Ancor Installation & Administration Guide

Version 2.0

Published on: January 15, 2016

Table of Contents

Chapter 1 Ancor Installation

SecPod Ancor™ is a scalable analytics and correlation engine that provides real-time, integrated security intelligence. It acts as the security intelligence platform for SecPod Saner. Using the services of Ancor, Saner identifies potential security vulnerabilities, misconfigurations and missing patches and remediates the system to keep it secure.

Ancor collates various types of information such as vulnerability, malware heuristics, vulnerability remediation, endpoint visibility and software reputation service from different sources, and combines it with the latest security standards and best practices to provide a robust security intelligence platform. The Ancor engine uses its web services API to guide Saner to collect information regarding the security posture of the system, perform assessments on the vulnerability state of the system, and offer remediation for those vulnerabilities, along with monitoring events in real-time and continuously enforcing security policies.

Installing Ancor On-Premise

To install Ancor within an enterprise, you must use the DVD that you received on purchase, or download the ISO image from the URL provided to you.

Hardware Prerequisites

- 64-bit Machine
- Minimum 40 GB hard disk space
- Minimum 8 GB RAM

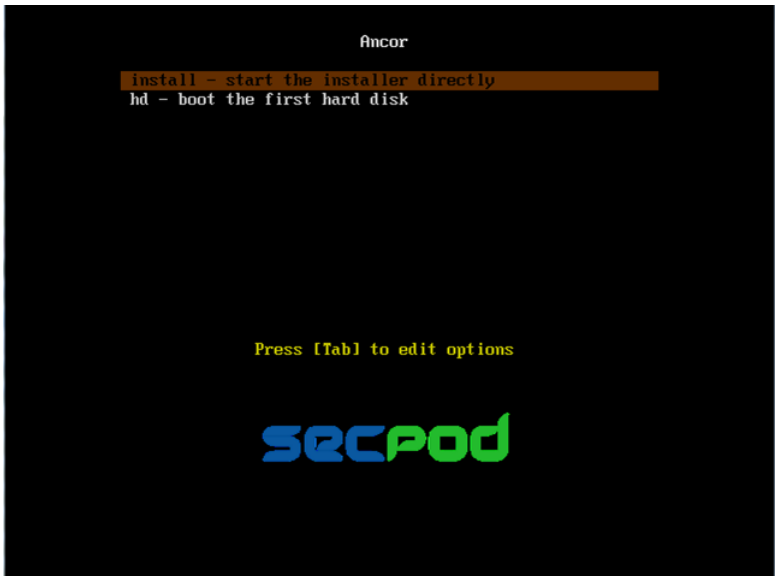
To install Ancor

The SecPod Ancor installer is bundled with a 64-bit Linux operating system. The installer package is a self-bootable ISO image that you may have downloaded from a link provided by SecPod or a DVD shipped to you.

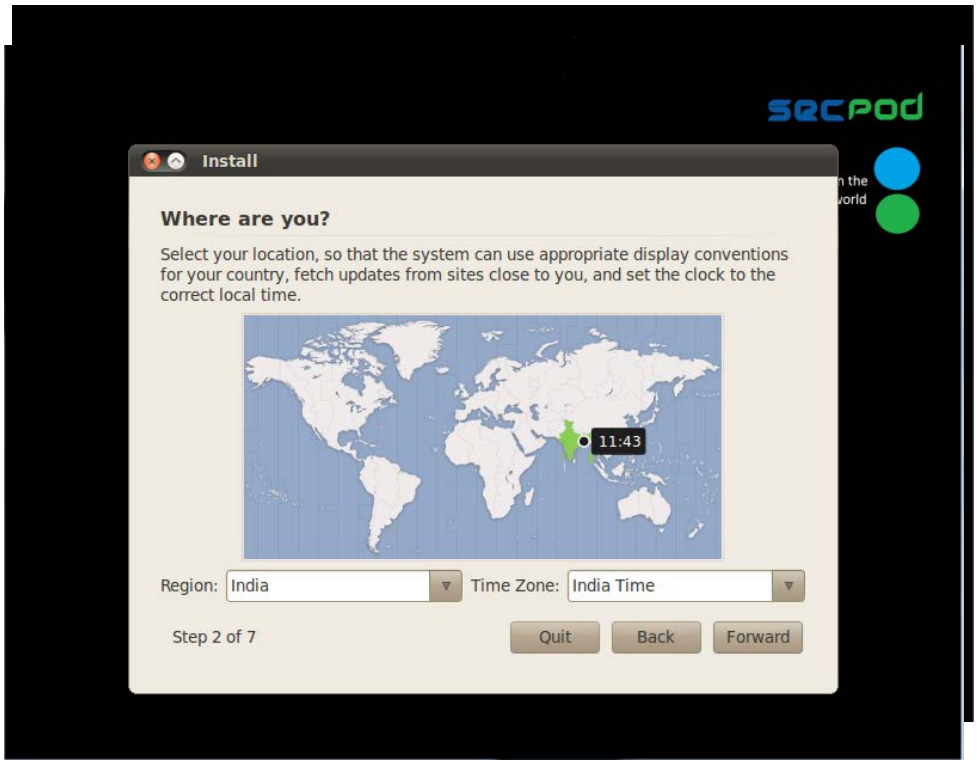
1. Mount the ISO image you have downloaded, or insert the DVD into the DVD drive. The Ancor setup program will start automatically.
2. Select the following option:

