Notice: This document contains information on products in the design phase of development. The information here is subject to change without notice. Do not finalize a design with this information.

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Warning: Altering PC clock or memory frequency and/or voltage may (i) reduce system stability and use life of the system, memory and processor; (ii) cause the processor and other system components to fail; (iii) cause reductions in system performance; (iv) cause additional heat or other damage; and (v) affect system data integrity. Intel assumes no responsibility that the memory, included if used with altered clock frequencies and/or voltages, will be fit for any particular purpose. Check with memory manufacturer for warranty and additional details.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance. Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Intel is a sponsor and member of the Benchmark XPRT Development Community, and was the major developer of the XPRT family of benchmarks. Principled Technologies is the publisher of the XPRT family of benchmarks. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, Intel TXT, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2019, Intel Corporation. All Rights Reserved.
Contents

1 Introduction .................................................................................. 10
  1.1 Overview .................................................................................. 10
  1.1.1 Trusted Computing .......................................................... 10
  1.1.2 Intel® Security Libraries for Datacenter Features .......... 13

2 Intel® Security Libraries Components ............................................ 16
  2.1 Certificate Management Service ............................................. 16
  2.2 Authentication and Authorization Service ................................ 16
  2.3 Verification Service ............................................................... 16
  2.4 Workload Service ................................................................. 17
  2.5 Trust Agent ............................................................................. 17
  2.6 Workload Agent ................................................................. 17
  2.7 Integration Hub ................................................................. 17
  2.8 Workload Policy Manager ................................................... 18
  2.9 Key Broker Service .............................................................. 18

3 Intel® Security Libraries Installation ............................................. 19
  3.1 Building from Source ............................................................. 19
  3.2 Recommended Service Layout .............................................. 19
    3.2.1 Platform Integrity ............................................................ 19
    3.2.2 Workload Confidentiality .............................................. 20
  3.3 Installing the Certificate Management Service ...................... 20
    3.3.1 Required For ................................................................. 20
    3.3.2 Package Dependencies .................................................. 21
    3.3.3 Supported Operating Systems .................................... 21
    3.3.4 Recommended Hardware ........................................... 21
    3.3.5 Installation ................................................................. 21
  3.4 Installing the Authentication and Authorization Service ............ 22
    3.4.1 Required For ................................................................. 22
    3.4.2 Prerequisites ................................................................. 22
    3.4.3 Package Dependencies .................................................. 22
    3.4.4 Supported Operating Systems .................................... 22
    3.4.5 Recommended Hardware ........................................... 22
    3.4.6 Installation ................................................................. 23
  3.5 Installing the Verification Service .......................................... 25
    3.5.1 Required For ................................................................. 25
    3.5.2 Package Dependencies .................................................. 25
    3.5.3 Supported Operating Systems .................................... 25
    3.5.4 Recommended Hardware ........................................... 25
    3.5.5 Installation ................................................................. 26
    3.5.6 Creating Service Users ................................................ 26
  3.6 Installing the Workload Service .............................................. 27
    3.6.1 Required For ................................................................. 27
    3.6.2 Prerequisites ................................................................. 27
    3.6.3 Package Dependencies .................................................. 27
    3.6.4 Supported Operating Systems .................................... 27
    3.6.5 Recommended Hardware ........................................... 28
3.6.6  Installation...............................................................28
3.7  Installing the Trust Agent for Linux.................................29
   3.7.1  Required For..........................................................29
   3.7.2  Package Dependencies..............................................29
   3.7.3  Supported Operating Systems ....................................29
   3.7.4  Prerequisites..........................................................30
   3.7.5  Installation............................................................30
3.7.6  Installing the Workload Agent.......................................32
3.8  Installing the Trust Agent for Windows.............................32
   3.8.1  Required For..........................................................32
   3.8.2  Supported Operating Systems ....................................32
   3.8.3  Prerequisites..........................................................32
   3.8.4  Installation............................................................34
3.9  Trust Agent Provisioning .................................................35
3.10 Trust Agent Registration ................................................35
3.11 Importing the HOST_UNIQUE Flavor....................................37
3.12 Installing the Integration Hub.........................................37
   3.12.1  Required For..........................................................37
   3.12.2  Package Dependencies..............................................38
   3.12.3  Supported Operating Systems ....................................38
   3.12.4  Prerequisites..........................................................38
   3.12.5  Recommended Hardware .......r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r........r....r....
12.1.2 Configuration Options ........................................ 124
12.1.3 Command-Line Options ..................................... 127
12.1.4 Directory Layout .............................................. 130
12.2 Trust Agent ....................................................... 131
  12.2.1 Installation Answer File Options ........................ 131
  12.2.2 Configuration Options .................................... 135
  12.2.3 Command-Line Options .................................. 137
  12.2.4 Directory Layout .......................................... 139
12.3 Integration Hub .................................................. 139
  12.3.1 Installation Answer File .................................. 139
  12.3.2 Configuration Options .................................... 140
  12.3.3 Command-Line Options .................................. 142
  12.3.4 Directory Layout .......................................... 143
12.4 Certificate Management Service ............................... 143
  12.4.1 Installation Answer File Options ......................... 143
  12.4.2 Configuration Options .................................... 144
  12.4.3 Command-Line Options .................................. 144
  12.4.4 Directory Layout .......................................... 146
12.5 Authentication and Authorization Service .................... 146
  12.5.1 Installation Answer File .................................. 146
  12.5.2 Configuration Options .................................... 147
  12.5.3 Command-Line Options .................................. 147
  12.5.4 Directory Layout .......................................... 150
12.6 Workload Service ............................................... 150
  12.6.1 Installation Answer File Options ......................... 150
  12.6.2 Configuration Options .................................... 151
  12.6.3 Command-Line Options .................................. 151
  12.6.4 Directory Layout .......................................... 152
12.7 Key Broker Service ............................................ 152
  12.7.1 Installation Answer File Options ......................... 152
  12.7.2 Configuration Options .................................... 153
  12.7.3 Command-Line Options .................................. 153
  12.7.4 Directory Layout .......................................... 154
12.8 Workload Agent .................................................. 155
  12.8.1 Installation Answer File Options ......................... 155
  12.8.2 Configuration Options .................................... 155
  12.8.3 Command-Line Options .................................. 155
  12.8.4 Directory Layout .......................................... 155
12.9 Workload Policy Manager ....................................... 155
  12.9.1 Installation Answer File Options ......................... 155
  12.9.2 Configuration Options .................................... 156
  12.9.3 Command-Line Options .................................. 156
13 Certificate and Key Management ................................ 159
  13.1 Verification Service Certificates and Keys .................. 159
    13.1.1 Root Certificate ......................................... 159
    13.1.2 TLS Certificate .......................................... 159
    13.1.3 SAML ....................................................... 160
## Revision History

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Revision Number</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>• Updated for all GA Failures</td>
<td>May 2019</td>
</tr>
<tr>
<td></td>
<td>1.5</td>
<td>• Updated for version 1.5 release</td>
<td>July 2019</td>
</tr>
<tr>
<td></td>
<td>1.6 BETA</td>
<td>• Updated for 1.6 BETA release</td>
<td>November 2019</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Overview

Intel Security Libraries for Datacenter is a collection of software applications and development libraries intended to help turn Intel platform security features into real-world security use cases.

