Installation Guide

Sepio Prime

Version 1.2 ● January 28, 2020

This Installation Guide provides guidance to those involved in the installation of the application.
This guide assumes that you have some knowledge of Linux and the Sepio software suite.

Sepio Systems Ltd.

9841 Washingtonian Blvd. # 200

Gaithersburg, MD

20852 USA

Tel: +1 (240) 660-8690

Last edited: 28 January 2020

Installation Guide

SepioPrime

Version: 1.2 Revision Date: Dec 26th 2019

Sign-Off / Approved By		

Revision History			
Rev #	**Revision Update**	**Revised By**	**Date**
1.0	Preliminary	Gal Broder	Aug 1st, 2019
1.2	Added OVF option	Gal Broder	Dec 26th, 2019

Table of Contents

1 Introduction 6
1.1 Purpose of this Document 6
1.2 Identification 6
1.3 Reference Information 6
1.4 Points of Contact 6
2 System Requirements 7
2.1 Overview of SepioPrime Installation 7
2.2 Software Requirements 7
2.3 Hardware Requirements 7
2.4 Operating Systems 8
2.5 Firewall Configuration 8
3 Installing SepioPrime 9
3.1 Prerequisites 9
3.2 Online Installation 9
3.3 Virtual Appliance Installation 10
4 Post Installation 12
5 Potential Problems or Issues 13
5.1 Docker is not running or supported 13
5.2 Repository Access 13

About this Guide

This Installation Guide explains how to install the SepioPrime. This guide assumes that you have some knowledge of the Linux environment.

For detailed information regarding features, capabilities, and software introduced with this release, please refer to the documents listed in the "Related Documentation" section.

For the most current version of this document, please visit: http://sepio.systems or contact your sales representative.

Who Should Use It

This Guide guides System Administrators involved in the installation of the application. It is also intended for -

- System Administrators responsible for installing the system and related components
- Deployment Planners plan the deployment of the system within your organization

Typographical Conventions

This document uses the following typographical conventions:

Command and option names appear in **bold type** in definitions and examples. The names of directories, files, machines, partitions, and volumes also appear in bold.

Variable information appears in *italic type*. The *italic type* includes user-supplied information on command lines.

Screen output and code samples appear in `monospace` type.

In addition, the following symbols appear in command syntax definitions.

Square brackets [ ] surround optional items.

Angle brackets < > surround user-supplied values.

The percent sign % represents the regular command shell prompt.

1 Introduction

SepioPrime is the management console that provides deep visibility and control on the USB devices and network.
The USB Device Security provides full visibility of all connected devices; it analyzes their capabilities and behavior in real-time and supports policy enforcement – thus allowing or blocking specific devices and interfaces according to the defined policy.

SepioPrime is continuously monitoring the network searching for rouge network (LAN) devices that are transparent to existing security tools.

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

1.1 Purpose of this Document

Introduce the system or components to be installed. If applicable, identify any benefits that arise from this installation, e.g., improved performance, system stability, as well as business, technological, or organizational objectives that may be achieved.

This guide covers the installation of SepioPrime.

1.2 Identification

SepioPrime version 19.11.27.1420

1.3 Reference Information

For information regarding Docker and Docker Compose installation, refer to the following links:
Docker - https://docs.docker.com/install/overview/

Docker Compose - https://docs.docker.com/compose/install/

1.4 Points of Contact

For more details, refer to the SepioPrime Admin guide or contact us at support@sepio.systems

2 System Requirements

This chapter includes the following sections:

- Overview of SepioPrime installation
- Software requirements
- Hardware requirements
- Operating systems
- Firewall Configuration

2.1 Overview of SepioPrime Installation

SepioPrime can be installed in one of 3 ways:

- Online installation – when the server has an internet connection, and all installation files can be downloaded and installed automatically.
- Virtual appliance – a provided OVF file to be used as a virtual appliance in VMware environments.

2.2 Software Requirements

The following software is required to install this application:

- Docker and Docker Compose installed.
- A non-root user to run docker

The recommended Docker environment is version 17.09 or above.

If Docker is not available and in use in the organization, the recommended OS is UbuntuServer 18.04 LTS.

2.3 Hardware Requirements

The recommended minimum specifications for the server include the following:

System Component	Cores	RAM	Disk
SepioPrime	4x cores	16GB	100GB

2.4 Operating Systems

SepioPrime operates on every OS that supports docker and that the docker supports running Linux containers.

2.5 Firewall Configuration

SepioPrime uses several TCP ports for communication between the server and other components of the solution. To support proper operation, the following ports should be enabled on the firewall:

Source	Destination	Protocol	Port	Comment
Sepio Agent	SepioPrime	TCP	80 / 443	
NetPoller	SepioPrime	TCP	443	
Management Machine	SepioPrime	TCP	443, 22	
SepioPrime	sepiocontainerrepo.azurecr.io	TCP	443	For pulling containers images from the cloud
SepioPrime	cloud.primefrontend.sepio.systems	TCP	443	**Optional** – for connecting to SepioCloud

3 Installing SepioPrime

Before you start installing the application, make sure you have the necessary resources available to implement the installation.

