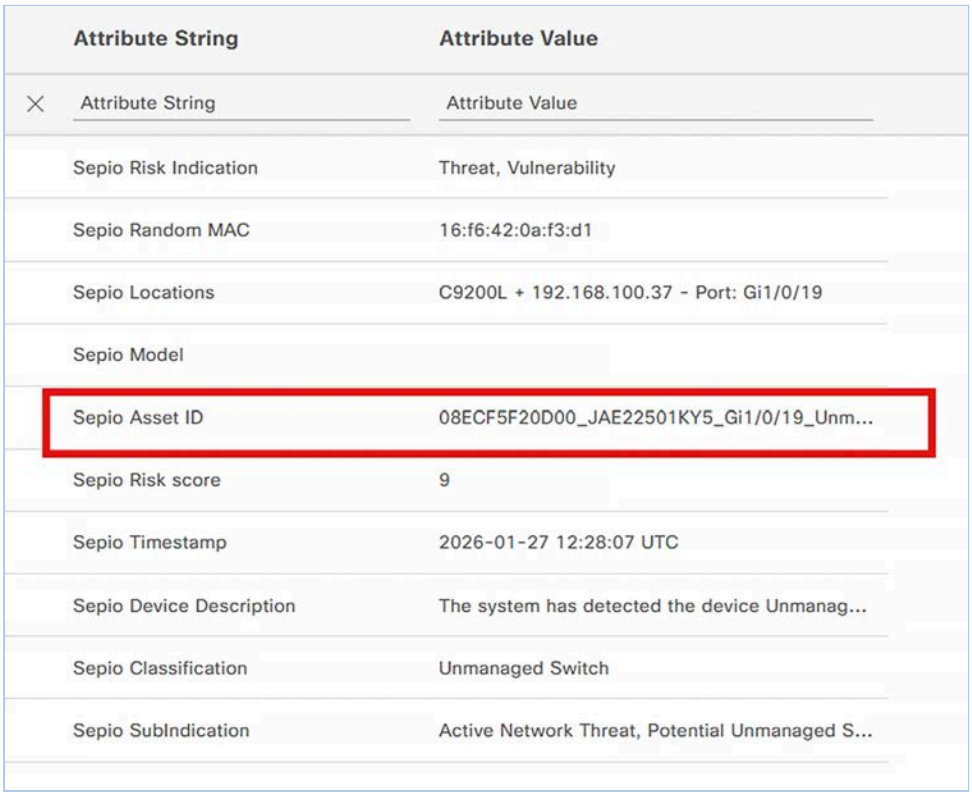
### Sepio Events ↔ Cisco ISE Endpoints

Correlation between Sepio events and Cisco ISE endpoints is achieved by matching the **Sepio Asset ID** value:

- The **Sepio Asset ID** included in the Sepio event
- The **Sepio Asset ID** stored as a custom attribute on the corresponding Cisco ISE endpoint

This method enables reliable correlation at the event level, even when a MAC address is not available.

Cisco ISE Sepio Asset ID attribute:



| Attribute String | Attribute Value |
|---|---|
| Sepio Risk Indication | Threat, Vulnerability |
| Sepio Random MAC | 16:f6:42:0a:f3:d1 |
| Sepio Locations | C9200L + 192.168.100.37 - Port: Gi1/0/19 |
| Sepio Model | |
| Sepio Asset ID | 08ECF5F20D00_JAE22501KY5_Gi1/0/19_Unm... |
| Sepio Risk score | 9 |
| Sepio Timestamp | 2026-01-27 12:28:07 UTC |
| Sepio Device Description | The system has detected the device Unmanag... |
| Sepio Classification | Unmanaged Switch |
| Sepio SubIndication | Active Network Threat, Potential Unmanaged S... |

Cisco ISE Sepio Asset ID

**Sepio Platform ↔ Cisco ISE Endpoints**

Correlation between assets in the Sepio platform and endpoints in Cisco ISE can be achieved using location-based matching:

- The **Sepio Location** custom attribute on the Cisco ISE endpoint
- The **Location** field in the Sepio UI

By comparing these two values, customers can logically associate MAC-less assets across both platforms when direct hardware identifiers are unavailable.

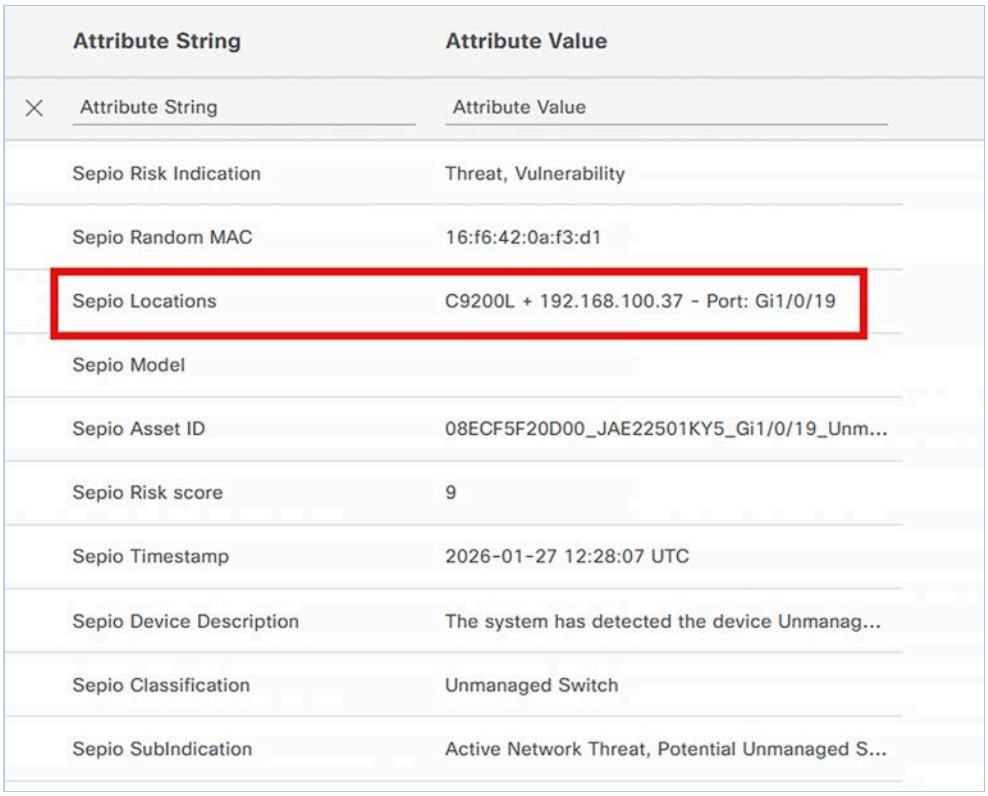
For example:
Sepio Location:



| Asset | Location ↓ | Last Seen | MAC Address |
|---|---|---|---|
| Unmanaged Switch | C9200L + 192.168.100.37 - Port: Gi1/0/19 | 2026-01-27 12:23:45 | |

Sepio Location

Cisco ISE location:



| Attribute String | Attribute Value |
|---|---|
| Attribute String | Attribute Value |
| Sepio Risk Indication | Threat, Vulnerability |
| Sepio Random MAC | 16:f6:42:0a:f3:d1 |
| Sepio Locations | C9200L + 192.168.100.37 - Port: Gi1/0/19 |
| Sepio Model | |
| Sepio Asset ID | 08ECF5F20D00_JAE22501KY5_Gi1/0/19_Unm... |
| Sepio Risk score | 9 |
| Sepio Timestamp | 2026-01-27 12:28:07 UTC |
| Sepio Device Description | The system has detected the device Unmanag... |
| Sepio Classification | Unmanaged Switch |
| Sepio SubIndication | Active Network Threat, Potential Unmanaged S... |

Cisco ISE location

## Known Limitations

**One-way synchronization**

The integration **pushes data only from Sepio to Cisco ISE.** Cisco ISE does not remove or update previously provided attributes if an asset no longer meets the configured criteria.

**Example:**

- Day 1: An asset is marked as Active Network Threat -> pushed to Cisco ISE
- Day 2: The asset is no longer considered an Active Network Threat -> Cisco ISE will keep the endpoint unchanged

**Recommended Mitigation:**

Configure a periodic cleanup task in Cisco ISE (for example, every 24 hours) to remove or reset Sepio custom attributes as needed.

**Endpoint Name Attribute in Cisco ISE**

The integration relies on the Cisco ISE endpoint name attribute, retrieved via the GET /ers/config/endpoint API, to correlate Cisco ISE endpoints with Sepio assets. The integration assumes that the endpoint name value represents the device MAC address. If, in a given Cisco ISE environment, the endpoint name attribute is not set to the MAC address, the integration will be unable to correlate that endpoint with Sepio data. **As a result, Sepio data will not be pushed to or updated on that Cisco ISE endpoint.**

# Configuring Forescout (legacy)

## Sepio Integration Methods with Forescout

Sepio provides two methods of integration with Forescout.

- Legacy Integration with Forescout CounterACT, attuned for legacy Forescout customers which uses the Forescout CounterACT Web API as well as the Data Exchange (DEX) Web Service.
- New Integration which uses the Sepio Connector App for Forescout.

> **Note:** See the new integration using Sepio Connector App for Forescout.

## Forescout Legacy integration

1. Open the Integration View
2. Enable the Integration
3. Go to HAC-1_ForescoutIntegration_221125

## Sepio Connector Application for Forescout

- For configuration details, please refer to the Sepio Connector App setup for Forescout.

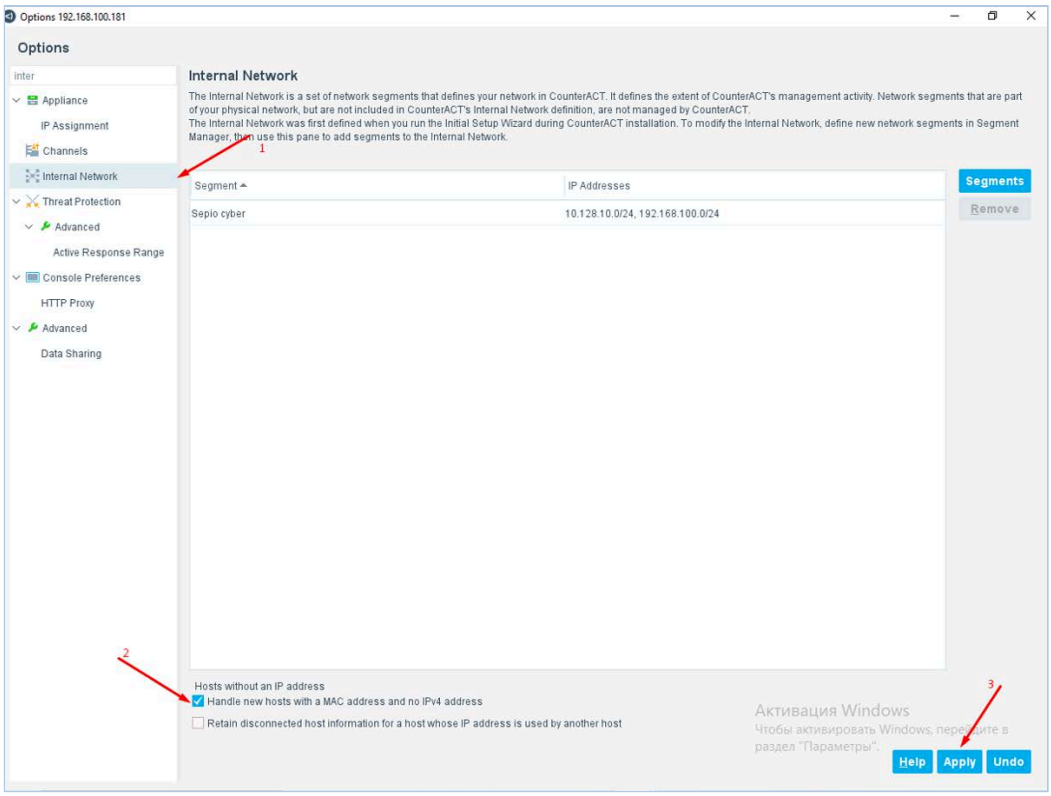
# Sepio Connector App for Forescout

The Forescout Connector App enables data transfer from the Sepio Management Platform (SMP) to the Forescout platform. It is installed on the Forescout machine and queries Sepio's API at a configurable, scheduled interval. The app provides information on assets that either have a Risk Indicator or lack a MAC address. Since the Forescout solution does not support MAC-less operations, the app assigns a random MAC address to any asset discovered by Sepio that lacks one.

> **Note:** Download the latest version of the Sepio Connector for Forescout from GitHub.

## Configuration Steps on Forescout Console

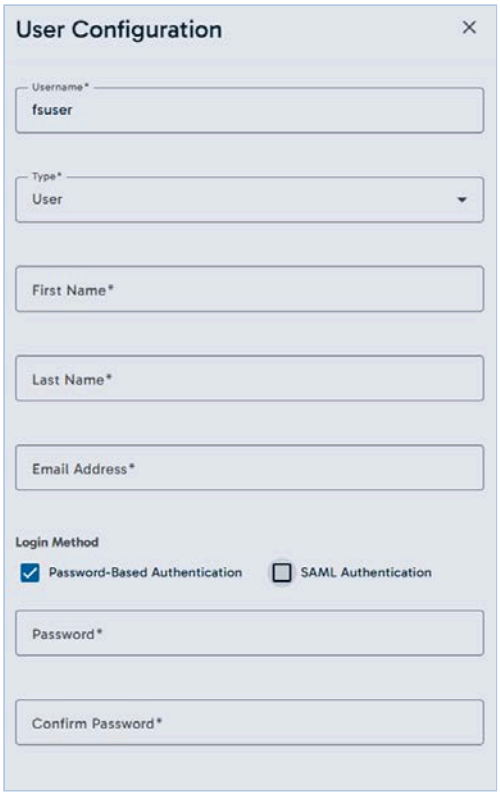
- Ensure the Connect Plugin is installed by following the Forescout installation instructions available **here**.
- In the Certificates section, navigate to Trusted Certificates and import the Authority Certificate (CA).
- In Internal Network, enable creation of a new host without an IP.




Internal Network

## Configuration Steps on Sepio Management Platform (SMP)

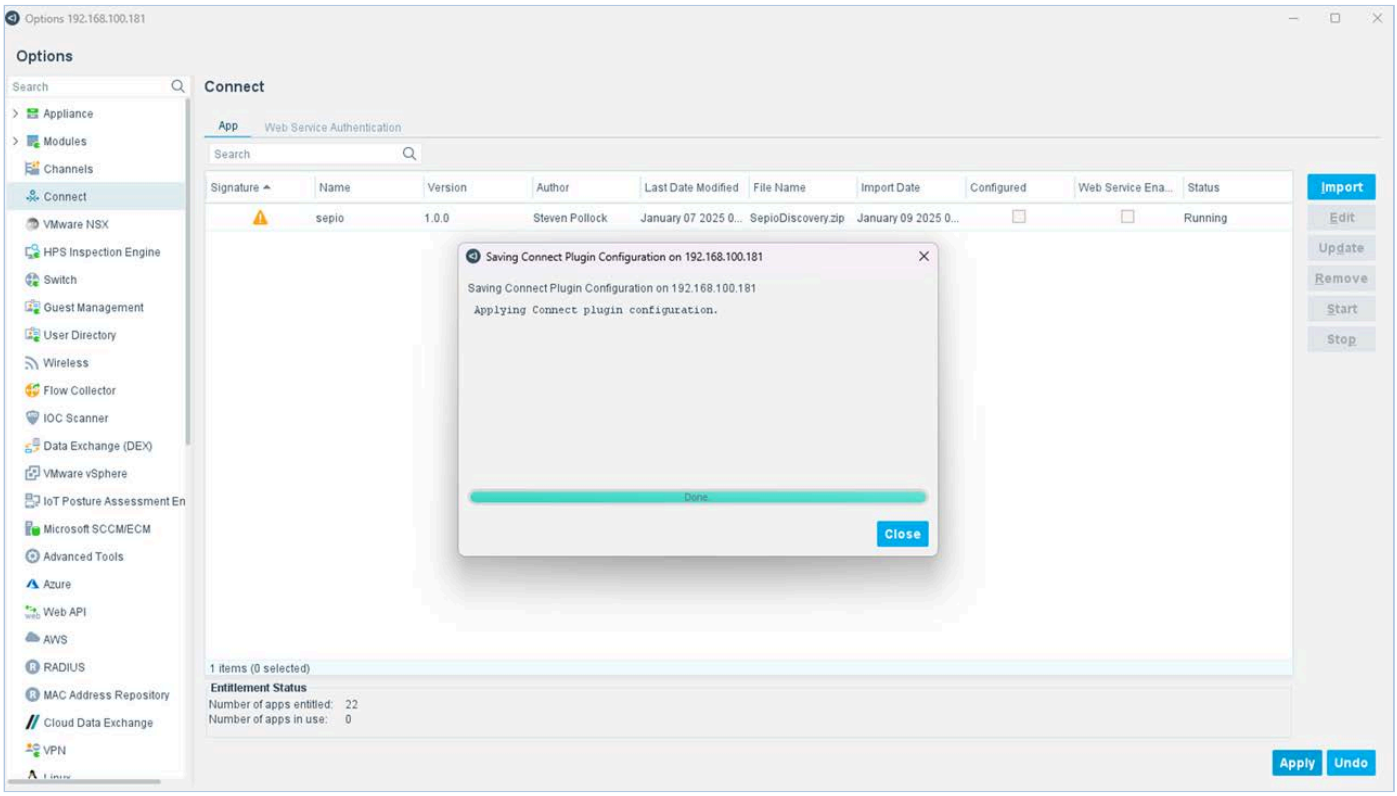
Create a dedicated user with “User” role and local password, for the connector app integration by navigating to **Settings** -> **Users.**




User Configuration

## Installation Method

1. Ensure you have the **Sepio Connector App zip** file saved on your PC, then log in to the Forescout Console.
2. Open **Options** (top-right corner) and navigate to the **Connect** option.
3. Click **Import** and select the **Sepio Connector App zip file.**
4. Press **Close**, then **OK** in the pop-up window, and click **Apply.**

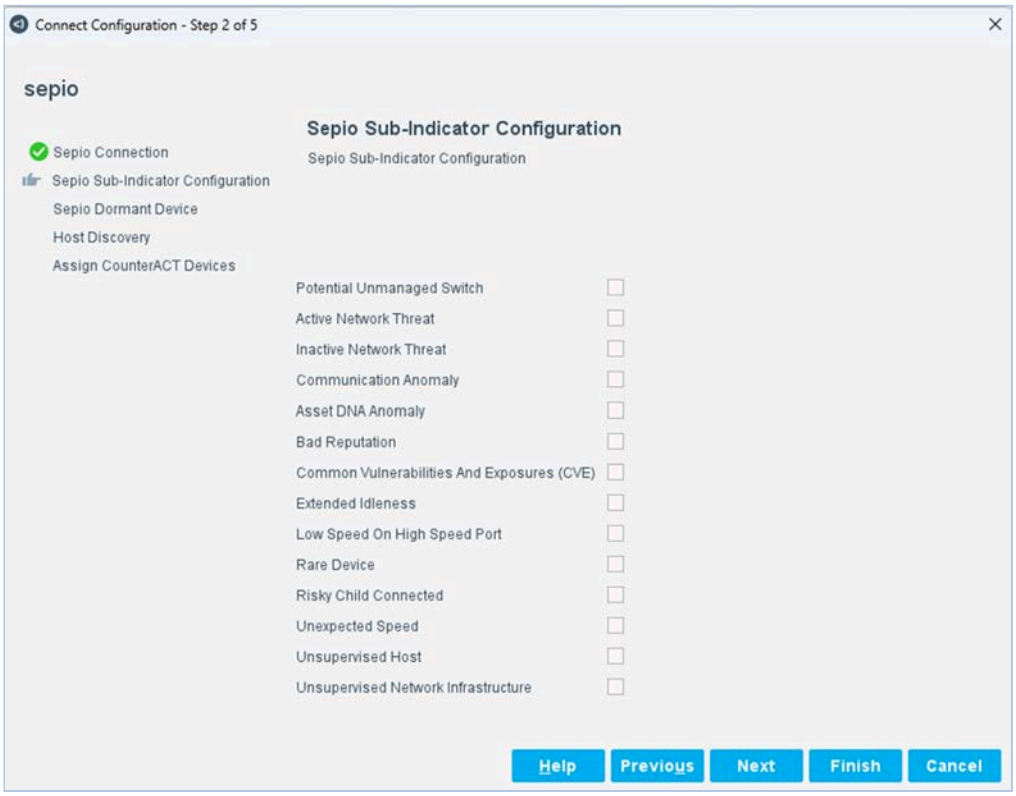


Connect options

5. **Double-click** on the **Sepio Connector App** to start configuration.

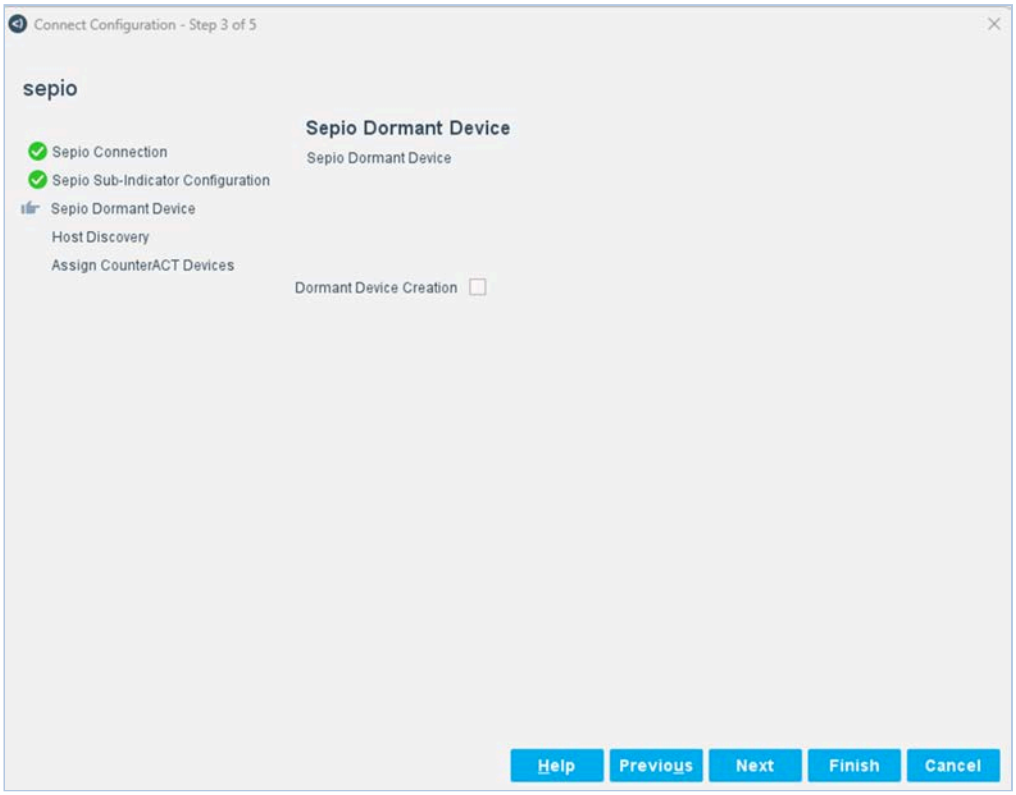
## Configure Sepio Connector App

1. Click **Add** to configure Sepio connection.
2. Enter the **Sepio SMP URL** (without “https”) and the credentials of the user created in the preparation steps.
3. Check the “**Validate server certificate**” box. Click **Next.**
4. Choose the desired **Sepio Sub-Indicator configuration** and click **Next.**
    - Sub-Indicator configuration means that any asset in Sepio containing one of the selected sub-indicators, will be pushed and updated in Forescout.



Connect Configuration – Step 2 of 5

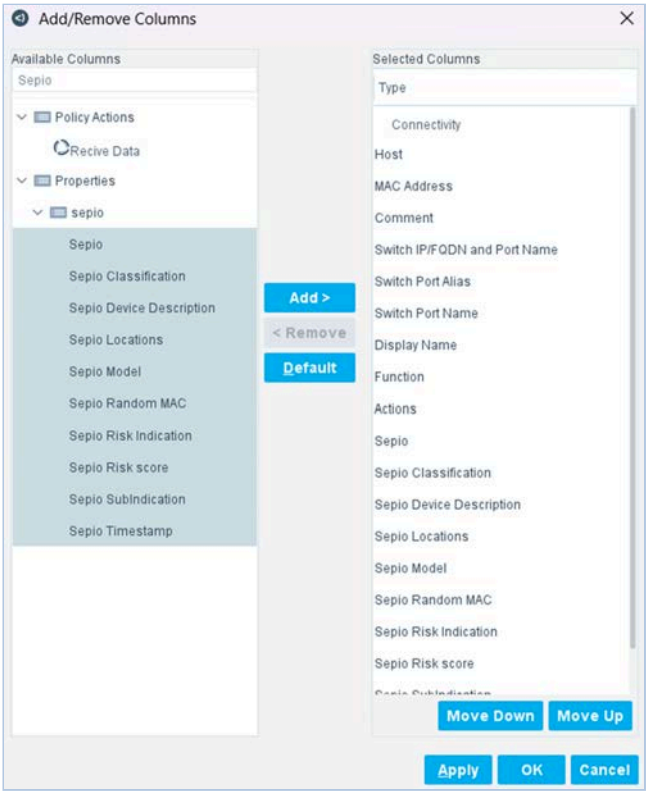
5. Choose whether to **enable Dormant Device Creation** and click **Next.**
    - When enabled, any dormant device in Sepio will be created in Forescout.



Connect Configuration – Step 3 of 5

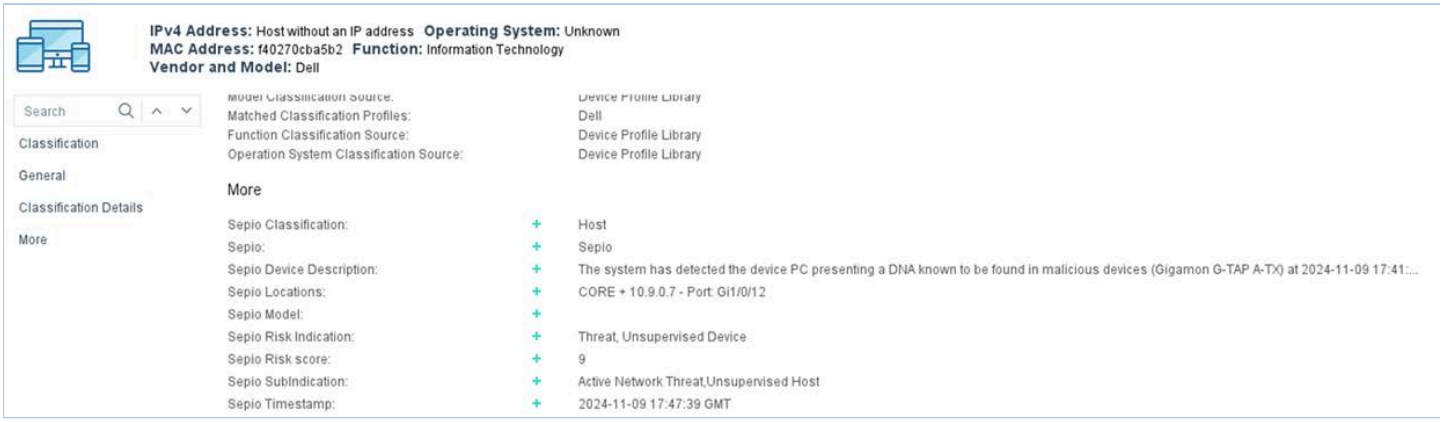
6. Check **Enable Host Discovery** and set the discovery rate, then click **Next.**
7. Press **Next**, then **Finish.**
8. Click **OK**, then **Apply.**

## Accessing Sepio Data in Forescout Hosts



Add/Remove Columns

Use the global search with the keyword “Sepio” to view hosts created or updated by Sepio.
By selecting a host, you can view any available information received from Sepio.



