Lastline Air Gap Manager Installation and Administration

Contents

Lastline Air Gap Manager Installation and Administration

This document describes the installation and administration of the Lastline Air Gap Manager .

About Lastline, Inc.

Lastline® develops and delivers the industry's most accurate AI-powered network security. The Lastline Defender™ provides AI-driven, dynamic, highest fidelity insights into advanced threats entering or operating in your network. Lastline security and protection platform is designed to detect, stop, and manage attacks, persistent threats, polymorphic viruses, zero-day exploits, and evasive cyber malware threats for private and public organizations. Lastline software provides real-time malware analysis of network, email, web, file, content, and mobile attacks.

About Lastline Air Gap Manager

The Lastline Air Gap Manager collects information, processes the data, and presents it to the user. The Air Gap Manager receives artifacts (such as executables and documents) that are downloaded or otherwise acquired by users and processes them. The results of the analysis are collected and presented to the user via a web portal using an incident-centered approach, in which evidence from run-time analysis, network monitoring, and anomaly detection are correlated to provide prioritized and actionable threat intelligence.

The Air Gap Manager is also responsible for acquiring the latest network behavior models that are associated with malware activity. These are downloaded from Lastline Labs and manually transferred to the Air Gap Manager.

The Air Gap Manager provides a dashboard, the Lastline Portal, from which you manage other Lastline appliances in your network.

Important: The Lastline Air Gap Manager is offered to customers in high security environments with stringent privacy and policy constraints as part of an physically isolated network deployment configuration. In this configuration, the Air Gap Manager stores all the information regarding the detection of infected hosts and the analysis of software artifacts locally within your data center.

Supported Hardware

Refer to the *Hardware specifications* (https://lastline.zendesk.com/hc/en-us/sections/115003021067-Hardware-specifications) page for details about the hardware certified for use with Lastline Air Gap Manager. If you cannot access that URL, *contact Lastline Technical Support* (see page 32).

Acquire the Air Gap Manager ISO

Prerequisites

Your account must be granted *can_operate_offline* permission before you can access the ISO image for the Air Gap Manager installation. Lastline Technical Support will provision your account with this permission.

Contact Lastline Technical Support (see page 32) if your account is not correctly provisioned.

Configuration Steps

To install the Lastline Air Gap Manager, you must download the ISO from Lastline.

Step 1: Refer to your Lastline welcome message

Using the information in the Lastline welcome email message, point your browser to the *Lastline Portal* (https://user.lastline.com/) and then login. For your initial login, use the *Forgot your password?* (https://user.lastline.com/password_reset) link and follow the subsequent instructions.

The licenses you need to run Lastline Air Gap Manager are included in the welcome message. The Lastline registration process displays these licenses. Compare the licenses it displays with the provided licenses.

Step 2: Download the ISO

Click the **[≡]** icon in the header to expose the **Main menu**, then click **[? Help]** . Click **Downloads** from the expanded menu. On the *iso-downloads* (https://user.lastline.com/portal#/iso-downloads) page, select the correct ISO and download it to your staging server.

Download the corresponding MD5 file for the ISO. Validate that the `md5sum` of the ISO matches the value in the MD5 file.

Step 3: Prepare the ISO for installation

There are various ways to prepare the ISO. You can burn it to a DVD, create a bootable USB stick, or, if you are using Dell hardware and the iDRAC interface is available on your server, you can use that.

DNS Setup

As part of the license registration, the system must be associated with a fully qualified domain name and corresponding certificate.

Assuming that the FQDN `lastline.example.com` was set for the Lastline Air Gap Manager, you must ensure that the following names all correspond to the same IP address to allow access to the Lastline Portal running on the system:

- `user.lastline.example.com`
- `update.lastline.example.com`
- `log.lastline.example.com`

Note: Determine the IP address of the server by running the `ifconfig` command on the console.

The installation domain name must always specify a top-level (root) domain, such as `.com`, `.edu`, or `.gov`.

SSL/TLS Certificate

All services on the Lastline Air Gap Manager are accessible through HTTPS only. The Air Gap Manager generates and uses a self-signed SSL certificate. This requires all managed appliances to store and trust this certificate during the registration phase.

If required, you can *replace the SSL/TLS certificate* (see page 13) on the Lastline Air Gap Manager.

Install Air Gap Manager

The installation process for the Lastline Air Gap Manager consists of three steps. In the first step, the base system is installed. In the second step, basic configuration information is collected and the configuration is applied to the system. In the final step, required data is retrieved from the Lastline backend servers.

Base System Installation

Configuration Steps

The Lastline Air Gap Manager uses Ubuntu Server 16.04 (Xenial Xerus distribution) as its underlying operating system. Therefore, many of the steps of the installation are similar to the ones required to install Ubuntu Server. Refer to the Ubuntu guide, *Installing Ubuntu 16.04* (https://help.ubuntu.com/16.04/installation-guide/index.html).

Note: Many of the steps involved in a standard Ubuntu installation have been automated and hidden from the Air Gap Manager Installer.