This chapter describes the procedure for installing SepioPrime. It includes the following sections:

- Prerequisites
- Online Installation
- Virtual Appliance Installation

3.1 Prerequisites

Before you install the system components, you must complete several pre-installation tasks:

- Verify that Docker and Docker Compose is installed.
- Allow a non-root user to run the Docker.
- Set the proper firewall rules (refer to section 2.5 above).

3.2 Online Installation

Several files have to be copied to the server before starting the installation:

- config.env – a configuration file that sets the configuration before the installation.
- update-script.sh – the installation script for SepioPrime.
- docker-compose.yml – Containers file. Being used by the installation script.

3.2.1 Editing the Configuration File

The config.env file is setting the configuration for the SepioPrime. The configuration has to be set before the installation with the correct parameters. The default parameters are commented on in the file.

Please edit the following:

1. TZ – Time zone for the server (e.g., TZ=America/New_York).
2. PRIME_HOST_NAME – The hostname for the SepioPrime server.
3. CLOUD_SEND_REPORTS – Determines if SepioPrime sends periodic health reports to SepioCloud. The default value is False.

3.2.2 Installing the server

1. Make sure that the installation script is executable:
   `sudo chmod +x update-script.sh`
2. Run the installation script.
   `sudo ./update-script.sh`

The installation creates the installation directories and downloads the installation files from the internet. At the end of the installation, the relevant containers switch to up mode, and the output is the running containers.

```
Creating sepioprime_pgserver_1  ... done
Creating sepioprime_dataapi_1   ... done
Creating sepioprime_netpoller_1 ... done
Creating sepioprime_netsapi_1   ... done
Creating sepioprime_agentsapi_1 ... done
Creating sepioprime_eventsapi_1 ... done
Creating sepioprime_adminwebapp_1 ... done
Creating sepioprime_rproxy_1      ... done
CONTAINER ID        IMAGE                                                      COMMAND                  CREATED             STATUS              PORTS                                      NAMES
5a60bb18753e        sepiocontainerrepo.azurecr.io/sepio.prime.rproxy:1.7       "nginx -g 'daemon of…"   2 seconds ago       Up Less than a second   0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp   sepioprime_rproxy_1
8885e308ebf9        sepiocontainerrepo.azurecr.io/sepio.prime.adminwebapp:2.5.12.0   "dotnet Sepio.Prime.…"   5 seconds ago       Up 2 seconds            0.0.0.0:32773->5124/tcp                    sepioprime_adminwebapp_1
fea01687fed9        sepiocontainerrepo.azurecr.io/sepio.prime.eventsapi:1.0.38.0     "dotnet Sepio.Prime.…"   9 seconds ago       Up 4 seconds            0.0.0.0:32772->5126/tcp                    sepioprime_eventsapi_1
bc5b203d9f7f        sepiocontainerrepo.azurecr.io/sepio.prime.netsapi:2.3.28.0      "dotnet Sepio.Prime.…"   9 seconds ago       Up 5 seconds            0.0.0.0:32771->5125/tcp                    sepioprime_netsapi_1
af0712d07595        sepiocontainerrepo.azurecr.io/sepio.prime.agentsapi:2.2.77.0    "dotnet Sepio.Prime.…"   9 seconds ago       Up 5 seconds            0.0.0.0:32770->5123/tcp                    sepioprime_agentsapi_1
a3d6ccad8862        sepiocontainerrepo.azurecr.io/sepio.prime.netpoller:3.36.3      "dotnet NetPoller.dll"   13 seconds ago      Up 10 seconds                                              sepioprime_netpoller_1
3ce9db79de05        sepiocontainerrepo.azurecr.io/sepio.prime.dataapi:1.1.23        "dotnet Sepio.Prime.…"   13 seconds ago      Up 10 seconds           0.0.0.0:32768->5127/tcp                    sepioprime_dataapi_1
4a15f85d5d6b        sepiocontainerrepo.azurecr.io/sepio.prime.postgres:1.0          "docker-entrypoint.s…"   13 seconds ago      Up 9 seconds            0.0.0.0:32769->5432/tcp                    sepioprime_pgserver_1
user@prime:~$
```

3.3 Virtual Appliance Installation

Another option for installation is to use a pre-installed virtual machine (Ubuntu Server + Docker + Docker Compose + SepioPrime) and to import it to any VMware virtual environment.

OVF + VMDK files are provided by Sepio and can be imported to the virtual environment.

The credentials for the virtual machine are:

Username: *prime*
Password: *Sep!oSyst5ms*

After importing, the configuration file has to be edited, and the docker containers have to be restarted.

3.3.1 Editing the Configuration File

The config.env file is setting the configuration for the SepioPrime (can be found in *~/prime-app*). The configuration has to be set before the installation with the correct parameters. The default parameters are commented on in the file.

Please edit the following:

1. TZ – Time zone for the server (e.g., TZ=America/New_York).
2. PRIME_HOST_NAME – The hostname for the SepioPrime server.
3. CLOUD_SEND_REPORTS – Determines if SepioPrime sends periodic health reports to SepioCloud. The default value is False.