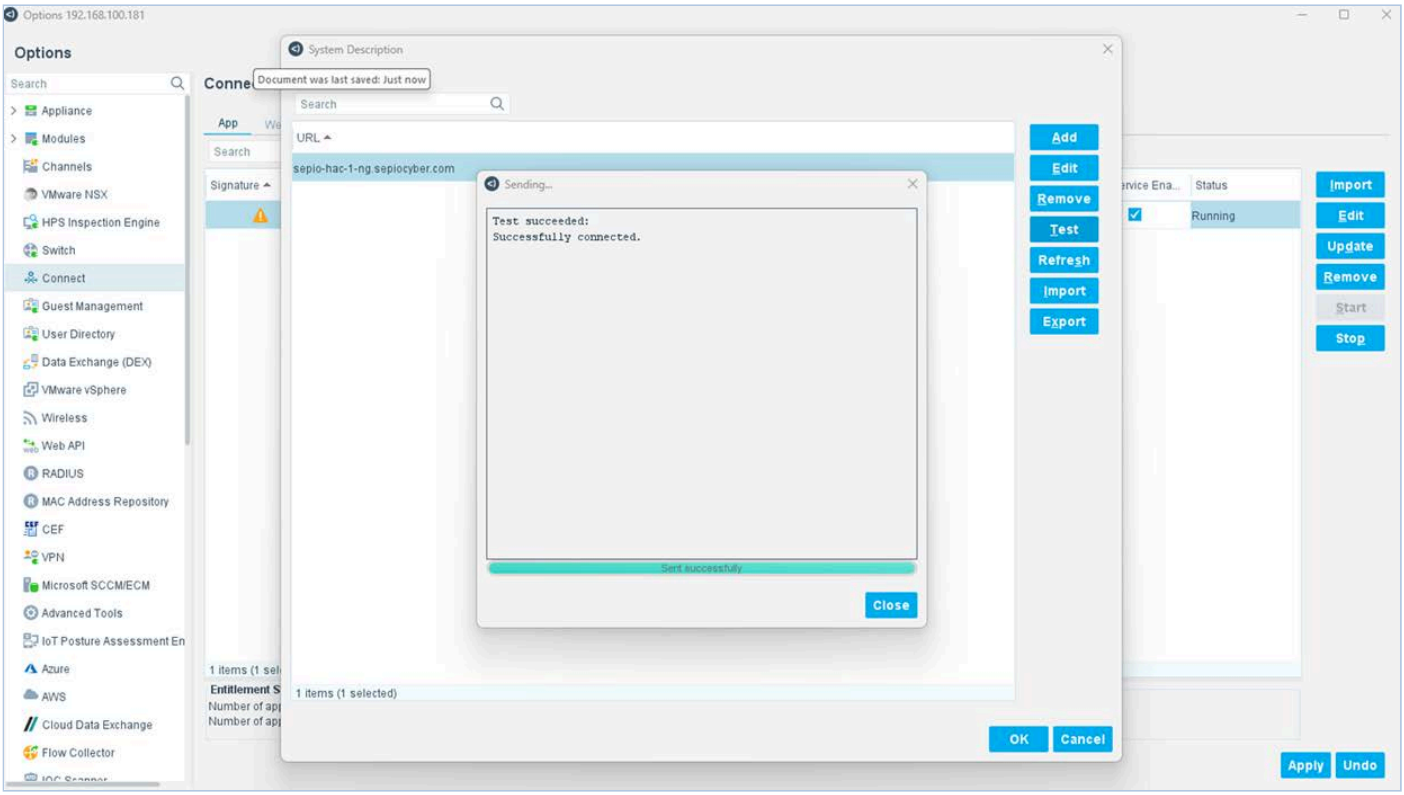
Available Host Information

## Verification

There are two ways to verify that the **Sepio Connector App** is running:

1. **Check the Sepio Timestamp Column**
    - Review the **Sepio Timestamp** column in Forescout to see the last update time.
    - This timestamp indicates when the Connector App last successfully transferred data from Sepio.

2. **Run a Connection Test**
    - From the **Connect** configuration in the **Options** menu, double-click on the Sepio Connector App.
    - Click on the **Sepio SPM URL** and press **Test.**
    - You should receive a "**Successfully connected**" message, confirming that the connection is active.



Connection Test – Successfully Connected

## Detailed Specification of the Connector App

The **Connector App** queries all assets in **Sepio SMP** based on the configurable time intervals and identifies those that meet **one of the following conditions:**

1. The asset has one of the following **Risk Sub Indicators:**
    - Active network threat
    - Asset DNA anomaly
    - Communication anomaly
    - Inactive network threat
2. The asset is **online but lacks a MAC address** (e.g., MAC-less devices).

All assets that meet these criteria are sent to Forescout, using the MAC address as the key. If an asset lacks a MAC address, the app generates a consistent, random MAC address based on Sepio's internal asset ID, using an internal hashing logic to ensure the same MAC address is always assigned to the same device.

- If an asset already exists in Forescout, the app will update Sepio-related fields.
- If the asset does not exist, the app will create a new entry.

### Limitations

If a risk is removed from an asset or it goes offline, the app does not automatically delete the asset from the Forescout Hosts list. Users can manually remove such assets based on the last updated timestamp from Sepio.

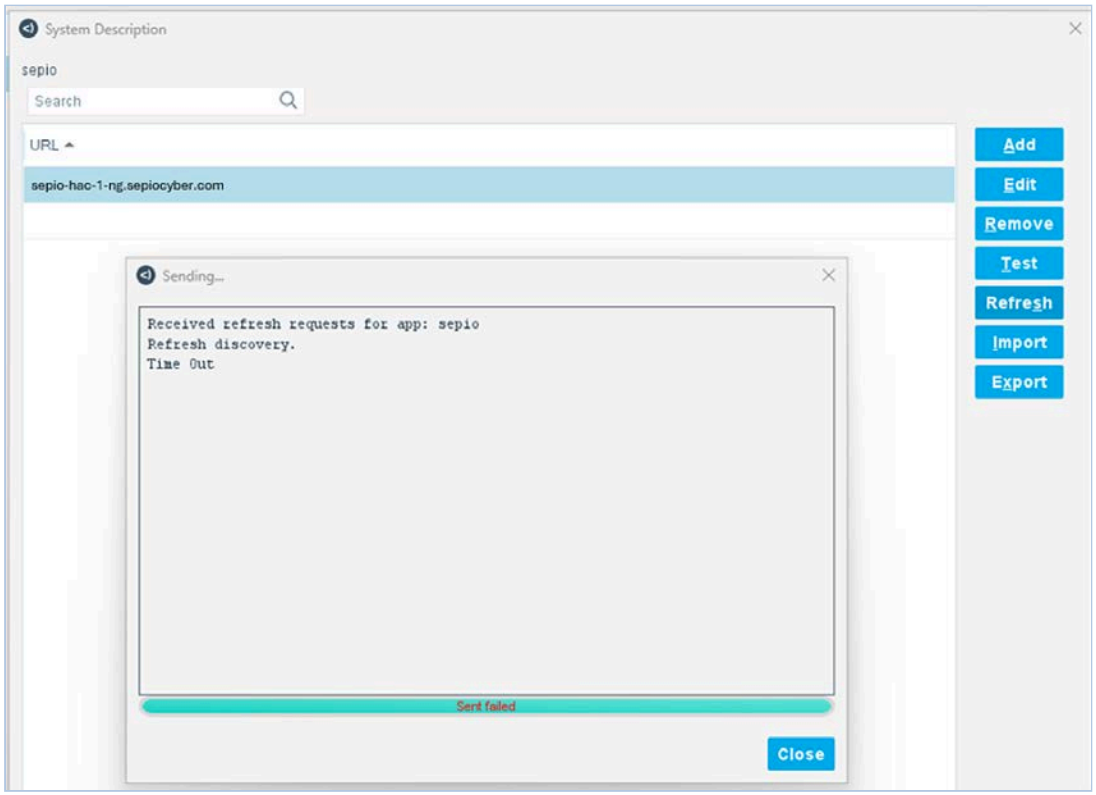
### Note – Random MAC Address

A MAC address is considered randomized if the **second character** of the address is either 2, 6, A, or E. This indicator helps distinguish randomized addresses from standard hardware-based MAC addresses.

In **Forescout**, you can identify such assets by adding the **Sepio Random MAC** column. If this column is populated for an asset, it indicates that the device is **MAC-less**, and the application has generated a random MAC address for it.

## Troubleshooting Forescout

### Issue: Refresh button results in a Timeout error




Refresh button results in a Timeout error

### Troubleshooting and Resolutions:

1. **Increase the Forescout Connect Timeout on the EM**

   Run the following commands to extend the timeout to 5 minutes (300 seconds):

   ```
   fstool connect_module set_property connect.python.socket.read.timeout.seconds 300
   fstool oneach -c 'fstool connect_module set_property
   connect.python.socket.read.timeout.seconds 300'
   ```

2. **Restart the connect module to apply changes**
3. **If the Issue Persists – Check the Following Logs and Contact Sepio Support**
   - Connect to the machine where Forescout is running.
   - Navigate to the Connect module directory and Increase debug level:

     ```
     cd /usr/local/forescout/plugin/connect_module
     fstool connect_module debug 10
     ```

   - Press the Forescout application refresh button and wait for the timeout.
   - Check Python logs:

     ```
     cd python_logs
     tail -f python_server.log
     ```

     (or run `ls -l` to find the most recent `python_server.log` file and copy it for investigation). Please make sure you send the **entire** log file.
   - It is also recommended to check the `connect_module.log` file located at:

     `/usr/local/forescout/log/plugin/connect_module/ connect_module.log`
4. **Important!**

   After completing the debugging session and collecting the logs, don't forget to return the debugging level back to its normal value:

   ```
   fstool connect_module debug 0
   ```

**Note:** If the issue persists, please send the entire log files to Customer support.

# Configuring Guardicore

## Configure Guardicore

1. Open the Integration View
2. Enable the Integration
3. Go to HAC-1_GuardicoreIntegration_210622.pdf.

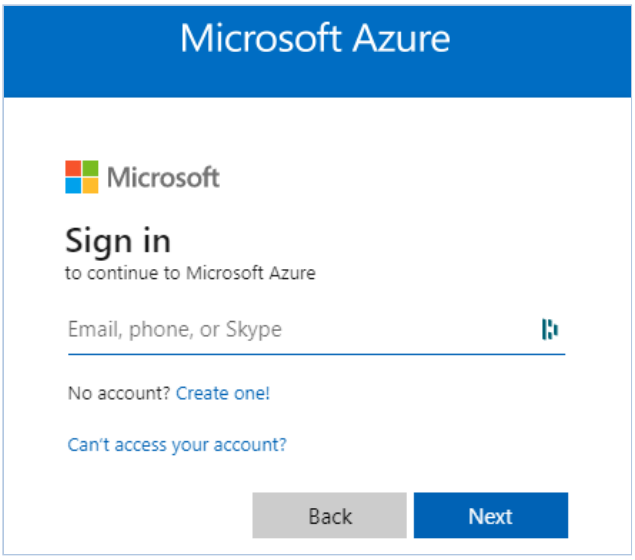
# Configuring SAML

This procedure assumes that Microsoft Active Directory (Azure) is your SAML Identity Provider (IdP) and that you have an Azure AD account set up. The Identity Provider (Azure) authenticates the end user's identity and verifies they are who they claim to be. It then sends this information, along with the user's access rights, to the service provider (Sepio).

> **Note:** SAML configuration is **case-sensitive.**

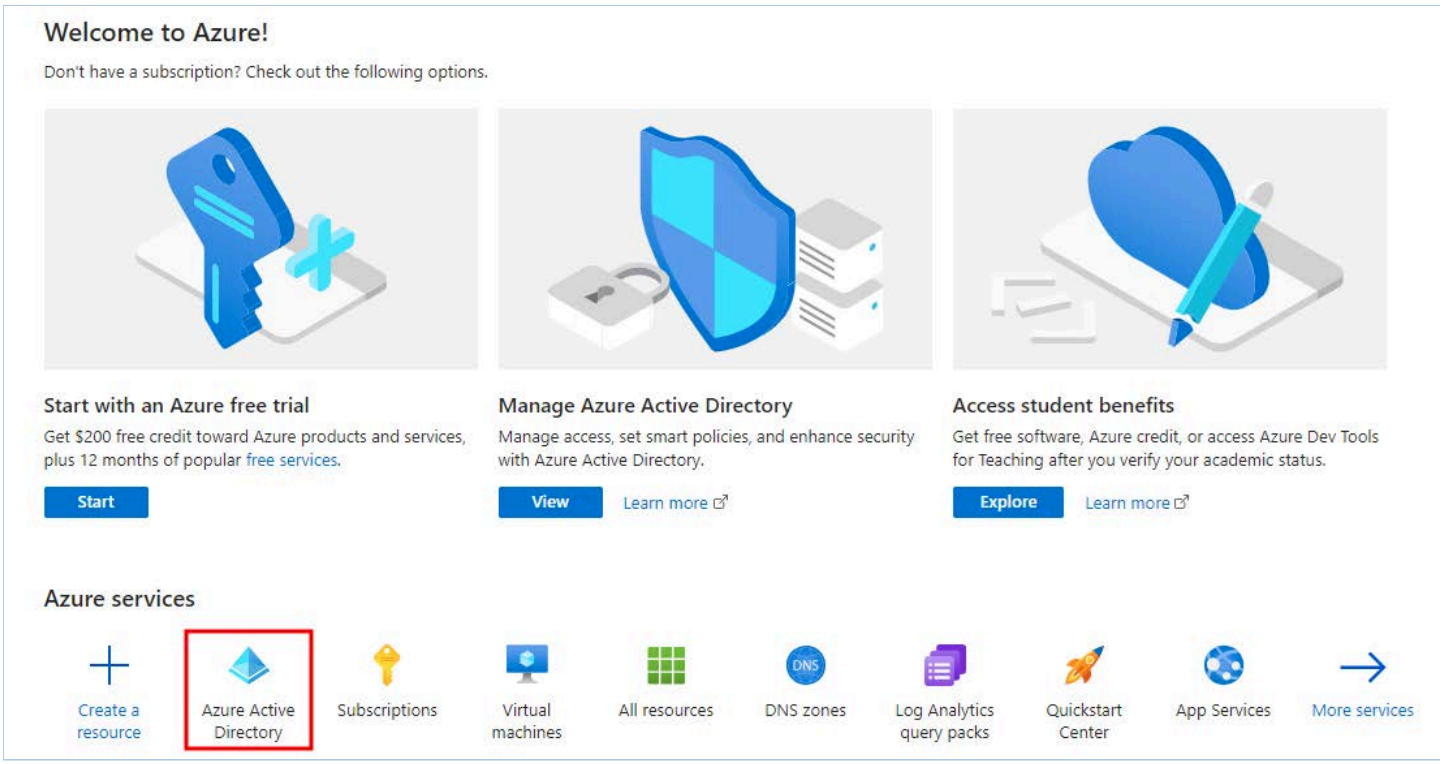
## To configure SAML

1. **Sign in to the Azure portal.**



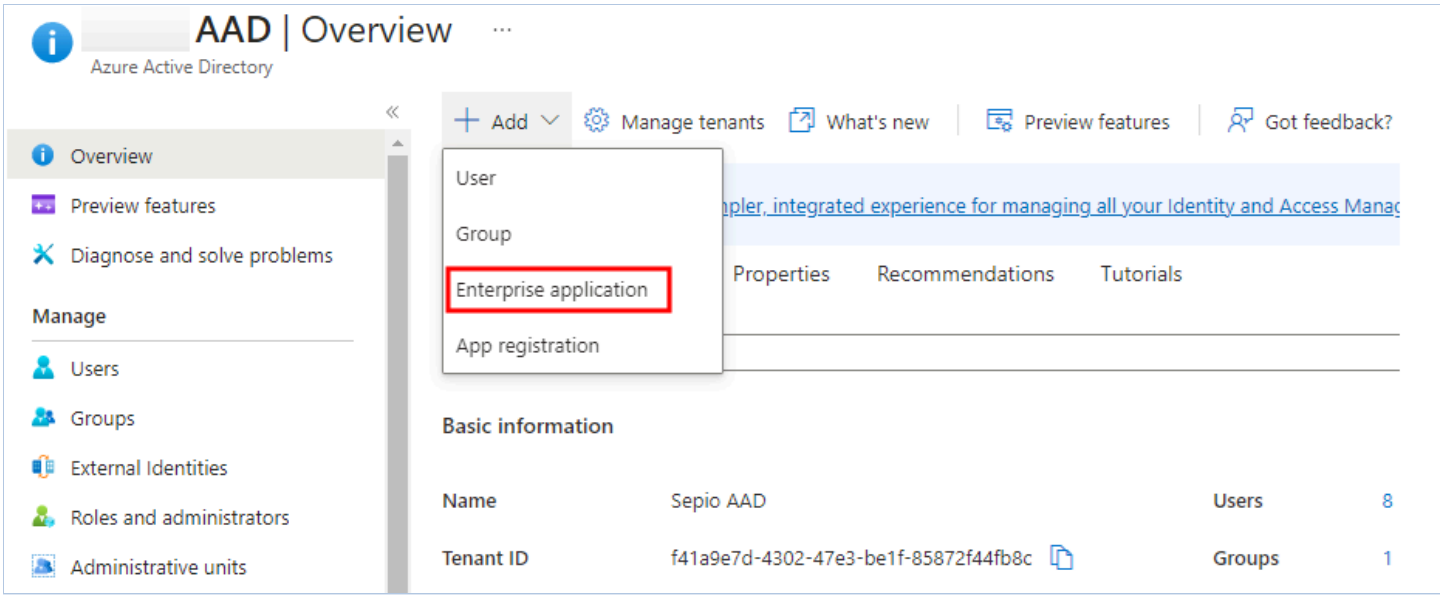

Microsoft Azure Sign in

2. **Navigate to Azure Active Directory.**
    - Select **Azure Active Directory** from the menu.

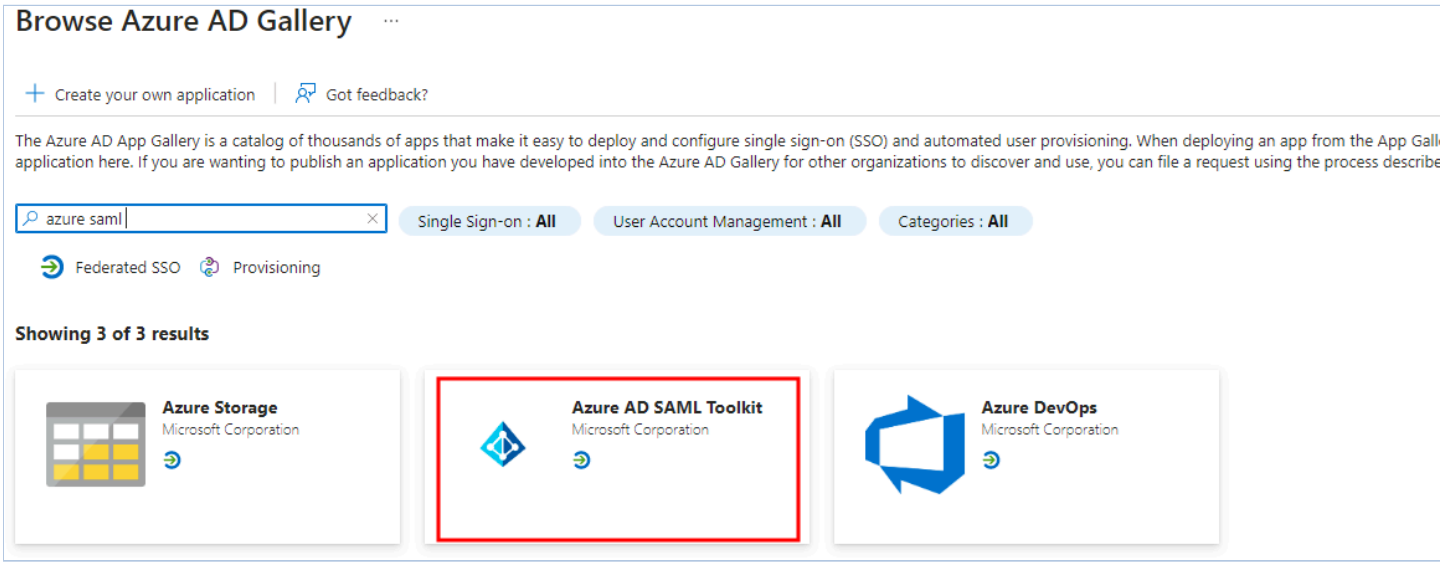



Azure Active Directory

3. **Add an Enterprise Application.**
    - On the **Add** menu, select **Enterprise application.**
    - Search for and select **Azure AD SAML Toolkit.**

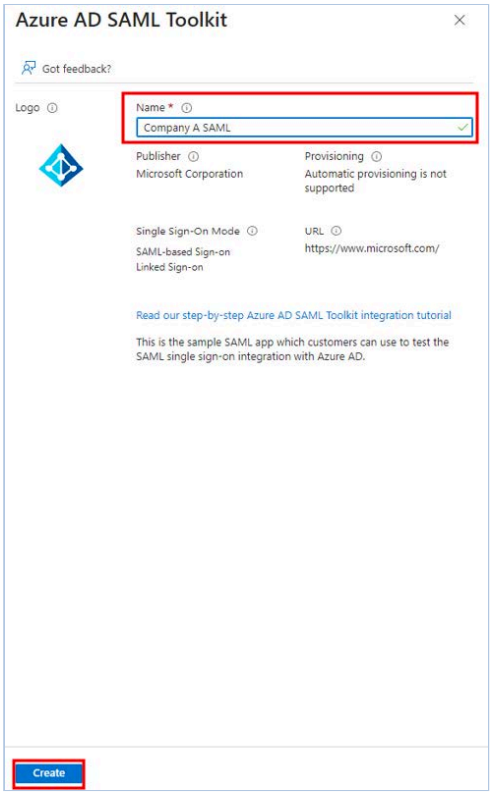



Select Enterprise application



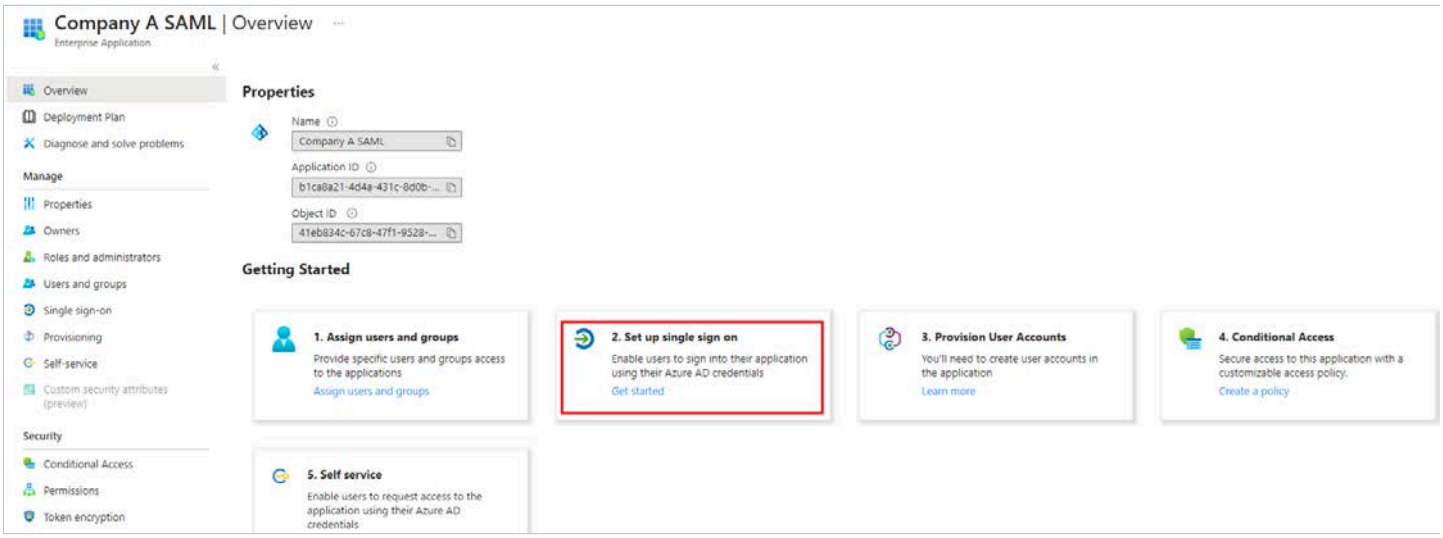

Select Azure AD SAML Toolkit

4. **Set Up the SAML Application.**
    - Enter the desired SAML application name (e.g., *Company A SAML*), then click **Create.**

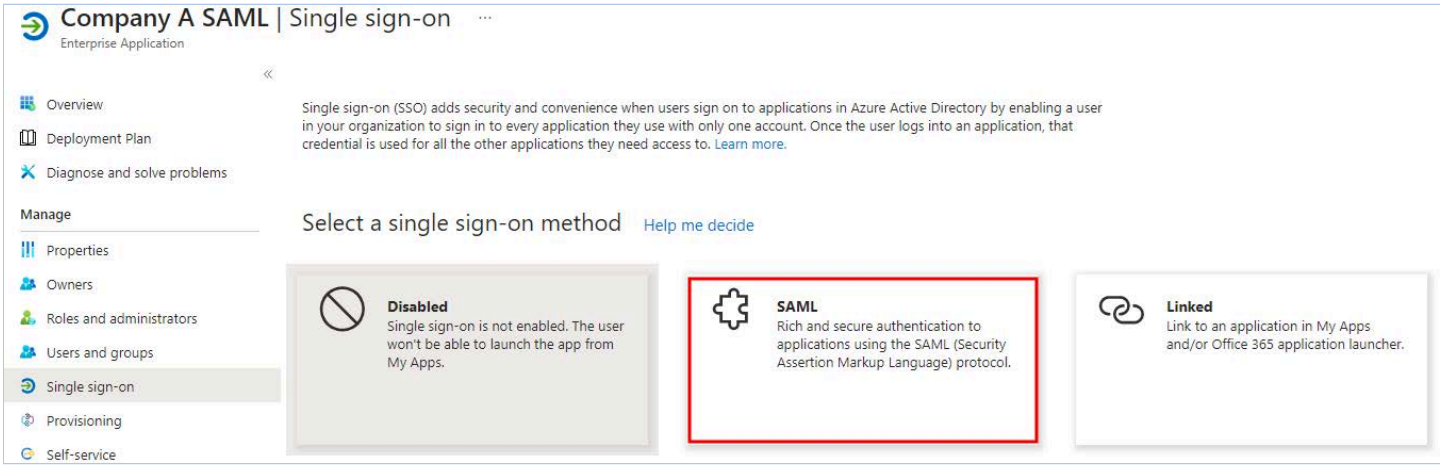



Enter the SAML application name

5. **Configure Single Sign-On.**
    - Select **Set up single sign-on** and choose **SAML.**

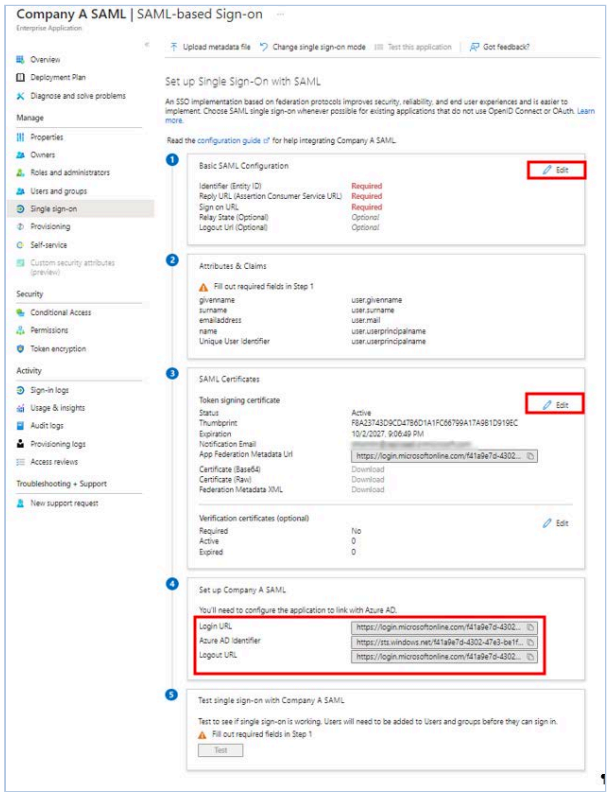



Set up single sign on

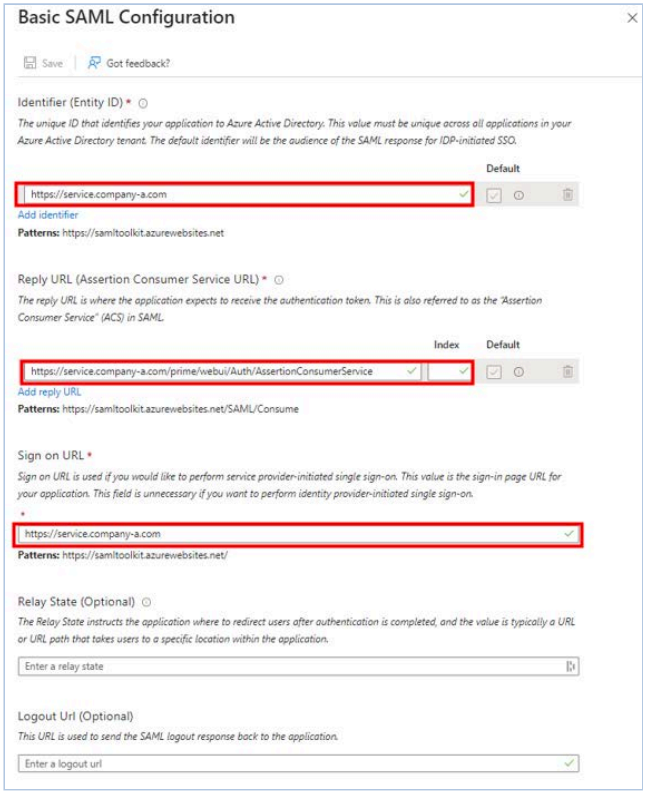



Select SAML

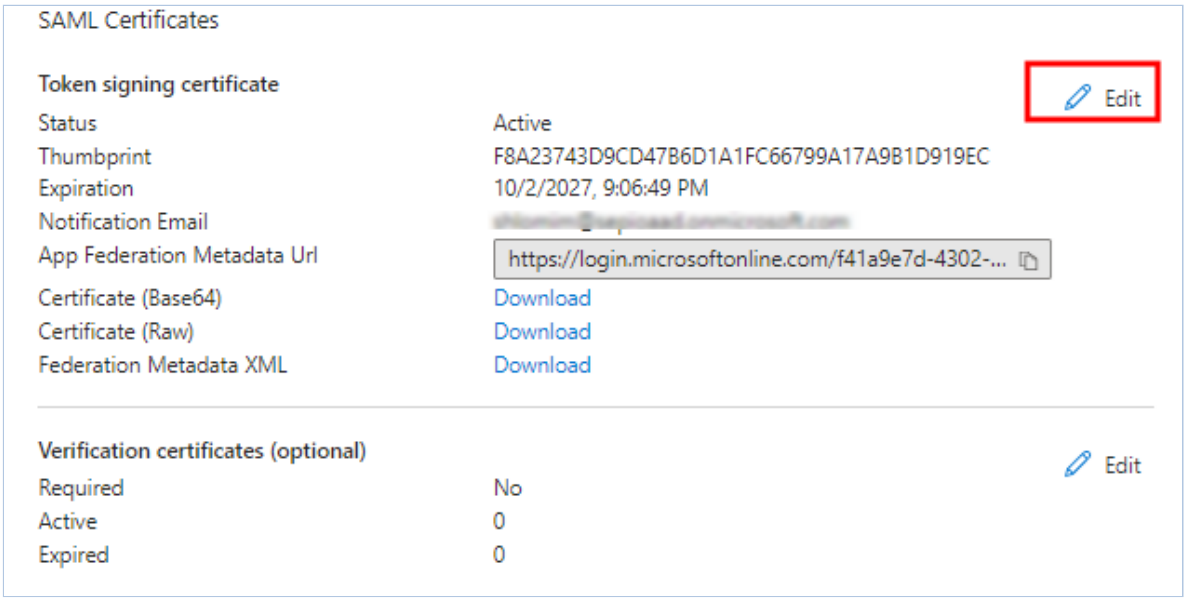
6. **Download the SAML Certificate.**
    - Complete the **Basic SAML Configuration** as guided.
    - Download the certificate, which will be saved to your computer.