Before starting the installation of the Air Gap Manager software, the RAID controller must be configured in RAID10. You must ensure your RAID controller is configured appropriately.

Step 1: Boot the server from the ISO image

Use the DVD or bootable USB stick you created (or for Dell hardware, the Dell iDRAC interface) to boot the ISO image.

Step 2: Select the Lastline Air Gap Manager from the boot loader splash screen

Press **[Enter]** to continue.

Step 3: Select keyboard options

The installer needs to localize your keyboard layout and language settings. Select the "Country of origin for the keyboard" and press **[Enter]**. The installer then displays a listing of appropriate keyboard layouts for the selected country. Select the desired "Keyboard layout" and press **[Enter]**.

Step 4: Wait for the system to install and reboot

After the base system is installed successfully, the system will automatically reboot. A login prompt is displayed at the end of the boot process.

Registration and Configuration

About Lastline PAPI Client

To support the data acquisition needs of the Lastline Air Gap Manager (license, threat intelligence, sandbox images), Lastline provides a client implementation for the Lastline PAPI, the *papi-client* (https://user.lastline.com/papi-doc/api/html/api/client.html), that you can *download* (https://user.lastline.com/papi-doc/api/client/papi_client.tar.gz) from the *Lastline Portal* (https://user.lastline.com/).

The Lastline PAPI client requires:

- python 2.7.
- The python *requests* (http://docs.python-requests.org/en/master/) module (version 2 or above).
- To use the interactive shell `scripts/papi_shell.py`, the *ipython* (https://ipython.org/) module is also required.

Lastline PAPI Configuration File

To effectively use the various scripts supplied, you need to create a configuration file. There are a number of example configuration file templates provided for you to start from. Use the `papi_client.ini.template` file. Rename it, for example, `config.ini`. The configuration file should be structured similar to the following:

```
[papi]
url = https://user.lastline.com/papi
auth_method = account
username = user@example.com
password = portal_password
verify_ssl = true|false
timeout = seconds

[sandbox_images]
destination_dir = path_to_directory
# sandbox images revision to download
revision = revision_number
```

```
# sets of sandbox images to download, comma-separated list
image_sets = windows,osx
compressed = true|false

[manager]
server_name=hostname|ip_address
username=server_username
ssh_key_location=path_to_ssh_key
password=server_password
```

The `[papi]` section is required:

`url` — URL to reach the Lastline backend. For Lastline PAPI, use `https://user.lastline.com/papi`.

`auth_method` — Method of authentication. Must be "**account**".

`username` — *Lastline Portal* (https://user.lastline.com/) account username. This account must be granted *can_operate_offline* customer permission by Lastline Technical Support.

`password` — *Lastline Portal* (https://user.lastline.com/) account password.

`verify_ssl` — Defines whether to perform SSL certificate validation. Set this to "**false**" if you are using a self-signed certificate.

`timeout` — HTTP request timeout in seconds. "20" is recommended.

The `[sandbox_images]` section is needed to download the sandbox images from the Lastline backend:

`destination_dir` — The downloaded sandbox images will be stored in this directory.

`revision` — Sandbox images revision to download. The correct revision for the current release can be found in the *release notes* (https://user.lastline.com/releasenotes/hosted/).

`image_sets` — The set of the sandbox images to download. Valid values are "**windows**" and "**osx**".

Note: The analysis of macOS (**osx**) artifacts is not supported in the current release.

`compressed` — Determines if the downloaded files should remain compressed ("**true**") or be extracted ("**false**") in the destination directory. We recommend you set this to "**true**".

The `[manager]` section is used to transfer the threat intelligence bundles to the Lastline Air Gap Manager:

`server_name` — The hostname or IP address of the Air Gap Manager.

`username` — The remote username on the Air Gap Manager.

`ssh_key_location` — (optional) The path to SSH private key to use to SSH into the Air Gap Manager.

`password` — (optional) The password for SSH password-based authentication. If you define a password, you must install and configure *sshpass* (http://freshmeat.sourceforge.net/projects/sshpass).

Install the Lastline PAPI Client

Configuration Steps

The Lastline PAPI client download contains a number of useful scripts.

Step 1: Download and install the papi-client

Download the *papi-client* (https://user.lastline.com/papi-doc/api/client/papi_client.tar.gz) to your staging server from the Lastline backend. Decompress the `papi_client.tar.gz` file and install it.

Note: Refer to the *Lastline API Documentation* (https://user.lastline.com/papi-doc/api/html/index.html). Specifically refer to the *`get_installation_license_bundle()`* (https://user.lastline.com/papi-doc/api/html/accounting/overview.html#accounting.license_bundle.get_installation_license_bundle) method. Also see *About Lastline PAPI Client* on page 5.

Step 2: Create a configuration file

Create a file, named for example `config.ini`, using the *structure shown above* (see page 5).

Download Air Gap License

Prerequisites

You have *installed the papi-client* (see page 7).

Configuration Steps

Your Lastline Air Gap Manager installation cannot be directly licensed using the *Lastline Portal* (https://user.lastline.com/). Instead you must download the needed licensing data and subsequently make it available to the registration process.