3.3.2 Restarting the Containers

From the Sepio installation directory (*~/prime-app*), run the following commands:

```
docker-compose -p sepioprime down
```

```
docker-compose -p sepioprime up -d
```

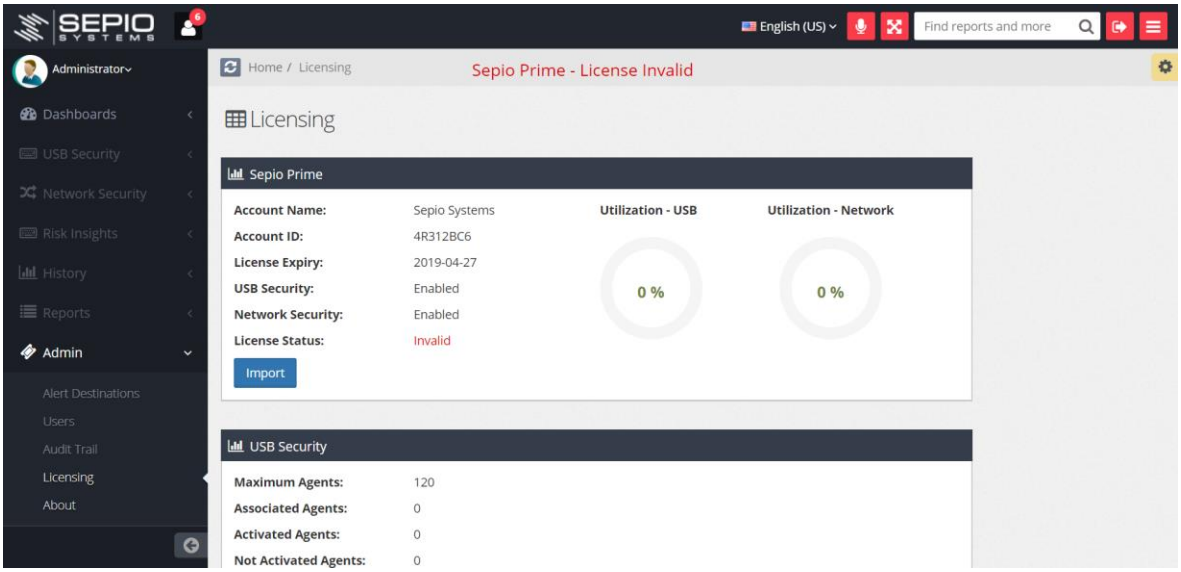
The containers will be restarted and the new configuration file will be used.

4 Post Installation

After the installation, a license has to be updated to the server. The license is provided by Sepio.

To update a license in the server:

1. Log in to SepioPrime (default username and password: Administrator / SepioSystems)
2. On the SepioPrime, on the left pane, click on **Admin > Licensing**



3. On the right pane, under the **Sepio Prime** section, click on **Import**.
4. Choose the zip file that was provided by Sepio and click on **Save**.
5. SepioPrime is activated.

5 Potential Problems or Issues

5.1 Docker is not running or supported.

```
user@prime:~$ sudo ./update-script.sh
./update-script.sh: line 10: docker: command not found
./update-script.sh: line 15: docker-compose: command not found
user@prime:~$
```

Possible cause: Docker is not installed or running.

Suggested correction:

1. Make sure the docker is running.
2. Install the docker and start it.

5.2 Repository Access

```
user@prime:~$ ./update-script.sh
WARNING! Using --password via the CLI is insecure. Use --password-stdin.
Error response from daemon: Get https://sepiocontainerrepo.azurecr.io/v2/: dial tcp: lookup sepiocon
tainerrepo.azurecr.io: Temporary failure in name resolution
Creating network "sepioprime_primenetwork" with driver "bridge"
Creating volume "sepioprime_primepgdata" with default driver
Creating volume "sepioprime_primentapidata" with default driver
Creating volume "sepioprime_primenetsapilogs" with default driver
Creating volume "sepioprime_primeeventsapilogs" with default driver
Creating volume "sepioprime_primeagentsapilogs" with default driver
Creating volume "sepioprime_primenetpollerlogs" with default driver
Creating volume "sepioprime_primeadminwebapplogs" with default driver
Creating volume "sepioprime_primerproxydata" with default driver
Creating volume "sepioprime_primerproxycertdata" with default driver
Creating volume "sepioprime_primedataapilogs" with default driver
Creating volume "sepioprime_primefilesdata" with default driver
Pulling pgserver (sepiocontainerrepo.azurecr.io/sepio.prime.postgres:1.0)...
ERROR: Get https://sepiocontainerrepo.azurecr.io/v2/: dial tcp: lookup sepiocontainerrepo.azurecr.io
: Temporary failure in name resolution
user@prime:~$ _
```

Possible cause: The server is unable to pull the docker images from the repository.

Suggested correction:

1. Make sure TCP port 443 is open to *sepiocontainerrepo.azurecr.io*
2. Make sure you have an internet connection.