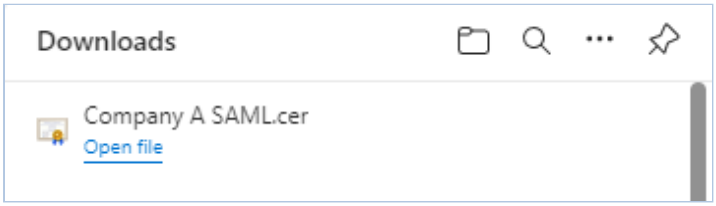

SAML-based Sign-on




Basic SAML Configuration




Download the certificate

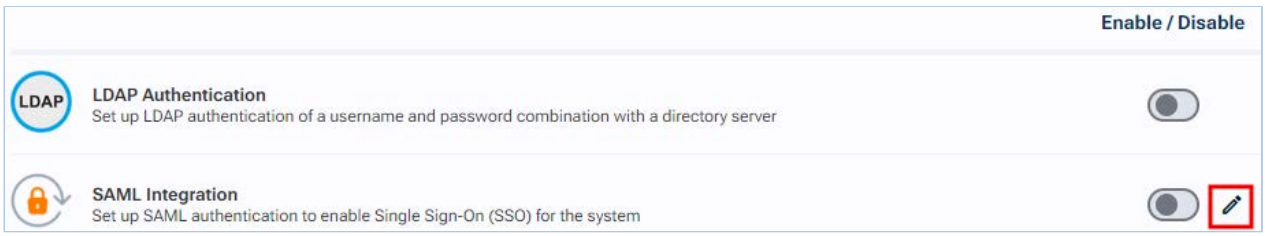



The certificate is downloaded to your computer.

**Note:** SAML configuration is **case-sensitive.**

## Configure SAML on Sepio

7. On Sepio main menu go to **Settings** -> **Integration** -> **SAML Integration.**
    - Click **Add.** The **SAML Configuration** view will appear.




SAML Integration

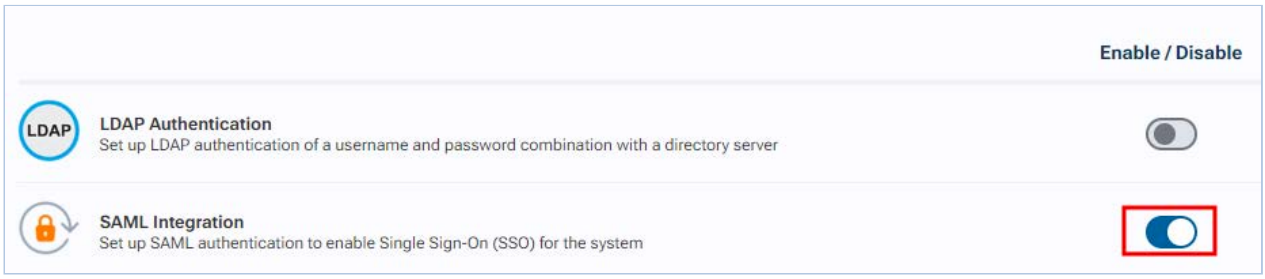


SAML Configuration view

8. **Enter SAML Parameters in Sepio.**
    - **SAML login URL:** Copy the login URL from Azure (step 4).
    - **SAML Service Provider Name:** Use Sepio's Management URL (e.g., *https://sepio.mydomain.com/*).
    - **SAML Certificate:** Copy and paste the details from the downloaded certificate.

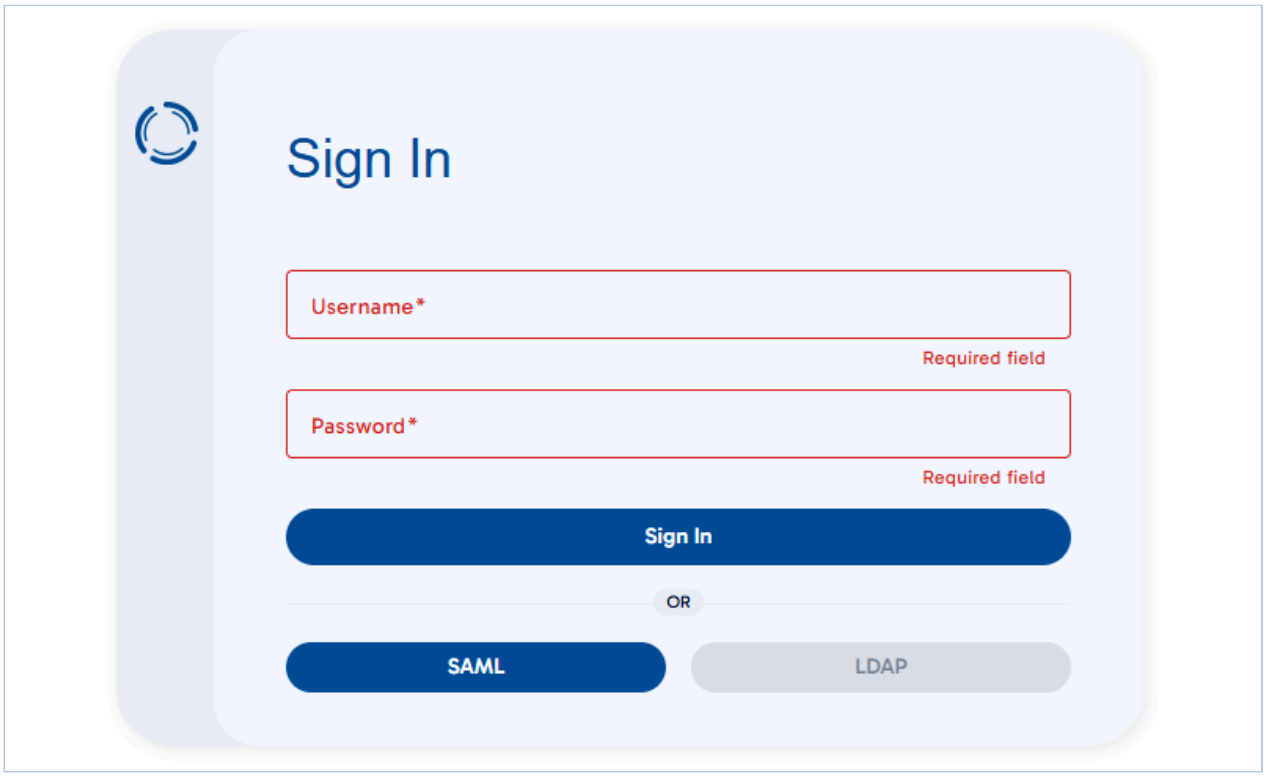



9. **Enable SAML for Users.**
    - For each user, enable **SAML Integration** during profile creation.




SAML Integration enable

10. **Sign In with SAML.**
    - After configuring SAML, users can click sign In with **SAML** and enter their credentials to authenticate.




Sign In with SAML

## Troubleshooting SAML

1. In case of SAML failures a message popup will appear on the screen stating that a “SAML login error” occurred. Should this happen, please contact support@sepiocyber.com.




2. SAML operation depends on proper time synchronization between the different solution components. If the Sepio Server and one of the other components are not synchronized or if time zones are not configured properly, it is expected to see error message indicating that assertion has expired. For example:

**Authentication mode is SAML. From IP Address: 19.153.51.42. Error message: Assertion has expired. Assertion valid NotOnOrAfter 07/15/2025 06:47:24 +00:00.**

**Note:** Assertions have expiration times for security reasons. If an assertion could be used indefinitely, it would create a vulnerability. By setting a “NotOnOrAfter” timestamp, the system ensures that even if an assertion is intercepted, it can only be used for a limited time.

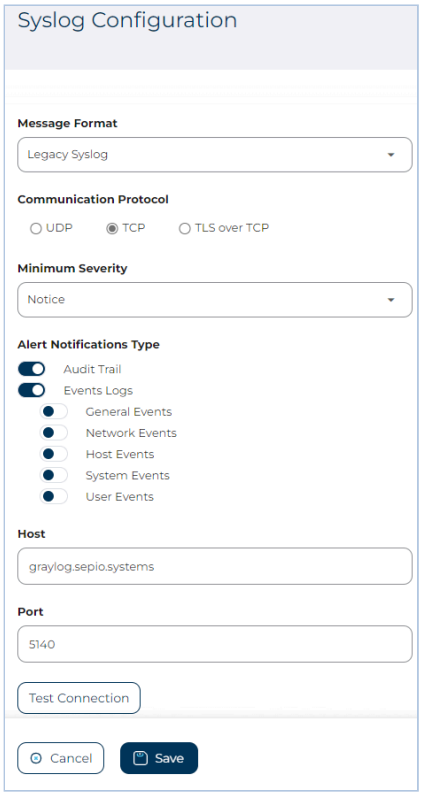
The most common reason for an “Assertion has expired” error is a **time synchronization issue** between the Identity Provider (IdP) and the Service Provider (SP). If the SP’s clock is significantly ahead of the IdP’s clock, the SP might receive an assertion that it considers expired, even if it was just issued by the IdP. Other less common causes could include:

- **Network latency:** While less common for simple expiration, very high network latency could cause a delay in the assertion reaching the SP, pushing it past its validity period.
- **Incorrectly configured assertion validity period:** The IdP might be issuing assertions with extremely short validity periods.

# Configuring Syslog

## To Configure Syslog

1. Open the Integration View.
2. Enable the Integration.
3. Hover your mouse over the integration and click the configuration icon. The **Syslog Configuration** view appears.
4. Enter and select the required parameters/values as described in the table below.



Syslog Configuration

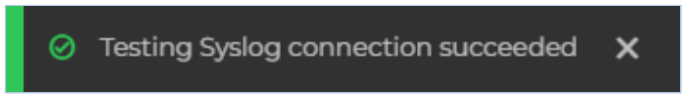
## Syslog Configuration Parameters

| Parameter | Description | Options / Values |
|---|---|---|
| **Message format** | Syslog message format | • JSON Syslog<br>• Legacy Syslog<br>• RFC5424 Syslog<br>• CEF |

| Parameter | Description | Options / Values |
| --- | --- | --- |
| **Communication Protocol** | Syslog Communication Protocol | • UDP<br>• TCP<br>• TLS Over TCP |
| **Minimum Severity** | Specifies the kinds of messages, by severity level, to be sent to the Syslog server. The Platform sends the highest selected severity messages and all messages with lower severity. For example, selecting **Notice** will send Notice, Informational, and Debug messages. | • Debug<br>• Informational<br>• Notice<br>• Warning<br>• Error<br>• Critical<br>• Alert<br>• Emergency<br><br>**Note:** Use **Debug** with caution, as it may generate a large volume of Syslog traffic in a busy network. |
| **Alert Notifications Type** | Specifies the Alert notification types the Platform sends to the Syslog server. | • Audit Trail – User events<br>• Event Logs – Platform events<br><br>**Event Logs types:** General Events, Network Events, Host Events, System Events, User Events |
| **Host** | Specifies the Syslog server (IP address or URL) that receives messages from the Sepio Platform | Enter IP address or URL |
| **Port** | Specifies the port the Syslog server listens to | Default port: 514 |

## Testing and Saving the Configuration

1. **Test the Connection**
    - Click **Test Connection** to verify the Syslog connection.
    - If successful, the following message appears:



Testing Syslog connection succeeded

2. **Save the Configuration**
    - Click **Save** to finalize your Syslog configuration.

# Integrating ServiceNow CMDB

Sepio application for ServiceNow provides device insights for Cyber-Physical Systems within the ServiceNow Platform. It enables extending existing processes and workflows already implemented with ServiceNow. Sepio's advanced discovery capabilities feed device information into the configuration management database (CMDB) that is invisible or not available from other sources. It combines ServiceNow's asset mapping and reporting with the ability to reconcile the data that is found inside the CMDB.

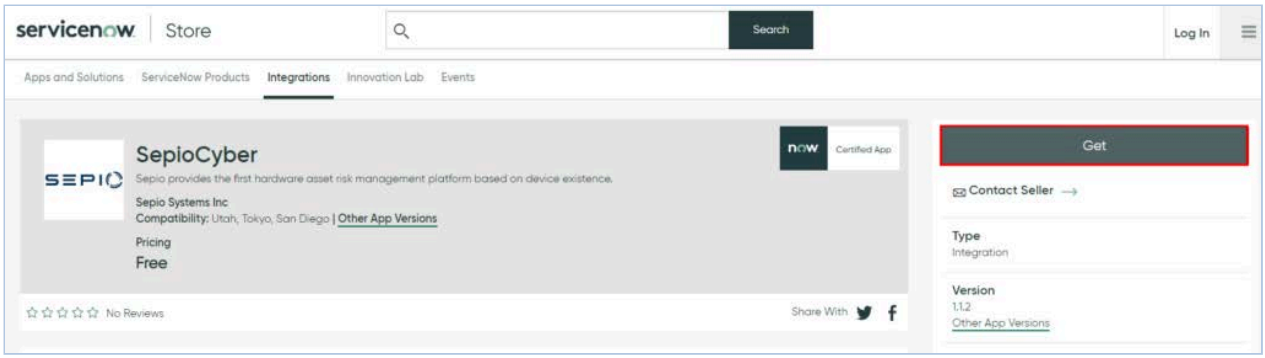
**This topic contains step-by-step instructions about integration with CMDB.**

> **Note:** Sepio uses **HTTPS** for communication between Sepio components and ServiceNow CMDB.

> **Note:** This step-by-step procedure assumes you have a ServiceNow account and can access the Sepio Platform with login credentials.

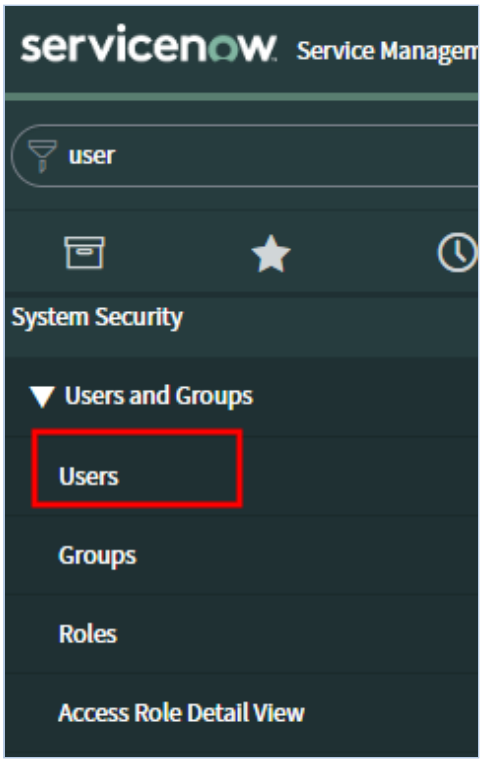
## Step 1 – Installation and Firewall Configuration

Go to ServiceNow Store and install the Sepio application.

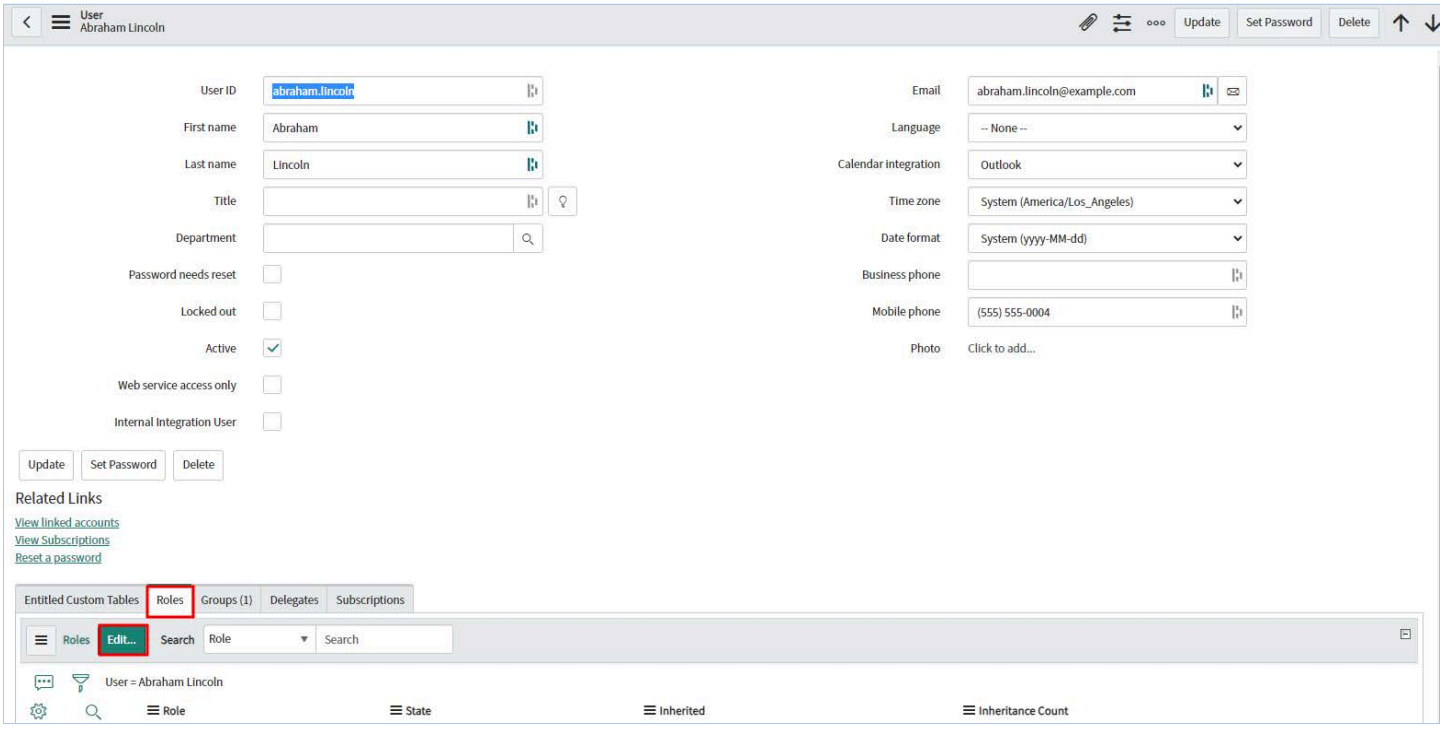



Install the Sepio application

In **ServiceNow Service Management**, create a user with Admin Role.




Servicenow -> Service Management -> Users

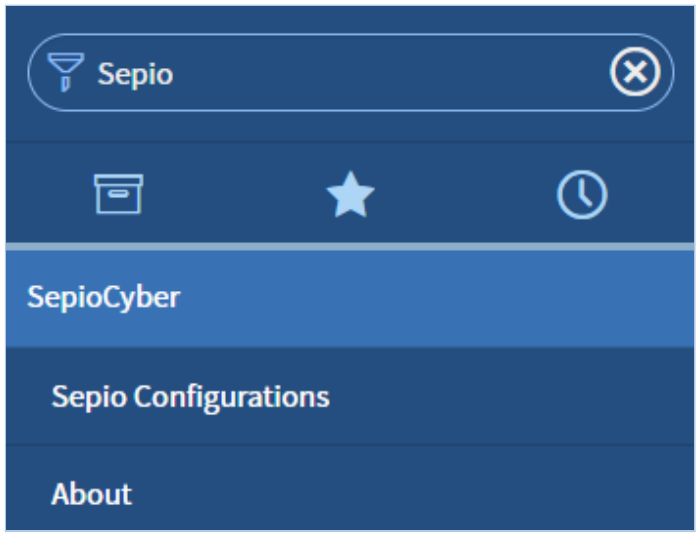



Creating a User with Admin Role

**Note:** Determine the specific use case and requirements for integrating Sepio with ServiceNow. Understand what data or events you want to exchange between the systems.

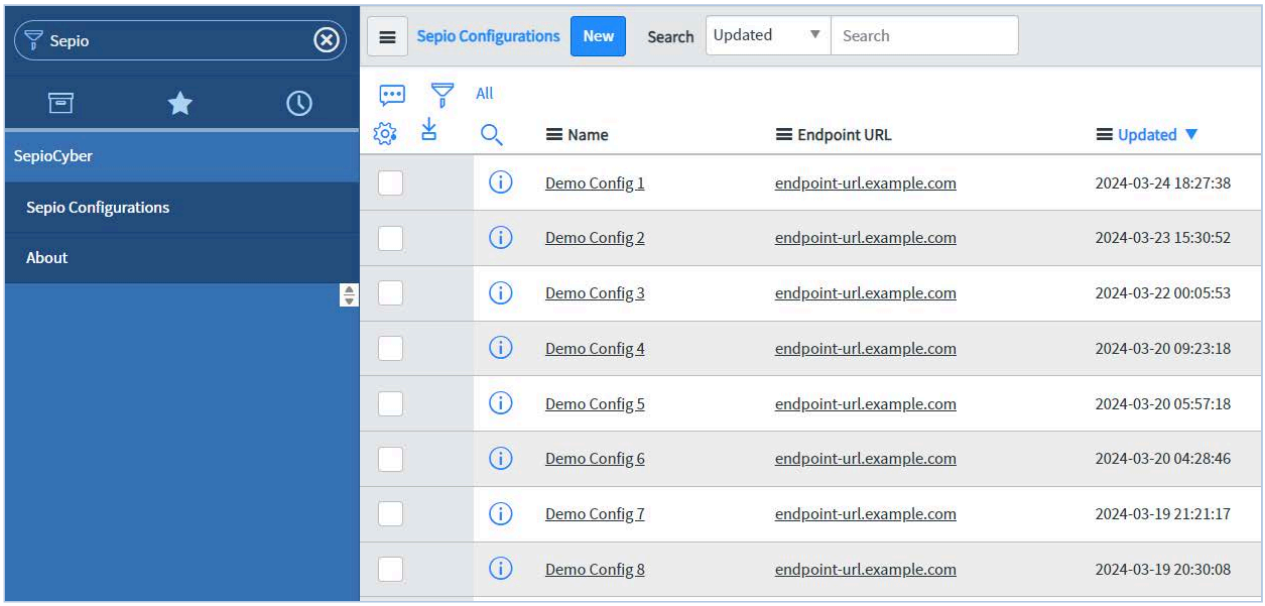
## Step 2 – Configuration Rule initialization

In Classic UI(UI15,UI16, Next Experience UI), type “Sepio” into Application Navigator to see the SepioCyber Application menu and “Sepio Configurations“ module:



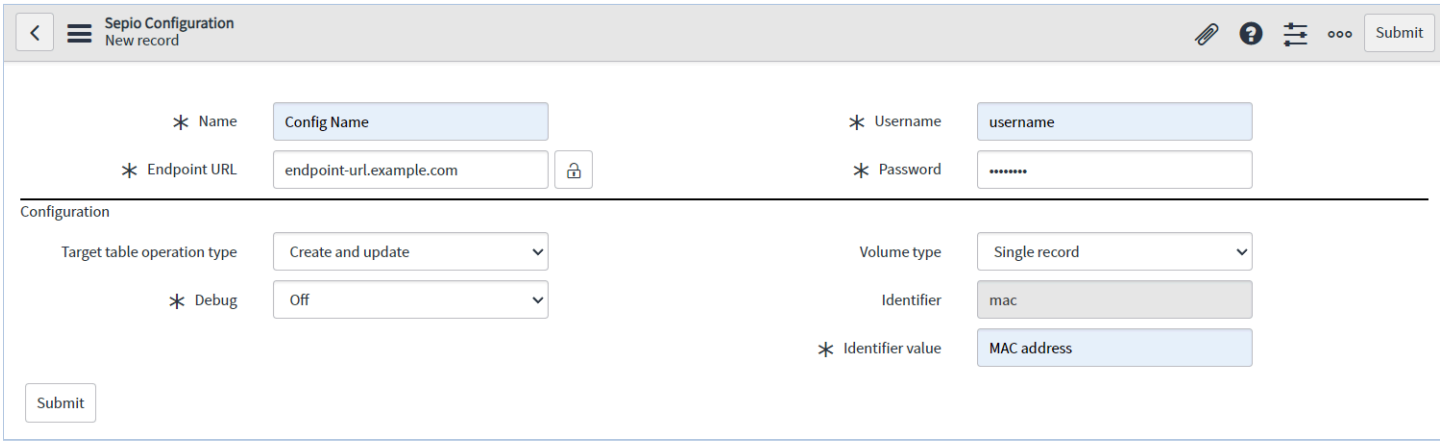

Type “Sepio” into Application Navigator

The Sepio Configuration section allows you to review your Configuration Rules. If Configuration Rules do not exist yet you will see an empty table. The picture below shows a screen with server configuration rules that are already created.




Sepio Configurations table with rules already created

Next, click the “New” button above the list to initialize or create a new Configuration Rule. After pressing the button, a form will appear. This form will have blank and some prepopulated fields:




Sepio Configurations – Adding a new record

To complete the initial configuration, you should provide both credentials and URL for Sepio's environment platform. The following fields are mandatory and should be populated to create the Configuration rule:

- **Name** (compose meaningful name for this Configuration Rule)
- **Endpoint URL** (URL of Sepio platform to connect to)

> **Note:** You can create a Configuration Rule without credentials; however, you cannot proceed further without a username and a password.

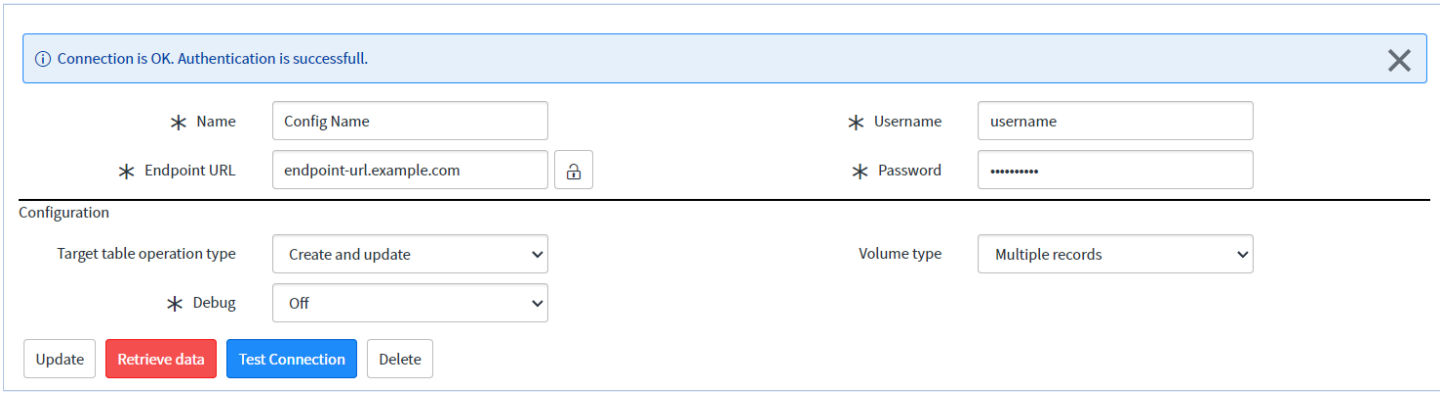
## Step 3 – Connectivity Test

Continue by providing the Sepio credentials and entering it into the Configuration Rule created in previous step. Use "Username" and "Password" fields for this step and save the record.




Sepio credentials

To verify that the connectivity between the systems is established, perform a connectivity test by clicking "Test Connection" button on the top of the Configuration Rule form. If the connection is established and is successful, the following message should appear:




Connection is OK message

If the connectivity test was not completed successfully, the following message should be displayed:



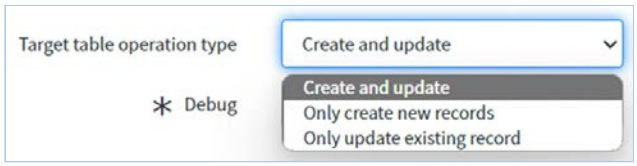

Testing Connection failed message

## Step 4 – Operation Type

When working with CMDB and using the Sepio integration, the admin may choose different integration options:

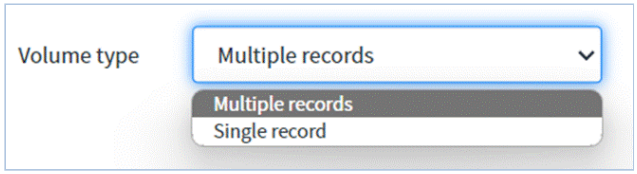
It is possible to create new records in CMDB, or update existing records only, or perform both types of actions.

Use the “Target table operation type” to select the operation type:




Target table operation type

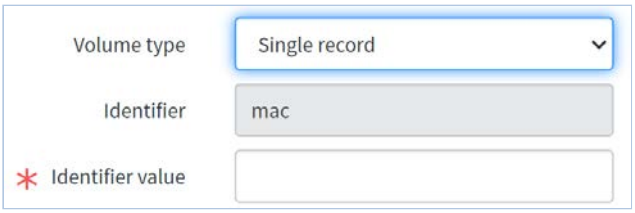
## Step 5 – Single/Multiple




Single or multiple records

Each Configuration Rule can be configured to retrieve single or multiple records, depending on your business requirements.