Obtain the licensing data bundle from the Lastline backend using the `download_offline_installation_license_bundle.py` script included with the *papi-client* (https://user.lastline.com/papi-doc/api/html/api/client.html).

Alternatively you can request the licensing bundle by *contacting Lastline Technical Support* (see page 32).

Note: The initial licensing bundle differs from the one used for updating licensing information on Lastline Air Gap Manager (see *Download License Updates* on page 30). It contains additional information needed for the installation of the appliance. The method for downloading this bundle can only be invoked once for an **On-Premises** installation. The licensing bundle is marked as installed and its license API-token is set to a new value as a side effect of the download request.

Step 1: Download and save the licensing bundle

Download and save the bundle to a file on the staging server by executing the `download_offline_installation_license_bundle.py` script:

```
staging-host# python scripts/download_offline_installation_license_bundle.py -c config.ini \
--local-bundle-path destination_file installation_access_key
```

Note: This assumes you installed the script in a sub-directory `scripts` and you created a configuration file in the current directory.

Replace *installation_access_key* with the key of the main license for your installation and *destination_file* with the name of the destination file, for example, `licensing_bundle.zip`.

Step 2: Copy the downloaded licensing bundle to the Air Gap Manager

Using some form of secure media, save the downloaded licensing bundle in, for example, `/tmp` on the Air Gap Manager.

```
lastline@lastline-manager:~$ cp /media/usb0/licensing_bundle.zip \
/tmp/licensing_bundle.zip
```

Download Threat Intelligence

Prerequisites

You have *installed the papi-client* (see page 7).

Configuration Steps

The Lastline Air Gap Manager installation cannot directly access the threat intelligence data that is needed for the registration phase of the appliance. Instead you must obtain the threat intelligence bundle from the Lastline backend and make it available to the registration process.

Step 1: Download the threat intelligence bundle

Use the `download_and_deploy_offline_bundle.py` python script to download the threat intelligence bundle.

```
staging-host$ python scripts/download_and_deploy_offline_bundle.py  --download-bundle
```

Note: See *Lastline PAPI Configuration File* on page 5 for further details and configuration instructions. Also refer to the API Documentation for details about the *`get_offline_bundle()`* (https://user.lastline.com/papi-doc/api/html/intel/overview.html#intel.offline.get_offline_bundle) method.

Step 2: Copy the downloaded threat intelligence bundle to the Air Gap Manager

Using some form of secure media, save the downloaded threat intelligence bundle in, for example, `/tmp` on the Air Gap Manager.

```
lastline@lastline-manager:~$ cp /media/usb0/threat_intel_bundle.tar.gz \
/tmp/threat_intel_bundle.tar.gz
```

Register the Air Gap Manager

Prerequisites

Ensure you download the needed licensing data and threat intelligence data and make both available to the registration process before you try to configure the Lastline Air Gap Manager.

Configuration Steps

Run the configuration and registration process.

Step 1: Login to the server console

Login to the console using the username `lastline` and password `lastline`.

Important: The default user is `lastline` and its password is `lastline`. For your security and protection, you should change the default password. Your password selection must meet the requirements specified on the *`passwd` command man page* (http://manpages.ubuntu.com/manpages/precise/man1/passwd.1.html).

Step 2: Start the registration process

Execute the `lastline_register` command, which will start the guided configuration and registration process. You must specify the location of the license and threat intelligence bundles on the command line.

```
lastline@lastline-manager:~$ lastline_register  --license-bundle /tmp/licensing_bundle.zip \
--threat-intelligence-bundle /tmp/threat_intel_bundle.tar.gz
```

Note: If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step Result

The `lastline_register` command first validates the server. If its hardware is not sufficient to run the Air Gap Manager, the command terminates with an error message.

Step 3: Select the primary network interface and network address

The registration process prompts you to select the "`Primary network interface`". It presents a list of interfaces discovered during the validation process. Select the interface that is used by the server to communicate with the other hosts on the network.

Then you are prompted to select how the server will obtain its network address. Your choice is "`Obtain via DHCP`" or "`Enter static address`".

To continue, select `<Ok>` or press **[Enter]**.

Step 4: *Optional:* Configure an HTTP proxy

Configure an HTTP proxy if it is required to access the Internet via HTTPS. Enter the address of the proxy server. This address can be a FQDN or an IP address. Specify the port for the proxy server. Examples of valid proxy configurations:

```
proxy.example.com:3128

192.168.0.1:8080
```

Otherwise if no proxy configuration is required, leave this field empty.

To continue, select <Ok> or press **[Enter]**.

Step 5: Provide the domain name

Enter the FQDN of the Lastline Air Gap Manager. The registration process will provide a suggested FQDN from the network settings. You can change this value.

To continue, select <Ok> or press **[Enter]**.

Step 6: Configure an NTP server

The Network Time Protocol (NTP) is used to set the correct time for the Air Gap Manager. Enter the address of the NTP server. This address can be a FQDN or an IP address.

Note: The selected NTP server must be reachable over UDP port 123.

