Illumio ASP 18.1 FIPS Addendum for PCE and VEN

Last Updated: 05/18/2018

Table of Contents

About Illumio

Illumio's products and services are built on our patented technologies. For information on Illumio's patents and patent applications, see https://www.illumio.com/patents.

Illumio ASP Training

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

To see available courses, login to your Illumio Support account and select the **Training** tab.

Search Knowledge Base and Documentation

For useful short articles about Illumio ASP, login to your Illumio Support account and select the **Knowledge Base** or **Documentation** tabs.

Illumio Support

If you cannot find what you are looking for in this document or the support knowledge base and documentation, contact us at:

- support@illumio.com
- +1-888-631-6354
- +1-408-831-6354

Recommended Skills

This document assumes your familiarity with the following:

- FIPS 1402-2 standard
- Illumio ASP PCE and VEN deployment and operations

Related Documentation

- *PCE Deployment guide*: requirements, planning, and installing the Policy Compute Engine (PCE)
- *PCE Operations guide: common* operational tasks on the Policy Compute Engine (PCE)
- *VEN Deployment guide:* installing and activating the Virtual Enforcement Node (VEN) on workloads
- *VEN Operations guide:* administering the Virtual Enforcement Node (VEN) directly on managed workloads

Overview to Illumio ASP 18.1-FIPS Release

In addition to the standard release of the Illumio Adaptive Security Platform (ASP) 18.1 GA, the Illumio ASP 18.1-FIPS release is now available for government customers who are required to comply with the NIST FIPS 140-2 standard.

This release supports FIPS compliance for the Policy Compute Engine (PCE) and Virtual Enforcement Node (VEN) on Linux and Windows. The 18.1-FIPS release is not supported for the PCE Virtual Appliance or the AIX and Solaris versions of the VEN.

This addendum details the operational requirements for FIPS compliance for both the PCE and the Linux and Windows VEN.

Non-Government Customers with No FIPS Requirement - Standard, not FIPS, 18.1 Release

Because the 18.1-FIPS release requires additional operational restrictions, such as specific operating system versions and server hardware models, Illumio recommends that non-government customers who have no requirement for FIPS 140-2 do not install the the 18.1-FIPS release. Instead, non-government customers should select the standard Illumio ASP 18.1 GA.

Compliance Affirmation Letters

Illumio ASP 18.1-FIPS is compliant with the NIST FIPS 140-2, Level 1 standard. Letters of affirmation are available on Illumio's Federal Solutions page.

Obtaining the FIPS-Compliant Release

To obtain to the Illumio ASP 18.1-FIPS release, contact your Illumio Sales Representative.

FIPS Compliance for the PCE

Prerequisites for PCE FIPS:

1. PCE server hardware requires Intel Ivy Bridge CPU (2012) or later
2. RHEL v7.4 required
3. Customer provided PCE certificates with a minimum RSA key size of 2048

Steps to operate the PCE in FIPS mode:

1. After installing RHEL7.4, follow Section 9.1 ("Crypto Officer Guidance") of the Red Hat Enterprise Linux OpenSSL Cryptographic Module NIST Security Policy.
2. Reboot the machine. After the OS boots, the setting `/proc/sys/crypto/fips_enabled` should be equal to 1.
3. Install 18.1-FIPS RPM as detailed in the PCE Deployment Guide.
4. During PCE installation, provide the PCE with certificates that contain a minimum RSA key size of 2048.
5. After completing the remainder of the PCE set up, the PCE will be operating in a FIPS compliant mode.

FIPS Compliance for Linux Workloads

For all Illumio-supported Linux Workloads, the standard 18.1 GA VEN release is the minimum ASP version required to operate VEN Linux as FIPS-compliant. Note that there is no special FIPS release for the VEN because the standard 18.1 GA release supports FIPS compliance for both VEN Linux and VEN Windows. With the VEN Linux 18.1 release, all VEN OpenSSL communications by default operate in a FIPS compliant mode. Because the VEN Linux OpenSSL module is built directly into the VEN (as opposed to being supplied by the underlying OS) there are no special Linux version requirements and there are no additional configurations required on the VEN to enable FIPS compliant OpenSSL communications.

To claim FIPS compliance for the VEN SecureConnect feature (IPSec encryption between workloads), the VEN must be installed on either RHEL v7.1 or RHEL v7.4 and configured to operate in FIPS mode as documented in Section 9.1 ("Cryptographic Officer Guidance") of the RHEL v7.1 Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v4.0 or in Section 9.1 ("Cryptographic Officer Guidance") of the RHEL v7.4 Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v5.0.

FIPS Compliance for Windows Workloads

For Windows Workloads, the standard 18.1 GA VEN release is the minimum ASP version required to operate VEN Windows as FIPS-compliant. VEN Windows supports FIPS compliance when installed on either Windows Server 2012 or Windows Server 2016. To operate the VEN in a FIPS compliant manner, the Windows server must be configured to operate in FIPS mode as documented in Section 2 of the Windows Server 2012 NIST Security Policy or Section 2 of the Windows Server 2016 NIST Security Policy.