By default, the field “Volume type” contains “Single record” option:

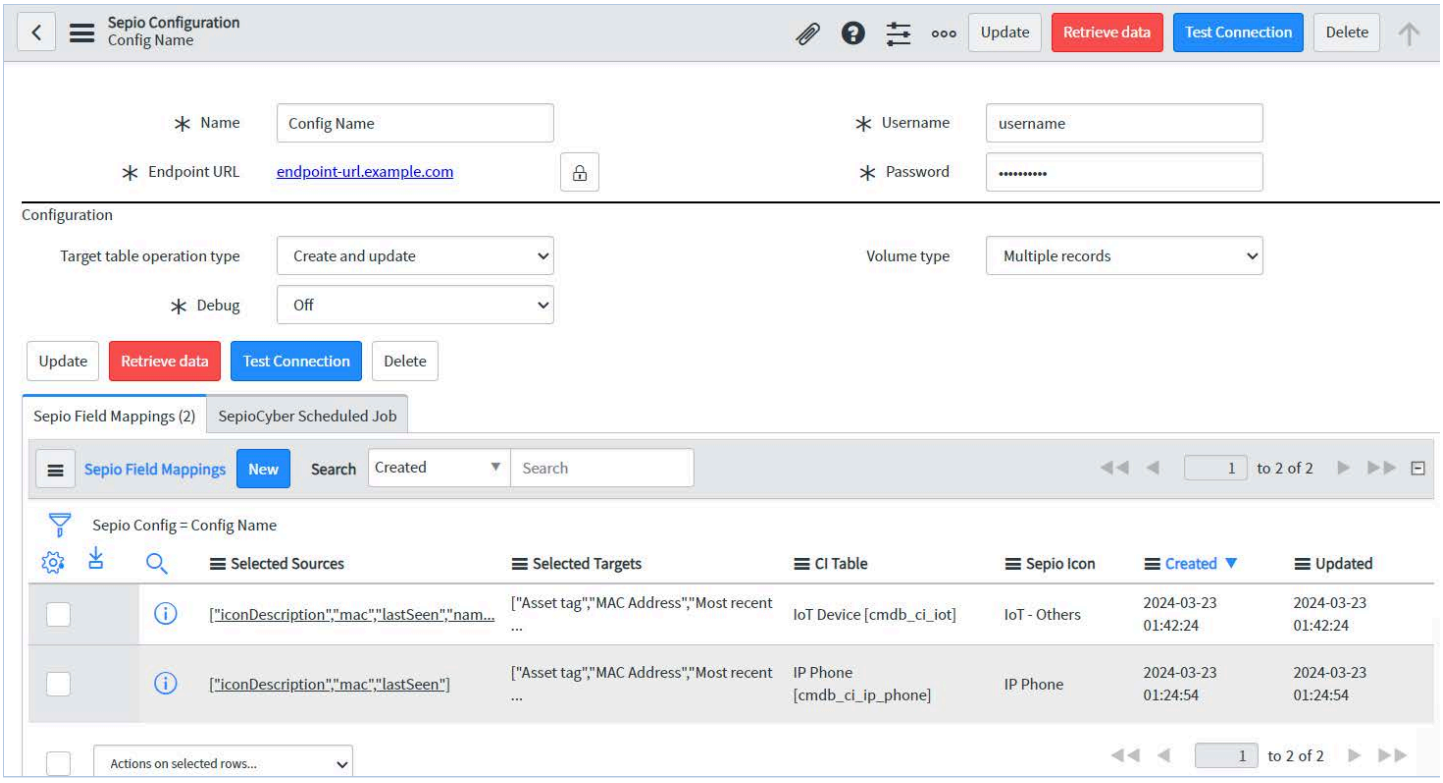



By default, the field “Volume type” contains “Single record”

And thus fields “Identifier” and “Identifier value” are displayed and are expected to contain value for a target single record unique identifier.
Currently MAC address is the only option for Identifier and therefore this field is configured with Read Only attribute.
If selecting “Multiple record” as “Volume type” option, “Identifier” and “Identifier” value fields will be hidden.

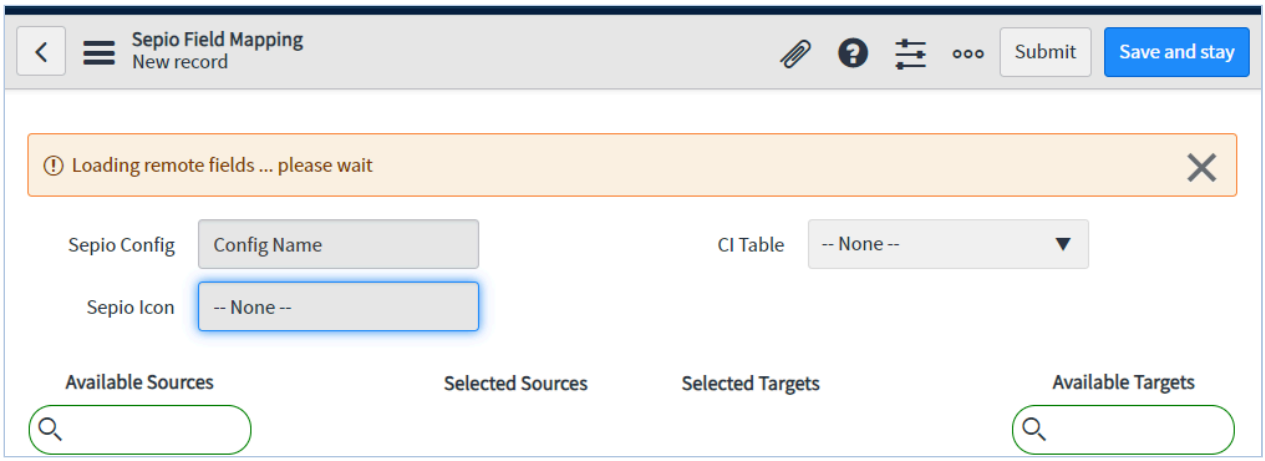
## Step 6 – Field Mapping

After performing the population Configuration Rule field, you should compose mapping between Sepio fields and selected ServiceNow CMDB Table fields. Right below the form of a Configuration Rule – there is Related List called Sepio Field Mappings – this is where administrator can create a set of mapping records.



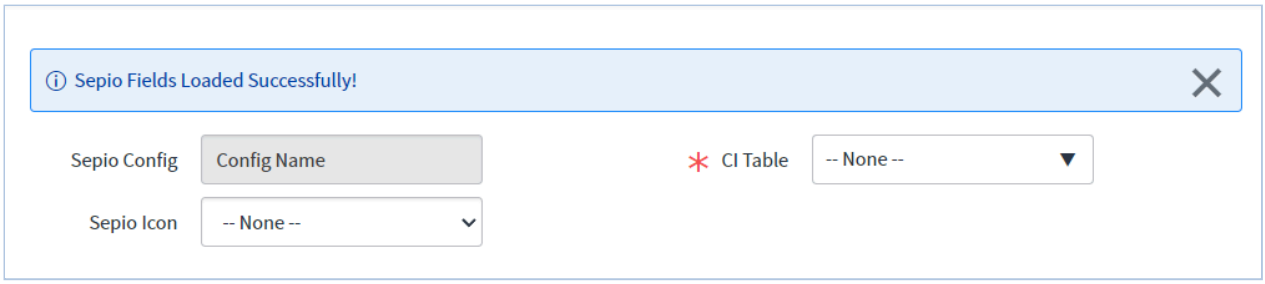

Sepio Field Mappings

Click “**New**” button on the top of the Related List. At first on the form will appear a message:



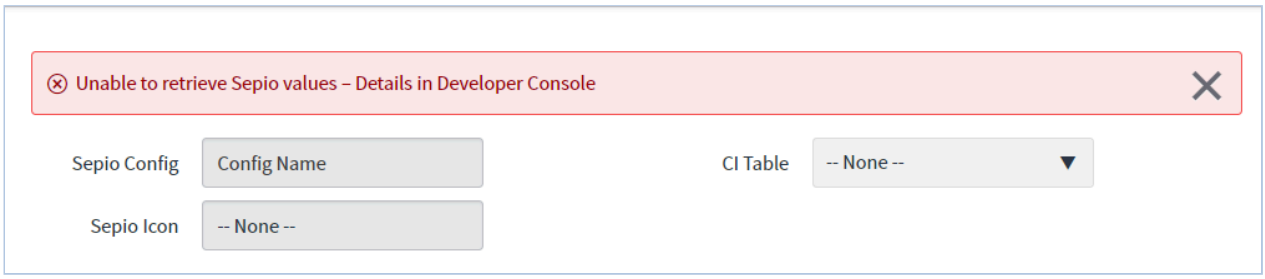

Loading remote fields message

And it will be replaced to another one if connection with server is success:



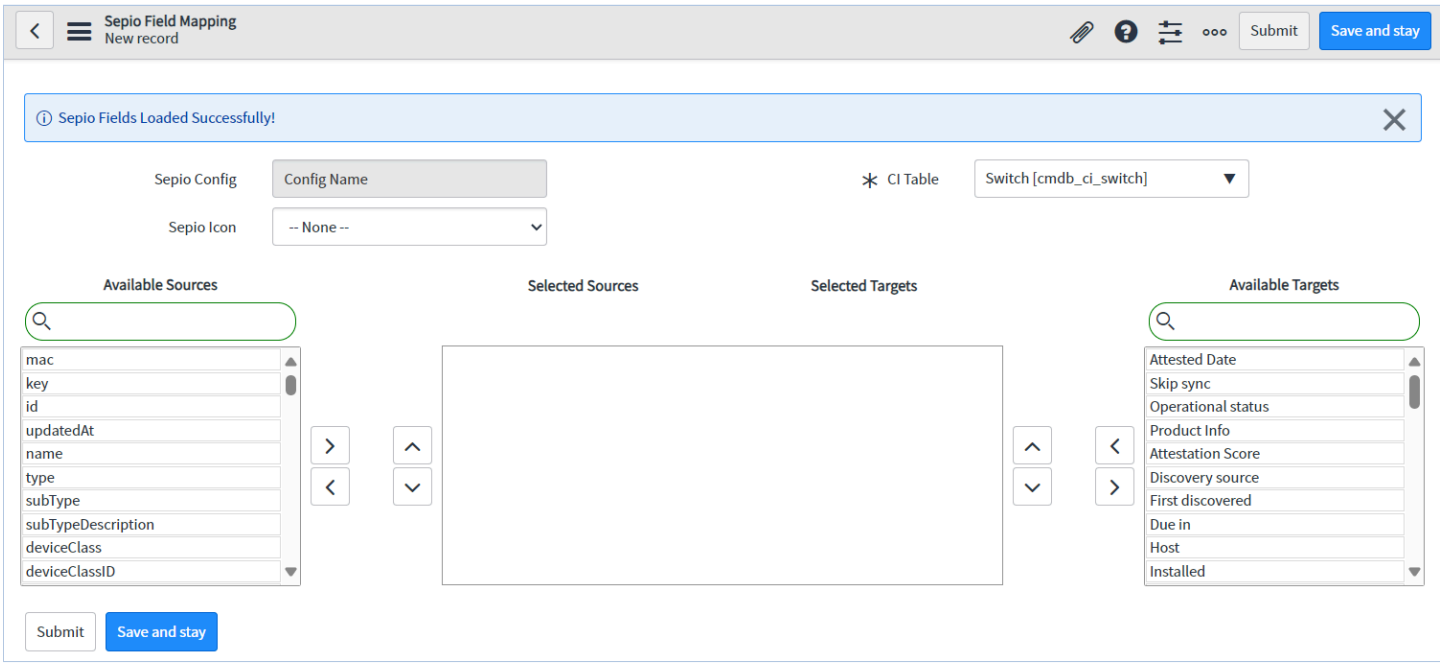

Sepio Fields Loaded Successfully!

Or another message if the connection was failed:



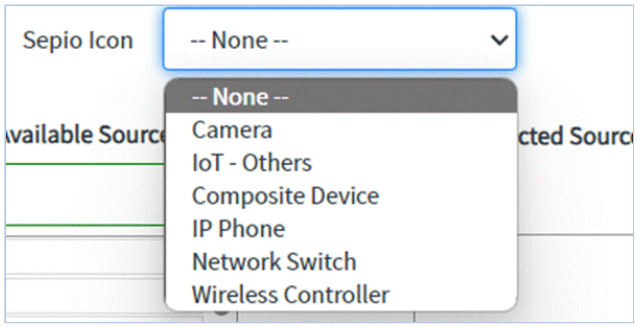

Unable to retrieve Sepio values

To see the following form with Sepio fields on the left in «Available Sources» and ServiceNow CMDB Table fields to the right, in «Available Targets», you have to select target CMDB CI table:



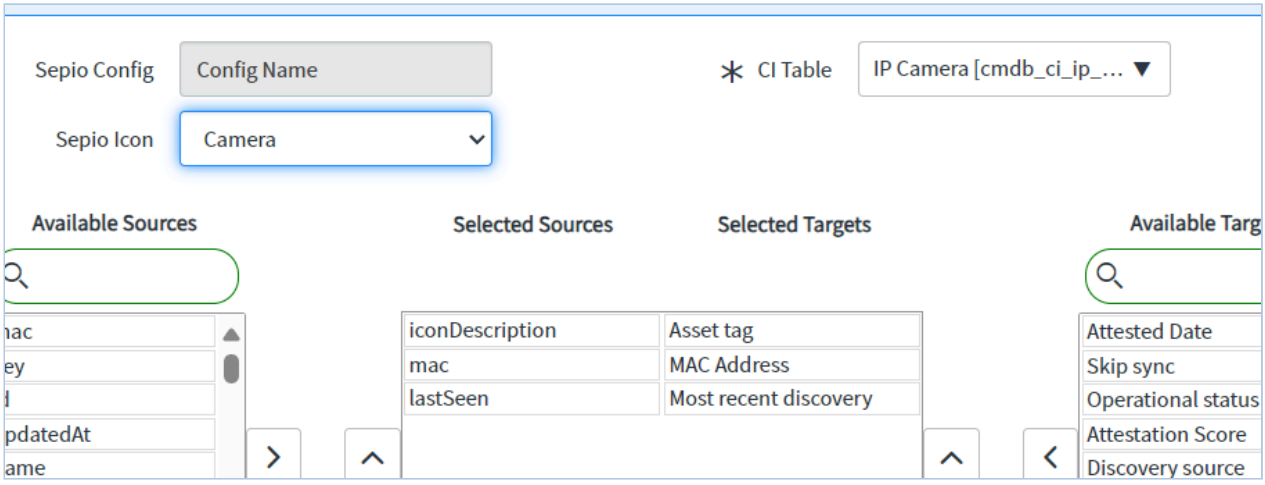

Select CMDB CI table

You can choose the table and fields completely by yourself, or use the templates from the Sepio Icon field:




Sepio Icon field

In this case, the CMDB table and several fields to be mapped will be selected automatically:




CI table and fields mapped automatically

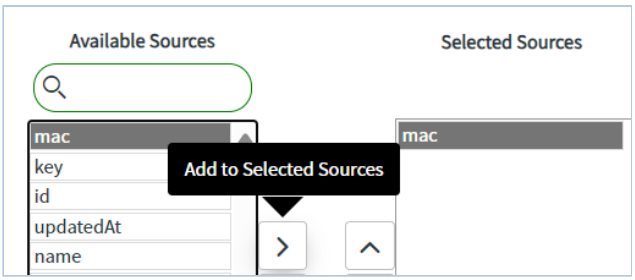
The selected fields for mapping will be displayed in the middle of the form. For that, you need to put the selected items to the «Selected Sources» and «Selected Targets». The Sepio field will correspond to the

CMDB field at the same level.

You can select fields for mapping one at the time or several at once.
You can select multiple fields at the same time in the following ways:

1. Hold the mouse button and drag from one field to another one.
2. Hold Ctrl and select the desired fields.
3. Click on one field, hold Shift and select another field. Fields between those two will be selected too.

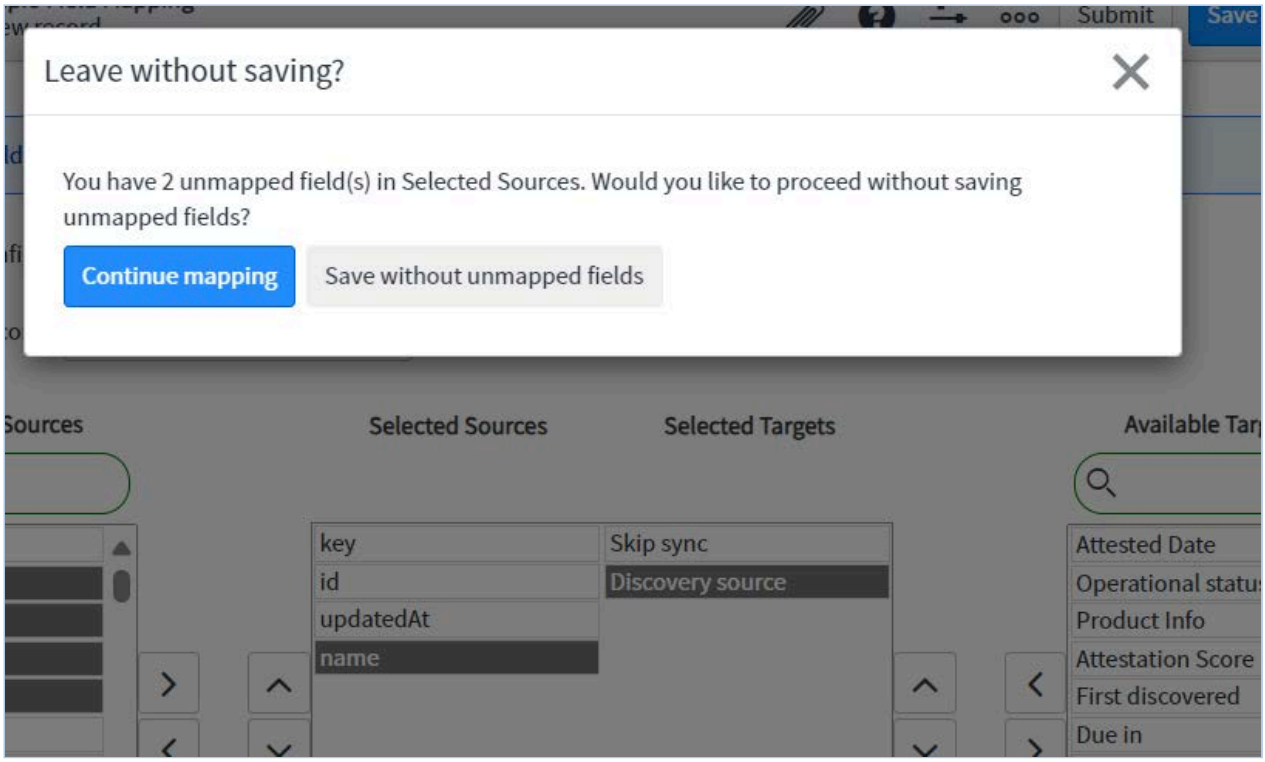
Now use buttons between lists to move items to configure mapping.



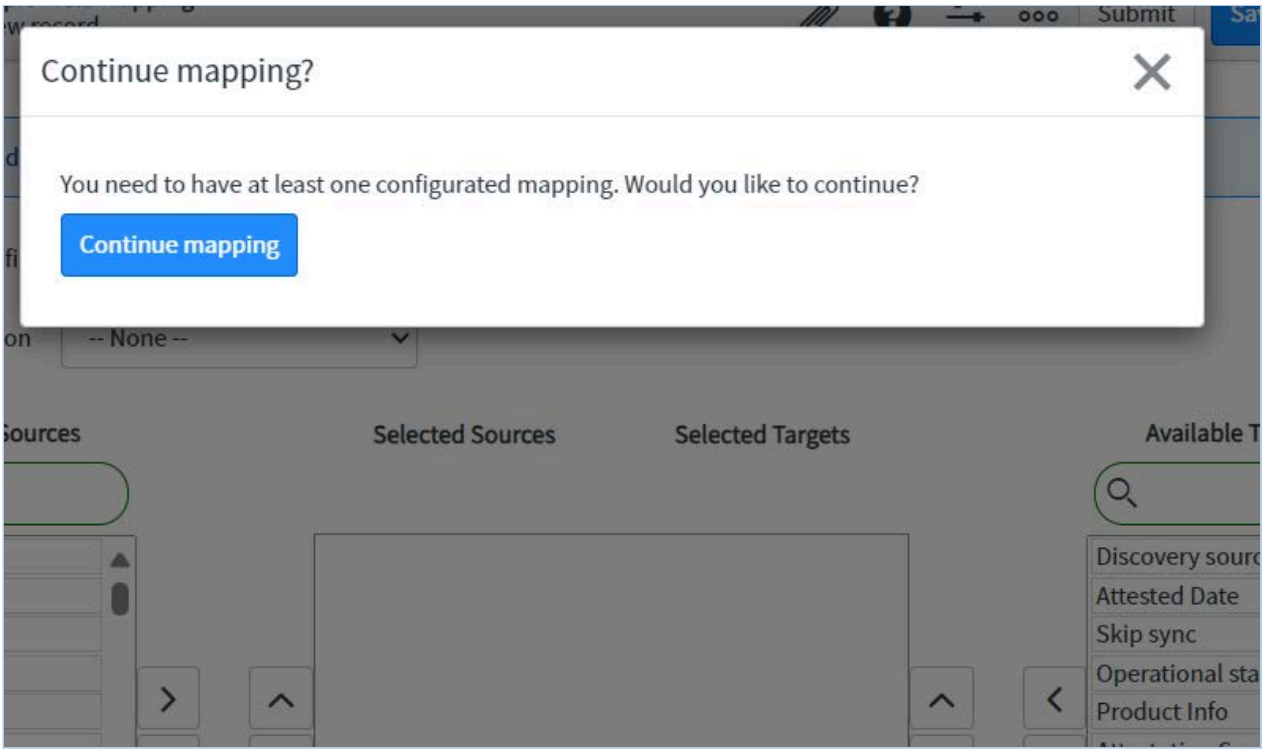
Add to Selected Sources

After selecting mapping – please click «Submit» or «Save and stay» to create new mapping record.

**Note:** If you try to save an empty mapping (without any selected fields) or if your selected fields have different fields numbers, you will be stopped with dialog windows:



Try to save an empty mapping



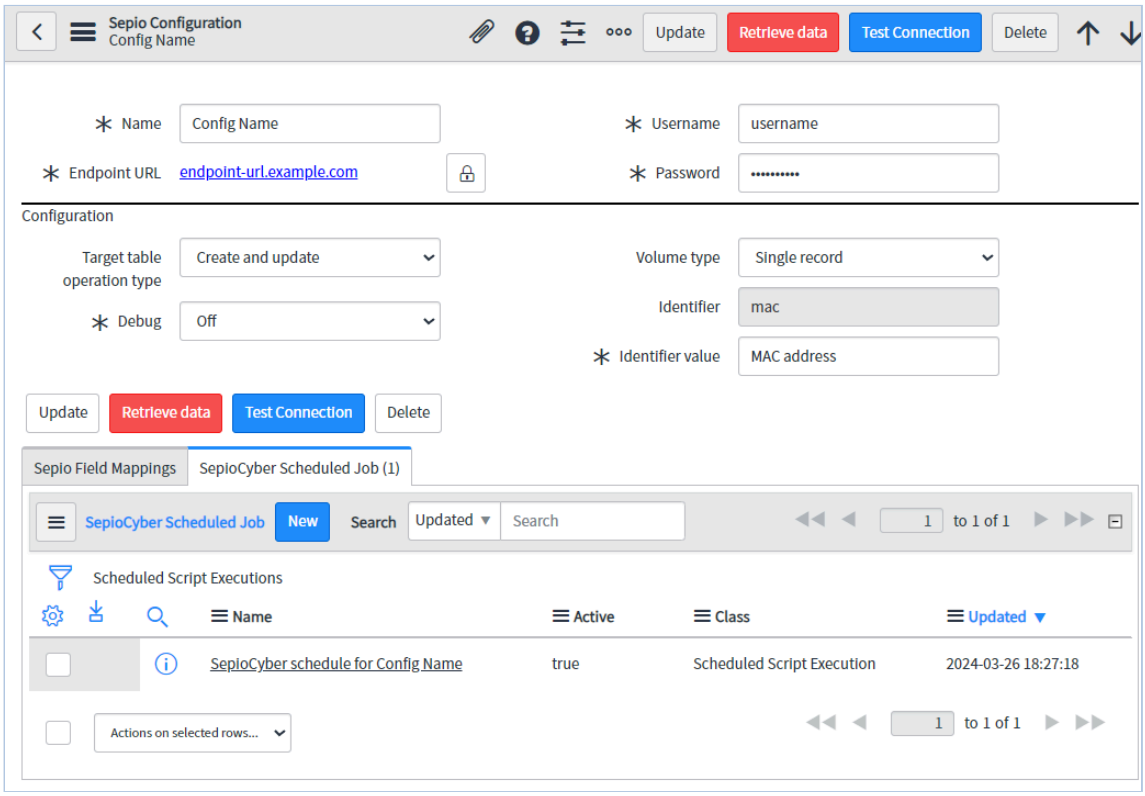

Select fields with different field numbers

## Step 7 – Run & Review

When the Configuration Rule ready and Field Mapping composed – it is time to run it and observe the results. Please click on “Retrieve data” button within a Configuration Rule form to retrieve data from Sepio’s platform and transform it into ServiceNow CMDB records of selected table.

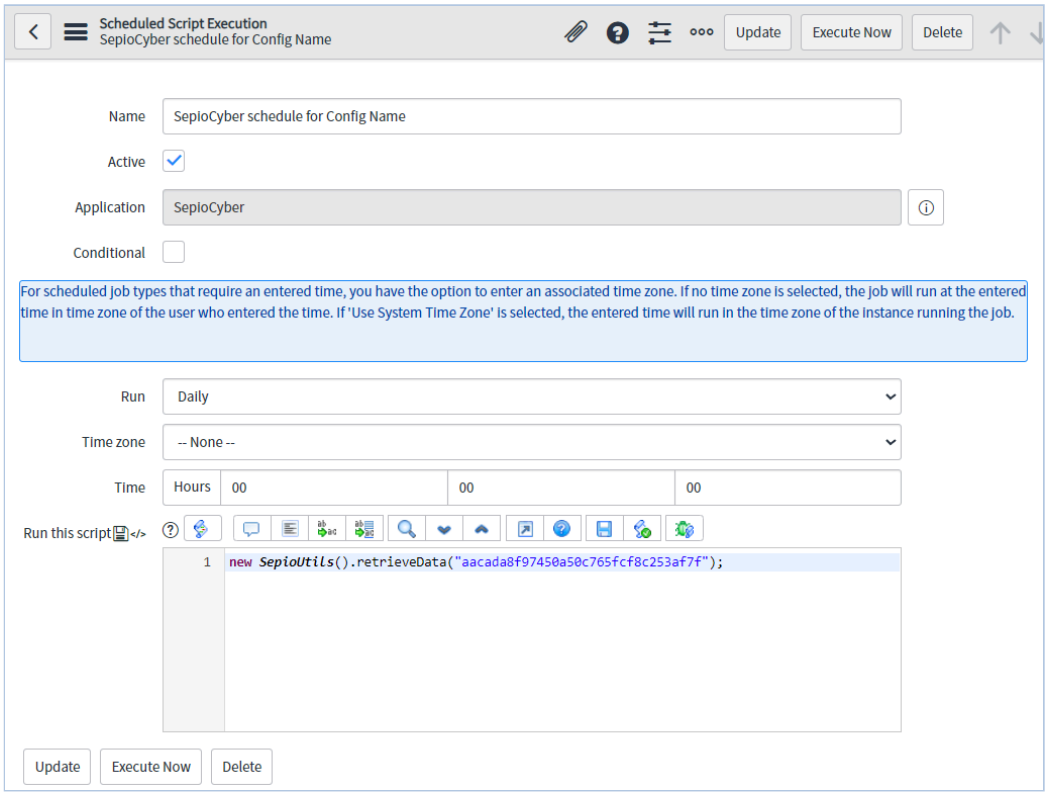
## Step 8 – Schedule

After running and successfully retrieving data from the Sepio platform and transforming it into selected CMDB table – there is a functionality to automize this process by Scheduled Jobs functionality in ServiceNow platform. Please switch to a Related List called SepioCyber Scheduled Job – this is where this is where administrator can create a list of Scheduled Jobs for current configuration record.




SepioCyber Scheduled Job

Click "**New**" button on the top of the Related List to see the following form for Scheduled Job configuration.




Scheduled Job configuration

The form for Scheduled Job configuration opens with autogenerated values for fields "Name" and "Run the script" do not change this values. Fields "Run", "Time zone", "Time" need to be populated according to your preferences.

After populating the form – please click “Submit” to a create new Schedule Job for current Configuration record.

## Integrating ServiceNow Queries

The **Sepio Query Tool for ServiceNow CMDB** runs from the Sepio SaaS platform, investigating assets against the customer's ServiceNow cloud instance. This tool is designed to help customers validate the structure of their ServiceNow CMDB before integrating with Sepio.

The tool uses the standard ServiceNow Query API to determine whether a Sepio Asset, identified by its **Key**, exists in any CMDB table. If the asset is found in ServiceNow, it is tagged in the Sepio platform with the name of the **CI** table in which it appears, indicating that it exists in the CMDB. Additionally, the following user-defined attributes are applied: `ServiceNow_ip`, `ServiceNow_hostname`, `ServiceNow_ci_id`, and `ServiceNow_source_table`.

If the asset is not found in the CMDB, it will be tagged as '`not_incmdb`'.

> **Note:** Changing the user-defined attributes requires assistance from Sepio Support.