To continue, select <Ok> or press **[Enter]**.

Step Result

The network configuration is tested to check for connectivity to the NTP server and the local Lastline appliances. This test may take a while.

Configuration Result

Since the license information is already provided from the downloaded license bundle, the registration process is complete. The software runs some tests to check hardware compatibility. The configuration is then applied to the machine. This process may take a while (20-40 minutes) depending on your network connectivity and system characteristics.

After the completed prompt is displayed, select <Ok> or press **[Enter]** to exit from the `lastline_register` command.

Acquire Sandbox Images

Prerequisites

You have *installed the papi-client* (see page 7).

Configuration Steps

The images used by the malware analysis sandbox component must be downloaded from the Lastline backend to a staging server that can communicate with the Lastline backend. The sandbox images are subsequently copied to the Lastline Air Gap Manager, for example, by using an external USB drive.

The image files consist of approximately 40 GB of data. Depending on the available network bandwidth this step might take several hours.

Step 1: Mount an external USB drive

On the staging server, mount the external USB drive.

```
staging-host# mount /dev/sdc1 /media/usb0/
```

Then add a `[sandbox_images]` section in the `config.ini` file. For example:

```
[sandbox_images]
destination_dir = /media/usb0/sandbox-images/
# sandbox images revision to download
revision = 2018-03-02-01
# sets of sandbox images to download, comma-separated list
image_sets = windows
compressed = true
```

For more information about the `[sandbox_images]` section, see *About Lastline PAPI Client* on page 5.

Step 2: Download the sandbox images

Use the `lastline_download_sandbox_images.py` python script to download the sandbox images. The script accepts the following command line options:

`--config-file|-c` — Path of the configuration file.

`--destination-dir|-d` — Store downloaded sandbox images here (overrides configuration file).

`--revision` — Images revision to download (overrides configuration file).

`--image-sets` — Set of the images to download (overrides configuration file).

`--no-resume-incomplete` — If this flag is present, the script will not attempt to resume incomplete downloads.

`--force|-f` — If this flag is present, the script will download the sandbox images even if they are already present in the destination directory.

`--verbose|-v` — Enable verbose logging.

```
staging-host$ python scripts/lastline_download_sandbox_images.py -c config.ini
```

After the download completes, unmount the external USB drive. Remove it from the staging server and plug it into the Air Gap Manager.

Step 3: Install the downloaded sandbox images

Mount the external USB drive on the Air Gap Manager.

```
lastline@lastline-manager:~$ mount /dev/sdc1 /media/usb0/
```

Then install the downloaded sandbox images.

```
lastline@lastline-manager:~$ lastline_apply_update /media/usb0/sandbox-images/2018-03-02-01
```

After the installation completes, unmount the external USB drive and remove it from the Air Gap Manager.

Deploy a New Certificate

Configuration Steps

You can optionally replace the SSL/TLS certificate on the Lastline Air Gap Manager. Assuming the Air Gap Manager has a FQDN of `lastline.example.com`, the certificate needs to be valid for:

```
user.lastline.example.com

log.lastline.example.com

update.lastline.example.com

user.standby.lastline.example.com
```

We recommend using `user.lastline.example.com` as the **commonName** for the certificate. You should then specify the domain names above as Subject Alternative Name (SAN). This way `user.lastline.example.com` will work even for clients that do not support SAN. The certificate needs to be in x509 format. Intermediate CA certificates need to be appended to the server certificate file.

To create a private certificate using the `openssl` command and then deploy it on the Lastline Air Gap Manager, perform the following steps:

Step 1: Create a configuration file

Create an OpenSSL configuration file. For example, create the following file naming it `example.com.cnf`:

```
[ req ]
prompt = no
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
x509_extensions = v3_req

[ req_distinguished_name ]
commonName = user.lastline.example.com

[ v3_req ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = log.lastline.example.com
DNS.2 = update.lastline.example.com
DNS.3 = user.standby.lastline.example.com
```

Step 2: Generate the certificate

Generate the certificate using the `openssl` command. For example:

```
lastline@lastline-manager:~$ openssl req -x509 -newkey rsa:4096 \
-keyout usr.lastline.example.com.key -out usr.lastline.example.com.pem \
-days 365 -nodes -config example.com.cnf
```

The certificate must be trusted by all the appliances (that is, signed by a CA trusted by the operating system or manually added to the trusted set of certificates. See *Trust the New Certificate* (see page 15).

Step 3: Store the certificate

Copy the certificate to `/etc/puppet/files/ssl-cert/`.

```
lastline@lastline-manager:~$ cp usr.lastline.example.com.pem /etc/puppet/files/ssl-cert/
```

Step 4: Store the private key

Copy the private key to `/etc/puppet/private/ssl-priv-key/`.

```
lastline@lastline-manager:~$ cp usr.lastline.example.com.key /etc/puppet/private/ssl-priv-key/
```

Step 5: Integrate the certificate

Run the `lastline_apply_config` command. This step will also restart the `nginx` web server.

```
lastline@lastline-manager:~$ lastline_apply_config
```

Trust the New Certificate

Configuration Steps

To add an SSL/TLS certificate to the set of certificates trusted by Lastline Air Gap Manager, perform the following steps.

