



# Illumio Adaptive Security Platform Advanced Command-line Interface Tool 1.1.0 Release Notes

---

12/03/2018

16000-100-1.1.0

## Table of Contents

|   |          |
|---|----------|
| <b>Welcome</b> .....  | <b>3</b> |
| <b>Product Version</b> .....  | <b>3</b> |
| About CLI Tool Version Numbering and Software.....                    | 3        |
| <b>About Illumio</b> .....  | <b>3</b> |
| Illumio Professional Services for Deployment.....                     | 3        |
| Preview Features Only for Evaluation Before General Availability..... | 3        |
| Illumio Adaptive Security Platform Training .....                     | 4        |
| Search Knowledge Base and Documentation.....                          | 4        |
| Illumio Adaptive Security Platform Support.....                       | 4        |
| <b>About the Advanced Command-Line Interface Tool</b> .....           | <b>4</b> |
| Supported Operating Systems .....                                     | 5        |
| Linux .....   | 5        |
| Microsoft Windows.....  | 5        |
| <b>New Vulnerability Data Formats</b> .....                           | <b>5</b> |
| Nessus Professional.....  | 5        |
| Rapid7.....   | 5        |
| Tenable Security Center .....   | 6        |
| Change in Syntax for Uploading Vulnerability Data .....               | 6        |
| <b>Resolved Issues</b> .....  | <b>7</b> |
| <b>Known Issues</b> .....   | <b>7</b> |
| <b>Documentation</b> .....  | <b>7</b> |

## Welcome

These release notes describe the new features and enhancements for the Illumio Adaptive Security Platform (ASP) Advanced Command-line Interface Tool 1.1.0 release.

## Product Version

**Current CLI Tool Version:** 1.1.0

The Illumio Adaptive Security Platform Advanced Command-Line Interface Tool is compatible with Illumio Adaptive Security Platform (ASP) versions 17.1 and later.

## About CLI Tool Version Numbering and Software

The Illumio ASP Advanced Command-Line Interface (CLI) Tool version numbering is independent from the release and version numbering of Illumio ASP PCE and VEN. The CLI tool works with multiple versions of the PCE and the VEN and does not necessarily need software changes in parallel with releases of the PCE and the VEN.

## About Illumio

Copyright © 2013-2019 Illumio, Inc. All rights reserved. 920 De Guigne Drive, Sunnyvale, CA 94085.

Illumio products and services are built on Illumio's patented technologies. For more information, see [Illumio Patents](#).

## Illumio Professional Services for Deployment

To ensure optimal deployment of the Illumio Adaptive Security Platform, contact your Illumio Professional Services representative.

## Preview Features Only for Evaluation Before General Availability

Any preview features in this release of Illumio Adaptive Security Platform are for your evaluation only.

**⚠ Do not deploy preview features in a production environment**

Be sure to install these preview features only on non-production systems. To avoid inadvertently impacting your current operations, do *not* install the preview features on production systems. The purpose of preview features is to make them more useful for your needs before general availability.

Illumio welcomes your comments and suggestions for improving preview features and documentation. For more information and to send feedback, contact Illumio Customer Support.

## Illumio Adaptive Security Platform Training

Illumio offers a wide yet focused training curriculum for Illumio Adaptive Security Platform, from beginning to advanced topics.

To see available courses, log into your [Illumio support account](#) and select the **Training** tab.

## Search Knowledge Base and Documentation

For useful short articles about Illumio Adaptive Security Platform, log into your [Illumio support account](#) and select the **Knowledge Base** or **Documentation** tab.

## Illumio Adaptive Security Platform Support

If you cannot find what you are looking for in this document or in support Knowledge Base and Documentation, contact us at:

- [support@illumio.com](mailto:support@illumio.com)
- +1-888-631-6354
- +1-408-831-6354

## About the Advanced Command-Line Interface Tool

With the Illumio Adaptive Security Platform Advanced Command-Line Interface (CLI) Tool, you can manage many of your PCE's resources directly from your local computer.

You can use the CLI tool to:

- Upload vulnerability data for analysis with Illumination®. After data upload, for information about vulnerability maps, see the *Illumio ASP PCE Web Console User Guide*.
- Help with automated management, such as security policy import and export.
- Help with tasks such as directly importing workload information to create workloads in bulk.

- Create, view, and manage your organization's security policy rules, rulesets, labels, and other resources.