1.1.1 Trusted Computing

Trusted Computing consists of a set of industry standards defined by the Trusted Computing Group to harden systems and data against attack. These standards include verifying platform integrity, establishing identity, protection of keys and secrets, and more. One of the functions of Intel Security Libraries is to provide a “Trusted Platform,” using Intel security technologies to add visibility, auditability, and control to server platforms.

1.1.1.1 The Chain of Trust

In a Trusted Computing environment, a key concept is verification of the integrity of the underlying platform. Verifying platform integrity typically means cryptographic measurement and/or verification of firmware and software components. The process by which this measurement and verification takes place affects the overall strength of the assertion that the measured and verified components have not been altered. Intel refers to this process as the “Chain of Trust,” whereby at boot time, a sequence of cryptographic measurements and signature verification events happen in a defined order, such that measurement/verification happens before execution, and each entity responsible for performing a measurement or verification is measured by another step earlier in the process. Any break in this chain leads to an opportunity for an attacker to modify code and evade detection.

1.1.1.2 Hardware Root of Trust

The Root of Trust, the first link in the chain, can be one of several different options. Anything that happens in the boot process before the Root of Trust must be considered to be within the “trust boundary,’’ signifying components whose trustworthiness cannot be assessed. For this reason, it’s best to use a Root of Trust that starts as early in the system boot process as possible, so that the Chain of Trust during the boot process can cover as much as possible.

Multiple Root of Trust options exist, ranging from firmware to hardware. In general, a hardware Root of Trust will have a smaller “trust boundary” than a firmware Root of Trust. A hardware Root of Trust will also have the benefit of immutability – where firmware can easily be flashed and modified, hardware is much more difficult to tamper with.
1.1.1.2.1 Intel® Trusted Execution Technology (Intel® TXT)

Intel® Trusted Execution Technology is a hardware Root of Trust feature available on Intel® server platforms starting with the Grantley generation. Intel® TXT is enabled in the system BIOS (typically under the Processor > Advanced tab), and requires Intel® VT-d and Intel VT-x features to be enabled as prerequisites (otherwise the option will be grayed out). Intel® TXT will ship “disabled” by default.

1.1.1.2.2 Intel® BootGuard (Intel® BtG)

Intel® BootGuard is a hardware Root of Trust feature available on Intel® server platforms starting with the Purley-Refresh generation. Unlike Intel® TXT, Intel® BtG is configured in platform fuses, not in the system BIOS. Intel® BtG is fused into several ”profiles” that determine the behavior of the feature. Intel® BtG supports both “verify” and “measure” profiles; in ”verify” profiles, Intel® BtG will verify the signature of the platform Initial Boot Block (IBB). In “measure” profiles, Intel® BtG will hash the IBB and extend that measurement to a TPM PCR. It is recommended that Intel® BtG be fused into the “measure and verify” profile for maximum protection and auditability.

Because the Intel® BtG profile is configured using fuses, the server OEM/ODM will determine the profile used at manufacturing time. Please contact your server vendor to determine what Intel® BtG profiles are available in their product line.

Because Intel® BtG only measures/verifies the integrity of the IBB, it’s important to have an additional technology handle measurements later in the boot process. Intel® TXT can provide this function using tboot to invoke SINIT, and UEFI SecureBoot can alternatively provide similar functionality (note that Linux users should properly configure Shim and use a signed kernel for UEFI SecureBoot).

1.1.1.3 Supported Trusted Boot Options

Intel® SecL-DC supports several options for Trusted Computing, depending on the features available on the platform.
Intel® recommends using UEFI boot mode, and either TXT + tboot, or TXT + BtG + UEFI SecureBoot, or BtG + UEFI SecureBoot. These options will avoid any incompatibilities and provide the best measured boot coverage. Take note that tboot is not currently compatible with UEFI SecureBoot.

### 1.1.1.4 Remote Attestation

Trusted computing consists primarily of two activities – measurement, and attestation. Measurement is the act of obtaining cryptographic representations for the system state. Attestation is the act of comparing those cryptographic measurements against expected values to determine whether the system booted into an acceptable state.

Attestation can be performed either locally, on the same host that is to be attested, or remotely, by an external authority. The trusted boot process can optionally include a local attestation involving the evaluation of a TPM-stored Launch Control Policy (LCP). In this case, the host’s TPM will compare the measurements that have been taken so far to a set of expected PCR values stored in the LCP; if there is a mismatch, the boot process is halted entirely.

Intel® SecL utilizes remote attestation, providing a remote Verification Service that maintains a database of expected measurements (or “flavors”), and compares the actual boot-time measurements from any number of hosts against its database to provide an assertion that the host booted into a “trusted” or “untrusted” state. Remote attestation is typically easier to centrally manage (as opposed to creating an LCP for each host and entering the policy into the host’s TPM), does not halt the boot process allowing for easier remediation, and separates the attack surface into separate components that must both be compromised to bypass security controls.
Both local and remote attestation can be used concurrently. However, Intel® SecL, and this document, will focus only on remote attestation. For more information on TPM Launch Control Policies, consult the Intel Trusted Execution Technology (Intel TXT) Software Development Guide (https://www.intel.com/content/dam/www/public/us/en/documents/guides/intel-txt-software-development-guide.pdf).

1.1.2 Intel® Security Libraries for Datacenter Features

1.1.2.1 Platform Integrity

Platform Integrity is the use case enabled by the specific implementation of the Chain of Trust and Remote Attestation concepts. This involves the use of a Root of Trust to begin an unbroken chain of platform measurements at server boot time, with measurements extended to the Trusted Platform Module and compared against expected values to verify the integrity of measured components. This use case is foundational for other Intel® SecL use cases.

1.1.2.2 Data Sovereignty

Data Sovereignty builds on the Platform Integrity use case to allow physical TPMs to be written with Asset Tags containing any number of key/value pairs. This use case is typically used to identify the geographic location of the physical server, but can also be used to identify other attributes. For example, the Asset Tags provided by the Data Sovereignty use case could be used to identify hosts that meet specific compliance requirements and can run controlled workloads.