Note: The following steps must be completed on all appliances (including the Air Gap Manager).

Step 1: Add the certificate to the trusted set

Copy the certificate into the `/usr/local/share/ca-certificates/` directory. Ensure its extension is `.crt`.

```
lastline@lastline-manager:~$ cp /etc/puppet/files/ssl-cert/usr.lastline.example.com.pem \
/usr/local/share/ca-certificates/usr.lastline.example.com.crt
```

Step 2: Update the certificates

Run the `update-ca-certificates` command.

```
lastline@lastline-manager:~$ sudo update-ca-certificates
```

Administer the Air Gap Manager

The Lastline Air Gap Manager was developed to require as little maintenance and administration as possible.

The following topics describe how to customize and configure some of the advanced features of the Air Gap Manager.

Lastline Configuration Tool

Configuration Steps

Use the Lastline configuration tool, `lastline_setup`, to administer and manage the Lastline Air Gap Manager.

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-manager:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step 2: Run the help option

To view all the supported options, type `help`.

```
-> help
Documented commands (type help <topic>):
========================================
EOF                                    email_relay_host
analysis_max_upload_filesize_mb        email_relay_password
analysis_queue_backlog                 email_relay_port
anonvpn_dns_server_ip                  email_relay_username
anonvpn_mode                           email_sender_address
anonvpn_upstream_gateway_ip            exit
anonvpn_upstream_ifname                fqdn
appliance_state                        heartbeats
appliance_uuid                         help
cloud_analysis                         https_proxy
cloud_analysis_push_apk                image_brand_replacement
cloud_analysis_push_download_metadata  inject_interface
cloud_analysis_push_download_source    inline_interfaces
```

```
cloud_analysis_push_macho               license_api_token
cloud_analysis_query_url_reputation     license_key
data_retention_code                     llama_images_server_override
data_retention_generated_files          monitoring_user_password
data_retention_memory_dumps             network
data_retention_process_dumps            new_monitoring_user_password
data_retention_screenshots              ntp_server
data_retention_traffic_captures         ntp_servers
data_retention_uploads                  offline_mode
data_retention_webpages                 save
disable_report_commenting               show
disable_support_channel                 sniffing_interfaces
edit                                    text_brand_replacement
```

Tip: Type the first few characters of an option name then type **[Tab]**. The command will auto-complete the name for you.

Step 3: View help details

To view a detailed description of individual options, type `help` *`topic`*, where *`topic`* is the name of a specific option.

```
-> help network
 network <variable> [<new-value>]
        Get/set network settings.
            network interface <iface>: interface used for network access
            network method dhcp|static: use DHCP or static IP address
                configuration for network access
        When static configuration is used, these values must also be set:
            network address <address>: IPv4 address of the interface
            network netmask <netmask>: dotted-quad netmask for the address
            network gateway <gateway>: default gateway for network access; if
                specified value is -, set gateway to None
            network dns_nameservers <nameserver> ...: space-separated list of
                DNS nameservers, if specified value is -, set dns_nameservers to
                None
```

Step 4: Exit the configuration tool

To quit from the configuration tool without saving your changes, type `exit`.

```
-> exit
lastline@lastline-manager:~$
```

Troubleshooting

Important: If you encounter an error running any of the `lastline_setup` command options, make a note of the error message returned and *contact Lastline Technical Support* (see page 32).

Network Configuration

Configuration Steps

You can easily change the network configuration of the Lastline Air Gap Manager. This may be needed if its assigned IP address changes (for example, upon a reconfiguration of the network).

Reconfigure for DHCP

Configuration Steps

To enable a network configuration using DHCP, use the `network` option of the `lastline_setup` command.

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-manager:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step 2: Check the network settings

To check the current network settings, type `network`.

```
-> network
network dns_nameservers = 8.8.8.8 8.8.4.4
network gateway = 10.0.2.2
network netmask = 255.255.255.0
network address = 10.0.2.15
network interface = eth0
network method = static
```

Step 3: Enable DHCP configuration for network access

To enable DHCP addressing, type `network method dhcp`.

```
-> network method dhcp
network method = dhcp  # changed; original value: static
```

Step 4: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Reconfigure for Static Addressing

Configuration Steps

To enable a network configuration using a static IP, you must provide values for the **address**, **netmask**, **gateway**, and **dns_nameservers** parameters. Use the `network` options of the `lastline_setup` command to make these changes.