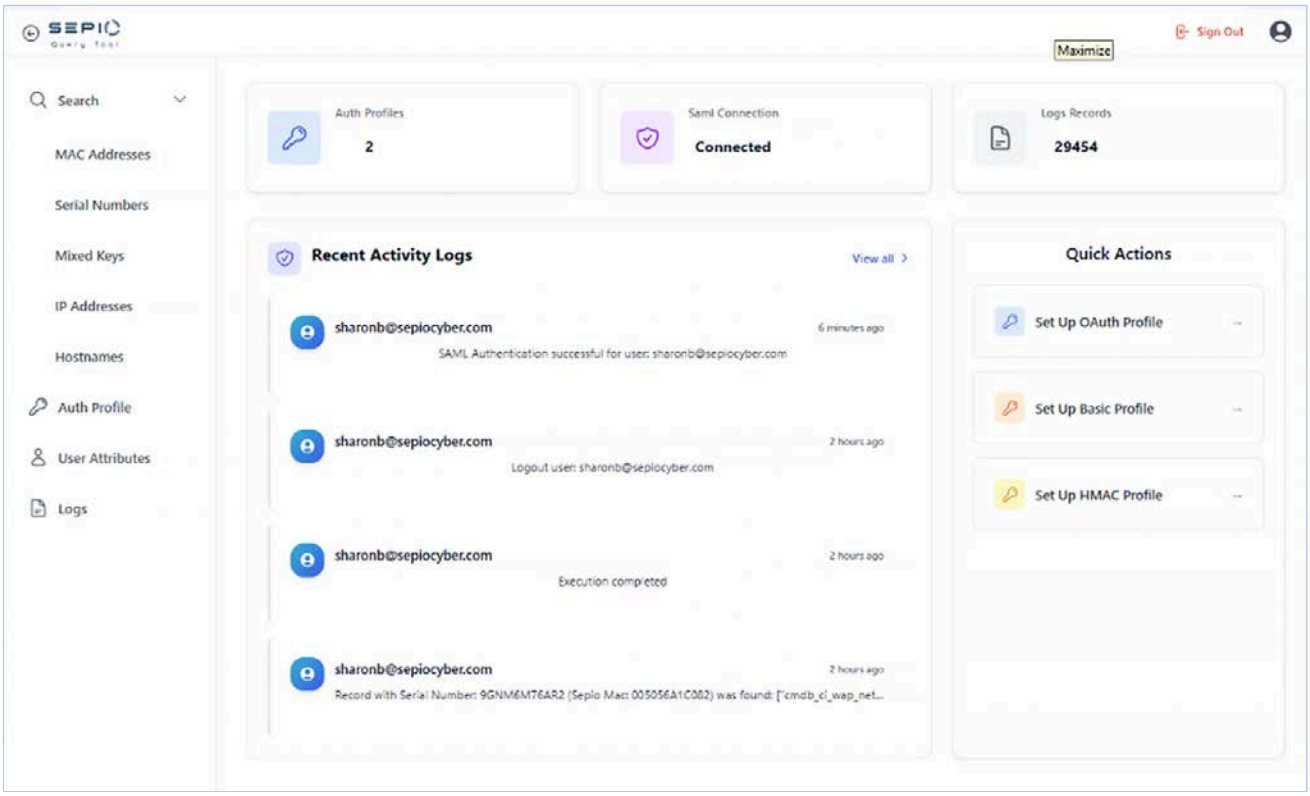
The Sepio asset key is the MAC address. Some organizations do not use MAC addresses in their CMDB. Therefore, the tool also supports searching using mixed key values, such as:

- Searching based on network infrastructure serial numbers
- Searching based on IP address or hostname in the CMDB and correlating it with the Sepio-discovered MAC address

The Sepio administrator should configure a **ServiceNow service account** (non-UI) that has administrative permissions to query the CMDB.

## Supported Authentication Methods

- **Sepio:** Password, SAML
- **ServiceNow:** Basic, OAuth, HMAC



Sepio Query Tool

## Troubleshooting

General log files, including errors, are stored in the application.log file, which is typically located in the Sepio-App/backend/logs directory.

For example:
`/Sepio-App/Sepio-App/backend/logs/application.log`

To manually restart the CQT server:

- Navigate to the directory: `Sepio-App/Sepio-App/backend`
- Find the server process: `ps aux | grep server.js`

```
^C
denisdaidai@pop-os:~/Downloads/Sepio-App/Sepio-App/backend$ ps aux | grep server
.js
denisda+   17021  0.0  0.0  19016  2304 pts/0    S+   00:26   0:00 grep --color=
auto server.js
denisdaidai@pop-os:~/Downloads/Sepio-App/Sepio-App/backend$
```

- Kill the current process: `kill 17021`
- Restart the server: `npx nodemon server.js`

# Integrating ServiceNow SecOps

This procedure assumes you have a ServiceNow account and can access the Sepio Platform.

## Configuration Steps

This section contains step-by-step instructions on how to configure the Sepio application/integration for ServiceNow. All actions performed as ServiceNow User with admin role. Before configuring the Sepio application ensure that the Sepio Environment is deployed within your business infrastructure. Please contact Sepio regarding this phase (support@sepiocyber.com).

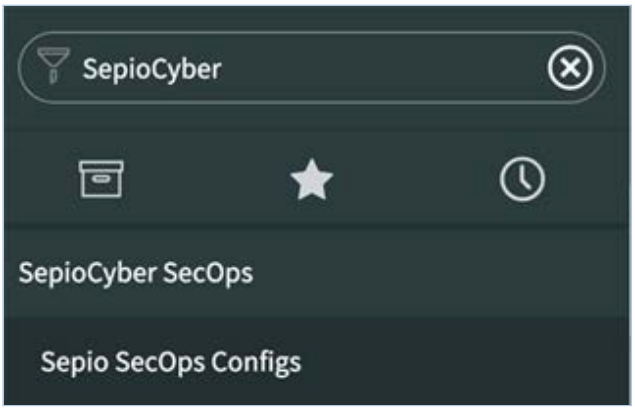
> **Note:** Before you begin, Go to ServiceNow Store and install the Sepio application.

### Step 1 – Credentials

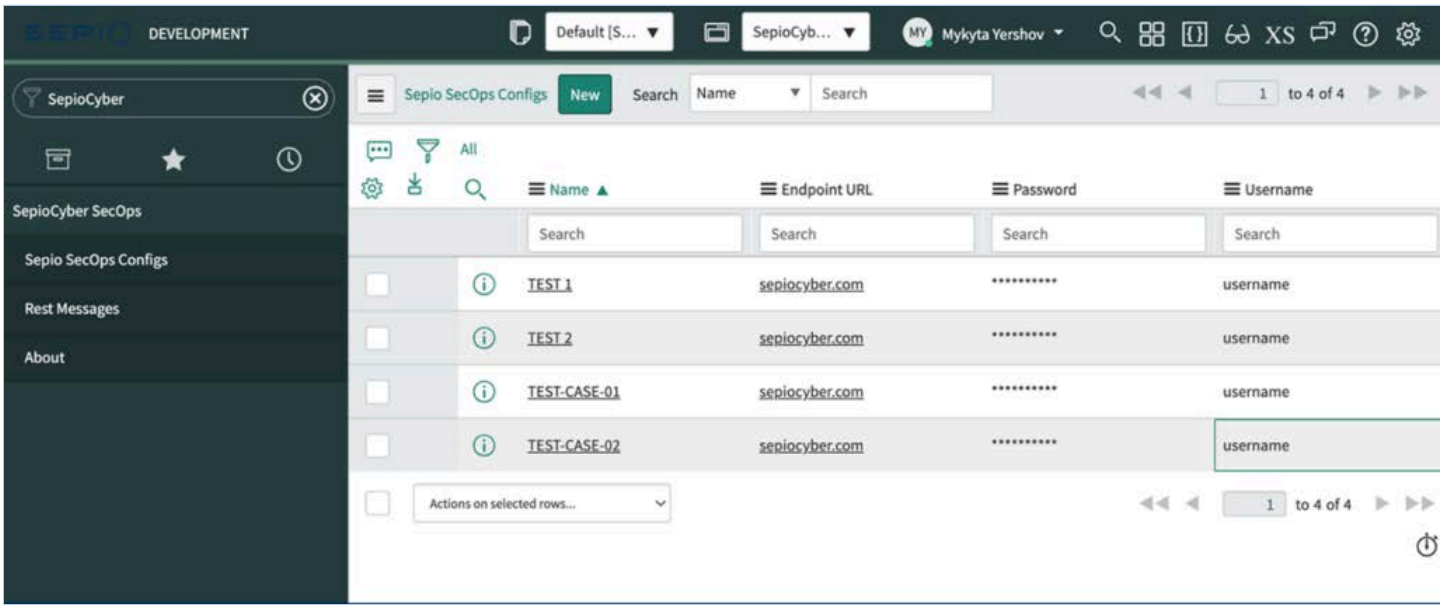
Once the Sepio Platform has been deployed in your business infrastructure, and you have installed the Sepio SecOps app for ServiceNow, this is the time to start configuring the app. You need to obtain credentials (username and password) from Sepio to begin the configuration.

### Step 2 – Configuration Rule initialization

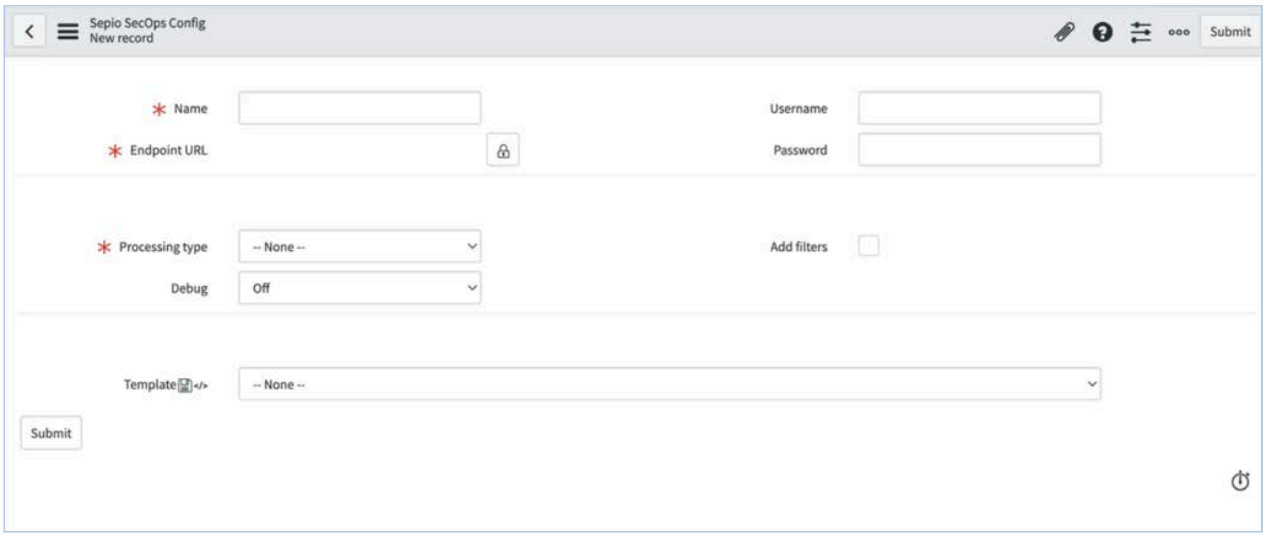
In Classic UI (UI15,UI16, Next Experience UI) please type “Sepio” into Application Navigator to see the Sepio Application menu and “Sepio Configurations“ module:




Here you will see all your Configuration Rules or no record if no Configuration Rule exists yet. On the picture below several configuration rules already created.




Please click the "**New**" button above the list to initialize/create a new Configuration Rule. After pressing the button, you will see a form with some blank and some pre populated fields:



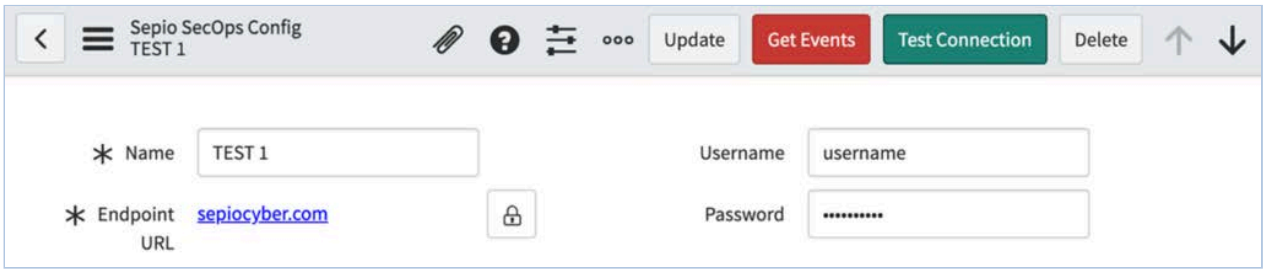

To complete this step, it is required to have both credentials and URL for Sepio environment platform. The following fields are required to populate to create the Configuration rule:

- **Name** (compose meaningful name for this Configuration Rule)
- **Endpoint UR** (URL of SepioCyber platform to connect to)

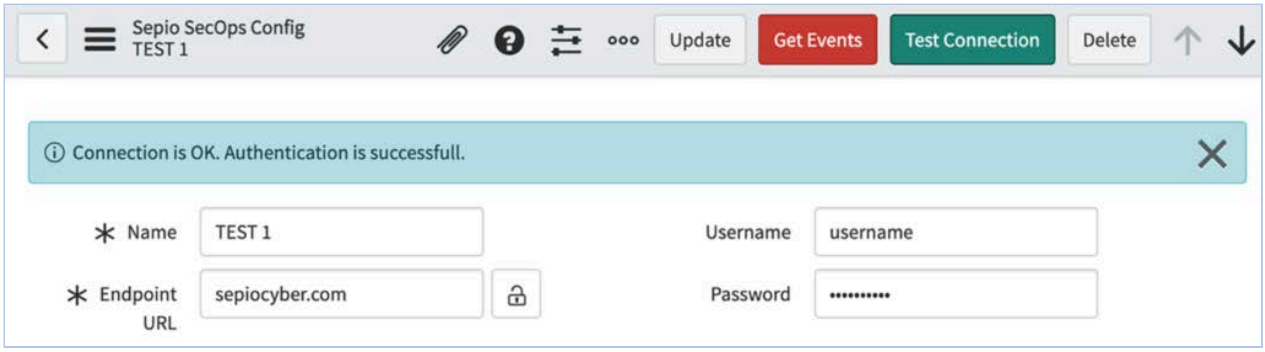
You can create a Configuration Rule without credentials; however, you cannot proceed further without username and password.

### Step 3 – Connectivity Test

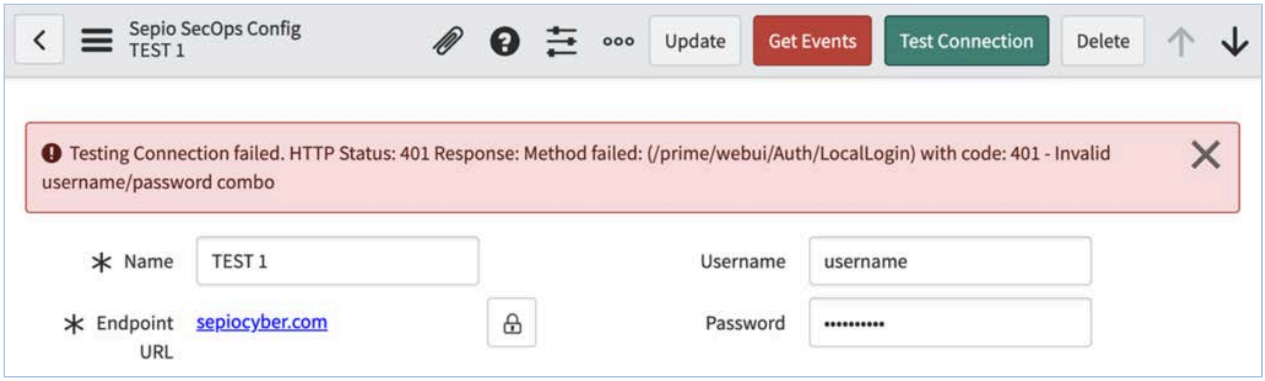
Please enter the credentials provided by Sepio into the Configuration Rule created in the previous step – use "Username" and "Password" fields for this step and save the record.




To test the connectivity, click the 'Test Connection' button at the top of the Configuration Rule form. If Connection Successful, you should see corresponding message appear.



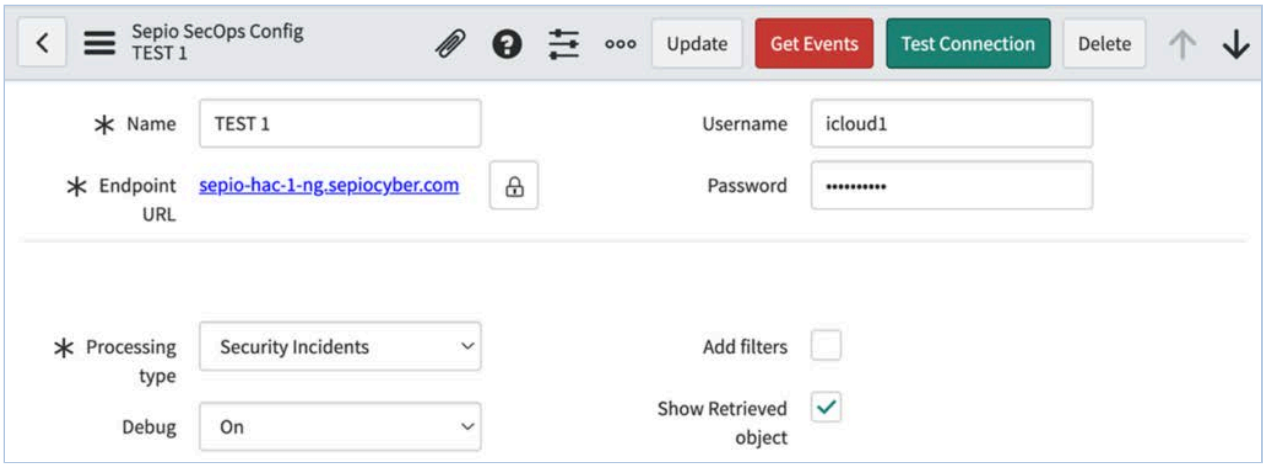

If the test fails, the following message will be displayed.

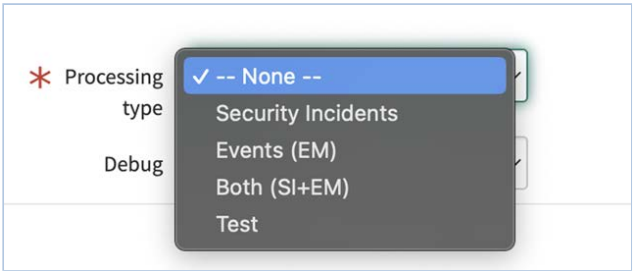



### Step 4 – Select Processing type

After connectivity testing, it is time to populate the second section of the configuration rule – provide processing type that determines the target table where new records will be processed. If system contains dependency tables and then Four options are available:

- Security Incidents – (Security Incident Response plugin has to be installed from SN Store)
- Events (EM) – (Event Management plugin must be installed from ServiceNow Store)
- Both (SI+EM) – and (Security Incident Response and Event Management plugins must be installed from ServiceNow Store)
- Test –

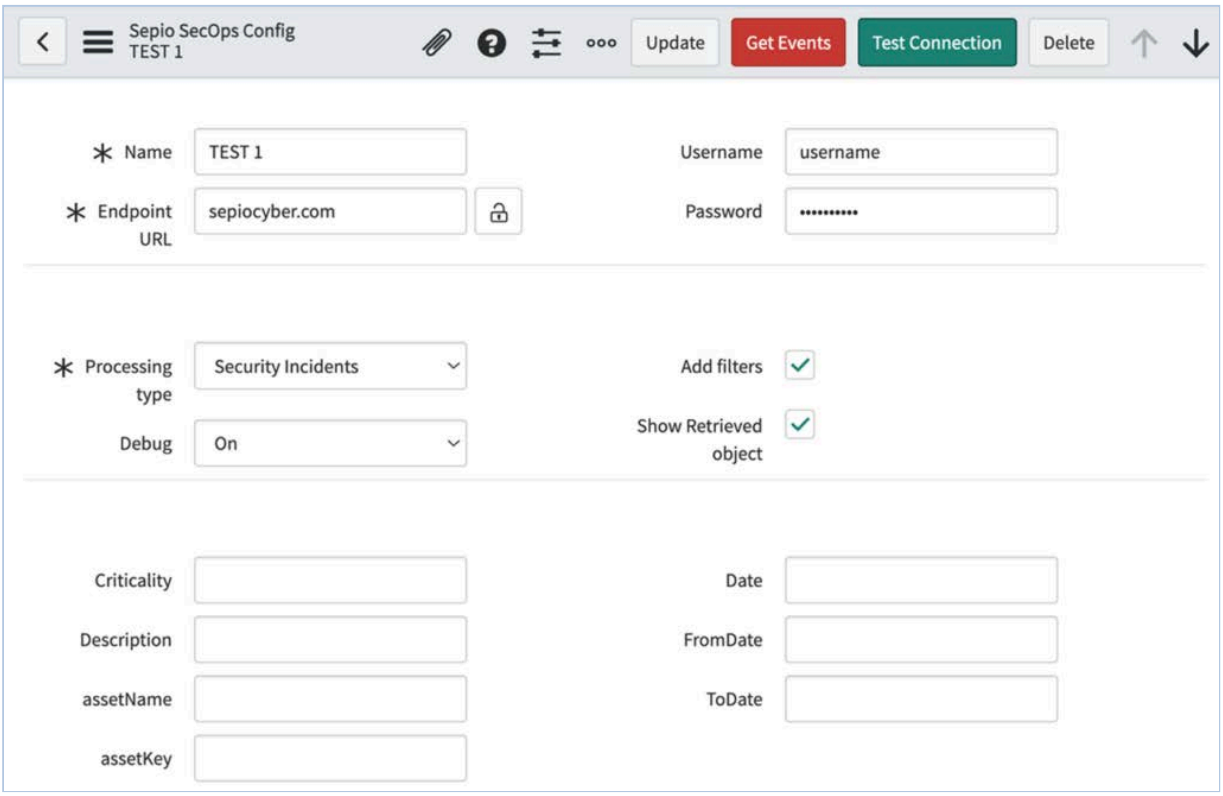



If the system doesn't contain a dependency table, the correspondent processing type will not be shown.

### Step 5 – Add filters

When working with Events and using Sepio integration, the administrator can choose the Filtering option and specify the filters that will be applied to the data. When the checkbox "Add filters" is active – filter fields are shown. When the checkbox "Add filters" is not active – all filter fields vanish from the form and their values become clear.




**Step 6 – Configure Debug**

By default, the Debug option is disabled. For detailed log generation into table please change Debug to On position.

**Step 7 – Run & Review**

Once the Configuration Rule is ready, it's time to run it and observe the results. Click the 'Get Events' button within the Configuration Rule form to retrieve data from the Sepio platform and transform it into ServiceNow Security Incidents or Event Management records, depending on the processing type.

## System Requirements

ServiceNow SecOps is designed to work with two non default ServiceNow plugins: Security Incident Response and Event Management Plugin.

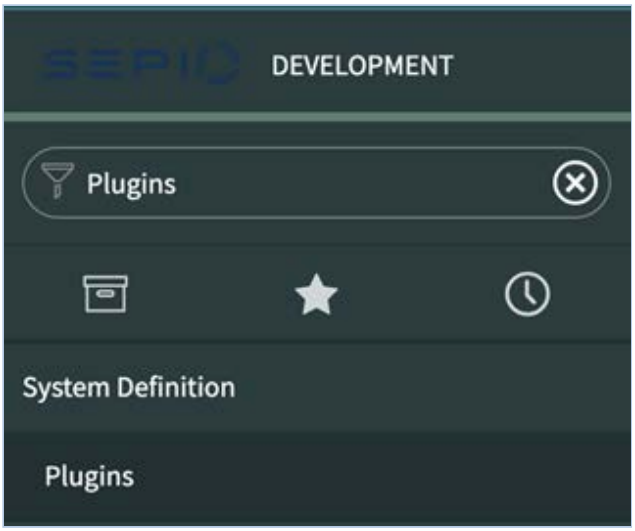
The configuration form contains three options of Processing type (Step 4):

- Security Incidents (SI) – Security Incident Response plugin must be installed from SN Store.
- Events (EM) – Event Management plugin must be installed from ServiceNow Store.
- Both (SI+EM) – Security Incident Response and Event Management plugins must be installed from ServiceNow Store.

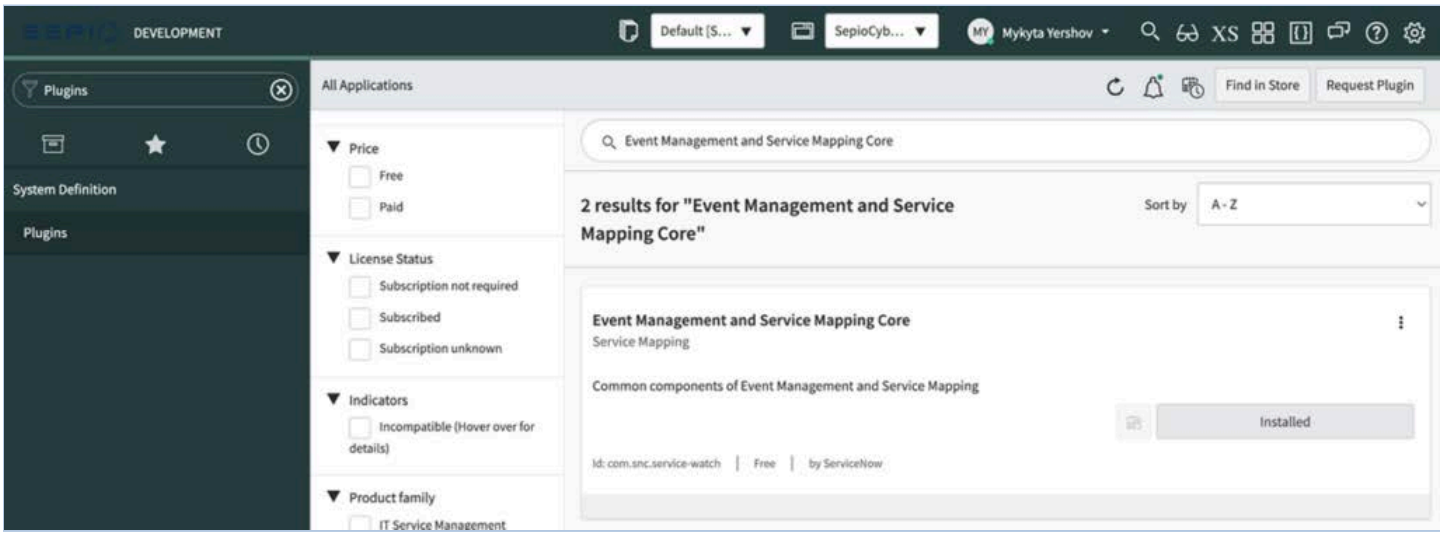
Depending on users' needs, it is necessary to install the listed plugins from the ServiceNow Store.

**Security Incident Response Installation guide:**

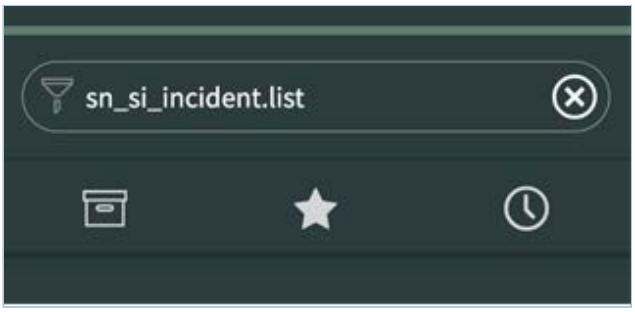
- Ensure that the ServiceNow platform is installed and configured.
- Navigate to Plugins Module.



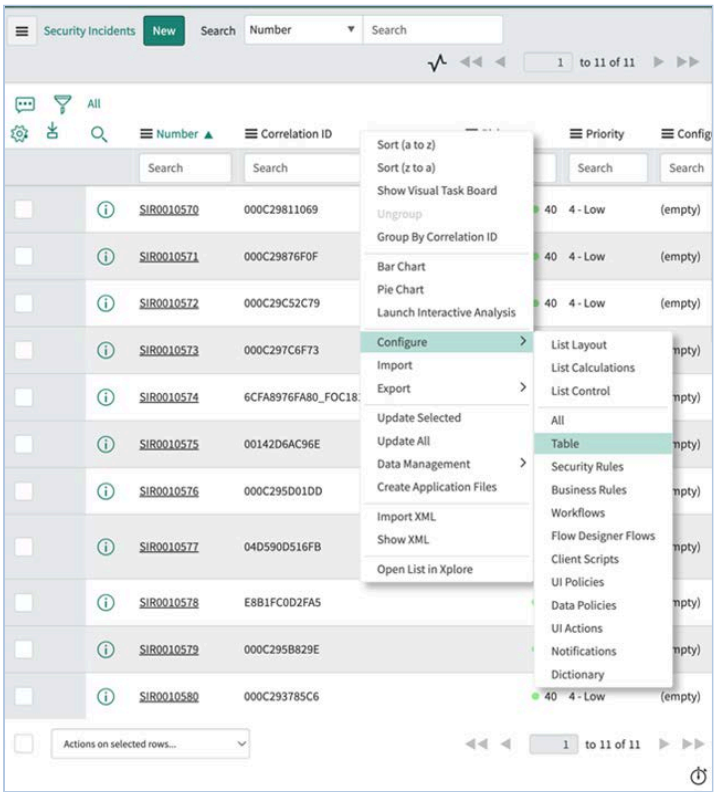

- Search for Security Incident Response bundle of plugins (11 plugins).