1.1.2.3 Application Integrity

Added in the Intel® SecL-DC 1.5 release, Application Integrity allows any files and folders on a Linux host system to be included in the Chain of Trust integrity measurements. These measurements are attested by the Verification Service along with the other platform measurements, and are included in determining the host’s overall Trust status. The measurements are performed by a measurement agent called tbootXM, which is built into initrd during Trust Agent installation. Because initrd is included in other Trusted Computing measurements, this allows Intel® SecL-DC to carry the Chain of Trust all the way to the Linux filesystem.

1.1.2.4 Workload Confidentiality for Virtual Machines and Containers

Added in the Intel® SecL-DC 1.6 release, Workload Confidentiality allows virtual machine and Docker container images to be encrypted at rest, with key access tied to platform integrity attestation. Because security attributes
contained in the platform integrity attestation report are used to control
access to the decryption keys, this feature provides both protection for at-rest
data, IP, code, etc in Docker container or virtual machine images, and also
enforcement of image-owner-controlled placement policies. When decryption
keys are released, they are sealed to the physical TPM of the host that was
attested, meaning that only a server that has successfully met the policy
requirements for the image can actually gain access.

Workload Confidentiality begins with the Workload Policy Manager (WPM) and
a qcow2 or Docker image that needs to be protected. The WPM is a
lightweight application that will request a new key from the Key Broker, use
that key to encrypt the image, and generate an Image Flavor. The image
owner will then upload the encrypted image to their desired image storage
service (for example, OpenStack Glance or a local Docker Registry), and the
image ID from the image storage will be uploaded along with the Image Flavor
to the Intel® SecL Workload Service. When that image is used to launch a
new VM or container, the Workload Agent will intercept the VM or container
start and request the decryption key for that image from the Workload
Service. The Workload Service will use the image ID and the Image Flavor to
find the key transfer URL for the appropriate Key Broker, and will query the
Verification Service for the latest Platform Integrity trust attestation report for
the host. The Key Broker will use the attestation report to determine whether
the host meets the policy requirements for the key transfer, and to verify that
the report is signed by a Verification Service known to the Broker. If the
report is genuine and meets the policy requirements, the image decryption
key is sealed using an asymmetric key from that host's TPM, and sent back to
the Workload Service. The Workload Service then caches the key for 5
minutes (to avoid performance issues for multiple rapid launch requests; note
that these keys are still wrapped using a sealing key unique to the hosts TPM,
so multiple hosts would require multiple keys even for an identical image) and
return the wrapped key to the Workload Agent on the host, which then uses
the host TPM to unseal the image decryption key. The key is then used to
create a new LUKS volume, and the image is decrypted into this volume.

This functionality means that a physical host must pass policy requirements in
order to gain access to the image key, and the image will be encrypted at rest
both in image storage and on the compute host.

1.1.2.5 Signed Flavors

Added in the Intel® SecL-DC 1.6 release, Flavor signing is an improvement to
the existing handling of expected attestation measurements, called “Flavors.”
This feature adds the ability to digitally sign Flavors so that the integrity of the
expected measurements themselves can be verified when attestations occur.
This also means that Flavors can be more securely transferred between
different Verification Service instances.

Flavor signing is seamlessly added to the existing Flavor creation process
(both importing from a sample host and “manually” creating a Flavor using the
POST method to the /v2/flavors resource). When a Flavor is created, the
Verification Service will sign it using a signing certificate signed by the Certificate Management Service (this is created during Verification Service setup). Each time that the Verification Service evaluates a Flavor, it will first verify the signature on that Flavor to ensure the integrity of the Flavor contents before it is used to attest the integrity of any host.
2 Intel® Security Libraries Components

2.1 Certificate Management Service
Starting with Intel® SecL-DC 1.6, most non-TPM-related certificates used by Intel® SecL-DC applications will be issued by the new Certificate Management Service. This includes acting as a root CA and issuing TLS certificates for all of the various web services.

***Note for the Intel® SecL-DC 1.6 BETA release***
In the Beta release, not all Intel® SecL services have yet been integrated with the AAS and CMS. Currently only the Workload Service uses the AAS and CMS. In the production release, all services will have their individual authentication and certificate management layers removed, and those functions will be integrated with the AAS and CMS.

2.2 Authentication and Authorization Service
Starting with Intel® SecL-DC 1.6, authentication and authorization for all Intel® SecL applications will be centrally managed by the new Authentication and Authorization Service (AAS). Previously, each application would manage its own users and permissions independently; this change allows authentication and authorization management to be centralized.

***Note for the Intel® SecL-DC 1.6 BETA release***
In the Beta release, not all Intel® SecL services have yet been integrated with the AAS and CMS. Currently only the Workload Service uses the AAS and CMS. In the production release, all services will have their individual authentication and certificate management layers removed, and those functions will be integrated with the AAS and CMS.

2.3 Verification Service
The Verification Service component of Intel® Security Libraries performs the core Platform Integrity and Data Sovereignty functionality by acting as a remote attestation authority.

Platform security technologies like Intel® TXT, Intel® BootGuard, and UEFI SecureBoot extend measurements of platform components (such as the system BIOS/UEFI, OS kernel, etc) to a Trusted Platform module as the server boots. Known-good measurements for each of these components can be
directly imported from a sample server. These expected measurements can then be compared against actual measurements from registered servers, allowing the Verification Service to attest to the "trustiness" of the platform, meaning whether the platform booted into a "known-good" state.

2.4 Workload Service

The Workload Service acts as a management service for handling Workload Flavors (Flavors used for Virtual Machines and Containers). In the Intel® SecL-DC 1.6 release, the Workload Service uses Flavors to map decryption key IDs to image IDs. When a launch request for an encrypted workload image is intercepted by the Workload Agent, the Workload Service will handle mapping the image ID to the appropriate key ID and key request URL, and will initiate the key transfer request to the Key Broker.

2.5 Trust Agent

The Trust Agent resides on physical servers and enables both remote attestation and the extended chain of trust capabilities. The Agent maintains ownership of the server’s Trusted Platform Module, allowing secure attestation quotes to be sent to the Verification Service. Incorporating the Intel® SecL HostInfo and TpmProvider libraries, the Trust Agent serves to report on platform security capabilities and platform integrity measurements.

The Trust Agent is supported for Windows* Server 2016 Datacenter and Red Hat Enterprise Linux* (RHEL) 7.4 and later.

