Pexip Infinity
Certification & Security Overview

Overview

The Pexip Infinity collaboration platform was designed with security as a primary focus. Leveraging architectural design combined with industry standard encryption and security protocols has afforded quick and easy achievement of the highest industry certifications. Despite being written for specific verticals, namely the United States (U.S.) Federal Government, these points of validation directly apply across a wide landscape, including global commercial, enterprise, government, and defense networks.

This document is intended to provide an overview of the public certifications and secure deployment of the Pexip Infinity collaboration platform. Links to the public reference points for the certifications are included inline.

United States Department of Defense Joint Interoperability Test Command Certification

On 26 March 2015, Pexip received a letter of certification and full listing on the Approved Products List (APL) from the U.S. Department of Defense (DoD) Joint Interoperability Test Command (JITC). In order to be certified as a Unified Capabilities Conferencing System (UCCS), the Pexip Infinity platform was rigorously tested against Information Assurance (IA) and Interoperability (IO) requirements to ensure the system not only protects the integrity of the DoD networks on which its installed but will fully interoperate with all other installed Unified Capabilities (UC) platforms already installed in customer networks.

Why is this important?

In practice, the JITC certification process affords manufacturers, such as Pexip, to focus development and testing efforts around a single validation process. This allows security conscious customers – not only those in the U.S. DoD, but others around the world – to leverage a single point of reference, streamlining adoption and deployment in their networks. As a part of the certification process, vendors, including Pexip, must supply a "Secure Deployment Guide" (more information contained later in this document) that outlines the configuration parameters as tested within the JITC labs. Any configuration variations must be reviewed by the site Security Officers to ensure IA posture will not be compromised.

The public information regarding the JITC APL listing can be found online directly on the JITC website: https://aplits.disa.mil. U.S. DoD customers can obtain more information regarding this certification directly from JITC and the Unified Capabilities Certification Office (UCCO).

U.S. Federal Information Processing Standard 140-2 Compliance

The Pexip implementation of the OpenSSL v2.0.5 as enabled in the Pexip Infinity Security Wizard (more details available in the "Secure Deployment Guide," below), as delivered via the Pexip Linux kernel (PexOS 1.0), was validated on 20 December 2013 to be compliant with the Federal Information Processing Standard (FIPS) 140-2 guidelines. The OpenSSL FIPS 140-2 validation can be found online directly on the National Institute of Standards and Technology (NIST) website. The PexOS 1.0 validation can be found directly under the OpenSSL Software Foundation v2.0.5 certification, certificate # 1747 and # 2454.

Why is this important?

Implementation of a FIPS 140-2 certified encryption algorithm allows public and private sector customers around the globe to reference a generally accepted process used to secure data within the Pexip Infinity platform. Similar to the JITC certification,

NIST publicly maintains an active certification records list and compliant modules that have implemented said modules. Verification can be found directly from the NIST website: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

Deployment Guidelines

Documentation of the configuration parameters used in JITC certification can be found via Pexip's "Secure Deployment Guide" (direct link to the live online document: http://docs.pexip.com/admin/secure_mode.htm). This guide outlines a number of considerations and configuration guidelines that are specifically focused around the security requirements of the certifications listed above. The guide is a living document and will be maintained on Pexip's website, updated for each version of software.

It is important to note this document is specifically structured around some of the guidelines required for JITC certification. For example, disabling some configuration and operational features are required for DoD deployments and not necessarily required for other environments. As a result, each organization should consider the configuration parameters as they translate to their environment and take appropriate action.

Questions?

If you have any questions, please reach out to your local Pexip representative or to the support team via email (support@pexip.com).