## Supported Operating Systems

### Linux

- RHEL/CentOS, versions 6 and 7
- Ubuntu, versions 14.04 and 16.04

### Microsoft Windows



#### **Windows 64-bit CPU Architecture required**

The CLI tool is not supported on Windows 32-bit CPU architecture. Ensure that you run it on Windows 64-bit CPU architecture.

- Microsoft Windows Server 2008R2, 64-bit
- Microsoft Windows 10, 64-bit
- Microsoft Windows 7, 64-bit

## New Vulnerability Data Formats

In addition to previously supported vulnerability data formats, the CLI Tool now supports uploading the following vulnerability data formats.

### Nessus Professional

Vulnerability data from Nessus Professional can be uploaded with the following CLI tool option:

```
ilo upload_vulnerability_report --source-scanner nessus-pro
```

See "Change in Syntax for Uploading Vulnerability Data".

### Rapid7

The CLI tool supports uploading vulnerability data from Rapid7.

**⚠️ Rapid7 data exported in Qualys format**

Before uploading to the PCE, Rapid7 vulnerability data must have been exported in Qualys XML format from Rapid7 with Qualys XML Export.

Rapid7 data exported in Qualys XML format can be uploaded with the following command:

```
ilo upload_vulnerability_report --source-scanner qualys
```

See "Change in Syntax for Uploading Vulnerability Data".

## Tenable Security Center

Tenable Security Center can be uploaded to the PCE in any of the following formats:

- CSV:

```
ilo upload_vulnerability_report --source-scanner tenable-sc --format csv
```

- Direct API for Tenable:

```
ilo upload_vulnerability_report --source-scanner tenable-sc --format api --api-server
ApiServerFQDNandPort --api-user username
```

## Changes Since Previous Release

### Change in Syntax for Uploading Vulnerability Data

The syntax of the `ilo` command for uploading vulnerability data has changed.

- Former syntax in CLI Tool 1.0.0:

```
ilo upload_qualys_report --input-file datafile.xml [--authoritative]
```

- New syntax in CLI Tool 1.1.0. New command-line options are highlighted:

```
ilo upload_vulnerability_report --input-file datafile.xml --source-scanner [nessus-
pro|qualys|tenable-sc] --format [xml|csv|api] [--authoritative]
```

The `--source-scanner qualys` argument is to upload both Qualys and Rapid7 vulnerability data. See "Rapid7".

See the *Illumio Adaptive Security Platform Advanced Command-Line Interface Tool Guide*.

## Resolved Issues

- **ilo login --server with URL printed stack trace (C-159)**  
When a user logged into the PCE and incorrectly specified a URL with the `ilo login --server` option instead of the server FQDN, a stack trace was displayed. This issue is resolved and the PCE now displays an error message.
- **Entering the ilo login\_user password command displayed an error (C-237)**  
When a user entered the `ilo login_user password` command without an argument, the CLI Tool displayed an undefined method error. This issue is resolved. The CLI Tool now displays a useful message prompting the user to check their command line syntax.
- **CLI Tool displayed OpenSSL::SSL:SSLError (C-129)**  
In this release, when an `ilo` command fails because of a certificate validation error, the CLI Tool now displays a user-friendly error message.

## Known Issues

These are the known issues in CLI Tool 1.1.0.

- **ilo --exclude-all-svc --json option outputs incorrect JSON (C-145)**  
The `ilo` command option `--exclude-all-svc --json` option results in incorrect JSON.
- **Single dash on ilo option --workload-id displays incorrect error message (C-20)**  
With only one dash on the `--workload-id` option, the `ilo` command displays the incorrect error message. All `ilo` command options require two leading dashes.
- **Spaces in comma-separated list of ilo command arguments do not generate error (C-8)**  
Extra spaces in the command-separated list of arguments on many `ilo` command options does not display an error message. There must be no spaces in a list of arguments.
- **More than 500 labels on workload sync command might fail (C-7)**  
Trying to process more than 500 labels with `ilo workload --label_sync_csv` can cause the command to fail intermittently.  
**Workaround:** Run the command with a decreased number of records and repeat as many times as necessary to complete the sync.
- **Existing Windows installation cannot be upgraded (C-375)**  
Trying to upgrade an existing Windows installation to CLI 1.1.0 fails.  
**Workaround:** Manually uninstall the existing Illumio CLI first.

## Documentation

The *Illumio Adaptive Security Platform Advanced Command-Line Interface Tool Guide* describes installation, setup, usage, and tutorials for the CLI tool.