2.6 Workload Agent

The Workload Agent is the component responsible for handling all of the functions needed for Workload Confidentiality for virtual machines and Docker containers on a physical server. The Workload Agent uses libvirt hooks to identify VM lifecycle events (VM start, stop, hibernate, etc), and intercepts those events to perform needed functions like requesting decryption keys, creation and deletion of encrypted LUKS volumes, using the TPM to unseal decryption keys, etc. The WLA also includes the Docker SecureOverlay Driver that performs analogous functionality for Docker containers.

2.7 Integration Hub

The Integration Hub acts as a middle-man between the Verification Service and one or more scheduler services (such as OpenStack* Nova), and "pushes" attestation information retrieved from the Verification Service to one or more scheduler services according to an assignment of hosts to specific tenants. In
this way, Tenant A can receive attestation information for hosts that belong to
Tenant A, but receive no information about hosts belonging to Tenant B.

The Integration Hub serves to disassociate the process of retrieving
attestations from actual scheduler queries, so that scheduler services can
adhere to best practices and retain better performance at scale. The
Integration Hub will regularly query the Intel® SecL Verification Service for
SAML attestations for each host. The Integration Hub maintains only the most
recent currently valid attestation for each host, and will refresh attestations
when they would expire. The Integration Hub will verify the signature of the
SAML attestation for each host assigned to a tenant, then parse the
attestation status and asset tag information, and then will securely push the
parsed key/value pairs to the plugin endpoints enabled.

The Integration Hub features a plugin design for adding new scheduler
endpoint types. Currently the Integration Hub supports an OpenStack Nova
endpoint plugin. Other integration plugins may be added.

2.8 Workload Policy Manager

The Workload Policy Manager is a Linux commandline utility used by an image
owner to encrypt VM (qcow2) or container (Docker) images, and to create an
Image Flavor used to provide the encryption key transfer URL during launch
requests. The WPM utility will use an existing or request a new key from the
Key Broker Service, use that key to encrypt the image, and output the Image
Flavor in JSON format. The encrypted image can then be uploaded to the
image store of choice (like OpenStack Glance), and the Image Flavor can be
uploaded to the Workload Service. The ID of the image on the image storage
system is then mapped to the Image Flavor in the WLS; when the image is
used to launch a new instance, the WLS will find the Image Flavor associated
with that image ID, and use the Image Flavor to determine the key transfer
URL.

2.9 Key Broker Service

The Key Broker Service is effectively a policy compliance engine. Its job is to
manage key transfer requests for encrypted images, releasing keys only to
servers that meet policy requirements. The Key Broker registers one or more
SAML signing certificates from any Verification Services that it will trust.
When a key transfer request is received, the request includes a trust
attestation report signed by the Verification Service. If the signature matches
a registered SAML key, the Broker will then look at the actual report to ensure
the server requesting the key matches the image policy (currently only overall
system trust is supported as a policy requirement). If the report indicates the
policy requirements are met, the image decryption key is wrapped using a
public key unique to the TPM of the host that was attested in the report, such
that only the host that was attested can unseal the decryption key and gain
access to the image.
3 Intel® Security Libraries 
Installation

3.1 Building from Source
Intel® Security Libraries is distributed as open source code, and must be compiled into installation binaries before installation.

Instructions and sample scripts for building the Intel® SecL-DC components can be found here:

https://01.org/intel-secl/documentation/build-installation-scripts

After the components have been built, the installation binaries can be found in the directories created by the build scripts:

<servicename>/packages/<servicename>/target/<servicename>-<version>-SNAPSHOT.bin

3.2 Recommended Service Layout
The Intel® SecL-DC services can be installed in a variety of layouts, partially depending on the use cases desired and the OS of the server(s) to be protected. In general, the Intel® SecL-DC applications can be divided into management services that are deployed on the network on the management plane, and host or node components that must be installed on each protected server.

Management services can typically be deployed anywhere with network access to all of the protected servers. This could be a set of individual VMs per service; containers; or all installed on a single physical or virtual machine.

Node components must be installed on each protected physical server. Typically this is needed for Windows and Linux deployments.

3.2.1 Platform Integrity
The most basic use case enabled by Intel® SecL-DC, Platform Integrity requires only the Verification Service and, to protect Windows or Linux hosts, the Trust Agent. This also enables the Application Integrity use case by default for Linux systems.

The Integration Hub may be added to provide integration support for OpenStack or Kubernetes. The Hub is often installed on the same machine as the Verification Service, but optionally can be installed separately.
3.2.2 **Workload Confidentiality**

Workload Confidentiality introduces a number of additional services and agents. For a POC environment, all of the management services can be installed on a single machine or VM. This includes:

- Certificate Management Service (CMS)
- Authorization and Authentication Service (AAS)
- Host Verification Service (HVS)
- Workload Service (WLS)
- Integration Hub (HUB)
- Key Broker Service (KBS) with backend key management
- Workload Policy Manager (WPM)

In a production environment, it is strongly suggested that the WPM and KBS be deployed (with their own CMS and AAS) separately for each image owner. For a Cloud Service Provider, this would mean that each customer/tenant who will use the Workload Confidentiality feature would have their own dedicated AAS/CMS/KBS/WPM operated on their own networks, not controlled by the CSP. This is because the Key Broker and WPM are the tools used to define the policies that will allow images to launch, and these policies and their enforcement should remain entirely under the control of the image owner.

The node components must be installed on each protected physical server:

- Trust Agent (TA)
- Workload Agent (WLA)

### 3.3 Installing the Certificate Management Service

#### 3.3.1 Required For

The CMS is REQUIRED for all use cases.

- Platform Integrity with Data Sovereignty and Signed Flavors
- Application Integrity
- Workload Confidentiality (both VMs and Docker Containers)
3.3.2 Package Dependencies

3.3.3 Supported Operating Systems


3.3.4 Recommended Hardware

- 1 vCPUs
- RAM: 2 GB
- 10 GB
- One network interface with network access to all Intel® SecL-DC services

3.3.5 Installation

To install the Intel® SecL-DC Certificate Management Service:


2. Create the cms.env installation answer file for an unattended installation.

   A sample minimal cms.env file is provided below. For all configuration options and their descriptions, refer to the Intel® SecL Configuration section on the Certificate Management Service.

   ```
   # CMS basic properties
   CMS_NOSETUP=false
   CMS_PORT=8445
   AAS_API_URL=https://<Hostname or IP address of the AAS>:8444/aas/
   AAS_TLS_SAN=<Comma-separated list of IPs/hostnames for the AAS>
   ```

3. Execute the installer binary.

   When the installation completes, the Certificate Management Service is available. The services can be verified by running `cms status` from the command line.