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-manager:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step 2: Check the network settings

To check the current network settings, type `network`.

```
-> network
network interface = eth0
network method = dhcp
```

Step 3: Enable static configuration for network access

To enable a static IP address, type `network method static`.

```
-> network method static
network method = static  # changed; original value: dhcp
```

Step 4: Set the network address

To set the IP address, type `network address` *`ip_address`*. Use an IPv4 address of four octets.

```
-> network address 10.0.2.15
network address = 10.0.2.15  # changed; original value:
```

Step 5: Set the netmask

To set the netmask, type `network netmask` *`netmask`*. Use an IPv4 netmask of four octets.

```
-> network netmask 255.255.255.0
network netmask = 255.255.255.0  # changed; original value:
```

Step 6: Set the gateway address

To set the gateway IP address, type `network gateway` *`ip_address`*. Use an IPv4 address of four octets.

```
-> network gateway 10.0.2.2
network gateway = 10.0.2.2  # changed; original value:
```

Step 7: Set the DNS server address(es)

To set the DNS server IP address, type `network dns_nameservers` *`ip_address`* `[`*`ip_address`*`]`. Use an IPv4 address of four octets for each address.

```
-> network dns_nameservers 10.2.1.1 10.2.2.1
network dns_nameservers = 10.2.1.1 10.2.2.1  # changed; original value:
```

Step 8: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Reconfiguration After Network Update

Configuration Steps

After a new network address has been assigned to Lastline Air Gap Manager (for example, after changing the static network address), the new configuration must be applied to all software on the host.

Step 1: Login to the console

Login to the console.

Step 2: Run the reconfiguration command

Execute the `lastline_apply_config` command, which will apply the new network address.

```
lastline@lastline-manager:~$ lastline_apply_config
```

Note: If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

SMTP Configuration

Configuration Steps

Lastline Air Gap Manager can be configured to send notifications or reset account passwords via email. To configure the way emails are sent, use the `email` options of the `lastline_setup` command.

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-manager:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step 2: Specify the SMTP relay host

To specify an SMTP relay host for delivering email messages, type `email_relay_host` *`fqdn`*.

```
-> email_relay_host smtprelay.example.com
email_relay_host = smtprelay.example.com  # changed; original value:
```

Step 3: Specify the SMTP relay port

To specify the port the SMTP relay host is listening on, type `email_relay_port` *`portnumber`*.

```
-> email_relay_port 25025
```

```
email_relay_port = 25025  # changed; original value:
```

Step 4: Specify the SMTP user

To specify the username to use when authenticating to the SMTP relay host (if required), type `email_relay_username` *`username`*.

```
-> email_relay_username admin
email_relay_username = admin  # changed; original value:
```

Step 5: Specify the SMTP password

To specify the password to use when authenticating to the SMTP relay host (if required), type `email_relay_password` *`password`*.

```
-> email_relay_password adminpassword
email_relay_password = adminpassword  # changed; original value:
```

Step 6: Specify the SMTP address

To specify the address from which to send emails, type `email_sender_address` *`emailaddress`*.

```
-> email_sender_address admin@example.com
email_sender_address = admin@example.com  # changed; original value:
```

Step 7: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Configure Honeypot AnonVPN

Configuration Steps

Lastline provides a secure tunnel for traffic generated inside the analysis sandbox, **AnonVPN** (Anonymization VPN), anonymizing the public IP of client connections. For the Lastline Air Gap Manager, a `honeypot` mode is available. Analysis traffic is not routed to the Internet. Instead any connections established inside the sandbox are redirected to the honeypot on the appliance.

The system supports the analysis of artifacts in a completely isolated network, without any outgoing connectivity. Because programs often require access to certain services on the Internet to function, the system emulates a set of services that use well-known protocols, such as (but not limited to) DNS, FTP, HTTP, HTTPS, and SMTP.

Any outgoing traffic using an unknown protocol is blocked to avoid accessing services in the local network.

Note: In `honeypot` mode, the analysis of URLs in the sandbox will fail. Since no traffic is allowed on the Internet, when the analysis engine attempts to access a URL that was submitted for analysis, it is unable to open the connection to the URL, and reports an error. As a consequence, the URL analysis fails and no report is generated.

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-manager:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step 2: Specify the honeypot VPN connection

To enable AnonVPN in `honeypot` mode, type `anonvpn_mode`.

```
-> anonvpn_mode honeypot
anonvpn_mode = honeypot  # changed; original value: lastline
```

Step 3: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Update Fully Qualified Domain Name

Configuration Steps

You can update the FQDN of the Lastline Air Gap Manager. This also creates a new self-signed certificate associated with the FQDN.

Important: After you complete the following steps, you must update all the Lastline appliances managed by Lastline Air Gap Manager to use the new FQDN. Refer to *Update On-Premises Manager FQDN* in the respective appliance installation guides.

Step 1: Login to the console

Login to the console.

Step 2: Run the registration process with the change FQDN option

Execute the `lastline_register` command, providing the new local FQDN for the Lastline Air Gap Manager in its arguments. This updates the original FQDN as shown in Register the Air Gap Manager, *Step* 5 (page 11).

```
lastline@lastline-manager:~$ lastline_register --change-local-fqdn new_manager.lastline.example.com
```

Note: If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step Result

The command generates a new self-signed certificate. If needed, you can replace the certificate.

Configure the Analysis Upload-Size Limit

Configuration Steps

By default, the system rejects uploads of files for analysis that are larger than 10MB. This value provides a reasonable compromise between the ability to analyze the vast majority of malicious artifacts and having to store overly large files. If required, you can modify this limit up to 100MB.