   ```
   Install – start the installer directly.
   ```

This will start the Ancor installation. The Ancor installation is simple and the setup program will guide you through the process.



3. Select the language and click the Forward button.



4. Select your location and click the Forward button.

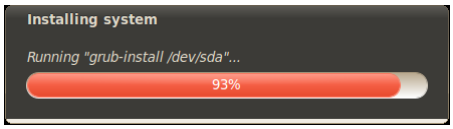
5. Select your keyboard layout and click the Forward button.

6. You will be prompted to partition the machine's disk. Click the Forward button if you would like to go with Ancor's recommendation. You can also choose to manually partition the disk; this is recommended if you have existing data on the machine.

7. Set up an account to access Ancor, and click the Forward button. (You can create multiple accounts to access Ancor after the installation. This may be required in scenarios where there are multiple enterprise networks running Saner with different administrators who need separate Viser login credentials.)

8. Click Install.

9. The installation starts.



10. You will be prompted to restart the system, to complete the installation. On restart, Ancor displays a CLI console; you will be prompted to provide a new secure password. The password must be alphanumeric, have 8 characters or more, and must contain a special character.
11. Once the new password is set, Ancor restarts the CLI session, and prompts you to enter the new password.

Note: By default, Ancor uses the super user account name.

On successful completion of the installation, you must activate Ancor to start using it. The Ancor console with the following CLI options is displayed:

- `Activate`
- `Servicemgmt`
- `Exit/Quit`

The `Activate` option is available only for a fresh installation. Thereafter, to access the activate command, you must go to the Ancormgmt CLI. For details, see CLI Commands to Manage Ancor.

Activating Ancor

To activate Ancor

1. Start a Linux shell and mount the Ancor license key available on the DVD or a directory. Copy the absolute path to the file `assertion.key`.

   Exit the Linux console by pressing `[Ctrl] + [d]` or typing `exit`. Exit the servicemgmt CLI.
2. Activate Ancor by issuing the following command:

   `activate`

   Provide the activation key or the absolute path to the activation key, when prompted. Press Enter to activate Ancor.
3. To verify that Ancor is activated, type `help`. The CLI options that are available to you should include commands for managing Ancor. For example: `ancormgmt`, `usermgmt`

On successful activation, SecPod Ancor is ready to provide updates and remediation to Saner. By default, the automatic update is scheduled for 12.00 am daily.

Setting the Hostname

You must set a hostname that Ancor can configure:

- As a web service for Viser, the front-end of Ancor, and
- For Saner API calls

To set a hostname

1. Issue the following command from the servicemgmt CLI:
   - `sethostname <IP address of the host/hostname>`

   To find the IP address of the host or the public hostname, use the following command:
   - `servicemgmt > display interface`, to get the IP address

OR

   - `Console > hostname`, to get the public hostname

Restart Ancor, using the stop/start commands provided in the servicemgmt CLI.

> Note: After a restart, you must log on to the web page using the root username and the password specified after the installation in Step 10. You can logout from the web page (root account). This root login is important to initialize the web service sessions and threads.