   # cms status

   After installation is complete, the CMS will output a bearer token to the console. This token will be used with other services to authenticate certificate requests from the CMS.
3.4 Installing the Authentication and Authorization Service

3.4.1 Required For

The AAS is REQUIRED for all use cases.
- Platform Integrity with Data Sovereignty and Signed Flavors
- Application Integrity
- Workload Confidentiality (both VMs and Docker Containers)

3.4.2 Prerequisites

The following must be completed before installing the Authentication and Authorization Service:

- The CMS must be installed and available

3.4.3 Package Dependencies

The Intel® SecL-DC Authentication and Authorization Service (AAS) requires a Postgresql 11 database. A script (install_pgdb.sh) is provided with the AAS that will automatically add the Postgresql repositories and install/configure a sample database. If this script will not be used, a Postgresql 11 database must be installed by the user before executing the AAS installation.

3.4.4 Supported Operating Systems


3.4.5 Recommended Hardware

- 1 vCPUs
- RAM: 2 GB
- 10 GB
- One network interface with network access to all Intel® SecL-DC services
3.4.6 Installation

3.4.6.1 Installing/Configuring the Database

The Intel® SecL-DC Authentication and Authorization Service (AAS) requires a Postgresql 11 database. Scripts (install_pgdb.sh, create_db.sh) are provided with the AAS that will automatically add the Postgresql repositories and install/configure a sample database. If this script will not be used, a Postgresql 11 database must be installed by the user before executing the AAS installation.

3.4.6.1.1 Using the Provided Database Installation Script

Install a sample Postgresql 11 database using the install_pgdb.sh script. This script will automatically add the Postgresql repository to the system and install the Postgresql database and client packages required.

Create the isecpgdb.env answer file:

ISECL_PGDB_IP_INTERFACES=localhost
ISECL_PGDB_PORT=5432
ISECL_PGDB_DBNAME=<database name>
ISECL_PGDB_USERNAME=<database_username>
ISECL_PGDB_USERPASSWORD=<database_password>
ISECL_PGDB_SAVE_DB_INSTALL_LOG=true

Execute the installation script:

./install_pgdb.sh

After installation, the database must be created initialized and tables created. Execute the create_db.sh script to configure the database.

./create_db.sh <database name> <database_username> <database_password>

3.4.6.2 Using an Existing Database

3.4.6.2 Installing the Authentication and Authorization Service

To install the AAS, a bearer token from the CMS is required. This bearer token is output at the end of the CMS installation. However, if a new token is needed, simply use the following command from the CMS command line:

cms setup cms_auth_token --force

Create the authservice.env installation answer file:

CMS_BASE_URL=https://<CMS IP or hostname>:8445/cms/v1/
AAS_NOSETUP=false
AAS_DB_HOSTNAME=<IP or hostname of database server>
AAS_DB_PORT=<database port number; default is 5432>
AAS_DB_NAME=<database name>
AAS_DB_USERNAME=<database username>
AAS_DB_PASSWORD=<database password>
AAS_ADMIN_USERNAME=<username for AAS administrative user>
AAS_ADMIN_PASSWORD=<password for AAS administrative user>
AAS_DB_SSLMODE=verify-ca
AAS_DB_SSLCERTSRC=/usr/local/pgsql/data/server.crt
AAS_JWT_CERT_SUBJECT="AAS JWT Signing Certificate"
AAS_JWT_TOKEN_DURATION_MINS=<length of time in minutes that tokens should be valid>
SAN_LIST=<comma-separated list of IPs and hostnames for the AAS>
BEARER_TOKEN=<bearer token from CMS installation>

Execute the AAS installer:

```
./authservice-v1.6-beta.bin
```

After installation is complete, a superadmin user and appropriate roles must be created. Create an environment variable to store the CMS bearer token:

```
export TOKEN=<token>
```

Use cURL to create the superadmin user:

```
```

Capture the ID of the new user created:

```
export ADMIN_ID=<uuid>
```

Create roles for the superadmin user:

```
```

```
```

```
curl -k -X POST https://<aas IP or hostname>:8444/aas/roles -H "Authorization: Bearer $TOKEN" -H 'Content-Type: application/json' -d '{"service": "CMS", "name": "CertApprover", "context": "CN=WLS TLS Certificate;SAN=<comma-separated list of IPs and hostnames for the CMS>";certType=TLS"}"
```

Each of these calls will return an ID for the created role; these IDs will be used to assign these roles to the superadmin user.

Assign the new roles to the superadmin user:

```
```
3.5 Installing the Verification Service

This section details how to install the Intel® SecL-DC services. For instructions on running these services as containers, see the following section.

3.5.1 Required For

The Verification Service is REQUIRED for all use cases.
- Platform Integrity with Data Sovereignty and Signed Flavors
- Application Integrity
- Workload Confidentiality (both VMs and Docker Containers)

3.5.2 Package Dependencies

The Intel® Security Libraries Verification Service requires the following packages and their dependencies:

- Monit
- Logback (optional)
- Java® 8 JDK
- OpenSSL
- Postgres® client and server 9.4 (server component optional if an external Postgres database is used)
- Unzip

If they are not already installed, the Verification Service installer attempts to install these automatically using the package manager. Automatic installation requires access to package repositories (the RHEL subscription repositories, the EPEL repository, or a suitable mirror), which may require an Internet connection. If the packages are to be installed from the package repository, be sure to update the repository package lists before installation.

3.5.3 Supported Operating Systems

The Intel® Security Libraries Verification Service supports Red Hat Enterprise Linux 7.4 and later.

3.5.4 Recommended Hardware

- 4 vCPUs
3.5.5 Installation

To install the Verification Service, follow these steps:

4. Copy the Verification Service installation binary to the /root/ directory.
5. Create the mtwilson.env installation answer file for an unattended installation.

A sample minimal mtwilson.env file is provided below. For all configuration options and their descriptions, refer to the Intel® SecL Configuration section on the Verification Service.

Execute the installer binary.

When the installation completes, the Verification Service is available. The services can be verified by running `mtwilson status` from the Verification Service command line.

```
# mtwilson status
```

3.5.6 Creating Service Users

After installation is complete, users should be created for any services that will be integrated with the Verification Service (such as the Trust Agent or Integration Hub).