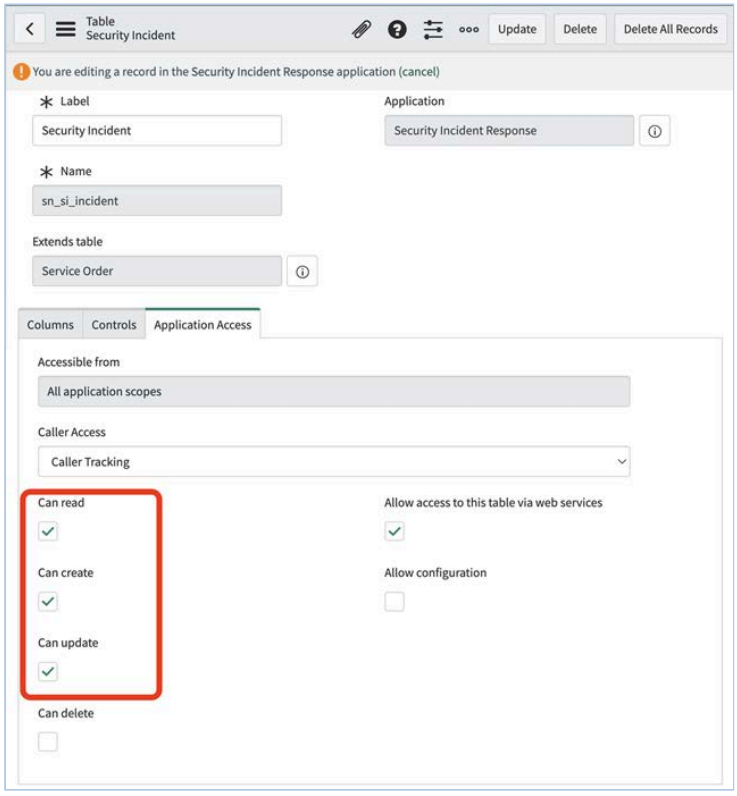

- Click on “Install/Update”.
- Wait until all plugins are installed.
- Navigate to by filter navigator “sn_si_incident.list” and press Enter.




- Do right click on the table columns name and select configure table.

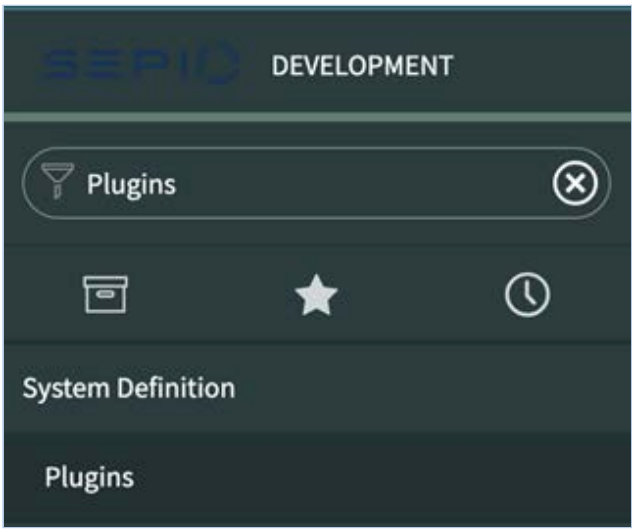



- Ensure that Application Access allows read, create, update operations.

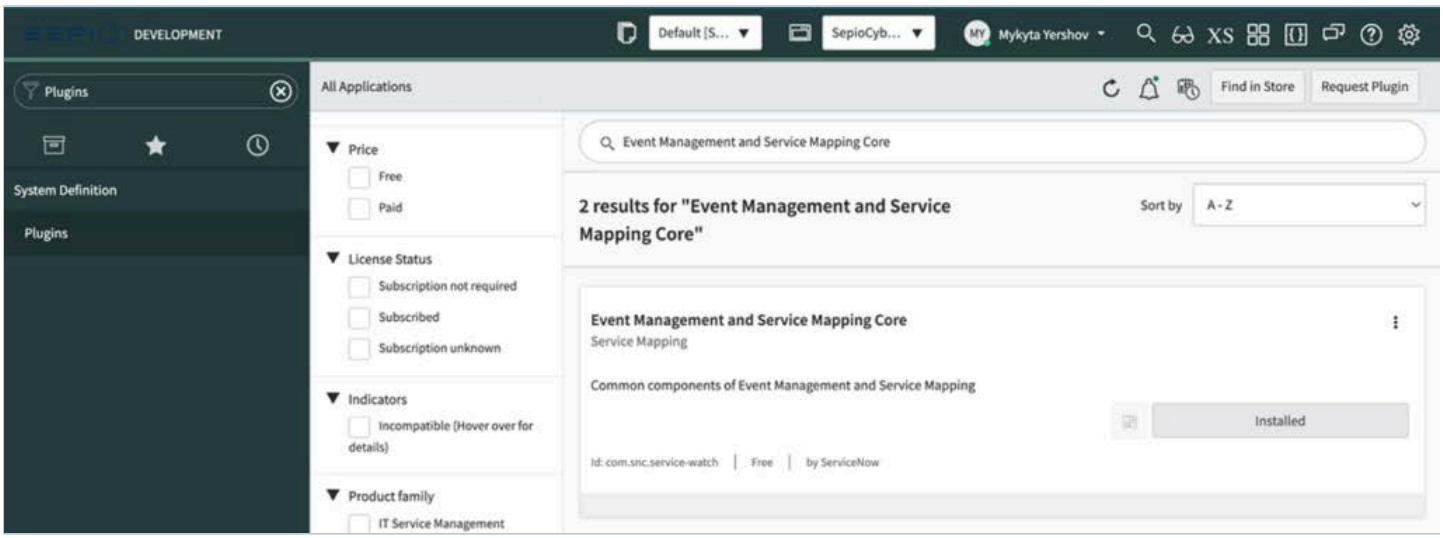



**Event Management Installation guide:**

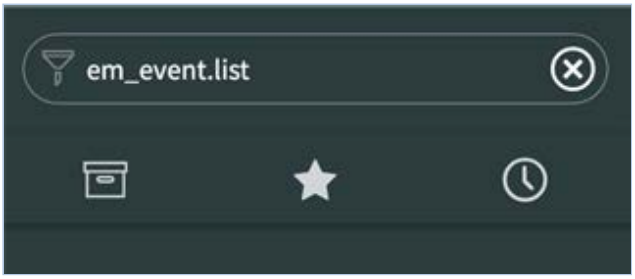
- Ensure that the ServiceNow platform is installed and configured.
- Navigate to Plugins Module.



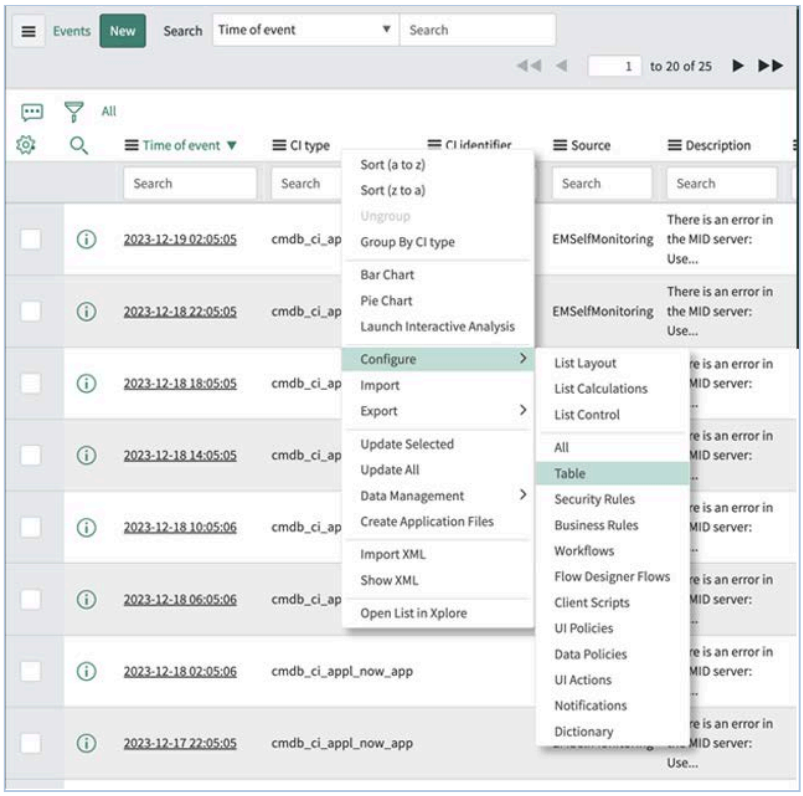

- Search for Event Management and Service Mapping Core plugin.



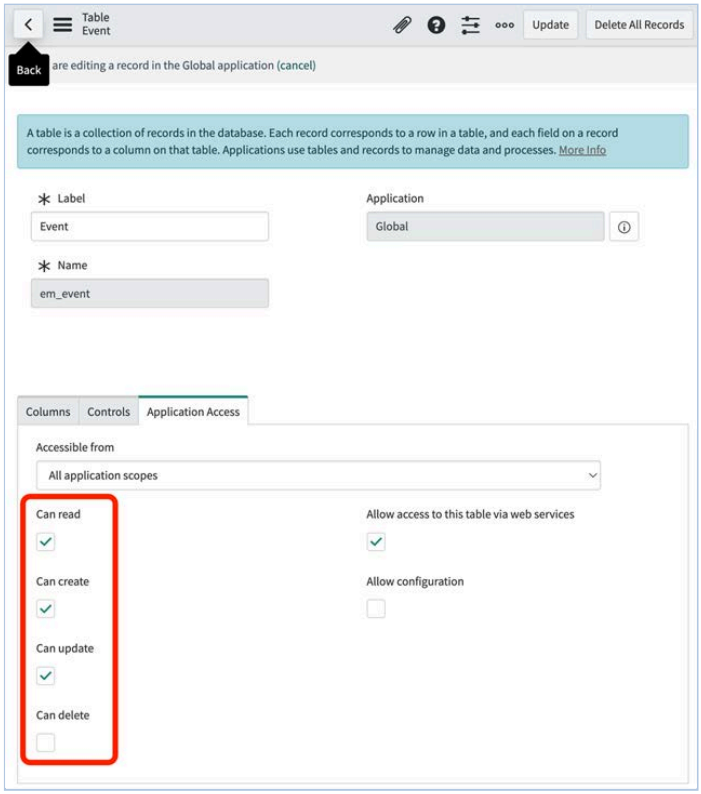

- Click on “Install”.
- Wait until all plugins are installed.
- Navigate to by filter navigator “em_event.list” and press Enter.




- Do right-click on the table columns name and select configure table.




- Ensure that Application Access allows read, create, update operations.



# Lightweight Directory Access Protocol (LDAP)

## Prerequisites

### Software requirements

- **Sepio Platform** installed.
- **Lightweight Directory Access Protocol (LDAP)** service installed.
- A user with at least **read permissions** for the LDAP service.
- **LDAP groups** for Sepio Platform roles (Administrator/Manager/Guest).
- The **root certificate** of the **Certificate Authority (CA)** used by the LDAPs.

## LDAP Configuration

Once configured, LDAP users can log in to the Sepio Platform according to their assigned permissions. The local root Administrator account on the Sepio Platform remains active regardless of LDAP status, while other local users become inactive.

### Steps to Configure LDAP

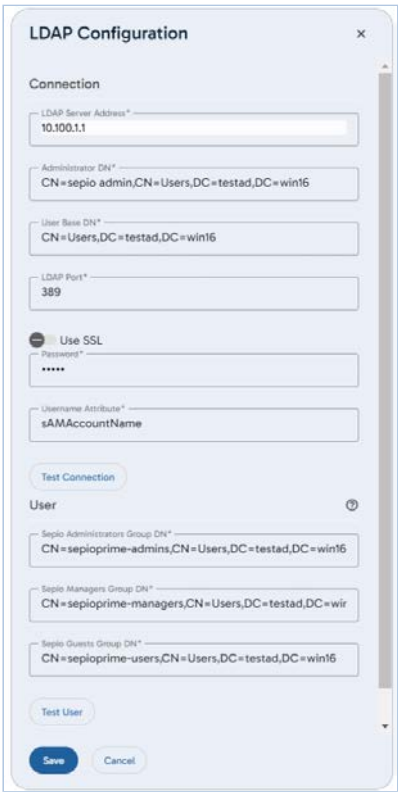
1. **Access LDAP Authentication Settings**
    - Open the Sepio Platform.
    - Navigate to **Settings > Integrations**.
    - Click the **edit** icon next to **LDAP Authentication**.




LDAP Authentication

> **Note:** Settings must be edited before LDAP authentication can be enabled.

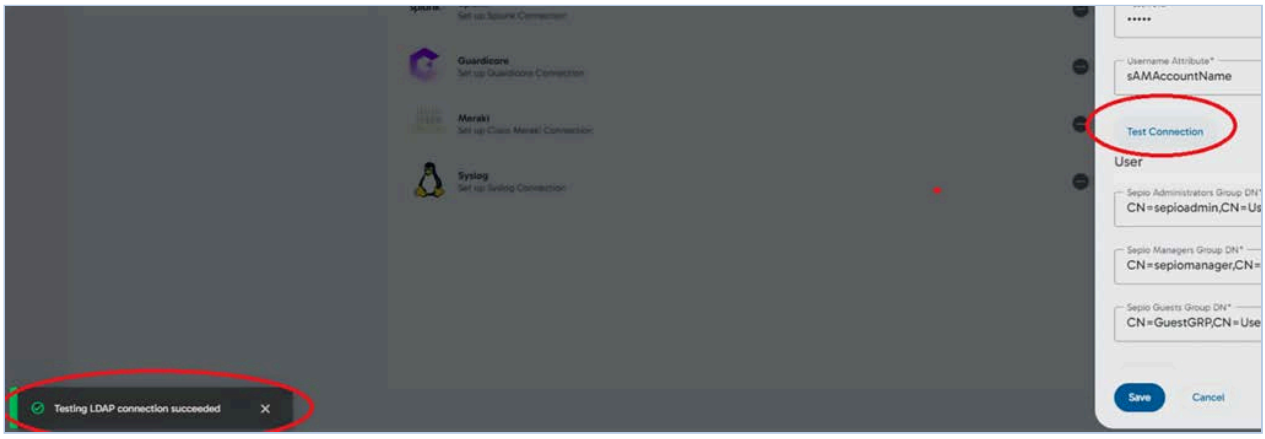
2. **Edit the Parameters**
    - All the fields will be pre-filled except for **LDAP Server address** and **Password**.
    - Edit the default settings as necessary.
    - Refer to the table below for detailed parameter descriptions and requirements.



LDAP Configuration

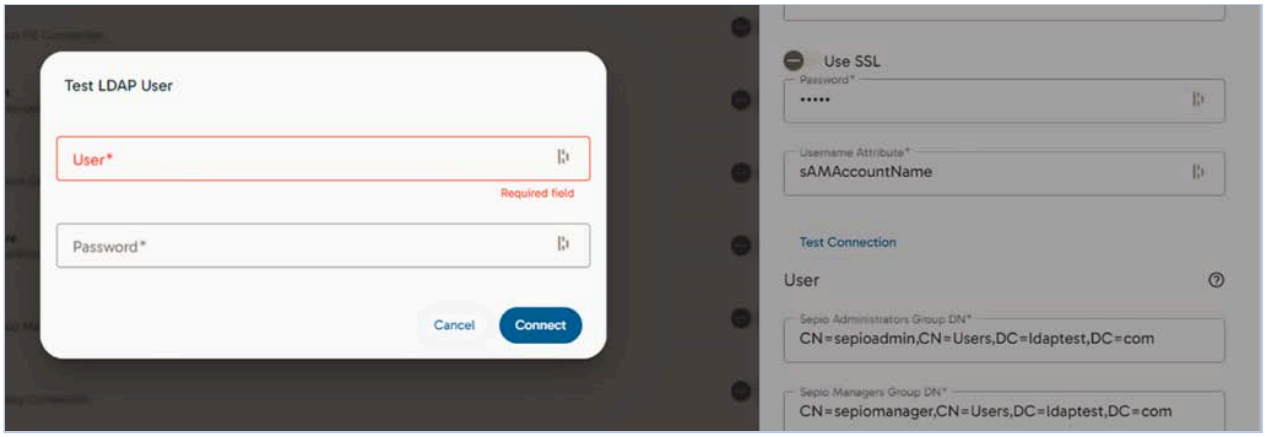
| **Parameters** | **Details** |
|---|---|
| LDAP Server Address | The IP/Server name of the LDAP server |
| Administrator DN | DN of a user that has 'read' permission to the LDAP server |
| Use SSL | Check if LDAPS is required. *** Check the appendix for further information on importing the CA certificate. |
| Users Base DN | Base DN for the users that will be allowed to log in to the Sepio Platform |
| LDAP Port | LDAP connection port (default: LDAP 389, LDAPS 636) |
| Password | Password for the user |
| Username Attribute | The LDAP attribute name of the username that will be used |
| Sepio Administrators Group DN | The LDAP group which its users will be mapped with the Administrator role on Sepio |
| Sepio Managers Group DN | The LDAP group which its users will be mapped with the Manager role on Sepio |
| Sepio Guests Group DN | The LDAP group which its users will be mapped with the Guest role on Sepio |

3. Click on **Test Connection** to test the connection and defined credentials for the LDAP server.



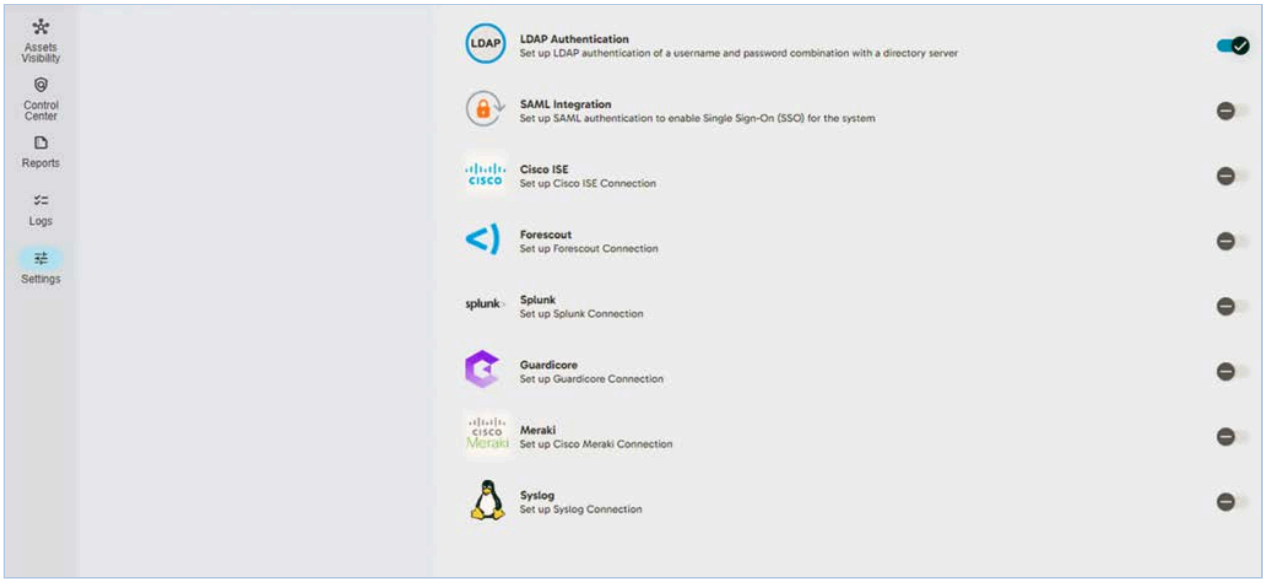

Test Connection

4. Click **Test User** to test authentication for a specific user.




Test LDAP User

5. Set the **Enable LDAP Authentication** radio button to enable, then confirm the notification.

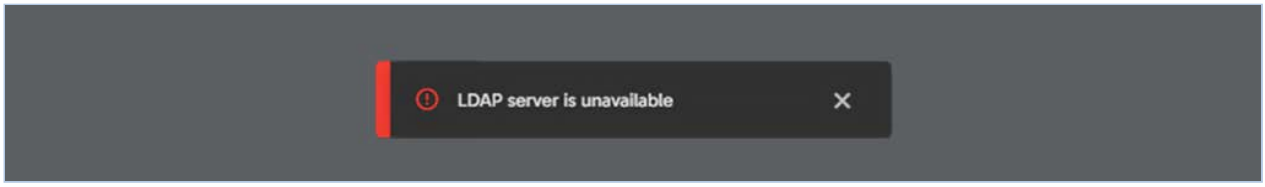



Enable LDAP Authentication

# Troubleshooting

## Error on Test Connection

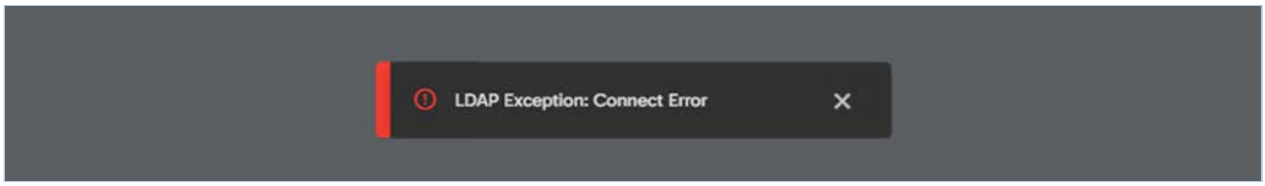
- **Error/Possible cause:** LDAP Server is unavailable.
- **Suggested correction:** Verify that the server address is correct.




LDAP Server is unavailable

### LDAP Exception

- **Error/Possible cause:** LDAP Exception.
  - **Suggested correction:** Verify that the server port is correct.
- **Possible cause:** Server credentials are wrong.
  - **Suggested correction:** Fix the server credentials and ensure the port is correct.




LDAP Exception: Connect Error

### User Test Fail

- **Error/Possible cause:** The tested user credentials are incorrect, or the tested user is not a member of any mapped group.
- **Suggested correction:** Ensure that the tested user is a member of one of the groups defined for mapping.




Testing LDAP user failed

## Importing the LDAP CA Certificate

When using LDAPs, the CA certificate must be imported into the Sepio platform to validate the SSL connection. Follow these steps:

**Note:** The CA certificate file must be base64 formatted. If the certificate is in x.509 format, convert it to .crt format using the following command:

```
openssl x509 -inform PEM -in <your_rootCA_certificate> -out certificate.crt
```

To ensure secure LDAP communication, the platform must trust a custom LDAP certificate. This certificate must be installed in:

1. sepioprime-adminwebapp-1 (for integration and test)
2. sepioprime-auth-1 (for authentication in production)

**1. sepioprime-adminwebapp-1 – Integration/Test Container**

- Step 1: Copy and Update the Certificate
  - `docker cp <certificate.crt> sepioprime-adminwebapp-1:/usr/local/share/ca-certificates/`
  - `docker exec -it sepioprime-adminwebapp-1 update-ca-certificates`
- Step 2: Verify the Certificate Installation
  - `docker exec -it sepioprime-adminwebapp-1 openssl verify /usr/local/share/ca-certificates/<certificate.crt>`

**2. sepioprime-auth-1 – Authentication Container**

- Step 1: Copy and Update the Certificate
  - `docker cp <certificate.crt> sepioprime-auth-1:/usr/local/share/ca-certificates/`
  - `docker exec -it sepioprime-auth-1 update-ca-certificates`
- Step 2: Verify the Certificate Installation
  - `docker exec -it sepioprime-auth-1 openssl verify /usr/local/share/ca-certificates/<certificate.crt>`

# Microsoft Intune

Microsoft Intune can be used to deploy Sepio Host Agents, allowing enterprises to take advantage of their centralized IT operations. This section describes the necessary steps to install Sepio on Windows machines that are managed by Microsoft Intune.

## Steps for Configuration

There are several steps to configure the Sepio Agent software for Intune deployment:

- Download and extract the Intune Win32 Content Prep Tool.
- Run the IntuneWinAppUtil.exe tool and specify the source, setup file, and output folders.
- Save the output file with the .intunewin extension.
- Add the App to Intune by selecting Windows App (Win32) as the App type.
- Browse and select the .intunewin file.
- Enter the app information, including publisher, category, show as featured App, and logo.
- Click Next and continue through the Program information, Requirements information, and Detection rules sections.
- For Assignments, use a pilot group for initial deployment and set Required to All devices and Available for enrolled devices to All Devices.
- Click Review + create and then Create.

## Convert Win32 App content for upload

#### 1. Download and Extract the Tool

- Download the Microsoft Win32 Content Prep Tool ZIP file
- Extract the content to C:\IntuneApp

#### 2. Create Required Folders

- Create the following folders on drive C:\
  - C:\IntuneAppInput
  - C:\IntuneAppOutput

#### 3. Run the Intune Package Prep Tool in CMD

- C:\IntuneApp>IntuneWinAppUtil.exe
- When prompted, provide the following information:
  - **Source folder:** `C:\IntuneAppInput`
  - **Setup file:** `SepioAgent_Win_64_00.000.00.msi`
  - **Output folder:** `C:\IntuneAppOutput`

- **Catalog folder:** N (No)

#### 4. Save the Output File

- File extension should be – SepioAgent_Win_64_00.000.00**.intunewin** (number will identify the Sepio Agent version).

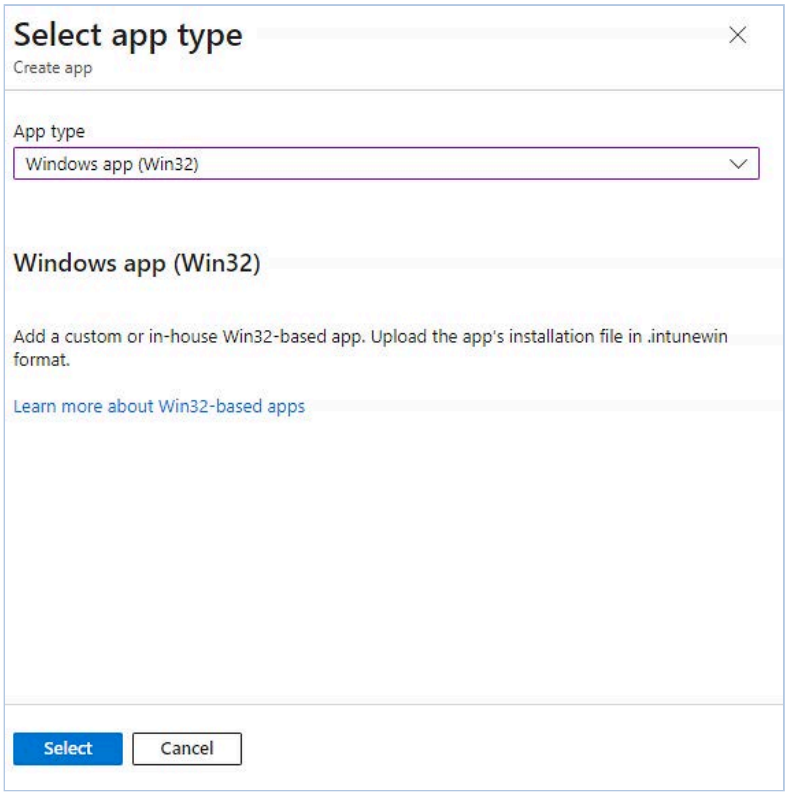
## Add App to Intune

#### 1. Sign in to the Microsoft Intune

- Microsoft Intune Admin Center
- Navigate to **Apps > All apps > Add.**

#### 2. Select App Type

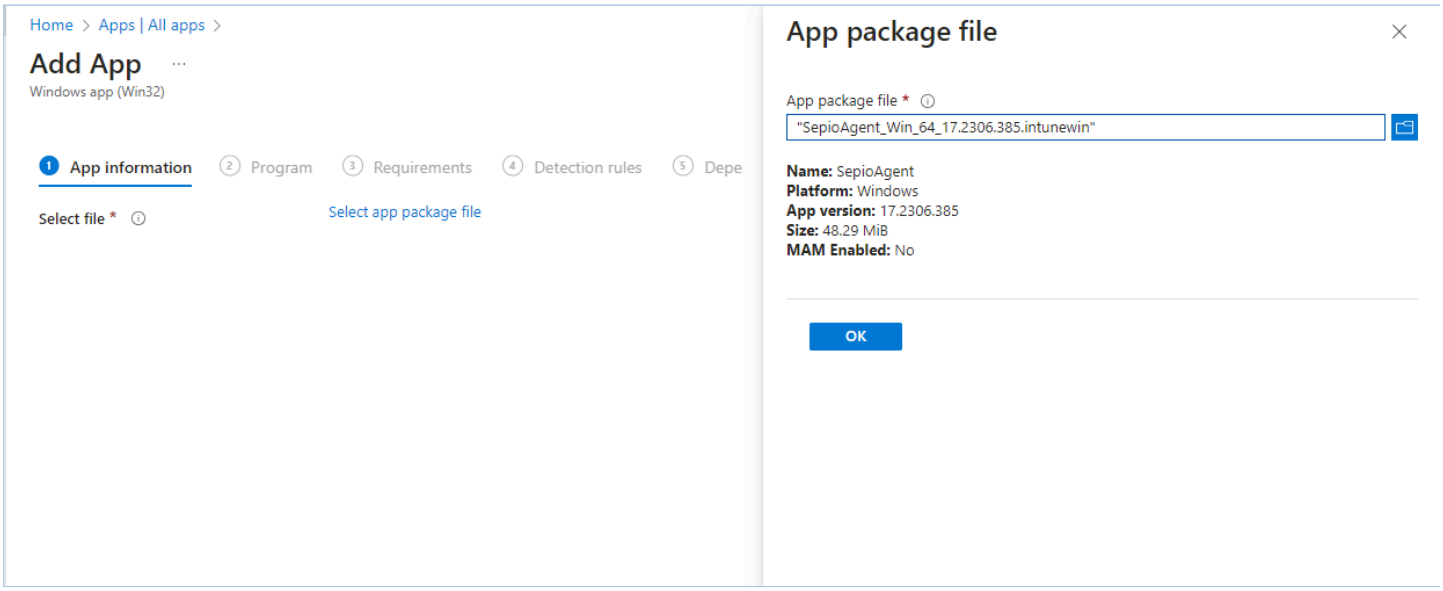
- Under “Other app types,” select **Windows app (Win32)** and click **Select.**




Select Windows app (Win32).