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-manager:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step 2: Modify the size limit for uploads

To modify the size limit for files that can be uploaded, type `analysis_max_upload_filesize_mb` *`size`*. Provide a *`size`* between 10 and 100.

```
-> analysis_max_upload_filesize_mb 100
analysis_max_upload_filesize_mb = 100  # changed; original value:
```

Step 3: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Configure Data Retention

Configuration Steps

The system tracks all of the stored files on the appliance and issues a notification through the web-based interface when usage of the local file-system disk exceeds certain thresholds.

Periodically, large analysis artifacts (such as the metadata that an analysis generates), are deleted according to data-retention policies that can be updated using the `lastline_setup` command. The following is a full list of its options:

`data_retention_uploads` — Files uploaded for analysis.

`data_retention_screenshots` — Screenshots taken during the dynamic analysis of a file submitted for analysis.

`data_retention_traffic_captures` — Network traffic captured during the dynamic analysis of a file submitted for analysis.

`data_retention_generated_files` — Files generated by a program during the dynamic analysis of a file submitted for analysis.

`data_retention_memory_dumps` — Memory allocation by a program during the dynamic analysis of a file submitted for analysis.

`data_retention_process_dumps` — Full-process snapshot of a program during the dynamic analysis of a file submitted for analysis.

`data_retention_webpages` — Web-page content captured during the analysis of a URL submitted for analysis.

`data_retention_code` — Web-code captured during the analysis of a URL submitted for analysis.

To avoid specific file-types from being affected by the data-retention policies, you can use the value `unlimited` (or `0`).

The following steps show how to define your configuration to discard files generated during an analysis run after 90 days, but to keep files uploaded for analysis indefinitely:

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-manager:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step 2: Modify the retention for generated files

To retain generated files to 90 days, type `data_retention_generated_files 90 days`.

```
-> data_retention_generated_files 90 days
data_retention_generated_files = 90 days  # changed; original value:
```

Step 3: Modify the retention for uploaded files

To retain uploaded files indefinitely, type `data_retention_uploads unlimited`.

```
-> data_retention_uploads unlimited
data_retention_uploads = unlimited  # changed; original value:
```

Step 4: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Configure Cloud Analysis

Cloud analysis is automatically disabled on Lastline Air Gap Manager. Therefore, no analysis data is queried and shared with the Lastline backend.

Configure the Analysis Queue

Configuration Steps

In some situations, it is convenient to automatically drop tasks scheduled for analysis from the queue. This way, even systems with limited resources can guarantee analyzing submitted artifacts in a timely manner, even when it is temporarily overloaded with a large number of submission.

The system allows this by pruning tasks from the analysis queue that have been pending for longer than a specified amount of time.

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-manager:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default user account, `lastline`.

Step 2: Specify the number of days of the analysis queue backlog

To specify the number of days tasks may remain in the analysis queue backlog, type `analysis_queue_backlog` *`days`*. The default is `unlimited`. Typing this option without an argument displays its current value.

```
-> analysis_queue_backlog 12
analysis_queue_backlog = 12 days  # changed; original value: unlimited
```

Step 3: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Test the Air Gap Manager

Configuration Steps

Check the state of the Lastline Air Gap Manager with the `lastline_test_appliance` command.

Step 1: Start the test appliance tool

Execute the `lastline_test_appliance` command.

```
lastline@lastline-manager:~$ lastline_test_appliance

> Lastline appliance check and fix utility.
>
> Version 2.0
>
> :Copyright:
>     Copyright 2014 Lastline, Inc.  All Rights Reserved.
...
```

Step Result

The `lastline_test_appliance` command takes for a few minutes to perform its analysis of the Air Gap Manager. When it is done, it provides a summary of the conditions it uncovered, if any.

Step 2: *Optional:* Fix any reported configuration errors

The test appliance tool checks for signs of common configuration errors and can help you with fixing them.

Note: *Contact Lastline Technical Support* (see page 32) if the test appliance tool displays an error that you cannot fix. Provide the error message that was displayed.

Update the Lastline Air Gap Manager

Configuration Steps

Lastline periodically releases appliance updates or hotfixes. However, the Lastline Air Gap Manager cannot automatically upgrade or receive information about the latest appliance versions. This also means that any dependent appliances cannot be upgraded to the latest available version, either automatically or manually, until the Lastline Air Gap Manager appliance has been upgraded.

Similarly to the *installation process* (see page 2), you must download the Air Gap installation ISO image for the latest version of the Lastline Air Gap Manager. You must also download the latest *threat intelligence bundle* (see page 9) and *license bundle* (see page 7). Once the downloads are complete, transfer the ISO and bundles to the Air Gap Manager, and then run the `lastline_apply_update` command.

Step 1: Download the air-gap installation ISO image

Browse to *Lastline Portal* (https://user.lastline.com/) and then login. Your account must be granted *can_operate_offline* permission before you can access the ISO image for the Air Gap Manager installation.

Download the air-gap installation ISO image to your staging server.