The administrative user created during installation (MC_FIRST_USERNAME) has full administrative privileges and can be used to all services and requests, but this is strongly not recommended for security reasons.
(Optional, required only if Trust Agent hosts will be registered.)

mtwilson login-password <username> <password> --permissions host_aiks:certify tpm_endorsements:create tpm_endorsements:search tpm_passwords:create tpm_passwords:retrieve tpm_passwords:search tpm_passwords:store tpm_passwords:search
host_signing_key_certificates:create store_host_pre_registration_details:create

To also allow automatic registration and HOST_UNIQUE flavor imports during Trust Agent installation, add the following permissions:

mtwilson login-password <username> <password> --permissions host_aiks:certify tpm_endorsements:create tpm_endorsements:search tpm_passwords:create tpm_passwords:retrieve tpm_passwords:search tpm_passwords:store tpm_passwords:search
tpm_passwords:store tpms:endorse host_signing_key_certificates:create store_host_pre_registration_details:create
hosts:search hosts:retrieve hosts:search hosts:retrieve
host_unique_flavors:create

(Optimal, required only if the Integration Hub will be used.)

mtwilson login-password <username> <password> --permissions hosts:search
hosts:retrieve reports:search reports:retrieve

3.6 Installing the Workload Service

3.6.1 Required For

The WLS is REQUIRED for the following use cases.
- Workload Confidentiality (both VMs and Docker Containers)

3.6.2 Prerequisites

The following must be completed before installing the Workload Service:

- The CMS must be installed and available
- The AAS must be installed and available
- The KBS must be installed and available

3.6.3 Package Dependencies

3.6.4 Supported Operating Systems

The Intel® Security Libraries Workload Service supports Red Hat Enterprise Linux 7.4 and later.
3.6.5 Recommended Hardware

3.6.6 Installation

3.6.6.1 Installing/Configuring the Database

The Intel® SecL-DC Workload Service (WLS) requires a Postgresql 11 database. Scripts (install_pgdb.sh, create_db.sh) are provided with the AAS that will automatically add the Postgresql repositories and install/configure a sample database. If this script will not be used, a Postgresql 11 database must be installed by the user before executing the WLS installation.

3.6.6.1.1 Using the Provided Database Installation Script

Install a sample Postgresql 11 database using the install_pgdb.sh script. This script will automatically add the Postgresql repository to the system and install the Postgresql database and client packages required.

Create the iseclpgdb.env answer file:

ISECL_PGDB_IP_INTERFACES=localhost
ISECL_PGDB_PORT=5432
ISECL_PGDB_DBNAME=<database name>
ISECL_PGDB_USERNAME=<database_username>
ISECL_PGDB_USERPASSWORD=<database_password>
ISECL_PGDB_SAVE_DB_INSTALL_LOG=true

Execute the installation script:

./install_pgdb.sh

After installation, the database must be created initialized and tables created. Execute the create_db.sh script to configure the database.

./create_db.sh <database name> <database_username> <database_password>

3.6.6.1.2 Using an Existing Database

3.6.6.2 Installing the Workload Service

Create the workload-service.env installation answer file:

WLS_DB_USERNAME=<database username>
WLS_DB_PASSWORD=<database password>
WLS_DB_HOSTNAME=<IP or hostname of database server>
WLS_DB_PORT=<Database port; 5432 by default>
WLS_DB=<name of the WLS database>
HVS_URL=https://<IP address or hostname of the Host verification Service>:8443/ntwilson/v2
KMS_URL=https://<Key Broker IP or hostname>/v1/
Run WLS installer

3.7 Installing the Trust Agent for Linux

3.7.1 Required For

The Trust Agent for Linux is REQUIRED for all use cases.
- Platform Integrity with Data Sovereignty and Signed Flavors
- Application Integrity
- Workload Confidentiality (both VMs and Docker Containers)

3.7.2 Package Dependencies

The Trust Agent requires the following packages and their dependencies:
- Tboot (Optional, for TXT-based deployments **without** UEFI SecureBoot only)
- openssl

If they are not already installed, the Trust Agent installer attempts to install these automatically using the package manager. Automatic installation requires access to package repositories (the RHEL subscription repositories, the EPEL repository, or a suitable mirror), which may require an Internet connection. If the packages are to be installed from the package repository, be sure to update the repository package lists before installation.

Tboot will not be installed if UEFI SecureBoot is detected as enabled on the platform.

3.7.3 Supported Operating Systems

The Intel® Security Libraries Trust Agent for Linux supports Red Hat Enterprise Linux 7.4 and later. Windows support is described in the section “Installing the Trust Agent for Windows.”
3.7.4 Prerequisites

The following must be completed before installing the Trust Agent:

- Supported server hardware including an Intel® Xeon® processor with Intel Trusted Execution Technology activated in the system BIOS.
- Trusted Platform Module (version 2.0) installed and activated in the system BIOS, with cleared ownership status.

  Note: For Linux systems, TPM 1.2 and TPM resource sharing to applications other than the Trust Agent is not supported at this time. Do not install trousers or another TSS stack application after installing the Trust Agent on Linux systems.

- System must be booted to a tboot boot option (for TXT-enabled systems only without UEFI SecureBoot enabled; Trust Agent installation will automatically install tboot if not present and if UEFI SecureBoot is not enabled, and then require a reboot before proceeding).

  Note: While both UEFI and Legacy Bios mode are supported, tboot is currently not supported when using UEFI SecureBoot. If UEFI SecureBoot is enabled while attempting to boot to tboot, the boot process will halt. UEFI Secure Boot must be disabled for Linux systems when using tboot. If UEFI SecureBoot is enabled, the Trust Agent installer will skip the installation of tboot and proceed to install normally.

- (Provisioning step only) Intel® SecL Verification Service server installed and active.
- (Optional, REQUIRED for Virtual Machine Confidentiality only):
  - QEMU/KVM must be installed
  - Libvirt must be installed
- (Optional, REQUIRED for Docker Container Confidentiality only): Docker 19.03 must be installed

  Note: The specific Docker version 19.03 is required for Docker Container Confidentiality. Only this version is supported for this use case.

- Docker engine must be run in experimental mode.

3.7.5 Installation

Installation of the Trust Agent is split into two major steps: Installation, which covers the creation of system files and folders, and Provisioning, which involves the creation of keys and secrets and links the Trust Agent to a specific Verification Service. Both operations can be performed at the same time using an installation answer file. Without the answer file, the Trust Agent can be installed and left in an un-provisioned state regardless of whether a Verification Service is up and running, until such time as the datacenter...
administrator is ready to run the provisioning step and link the Trust Agent to a Verification Service.

To install the Trust Agent for Linux:

1. (Optional; required to perform Provisioning and Installation at the same time.) Create the trustagent.env answer file in the /root/ directory (for full configuration options, see section 9.2). The minimum configuration options for installation are provided below.