Chapter 2 Managing Ancor

Once Ancor is started and is running, there may be a set of operations that you need to perform from time to time to manage:

- Ancor
- Ancor Users
- Ancor Services

In addition, there are tasks you will need to perform in a sequence, such as:

1. Creating MSP (Managed Service Provider) Account
2. Syncing Updates from the SecPod Cloud (Ancor) to the On-premise Ancor
3. Creating User Accounts

Creating MSP (Managed Service Provider) Accounts

To create and deploy Saner software on user machines, the URL for downloading Saner has to be accessed from Viser. Therefore, you must create Viser accounts for administrators.

To create an MSP account

1. Type `usermgmt` to go to the Ancor User Management CLI
2. Type the `createadmin` command to create an MSP account.

Syncing Updates from the SecPod Cloud (Ancor) to the On-premise Ancor

Ancor synchronizes data from the SecPod Cloud (Ancor) to the on-premise Ancor, to ensure updates and the latest definitions. This occurs automatically at 12 am daily. However, there may be scenarios when you need to do this manually, such as when you receive an update notification from the SecPod Cloud, or when you create a new Viser account.

To synchronize definitions and data between the on-premise Ancor and SecPod Cloud

1. Type ancormgmt to go to the Ancor Management CLI.

2. Type `sync` and press ENTER.

The speed of the sync operation will depend on your internet speed. Once definitions and data has been synchronized between Ancor and Saner, you can create Viser accounts for users.

Creating User Accounts

When sync operation is completed admin needs to create user accounts through MSP accounts.

Log in to MSP account through browser, create a user account by clicking Plus icon. While creating a user account Ancor will create a Saner software for each operating system. Once user creation is completed, user can log in and deploy Saner software on endpoints.

CLI Commands to Manage Ancor

You can manage Ancor from the Ancor Management CLI, using the `Ancormgmt` command. To use any of the following commands, type the command at the Ancormgmt CLI.

Command	Use
`activate -t <SecPod Ancor Token String>` OR `<Absolute path of the file that contains the token>`	Activates the Ancor server.
`resetadminpasswd -p password`	Resets the admin password for Ancor.
`sync`	Synchronizes data between the SecPod Cloud and Saner. This is the default sync operation.
`Sshsync <enable/disable>`	Synchronizes data between the SecPod Cloud and Saner using the SSH protocol
`installkeystore`	Sets up a trusted key store
`importcontent -f <Absolute file/directory path to the oval definitions file>`	Imports the Custom Oval definitions for scanning
`cleanupresource`	Cleans up the resource directory (`ancor /usr/local/scaprepo/resources`) by removing unwanted files; the resource directory contains patches for remediation
`createsanerbuild [-u <username> -a <architectecture x86|x64|all> -t <type exe|rpm|dpkg|osx-noui|exe-noui|rpm-noui|dpkg-noui|noui|ui|all>]>`	Creates the saner builds for a Viser account
`createsanerupdatebuild [-u <username> -a <architectecture x86|x64|all> -t <type exe|rpm|dpkg|osx-noui|exe-noui|rpm-noui|dpkg-noui|noui|ui|all>]>`	Creates the saner upgrade builds for a Viser account.

Command	Use
`help`	Prints the commands supported by the CLI
`exit/quit`	Exits the Ancor Management Interface

CLI Commands to Manage Ancor Users

You can perform user management operations from the UserMgmt CLI. To use any of the following commands, type the command at the UserMgmt CLI.

Command	Use
`viewsubscription`	Displays the Saner subscription
`createviseruser -u <username> -p <password> -o <organization> -em <emailid> [-count <no. of saner subscriptions>]`	Creates a Viser account to manage saner enabled devices

`addvisersubscription -u <username> [-num <no_of_subscriptions> -d <date-of-expiry>]`
`-d` is optional, the value should be provided in yyyy-mm-dd format. The default value is the expiry date of the user information.
`-num` is optional, the default value is `1`
	Adds a Saner subscription for a Viser account.