#### 3. Upload App Package

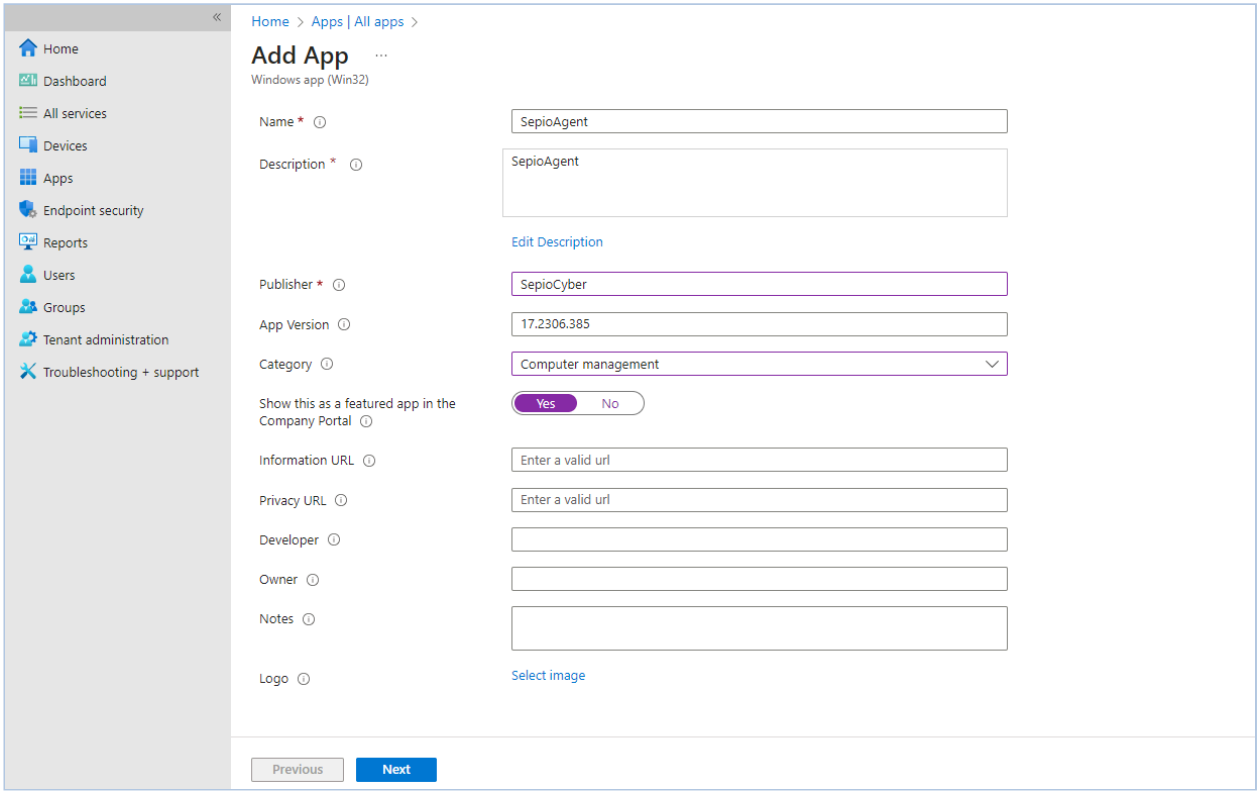
- On the Add app pane, click **Select app package file.**
- Select the **C:\IntuneAppOutput\SepioAgent_Win_64_00.000.00.intunewin** file.
- Confirm by clicking **OK.**




On the App package file pane, select C:\IntuneAppOutput\SepioAgent_Win_64_00.000.00.intunewin

## 4. Set App Information

- **Publisher:** Enter “SepioCyber”.
- **Category:** Select “Computer management” (or any category according to your organization policy).
- **Show this as a featured app in the Company Portal:** Yes.
- **Logo:** Upload Sepio logo.
- Click **Next.**

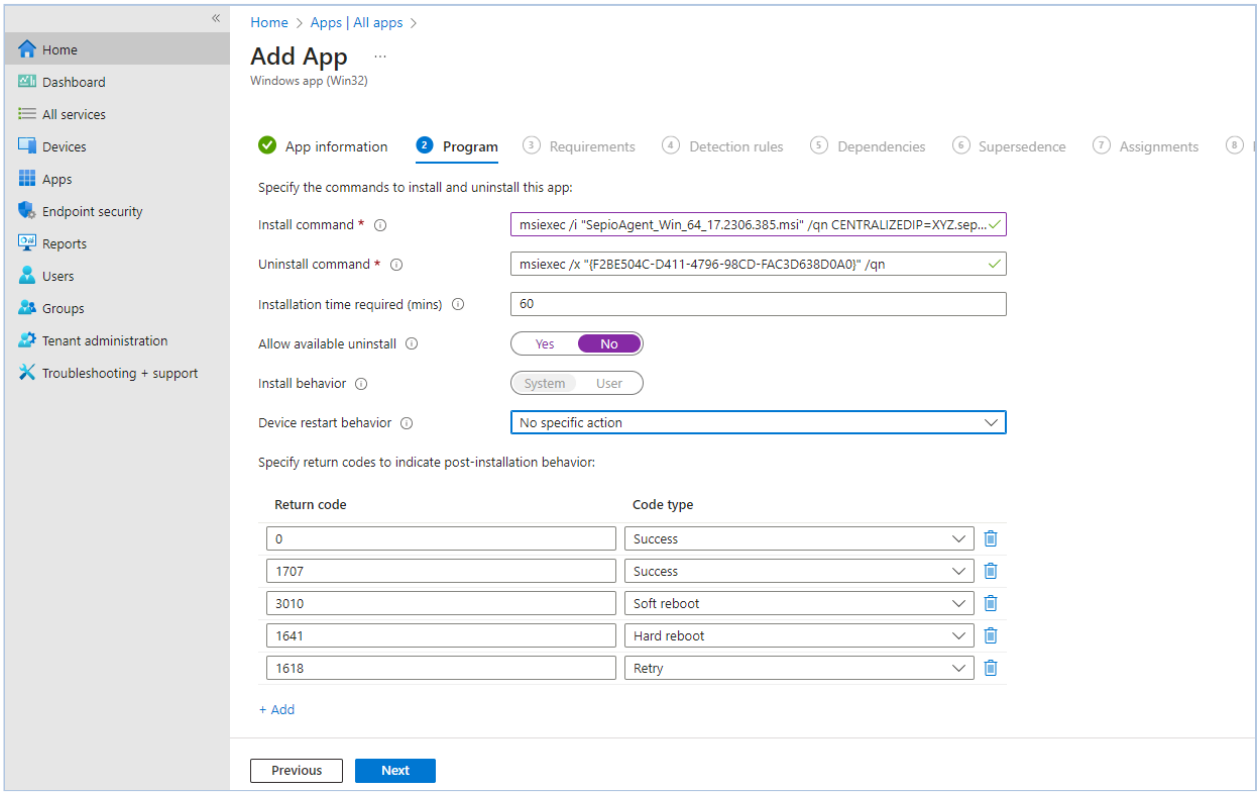



Set App information

## 5. Program Information

- **Install command:** At the end of the line, add: `CENTRALIZEDIP=<Sepio Managment Portal FQDN>`

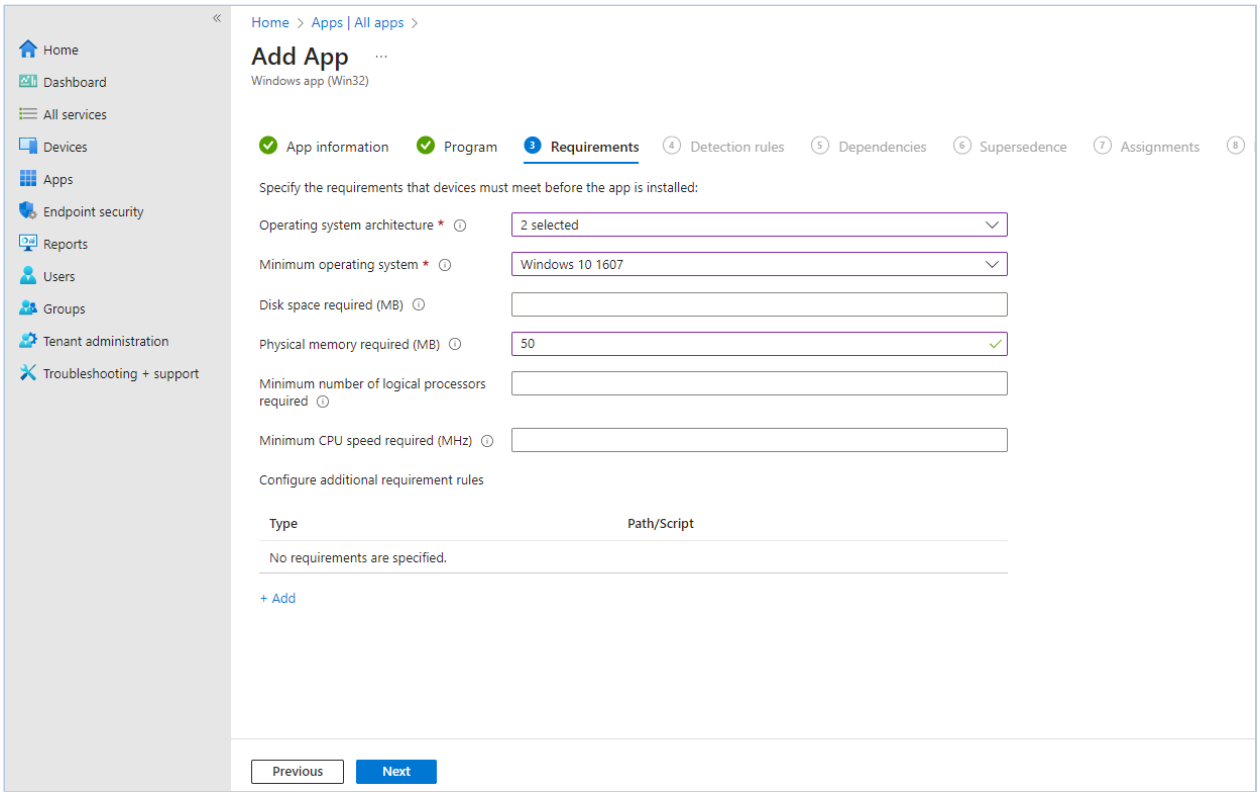
- **Uninstall command:** No change
- **Allow available uninstall:** Select No
- **Device restart behavior:** Select No specific action
- Click **Next.**




Set Program information

## 6. Requirements Information

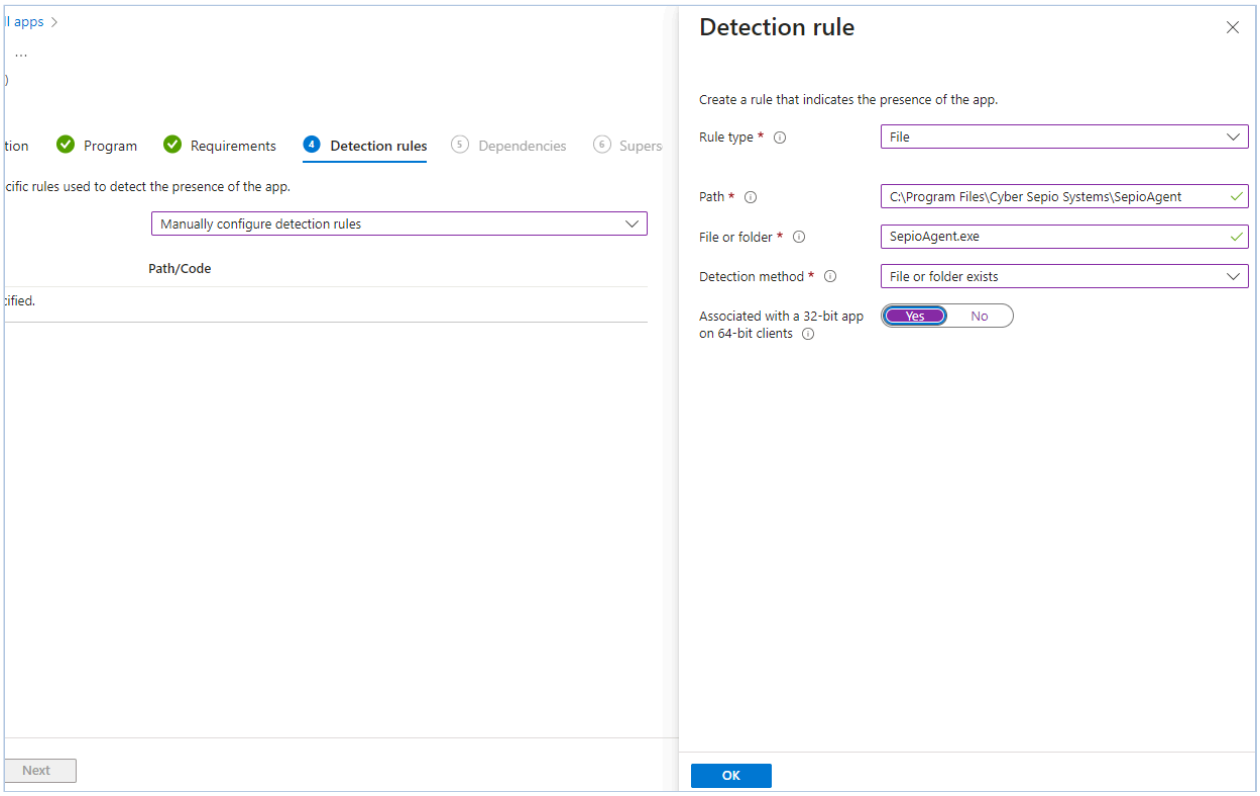
- **Operating system architecture:** Select both 32bit and 64bit.
- **Minimum operating system:** Select Windows 10 1607.
- **Physical memory required (MB):** 50MB.
- Click **Next.**



Set Requirements information

## 7. Detection Rules

- **Rules format:** Select “Manually configure detection rules”.
- **Add new Detection rule:**
  - **Type:** File or folder.
  - **Path:** C:\Program Files\Cyber Sepio Systems\SepioAgent.
  - **File:** SepioAgent.exe
  - **Detection method:** File or folder exists.
  - **Associated with a 32-bit app on 64-bit client:** Yes.
- Click **Next.**



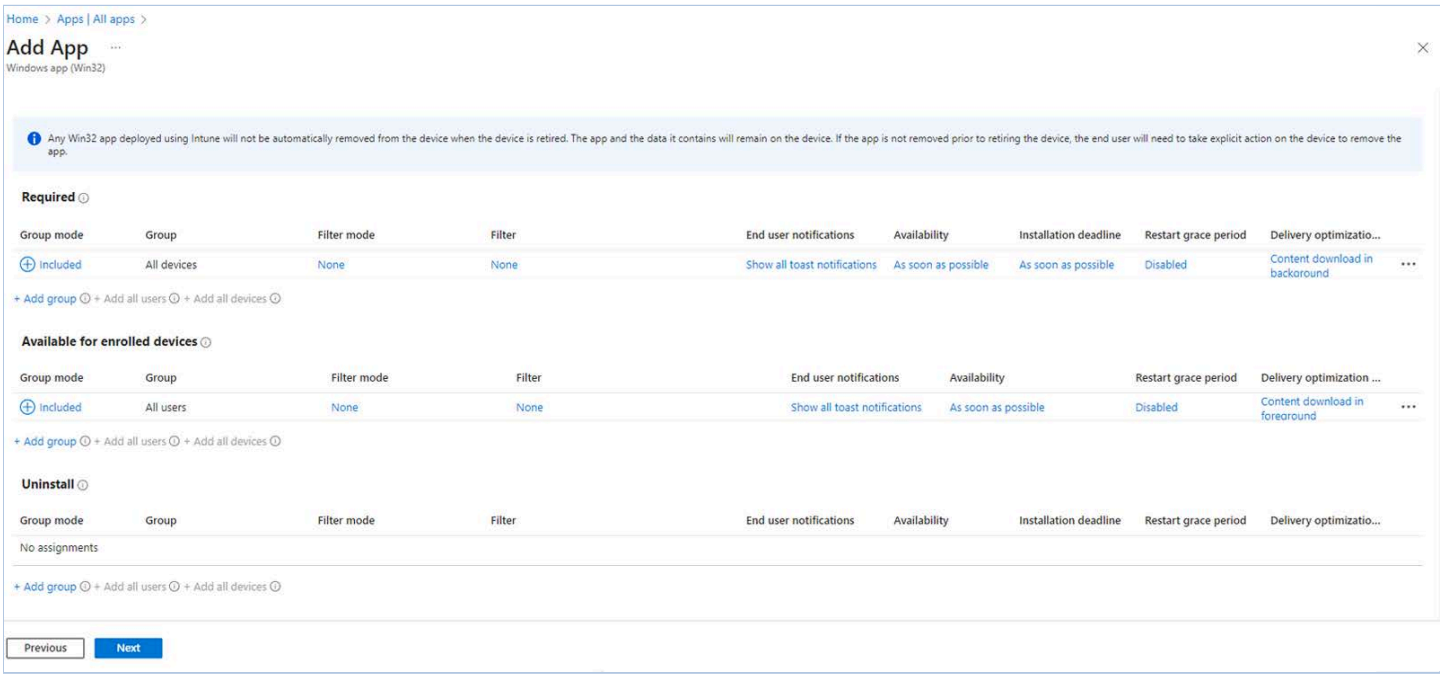
Set Detection rules

**8. Dependencies:** No change.

**9. Supersedence:** No change.

**10. Assignments**

- For initial deployment, use a pilot group to minimize impact.
- **Required:** All devices.
- **Available for enrolled devices:** All Users.
- Click **Next.**




Set Assignments

## 11. Review and Create

- Review your settings and click **Create.**

# Network HTTP Proxy

## Overview

Network HTTP proxy support was initially developed to enhance secure and controlled access to the Meraki Cloud through security gateways. This capability allows a Scan Engine running as either an Internal or External Scan Engine, to communicate with the Meraki API on Meraki Cloud, while utilizing a proxy to ensure secure and controlled communication when needed.

## Proxy Configuration Options

There are two configuration options available for setting up proxy communication:

1. **Proxy without Credentials**
   Allows the Scan Engine to communicate with the Meraki Cloud through a proxy that does not require authentication.
2. **Proxy with Credentials (Username and Password)**
   Enables communication through a proxy that requires authentication.

### Proxy without Credentials Configuration Details

To enable this feature, add the following configuration settings to the Scan Engine configuration file located at `/etc/systemd/system/netpoller.service`

1. **ENABLE_PROXY_MERAKI**
   - **Type:** Boolean (true / false)
   - **Purpose:** This flag determines whether communication between the Scan Engine and the Meraki API should occur through a proxy.
   - **Default Value:** false
   - **Example Usage:**
   - `Environment="ENABLE_PROXY_MERAKI=true"`

2. **PROXY_ADDRESS_MERAKI**
   - **Type:** String (URL or IP address)
   - **Purpose:** Specifies the address of the proxy server through which the Scan Engine will route its communication with the Meraki API.
   - **Example Usage:**
   - `Environment="PROXY_ADDRESS_MERAKI=http://192.168.1.100:8080"`

3. **Apply Configuration**
   - **Restart the Scan Engine Service**: After making changes to the configuration file, restart the Scan Engine service for the new settings to take effect. Use the following command to restart

the service:

- **Command:**
- `systemctl daemon-reload`
  `sudo systemctl restart netpoller`

### Proxy with Credentials Configuration Details

1. **Call UpdateMerakiProxy netsAPI endpoint for saving proxy credentials:**
   - `docker exec -it sepioprime-netsapi-1 curl -X POST "http://netsapi:5125/prime/netsapi/UpdateMerakiProxy" -H "Content-Type: application/json" \ -d '{"username":"<USER_NAME>", "password":"<PASSWORD>", "address":"http://<HOST>:<PORT>"}'`
   - If all details have been entered and saved, you should get **credentials saved** message.
   - **Example Usage:**
   - `docker exec -it sepioprime-netsapi-1 curl -X POST "http://netsapi:5125/prime/netsapi/UpdateMerakiProxy" -H "Content-Type: application/json" \ -d '{"username":"Sepio", "password":"123", "address":"http://192.168.1.100:8080"}'`
   - Add the following configuration settings to the Scan Engine configuration file located at `/etc/systemd/system/netpoller.service`
2. **ENABLE_PROXY_MERAKI**
   - **Type:** Boolean (true / false)
   - **Purpose:** This flag determines whether communication between the Scan Engine and Meraki API should occur over a proxy.
   - **Default Value:** false
   - **Example Usage:**
   - `Environment="ENABLE_PROXY_MERAKI=true"`
3. **Apply Configuration**
   - **Restart the Scan Engine Service:** After making changes to the configuration file, restart the Scan Engine service for the new settings to take effect. Use the following command to restart the service:
   - **Command:**
   - `systemctl daemon-reloadsudo systemctl restart netpoller`

# Splunk Integration

Sepio Add-On for Splunk allows customers with joint Splunk and Sepio deployments to receive Syslog events from Sepio Platform. The add-on is available for download from Splunk Base. This add-on is supported by Sepio. It is possible to collect events and audit feeds from multiple Sepio Platforms into a single Splunk instance.

> **Note:** Always use the latest version of the Splunk Application add-on. Download and install the add-on, then perform the configuration tasks.

## Splunk Add-on for Sepio Installation

### Prerequisites

1. Splunk 8.2 or higher.
2. Sepio account and host URL. Please contact Sepio support for the details.
3. Create indexes to store the Sepio logs (default is main).

### Upgrade Instructions

When you currently have an input configured, follow these steps to upgrade from version 2:

1. Disable all inputs (to avoid errors being logged in **_internal**).
2. Follow Splunk best practice and upgrade the TA via UI or CLI (Splunk Enterprise only).
3. After the upgrade, under the configuration tab, configure the account in the Sepio platform and save.
4. Navigate to the original inputs tab and edit your input. (Select the Sepio platform to use and the log type).
5. **Save** and **re-enable the input**.

### New Installation Instructions

#### Via UI

1. Search for the Sepio Systems add-on for Splunk by clicking on **Apps**->**Find More Apps** in in your Splunk GUI or browse to https://<Your Splunk Server>:8000/en-US/manager/system/appsremote.
2. Perform a search for “Sepio”, and the Sepio Systems add-on for Splunk will be displayed in the results.
3. Click “Install,” and complete the displayed dialog.
4. After installation is complete, you will be prompted to restart your Splunk server. Click **Restart Now**
5. or **Restart Later** depending on your preference. Continue with the configuration steps once the restart is complete.

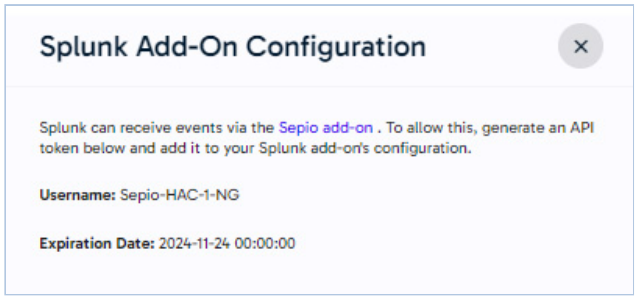
6. Login into the Splunk UI. You will see the Sepio Systems add-on for Splunk listed in the **Apps** menu.

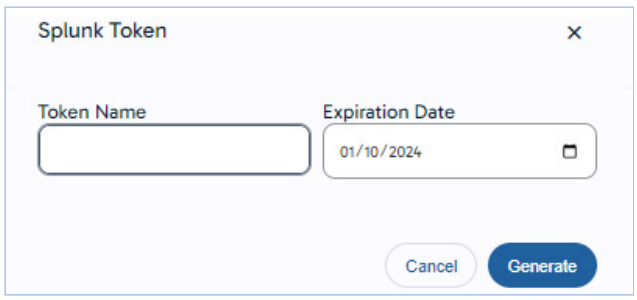
**Via CLI (Splunk Enterprise only)**

1. Find the Sepio Systems add-on for Splunk on Splunkbase.
2. Uncompress the file in **$SPLUNK_HOME/etc/apps/**.
3. Restart the Splunk instance.
4. See Splunk docs for further details on add-on installations.
5. For Splunk Search Head Clusters/ Distributed Environment Installation, refer to Splunk docs.

**To Configure the Splunk Integration:**

1. Open the Integration View.
2. Enable the Integration.
3. Generate an API token. You must define a name and the expiration date.




**Note:** Once you exit this window, it is impossible to retrieve the generated token. It is recommended to immediately **copy the token** into the Splunk Add-on and refrain from saving it in any other location.

## Sepio Add-on for Splunk Configuration

The following instructions use screenshots from **Splunk Cloud**, but the procedure is the same for **on-premises** installations of Splunk.

### Step 1: Create a New Index

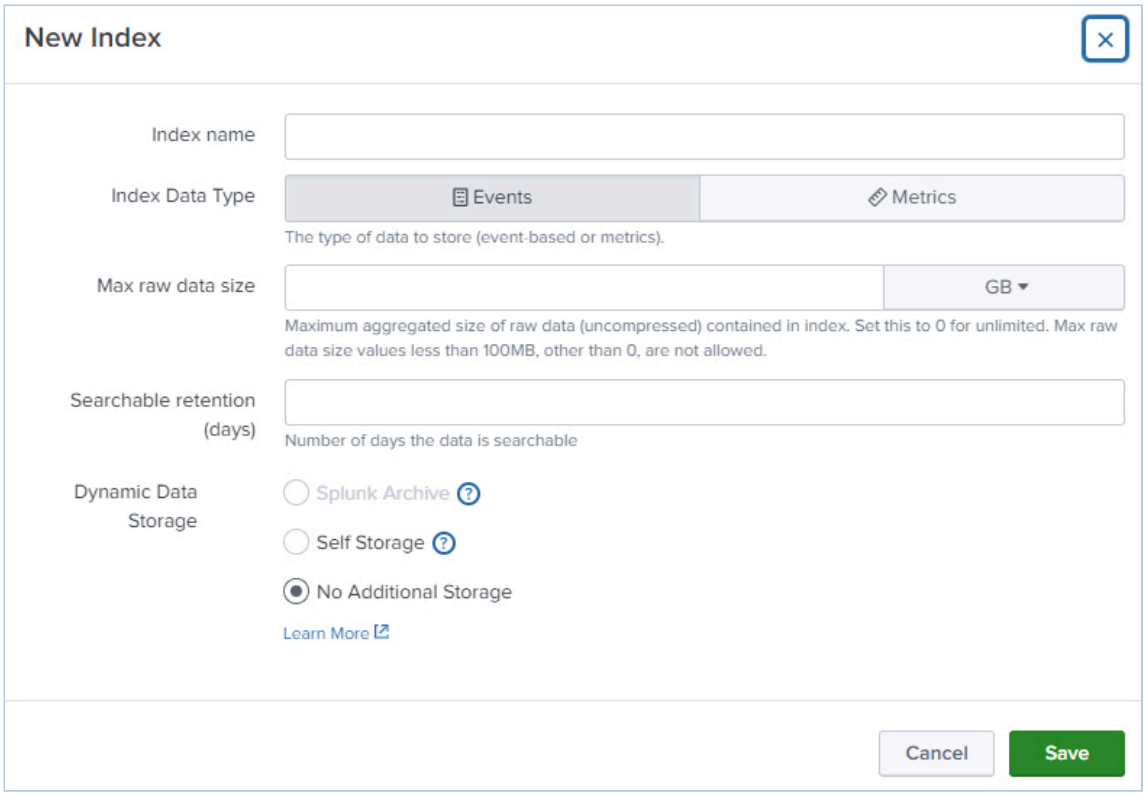
If no index exists, you must create one before configuring the Sepio inputs.

1. Go to **Settings > Data > Indexes.**
2. Click the **New Index** button (green) in the top-right corner.




Add New Index

3. Fill in the following fields:
    - **Index Name**
    - **Maximum raw data size**
    - **Searchable retention**
4. Click **Save.**
5. Ensure the new index is **enabled** under the **Status** column.