For Docker Container Encryption only, add the following line to the trustagent.env installation answer file:

```
WLA_WITH_CONTAINER_SECURITY="yes"
```

Note:
The MTWILSON_API_USERNAME and password required by the Trust Agent can be satisfied by the PRIVACYCA_DOWNLOAD_USERNAME user created during the installation of the Verification Service, or by any user with the following Verification Service permissions:

- host_aiks:certify
- tpm_endorsements:create
- tpm_endorsements:search
- tpm_passwords:create
- tpm_passwords:retrieval
- tpm_passwords:search
- tpm_passwords:store
- tpm:endorse
- host_signing_key_certificates:create
- store_host_pre_registration_details:create
- MTWILSON_API_URL=https://<Verification Service IP or Hostname>:8443/mtwilson/v2
- MTWILSON_TLS_CERT_SHA384=<SHA384 of Verification Service TLS Certificate>
- MTWILSON_API_USERNAME=< Verification Service PrivacyCA username>
- MTWILSON_API_PASSWORD=< Verification Service PrivacyCA password>
- REGISTER_TPM_PASSWORD=y
- TRUSTAGENT_LOGIN_REGISTER=true
- PROVISION_ATTESTATION=y
- GRUB_FILE=<path to grub.cfg>
- CURRENT_IP=<Trust Agent IP address>

```
MTWILSON_API_URL=https://<Verification Service IP or Hostname>:8443/mtwilson/v2
MTWILSON_TLS_CERT_SHA384=<SHA384 of Verification Service TLS Certificate>
MTWILSON_API_USERNAME=< Verification Service PrivacyCA username>
MTWILSON_API_PASSWORD=< Verification Service PrivacyCA password>
REGISTER_TPM_PASSWORD=y
TRUSTAGENT_LOGIN_REGISTER=true
PROVISION_ATTESTATION=y
GRUB_FILE=<path to grub.cfg>
CURRENT_IP=<Trust Agent IP address>
```

Note: The MTWILSON_API_USERNAME and password required by the Trust Agent can be satisfied by the PRIVACYCA_DOWNLOAD_USERNAME user created during the installation of the Verification Service, or by any user with the following Verification Service permissions:

- host_aiks:certify
- tpm_endorsements:create
- tpm_endorsements:search
- tpm_passwords:create
- tpm_passwords:retrieval
- tpm_passwords:search
- tpm_passwords:store
- tpm:endorse
- host_signing_key_certificates:create
- store_host_pre_registration_details:create

The MTWILSON_TLS_CERT_SHA384 value can be retrieved from the Verification Service using the command:

```
cat /opt/mtwilson/configuration/https.properties
```

from the Verification Service command line.

2. Copy the Trust Agent installer binary to the /root/ directory.

3. Execute the Trust Agent installer, and wait for the installation to complete.
   - The Trust Agent will install tboot and other prerequisites if not already present. Tboot will **not** be installed if the server is booted using UEFI SecureBoot, due to incompatibility.
   - If tboot is installed by the Trust Agent installer, the installation will abort and reboot the host. This is because the Trust Agent requires the host to
be booted into a tboot boot option, which populates the OS-level measurements in the host TPM.

- After the host reboots, re-run the Trust Agent installation binary to resume the installation.

If the trustagent.env answer file was provided with the minimum required options, the Trust Agent will be installed and also Provisioned to the Verification Service specified in the answer file.

If no answer file was provided, the Trust Agent will be installed, but will not be Provisioned. TPM-related functionality will not be available from the Trust Agent until the Provisioning step is completed.

**Note:** If the Linux Trust Agent is installed without being Provisioned, the Trust Agent process will not actually run until the Provisioning step has been completed.

4. After Provisioning is completed, the Linux Trust Agent must be rebooted so that the default SOFTWARE Flavor manifest can be measured and extended to the TPM.

### 3.7.6 Installing the Workload Agent

The Workload Agent installation is built into the Trust Agent installer.

For Docker Container Encryption only, add the following line to the trustagent.env installation answer file:

```
WLA_WITH_CONTAINER_SECURITY="yes"
```

### 3.8 Installing the Trust Agent for Windows

#### 3.8.1 Required For

The Trust Agent for Windows is REQUIRED for the following use cases:

- Platform Integrity with Data Sovereignty and Signed Flavors

Other use cases are currently not supported for Windows.

#### 3.8.2 Supported Operating Systems

The Trust Agent for Windows supports Windows Server 2016 Datacenter.

#### 3.8.3 Prerequisites

The following must be completed before installing the Trust Agent:
• Supported server hardware including an Intel® Xeon processor.
• Trusted Platform Module (version 1.2 or 2.0) installed and activated in
  the system BIOS, with cleared ownership status.
• Coreinfo (https://docs.microsoft.com/en-us/sysinternals/downloads/coreinfo) must be installed
• (Provisioning step only) Intel® SecL Verification Service server installed
  and active.

3.8.3.1 TPM Ownership

The Intel® SecL-DC Trust Agent for Windows requires the TPM ownership
secret to be stored in the local system registry. To confirm that the secret is
populated in the registry:

1) Open a Command Prompt as Administrator
2) Run the following command:
   REG QUERY hklm\system\controlset001\services\tpm\wnl\admin
3) If the output contains the OwnerAuthFull key and a corresponding value,
   the ownership secret is present in the registry and no further action is
   needed.

If the output does not contain the secret, system must be configured to store
the secret in the registry.

To configure GPO to store the ownership secret in the local registry:
1) Open a Command Prompt as an Administrator
2) Run gpedit.msc
3) In the GP Editor, browse to Computer Configuration\Administrative
   Templates\System\Trusted Platform Module Services
4) Set the Operating System Managed TPM Authentication Level to "Full"
5) Clear the TPM ownership and reboot
   To clear TPM ownership from within Windows:
   a) Open a Command Prompt as Administrator
   b) Run tpm.msc
   c) From the TPM Management Console that appears, click “Clear TPM”
   d) After the process is complete, reboot
### Installation

Installation of the Trust Agent is split into two major steps: Installation, which covers the creation of system files and folders, and Provisioning, which involves the creation of keys and secrets and links the Trust Agent to a specific Verification Service. Both operations can be performed at the same time using an installation answer file. Without the answer file, the Trust Agent can be installed and left in an un-provisioned state regardless of whether a Verification Service is up and running, until such time as the datacenter administrator is ready to run the provisioning step and link the Trust Agent to a Verification Service.

