Troubleshooting Guide for Advanced Malware Detection AirGap v1.0

Staging server and script

When run, Papi_client python scripts can fail to start and produce a python error.

```
root@staging-server:~/amd-airgap/papi_client# python
scripts/download_and_deploy_offline_bundle.py --download-
bundle
Traceback (most recent call last):
File "scripts/download_and_deploy_offline_bundle.py", line
19, in <module>
    import papi_client.papi_client
ImportError: No module named papi_client.papi_client
```

This error is caused by the python script not being able to import all modules it expects.

Workaround options:

1. Adjust PYTHONPATH environment variable to include papi_client folder with needed modules in it. Exact details are OS dependent.

   Example for linux:

   `'export PYTHONPATH=.' in the papi_client root folder`
2. Copy papi_client folder into scripts folder.

   Example for linux:

   `'cp -r papi_client scripts'`

Installing and registering ISO

For detailed steps on installation of the ISO including registration, see the Lastline Manager Airgap Installation Manual.

© 2020 Forcepoint

Licensing

If there is more than one license and user account provided, when registering, use the main account that was created. The main account email is what is used when downloading and authenticating your account for registration.

User Accounts

If you have created additional accounts within cloud portal, you may have trouble registering the appliance.

Cloud portal accounts do not get propagated to the Advanced Malware Detection Airgap Manager. Be sure to complete installation and registration on the Advanced Malware Detection Manager first, and use the On-Premises Manager portal to create additional accounts.

Download File Reputation

A new Threat Intelligence update bundle is available. See the Installation Manual for update instructions.

Update Manager ISO

Forcepoint makes periodic releases available that include updates or hotfixes. However, the Forcepoint Advanced Malware Detection AirGap Manager by its offline nature cannot automatically upgrade or receive information about the latest versions. Follow the first time installation process (see page 2) of the Installation Manual. The AirGap Manager installation ISO image is available from the Forcepoint Support Download pages. Ensure to update all Advanced Malware Detection Engines to latest version when updating Advanced Malware Detection AirGap Manager, as the versions of Manager and Engine must remain in sync.

You must also download the latest license bundle (see page 7) and threat intelligence bundle (see page 9). Once the downloads are complete, transfer the ISO and bundles to the Advanced Malware Detection AirGap Manager, and then run the "lastline_apply_update" command.

How often should user update file reputations

It is recommended to update the threat intelligence bundle as frequently as possible. At a minimum, we recommend at least daily and multiple times a day for highly secure locked down environments.

Engine compatibility

To ensure engine compatibility with the Advanced Malware Detection Airgap Manager, please download and install that latest versions for both Advanced Malware Detection Airgap Manager and Advanced Malware Detection Engine.

Get the latest versions of Advanced Malware Detection by downloading it from the Forcepoint Support Page.

Note

For on-premises instances, ensure that the Advanced Malware Detection Manager is the same version as the Advanced Malware Detection Engine if updating to latest Advanced Malware Detection Engine.

Advanced Malware Detection Engine update

The Advanced Malware Detection Engine might be in an error state after the Advanced Malware Detection AirGap Manager update.

Download latest sandbox images and upgrade the images in Advanced Malware Detection AirGap Manager as described in the Installation Guide, then trigger reconfiguration for the Advanced Malware Detection Engine.

© 2020 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.