Step 2: Download the license and threat intelligence bundles

For the license bundle, see *Download Air Gap License*, *Step* 1 (page 8). For the threat intelligence bundle, see *Download Threat Intelligence*, *Step* 1 (page 9).

Step 3: Copy the downloaded data to an external USB drive

Mount a USB drive on your staging server and copy the ISO, the threat intelligence bundle, and the license bundle to it.

Step 4: Install the downloaded ISO image

Mount the external USB drive on the Air Gap Manager. Then run the `lastline_apply_update` command:

```
lastline@lastline-manager:~$ lastline_apply_update /media/usb0/offline_appliance.iso \
/media/usb0/licensing_bundle.zip /media/usb0/threat_intel_bundle.tar.gz
```

In the above example `/media/usb0/` is the mount location of the USB drive and `offline_appliance.iso` is the name of the ISO image. You can specify the options in any order.

Step 5: Update the malware analysis sandbox images

Refer to *Acquire Sandbox Images* on page 11 for instructions on how to update malware analysis sandbox images to the latest revision.

Update Threat Intelligence

Prerequisites

You have *installed the papi-client* (see page 7).

Configuration Steps

The Lastline Air Gap Manager cannot receive automatic periodic updates, since it is disconnected from the Lastline backend. The most important missing data is threat intelligence information, which includes information about new malware, malware classes, updated blacklists, and other vital data.

In order to keep the threat intelligence information up-to-date, we provide downloadable updates in the form of threat intelligence bundles.

The process for updating the threat information is to download the threat intelligence bundles to your staging server, copy the data to the Air Gap Manager, then run the `lastline_apply_update` to install the data. This process must be run frequently, at least weekly. Hourly updates would be the optimal choice.

Step 1: Download the threat intelligence bundle

Use the `download_and_deploy_offline_bundle.py` python script to download the threat intelligence bundle.

```
staging-host$ python scripts/download_and_deploy_offline_bundle.py  --download-bundle
```

Alternatively, you can login to your *Lastline Portal* (https://user.lastline.com/) account (your account must be granted *can_operate_offline* permission), then point your browser to https://user.lastline.com/papi/intel/offline/get_offline_bundle.

Step 2: Transfer the downloaded threat intelligence bundle to the Air Gap Manager

Save the downloaded bundle to, for example, `/tmp/bundle.tar.gz`, on the Air Gap Manager

Step 3: Install the threat intelligence update

Use the `lastline_apply_update` command to install the downloaded threat intelligence bundle.

```
lastline@lastline-manager:~$ lastline_apply_update /tmp/bundle.tar.gz
```

Download License Updates

Prerequisites

You have *installed the papi-client* (see page 7).

Configuration Steps

You cannot automatically update any license information for the Lastline Air Gap Manager and it cannot be edited locally. Instead you must download the updated license bundles to your staging server from the Lastline backend.

Step 1: Update license information of the *Lastline Portal* (https://user.lastline.com/)

Login to your account on the *Lastline Portal* (https://user.lastline.com/). Click the **[≡]** icon in the header to expose the **Main menu**, then click **[⚙ Admin]** . On the **Admin** page, select **Licensing** from pull-down menu. Then click the **License information** tab.

You can make the following changes on this tab:

- Update customer information
- Update main account information
- Add new licenses
- Update licenses information, for example, extending a license that is going to expire
- Add new sensors
- Update sensors information

Any material changes will result in an updated license being issued. *Contact Lastline Technical Support* (see page 32) for the updated license.

Step 2: Download the license bundle

Login to your *Lastline Portal* (https://user.lastline.com/) account (your account must be granted *can_operate_offline* permission), then point the browser to https://user.lastline.com/papi/accounting/license_bundle/get?access_key=*installation_access_key*, where you substitute *installation_access_key* in the URL with the **Installation Key** of your license. This key is a string of characters, for example *ABCDEFGHIJ0123456789*.

Save the bundle on your staging server, for example `/tmp/licensing_bundle.zip`.

Step 3: Copy the downloaded licensing bundle to the Air Gap Manager

Step 4: Install the updated license

Use the `lastline_apply_update` command to install the downloaded licensing bundle.

```
lastline@lastline-manager:~$ lastline_apply_update /tmp/licensing_bundle.gz
```

Step Result

The Air Gap Manager will report its updated license.

Technical Support

For technical support issues, login to your account at the *Lastline Support Portal* (https://lastline.zendesk.com/hc) and submit a support ticket. Alternatively, send email to support@lastline.com.

License Extensions

To renew an expired license, contact sales@lastline.com. Once your request has been processed, licensing information is automatically downloaded by Lastline Air Gap Manager and updated locally. However, see *Download License Updates* on page 30 for Air Gap Air Gap Manager.

Legal Notice

Trademarks

Open Source Software

Lastline appliances and containers run on *Ubuntu Linux* (https://www.ubuntu.com/) and therefore use code from a number of open-source projects. For a full list of open-source packages included and attribution of authorship and license/copyright, refer to https://update.lastline.com/updates/distros/open-source-licenses.txt.