`getsanercount`	Retrieves the number of Saner instances installed for an Ancor or a Viser user.
`updatesanercount -u <viser username> -count <no. of saner subscriptions>`	Updates the number of saner licenses assigned to an existing Viser user
`deleteuserinfo -u <username>`	Deletes the information corresponding to the specified user
`viewuserinfo -u <username>`	Retrieves the information corresponding to the specified user
`updateuserinfo -u <user id> -n <name> -o <organization> -en <entitlement> -s <start_date[YYYY-MM-DD]> -e <expiry_date [YYYY-MM-DD]> -em <email> -l <license(EULA/EVALUATION)> -lt <licensetype(Redistributable/EULA)> -a <active(true/false)>`	Updates the information corresponding to the specified user
`updateuserpwd <username>`	Updates the password of an existing user
`deleteuser <username>`	Deletes an existing user
`getusers`	Retrieves information about the users
`help`	Prints the supported commands

Command	Use
`exit/quit`	Exits the User Management Interface

CLI Commands to Manage Ancor Services

You can manage Ancor services from the ServiceMgmt CLI. To use any of the following commands, type the command at the ServiceMgmt CLI.

Command	Use
`start`	Starts the Ancor server
`stop`	Stops the Ancor server
`status`	Prints the status of the Ancor server
`console`	Starts the System Admin console
`reset -u <userid> -t <weservice/web>`	Resets all the user login sessions
`sethostname <Ancor IP/Ancor Hostname>`	Sets the hostname or IP of the machine for Ancor services
`updateip -i <ip> -m <subnetmask> -g <gateway> -d <device>`	Updates the IP of the Ancor interface
`addroute -n <network address> -r <route> -d <device>`	Adds a static route for the network
`delroute -n <network address>`	Deletes a static route for the network
`display <interface|route> [-d <device>]`	Displays the network configuration
`installservercert <Absolute file path to server certificate>`	Installs the server certificate
`installserverkey [-f <File path of ServerKeyTrustedCertPasswd>] <Absolute file path to server private key>`	Installs the server key
`addproxy -f <field name> -v <field value>`	Sets the configuration values related to the ancor service For example, `addproxy -f <ProxyServer|ProxyServerPort|ProxyServerUser|ProxyServerPasswd> -v <field value>`
`help`	Prints the supported commands
`exit/quit`	Exits the Service Management Interface

3 Managing Ancor in Air Gap Network

What is an Air Gap Network?

An air gap, air wall or air gapping is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.

Air Gap Ancor should be activated and synced using the internet in the beginning. Later it can be kept in an isolated network and managed using the steps mentioned below:

1. Pairing the Device with Air Gap Ancor

Connect the Pen Drive of size more than 32 GB to Ancor and pair it with the Ancor.
Issue the following command from servicemgmt CLI:

```
servicemgmt>listdevice
```

it will list the device path, copy the path and paste for the below command

```
servicemgmt>pairdevice <absolute path>
```

Ancor will copy the offlinesync script, license.key files to Pen Drive.

Using this Pen Drive user can get latest updates from the Cloud Server (saner.secpod.com)

2. Syncing updates from SecPod Cloud Ancor to Paired Device

During the first update, we can run the script on the same machine (Air Gap Ancor) to get the updates or,

Connect the device to the Linux/Windows machine where the internet is there,

For Linux machine run the following command to mount using shell,

```
$mount -o umask=0077 <device path> <folder>
```

go to that folder, run offlinesync script

```
$./offlinesync
```

For Windows Machine install the latest cygwin or Babun software

connect to babun or cygwin

```
$mount -o umask=0077 <device path> <folder>
```

go to that folder, run offlinesync script

```
$./offlinesync
```

Since it is fresh offline sync it takes around 30 minutes.

Once it is done unplug the device and plug to Air Gap Ancor and apply offline sync.

3. Syncing Updates from Device to Air Gap Ancor

Ancor synchronizes data from the pen drive to the Air Gap Ancor.

To synchronize definitions and data between the Device and Air Gap Ancor

Attach the Device (pen drive) to Air Gap Ancor and mount the device
mount -o <device path> <folder>

Mention the folder where we want to mount.

Go to Ancor CLI ancormgmt:

1. syncoffline <path of device/mount folder>

2. ENTER.

It takes around 30 min to complete in the beginning. Once synchronization is done, latest upgrades are available for the users.

4. Applying Offline Sync Regularly

Repeat steps 2 & 3 whenever admin wants to update Air Gap Ancor with Cloud Ancor.