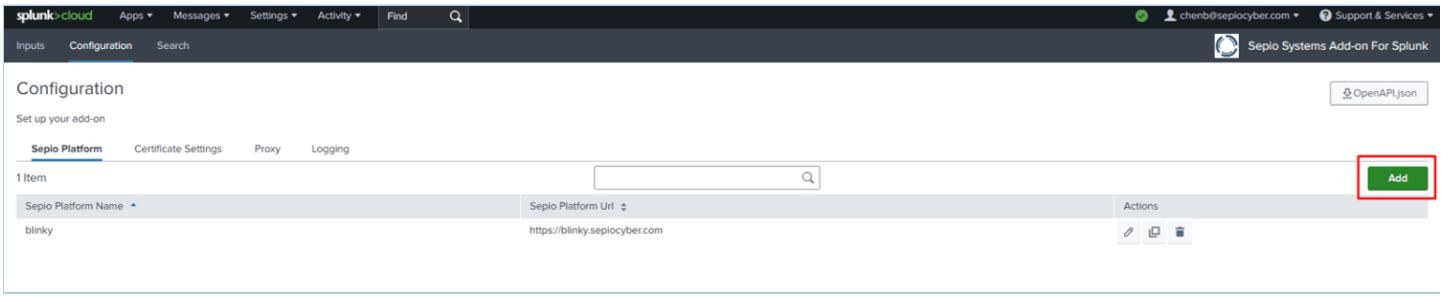

Add New Index

### Step 2: Add Sepio Platform Configuration

Before creating any input, you must first configure the Sepio Platform:

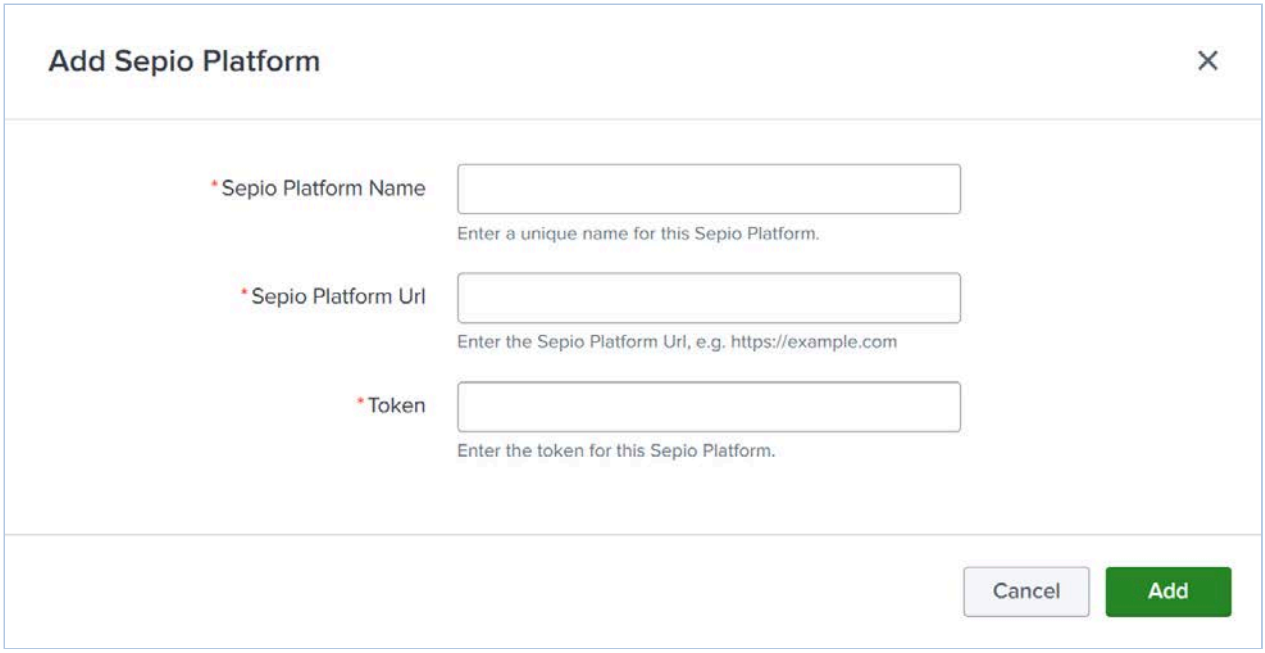
1. Click on the **Configuration** tab in the **Sepio Systems Add-on for Splunk.**

2. In the **Sepio Platform** section, click **Add.**




Add Sepio Platform Configuration

3. Provide
    - A **name** for the platform
    - The **Sepio platform URL**
    - The **token** from the Sepio instance (under Splunk integration settings)
4. Click **Add** to save the platform.

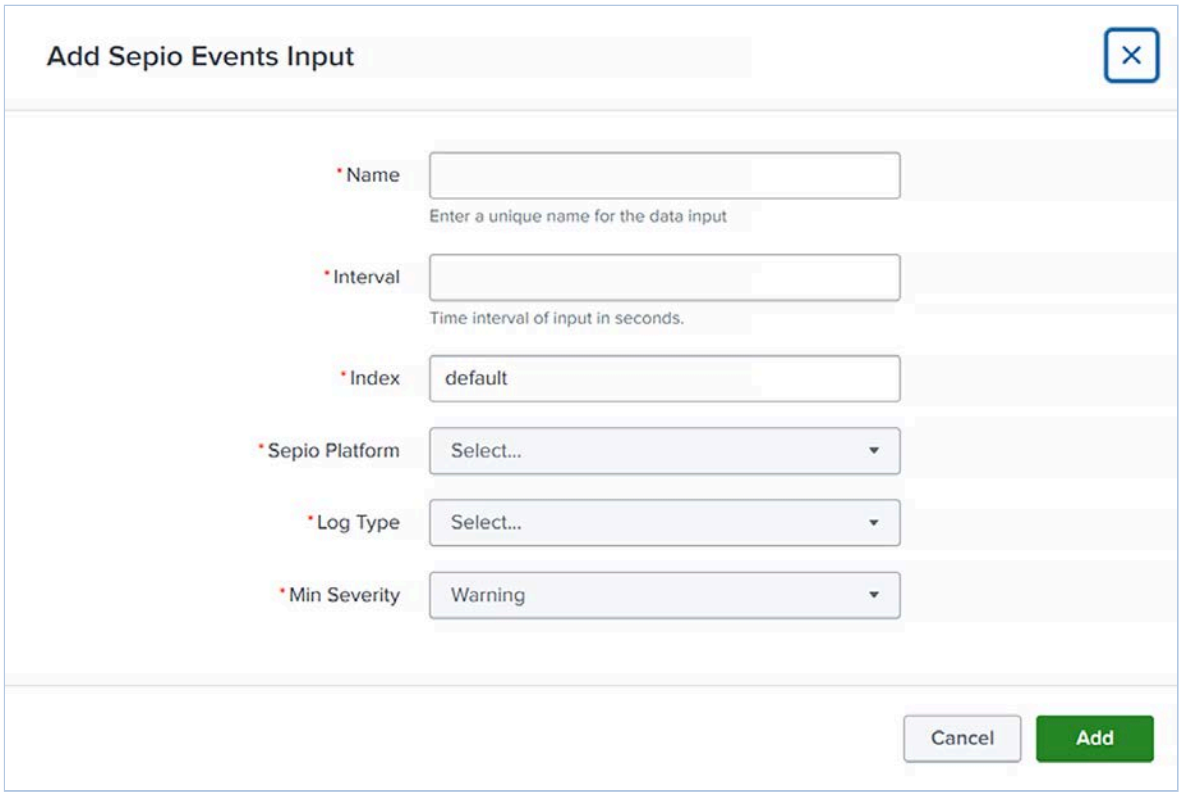



Add Sepio Platform Configuration

### Step 3: Create Data Inputs

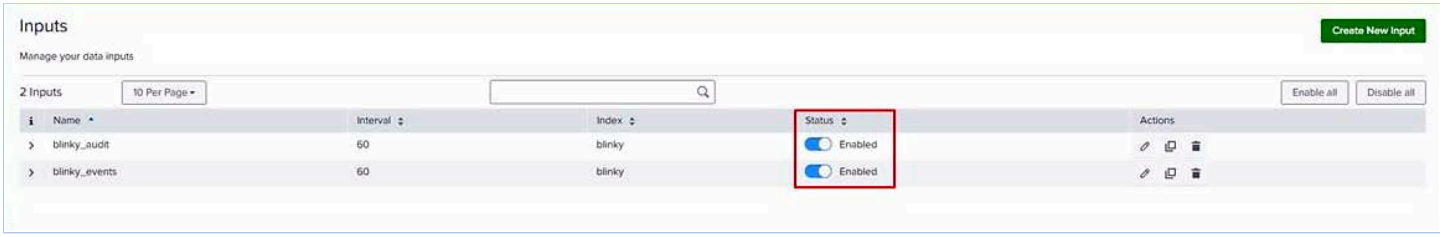
1. Go to the **Inputs** tab.
2. Click the **Create New Input** button (green, upper right).
3. Fill out the form:
    - **Input Name**
    - **Interval**
    - Select the **index** created earlier
    - Select the **Sepio platform** added in Step 2
    - Choose **Log Type:** *Events* or *Audit*
    - Set the **Minimum Security Level**

**Note:** You can create one input for events (i.e. _events) and one input for audit logs (i.e. _audit).




Add Sepio Events Input

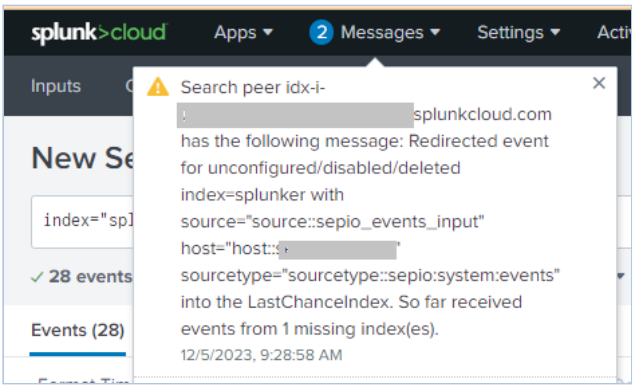
4. Click **Add.**
5. Verify that the inputs are **enabled.**



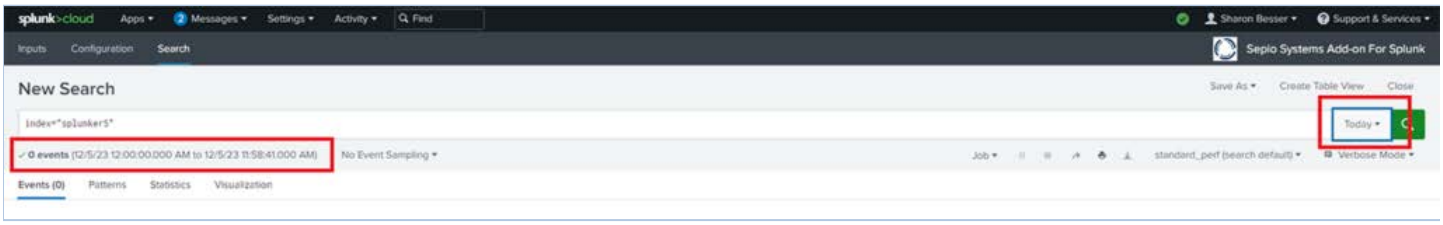

- Under the **Proxy** tab, you can enable a proxy if needed, fill out the relevant information and click on the green **Save** button.
- Under the **Logging** tab, the add-on application log level can be set (Debug, Info, Warning, Error, or Critical). Select the necessary level and click the green Save button to confirm your choice.

## Splunk Add-on Tips

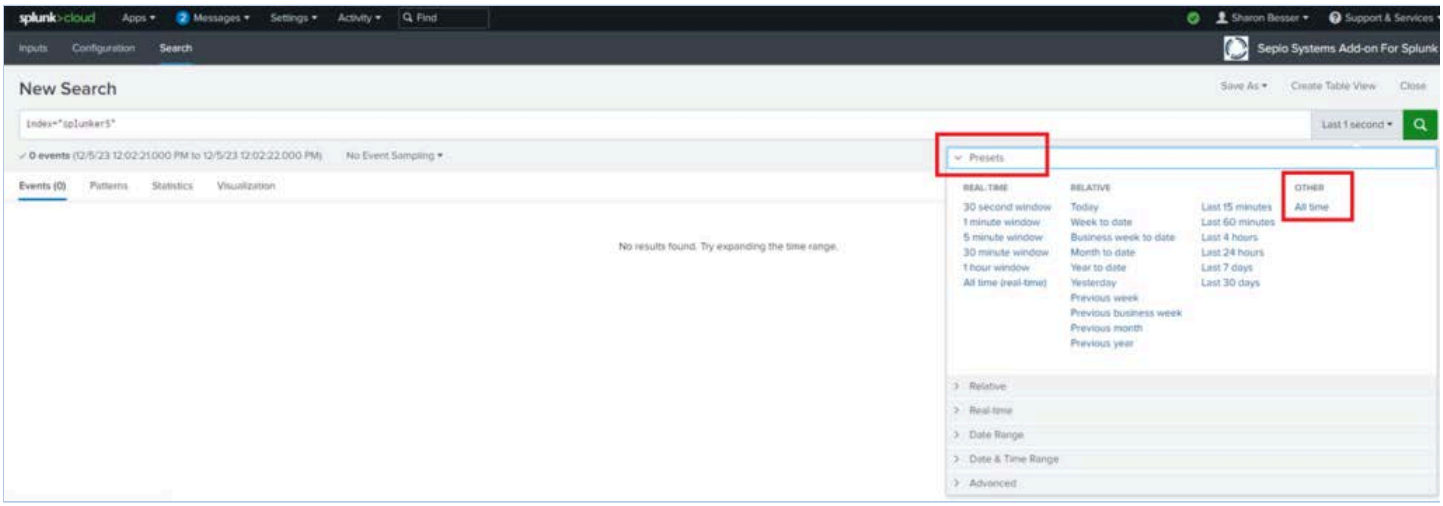
1. Check for any error in the Splunk messages tab. Here for example, I can see that events are received from the host, however there's an issue with the index.



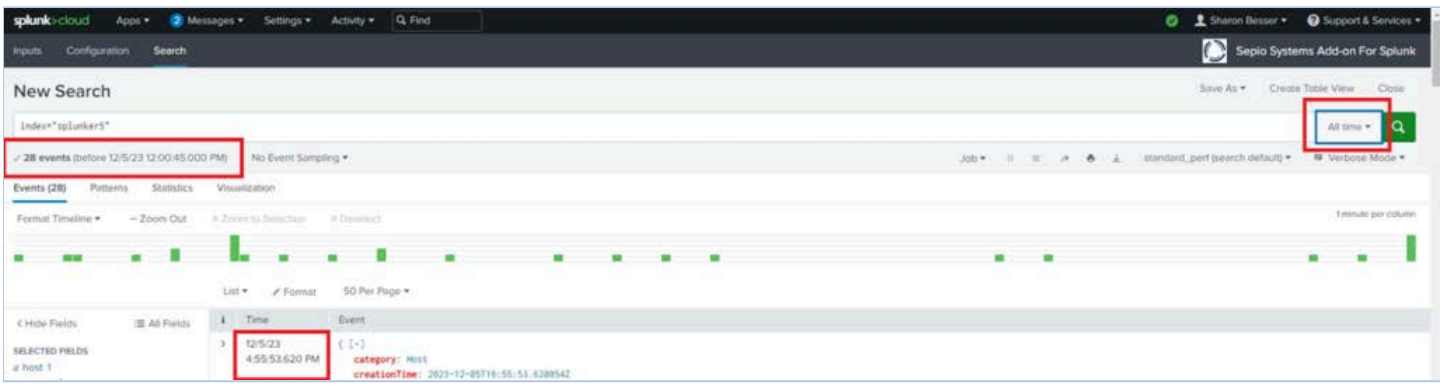

2. When creating a new index and using preset Splunk timers, sometimes Splunk will present 0 events when choosing recent timers. This issue might have to do time synchronization.




3. To validate that indeed Splunk is receiving and storing Sepio events, choose ‘All time’:




4. To view today’s events and then make sure that the clocks are synchronized.



# Splunk Add-on Troubleshooting

### General

One can view the add-on application logs from within Splunk by using the Splunk Search function with the following index.

```
index="_internal" sourcetype="tasepiosystemsaddonforsplunk:log"
```

### Splunkcloud and Sepio Platform SSL Certificate

If the following error is noticed in the logs, the issue may be an incorrectly installed SSL certificate on the Sepio server.

certificate verify failed: unable to get local issuer certificate

The error indicates an SSL certificate installed on the Sepio server without the root certificate as part of the certificate file. You can test this with the following OpenSSL command:

```
openssl s_client -connect example.sepio.systems:443
```

To resolve this issue, reinstall the SSL certificate on the Sepio Platform's server, including the root certificate as part of the chain.

### Splunk Local Certificates

If you have installed Splunk on-premises, you may also find the following error appearing:

certificate verify failed: unable to get local issuer certificate

Suppose you are using a third-party or self-signed certificate and receiving this error. In that case, the Python module certificate used in the Sepio Splunk Add-on does not have the root certificate as part of its trusted bundle. To resolve this issue, please ensure you run the latest version of the Sepio Splunk Add-on and add the root CA, internal or otherwise, to the bundle. The bundle that needs to be updated exists in the following location:

```
$SPLUNK_HOME/etc/apps/TA-sepio-systems-add-on-
forsplunk/bin/ta_sepio_systems_add_on_for_splunk/aob_py3/certifi/cacert.pem
```

For instance, in a typical Linux installation, '/opt/splunk/' would be the $SPLUNK_HOME:

```
/opt/splunk/etc/apps/TA-sepio-systems-add-on-
forsplunk/bin/ta_sepio_systems_add_on_for_splunk/aob_py3/certifi/cacert.pem
```

The file can be manually appended to, or with appropriate permissions you may be able to append it via the command line:

```
cat path/to/rootCA.crt >> $SPLUNK_HOME/etc/apps/TA-sepio-systems-add-on-forsplunk/bin/ta_sepio_systems_add_on_for_splunk/aob_py3/certifi/cacert.pem
```

> **Note:** Once the cacert.pem file has been updated with the new certificate, a restart of Splunk is not required.

### Proxy Error Messages

Splunk PersistentScript error for proxy password might appear even if no Proxy configuration was created or saved.

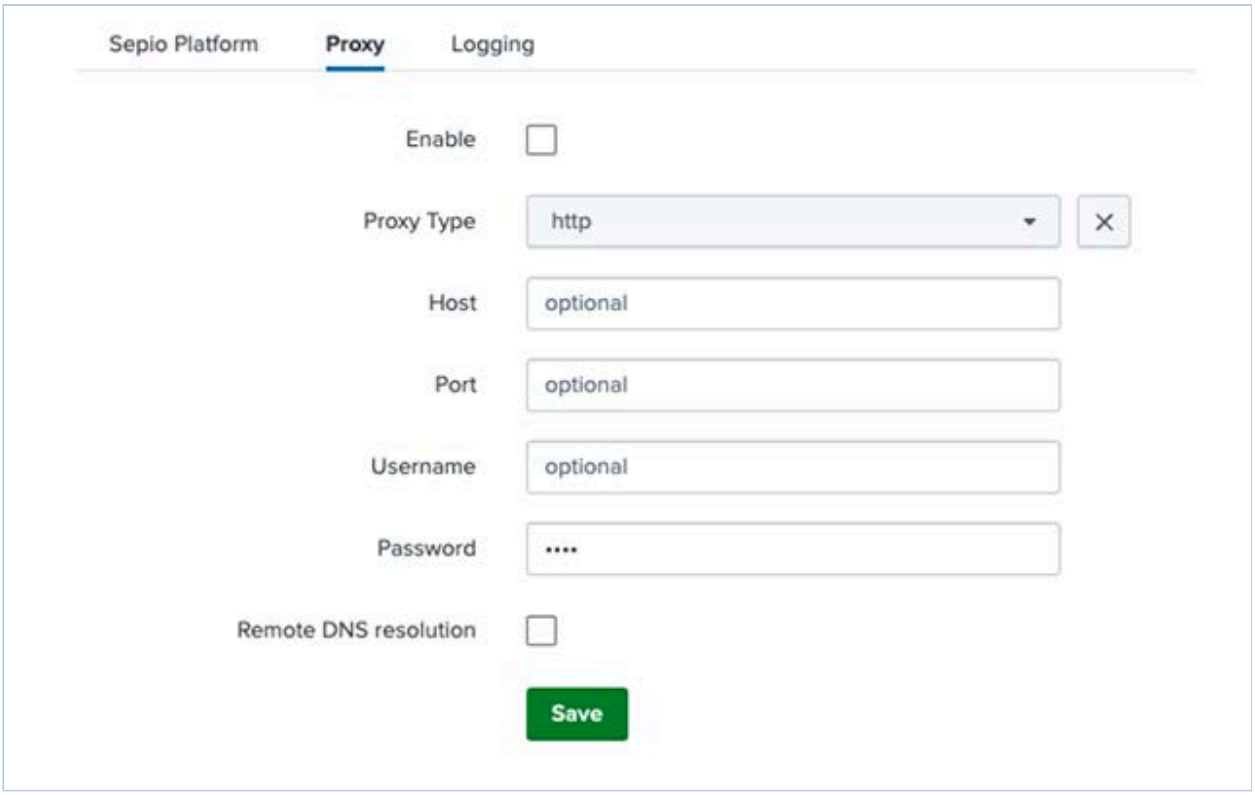
In this case, the following error message would appear in the logs.

```
01-15-2024 13:07:01.818 +0200 ERROR PersistentScript [137243 PersistentScriptIo] - From {/Applications/Splunk/bin/python3.7 /Applications/Splunk/etc/apps/TA-sepio-systems-add-on-for-splunk/bin/TA_sepio_systems_add_on_for_splunk_rh_settings.py persistent}: solnlib.credentials.CredentialNotExistException: Failed to get password of realm=__REST_CREDENTIAL__#TA-sepio-systems-add-on-for-splunk#configs/conf-ta_sepio_systems_add_on_for_splunk_settings, user=additional_parameters.
```

### Fixing the issue

Via UI

1. Navigate to the Proxy tab in the Configuration page.
2. Enter None in the Password text box.
3. Click Save.




Proxy tab

### Via CLI (Splunk Enterprise only)

1. Edit the file:

   `$SPLUNK_HOME/etc/apps/TA-sepio-systems-add-on-forsplunk/local/ta_sepio_systems_add_on_for_splunk_settings.conf.`
2. Add the following stanza to the file:

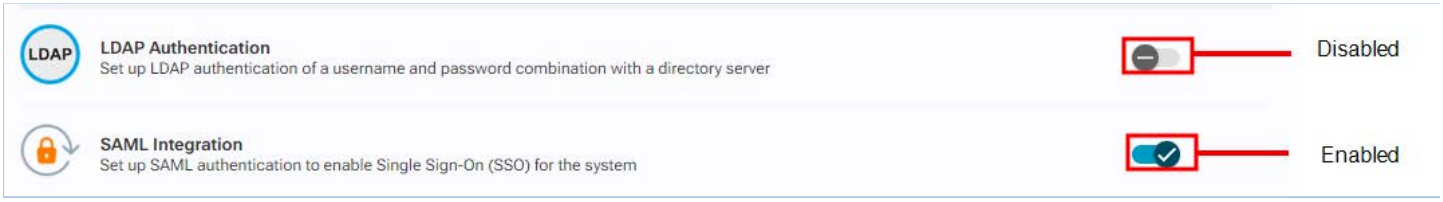
   ```
   proxy_password = None
   ```
3. Save the file.

# Enabling and Disabling Integrations

You can enable or disable integration connections from the **Integration View**.

## Steps to Enable or Disable Integrations

1. From the **Sepio menu**, select **Settings** -> **Integration**.
2. Locate the configured integration you want to modify.
3. Select the option to **enable** or **disable** the integration.
    - The integration's status will be updated accordingly.




Enable or disable the integration

## Best Practices

The purpose of implementing best practices is to streamline the configuration process, enhance reliability, and achieve consistent results, ultimately contributing to a successful and secure network environment.

## Related Topics

- Managing Network Infrastructure
- Host Agent Best Practices
    - Policy Management Best Practices
- Frequently Asked Questions (FAQ)

# Managing Network Infrastructure

## Overview

Best practices for configuring Scan Engines and adding network elements to the Sepio Platform are designed to create a structured, efficient approach that minimizes errors and ensures optimal performance. By following these guidelines, organizations can avoid common pitfalls, enhance security posture, and maintain a well-functioning system.

See the configuration steps here: Network Infrastructure Management.

## Using Multiple Scan Engines for the Same Domain

It is recommended to use multiple Scan Engines for the same domain to improve availability and performance. Having more than one Scan Engine allows you to perform gradual upgrades, validate different configurations, and run different tests.

When adding the first switches to the Sepio Platform, it is best to keep only one Scan Engine in **Active** mode and set the others for that domain to **Deactivated** mode.

## Adding the First Network Infrastructure Element Manually

> **Note:** When adding the first network infrastructure element, follow these steps:

1. If multiple Scan Engines are configured for a domain, make sure that only one is activated.
2. Make sure that the Scan Engine is at the desired version.
3. Confirm SSH connectivity between the Scan Engine server and the target device. In addition to using the ping command, try to SSH into the device and ensure you receive a response within 10 seconds.
4. Verify that your credentials provide sufficient execution privileges.
5. Use the same credentials (username and password) that will be used from the UI.

## Adding Network Infrastructure using Bulk Upload (CSV file) for the First Time

Follow the same recommendations as when adding elements manually. Most issues are related to SSH connectivity and credentials. If multiple Scan Engines are configured for a domain, make sure only one is activated.

1. Verify that the Scan Engine is running the desired version.

2. Confirm SSH connectivity between the Scan Engine server and the target device (use `ping` and SSH; ensure a response within 10 seconds).
3. Verify that your credentials provide sufficient execution privileges.
4. Use the same credentials (username and password) that will be used from the UI.
5. Start with a CSV file that contains only a few items before scaling up.

## Run Scan Now After Making a Change

Network infrastructure is scanned according to the defined scanning priority. To immediately verify that a change has taken effect, use the **Scan Now** command from the UI.

## Update Knowledge Base and Run Scan After Upgrade

> **Note:** Following an Upgrade, Upload the latest Knowledge Base package and run a **Scan Now** to apply the latest definitions.

After performing an upgrade, it's a best practice to update the new Knowledge Base (KB) package and then immediately perform a **Scan Now** to ensure the new definitions are applied. This guarantees that device classifications and risk calculations are up-to-date, reflecting the latest threat intelligence.

# Host Agent Best Practices

## Overview

Many organizations are utilizing various Information Technologies tools to manage and provision their infrastructure. This section provides best practices for deploying Sepio Host Agents at large scale, offering an approach that minimizes errors and ensures optimal performance. By following these guidelines, organizations can avoid common pitfalls, enhance their security posture, and maintain a well-functioning system across all deployed agents.

## Using Unified Endpoint Management (UEM) to Provision Sepio Host Agents

Here is a list of best practices for installing the Sepio Host Agent using UEM tools like Microsoft Intune, ensuring a smooth and secure deployment. It is recommended to follow these steps before deployment, ideally as part of a proof of concept or pilot deployment.

### 1. Testing

- Before widespread deployment, test the installation process on a small group of devices that are representative of your target environment. This helps identify and resolve any issues before impacting more devices.
- Compatibility Checks: Ensure the security product agent is compatible with the target operating systems and UEM platform versions.

### 2. Centralized Configuration

- UEM Policies: Leverage UEM policies to configure the security product agent's settings, such as installation location and installation parameters.
- Group Policies (Optional): If applicable, use Group Policies to complement UEM policies and enforce additional security settings.

### 3. Efficient Deployment

- Software Distribution: Use the UEM platform's software distribution capabilities to deploy Microsoft Installer (MSI) packages efficiently to target devices.
- Scheduling: Schedule installations during off-peak hours to minimize disruption to users.
- Deployment Rings: Deploy the agent in phases (e.g., pilot group, specific departments) to facilitate monitoring and troubleshooting.

### 4. Monitoring and Reporting

- UEM Console: Use the UEM console to monitor installation status, agent health, and security alerts.

- Reporting: Generate reports to track the deployment progress, identify any issues, and assess the effectiveness of the security solution.

**5. Additional Considerations**

- Rollback Mechanism: Plan for a rollback mechanism to address installation failures or unexpected issues.

**6. Agent Default Mode Configuration**

- Sepio Platform Management provides the capability to automatically assign a default mode to newly connected hosts.
- It is not recommended to set the agent default mode to **Armed**, as this will cause every new agent to switch to Armed mode before its connected peripherals are approved. As a result, all connected peripherals will be blocked.

> **Warning:** Avoid setting the agent default mode to **Armed**, as it may block all newly connected devices.

## Using Unified Endpoint Management (UEM) to Upgrade Sepio Host Agents

The Sepio Host Agent has a built-in Auto-Update capability. When using UEM verify that the auto-update feature is turned off. This will ensure that there are no conflicts between the Platform Management's "desire" to have the latest version of the Host Agent installed on all endpoints and the organization's UEM policies.

# Policy Management Best Practices

## Use Scope Default Mode Carefully When Enforcing Policy Mode

If you plan to use the **Scope Default Mode** to force agents into **Policy Mode**, it is recommended to add an additional scope filter for:

- “Version is ”

This ensures that only agents capable of Policy Mode are included in that scope.

**Why this matters:**
Enforcing Policy Mode on agents that do not support it is considered a **bad practice** and may lead to inconsistent or unexpected behavior.
Always validate that the scope’s query includes the minimum required version before enforcing Policy Mode.

## Assess the Impact of New Block Rules Before Applying Them Globally

Before applying a blocking rule across all agents, it is recommended to understand which peripherals **will be affected.**
**Example:** if you plan to block all cameras “Peripheral Type = Camera” across the organization:

- Go to **All Assets**
- Query the following:
  - Type = Camera
  - Connection Type = USB
  - Is Online = Yes

This query will show all currently connected cameras that would be blocked if the rules were applied.
Conducting this proactive assessment helps avoid accidental disruption across the organization.

# Frequently Asked Questions

## Network Visibility

Expand All

- Why in some cases Sepio did not create a potential Unmanaged Switch Risk Indicator when it reports multiple assets connected to the same edge port?
- Why, in some cases, a new potential Unmanaged Switch is seen on an edge port even though there is only one asset connected?
- Can a port appear to be online while having no assets connected to it?
- Can a trunk port on Cisco switch show status “up” while no devices are connected?
- How do assets connected to Port Channel appear in Sepio?
- Does Sepio present Cisco Discovery Protocol (CDP) and MAC on routed ports?
- Is it possible to see a dormant device on a port that is showing CDP/LLDP data?
- Why Supervised assets (Wireless Lan Controller (WLC), Access Point (AP), Network Switch) might have empty locations?

## Functionality

Expand All

- Is there a difference in platform capabilities for SaaS, on-prem and air-gapped deployments?
- How are Mass Storage Devices blocked in BST mode?

## Risk Indicators

Expand All

- Which interfaces are used for “Low Speed on High-Speed” Port Risk Indicator calculations?
- Can a non-Dormant asset show an extended idleness risk?
- Why is the agent not detecting a potential WiFi keylogger?

## Scan Engine

Expand All

- When using Event-Based Scan Engine, does each Link-Up trap create a new SSH session?
- When using Event-Based Scan Engine, how does the system handle frequent link-up/link-down events (port flapping)?
- How does the Scan Engine store its credentials for authentication against the Platform?
- How are customer-provided, privileged credentials stored and protected on the Scan Engine?
- Is the Scan Engine stateless?
- How is data collected by the engine handled prior to transmission to the Platform? Is it ever written to temporary storage?
- Is the Scan Engine run from immutable storage? If not, why not?
- How does the Scan Engine authenticate and verify the legitimate Platform instance?
- How does the Scan Engine verify update authenticity and is the process audited?
- Are there plans to improve Scan Engine security and update processes?

**How does the Scan Engine operate in air-gapped environments and what is meant by ‘call home’?**