To install the Trust Agent for Windows:

1. (Optional; required to perform Provisioning and Installation at the same time.) Create the trustagent.ini answer file in the C:\Temp directory (for full configuration options, see section 9.2). The minimum configuration options for installation are provided below.

```plaintext
[TRUST_AGENT]
MTWILSON_API_URL=https://<Verification Service IP or Hostname>:8443/mtwilson/v2
MTWILSON_TLS_CERT_SHA384=<SHA384 of Verification Service TLS Certificate>
MTWILSON_API_USERNAME=< Verification Service PrivacyCA username>
MTWILSON_API_PASSWORD=< Verification Service PrivacyCA password>
REGISTER_TPM_PASSWORD=y
TRUSTAGENT_LOGIN_REGISTER=true
PROVISION_ATTESTATION=y
CURRENT_IP=<Trust Agent IP address>
```

**Note:** The MTWILSON_API_USERNAME and password required by the Trust Agent requires a Verification Service user with the "trustagent_provisioner" role. See the Verification Service installation subsection "Creating Service Users" for details on user creation.

*The MTWILSON_TLS_CERT_SHA384 value can be retrieved from the Verification Service using the command:*

```bash
cat /opt/mtwilson/configuration/https.properties
```

from the Verification Service command line.

2. Copy the Trust Agent installer executable to the C:\Temp directory.

3. Execute the Trust Agent installer, and wait for the installation to complete.

If the trustagent.ini answer file was provided with the minimum required options, the Trust Agent will be installed and also Provisioned to the Verification Service specified in the answer file.
3.9 Trust Agent Provisioning

"Provisioning" the Trust Agent involves connecting to a Verification Service to download the Verification Service PrivacyCA certificate, create a new Attestation Identity Keypair in the TPM, and verify or create the TPM Endorsement Certificate and Endorsement Key. The Verification Service PrivacyCA root certificate is used to sign the EC, and the EC is used to generate the Attestation Identity Keypair. The AIK is used by the Verification Service to verify the integrity of quotes from the host’s TPM.

Provisioning can be performed separately from installation (meaning you can install the Trust Agent without Provisioning, and then Provision later). If the trustagent.env answer file is present and has the required Verification Service information during installation, the Agent will automatically run the Provisioning steps.

**Note:** The trustagent.env answer file must contain user credentials for a user with sufficient privileges. The minimum role required for performing provisioning is the "trustagent_provisioner" role.

**Note:** If the Linux Trust Agent is installed without being Provisioned, the Trust Agent process will not actually run until the Provisioning step has been completed.

If the answer file is not present during installation, the Agent can be Provisioned later by adding the trustagent.env file and running the following command:

tagagent provision-attestation <trustagent.env or trustagent.ini file path>

3.10 Trust Agent Registration

Registration creates a host record with connectivity details and other host information in the Verification Service database. This host record will be used by the Verification Service to retrieve TPM attestation quotes from the Trust Agent to generate an attestation report.

**Note:** Host registration requires user credentials for a user with sufficient privileges. The minimum role required for performing host registration is the "host_manager" role.

The Trust Agent can register the host with a Verification Service by running the following command (the trustagent.env or trustagent.ini answer file must be present in the current working directory):
tagent create-host

Hosts can also be registered using a REST API request to the Verification Service:

POST https://verification.service.com:8443/mtwilson/v2/hosts
{
    "host_name": "<hostname of host to be registered>",
    "tls_policy_id": "TRUST_FIRST_CERTIFICATE",
    "connection_string": "intel:https://<hostname or IP address>:1443;u=<TAgent username>;p=<TAgent password>",
    "flavor_group_name": "",
    "description": "<description>"
}

**Note:** When a new host is registered, the Verification Service will automatically attempt to match the host to appropriate Flavors. If appropriate Flavors are not found, the host will still be registered, but will be in an Untrusted state until/unless appropriate Flavors are added to the Verification Service.
3.11 Importing the HOST_UNIQUE Flavor

RHEL and VMware ESXi hosts have measured components that are unique to each host. This means that a special HOST_UNIQUE flavor part needs to be imported for each RHEL and ESXi host, in addition to any other OS or Platform Flavors.

**Note:** Importing a Flavor requires user credentials for a user with sufficient privileges. The minimum role required for creating the HOST_UNIQUE Flavor part is the "host_unique_flavor_creator" role. This role can only create HOST_UNIQUE Flavor parts, and cannot create any other Flavors.

On Red Hat Enterprise Linux hosts with the Trust Agent, this can be performed from the Trust Agent command line (this requires the trustagent.env answer file to be present in the current working directory):

```bash
tagent create-host-unique-flavor
```

This can also be performed using a REST API (required for VMware ESXi hosts):

```json
POST https://verification.service.com:8443/mtwilson/v2/flavors
{
  "connection_string": "<Connection string>",
  "partial_flavor_types": ["HOST_UNIQUE"],
  "tls_policy_id": "TRUST_FIRST_CERTIFICATE"
}
```

3.12 Installing the Integration Hub

**Note:** The Integration Hub is only required to integrate Intel® SecL with third-party scheduler services, such as OpenStack Nova or Kubernetes. The Hub is not required for usage models that do not require Intel® SecL security attributes to be pushed to an integration endpoint.

3.12.1 Required For

The Hub is REQUIRED for the following use cases.

- Workload Confidentiality (both VMs and Docker Containers)

The Hub is OPTIONAL for the following use cases (used only if orchestration or other integration support is needed):

- Platform Integrity with Data Sovereignty and Signed Flavors
- Application Integrity
3.12.2 Package Dependencies

The Intel® SecL Integration Hub requires a number of packages and their dependencies:

If these are not already installed, the Integration Hub installer attempts to install these packages automatically using the package manager. Automatic installation requires access to package repositories (the RHEL subscription repositories, the EPEL repository, or a suitable mirror), which may require an Internet connection. If the packages are to be installed from the package repository, be sure to update your repository package lists before installation.

3.12.3 Supported Operating Systems

The Intel Security Libraries Integration Hub supports Red Hat Enterprise Linux 7.4 and later.

3.12.4 Prerequisites

The Intel® Security Libraries Integration Hub can be run as a VM or as a bare-metal server. The Hub may be installed on the same server (physical or VM) as the Verification Service.

3.12.5 Recommended Hardware

- 1 vCPUs
- RAM: 2 GB
- 1 GB free space to install the Verification Service services. Additional free space is needed for the Attestation Hub database and logs (database and log space requirements are dependent on the number of managed servers).
- One network interface with network access to the Verification Service.
- One network interface with network access to any integration endpoints (for example, OpenStack Nova).

3.12.6 Installation

To install the Integration Hub, follow these steps:

1. Copy the Integration Hub installation binary to the /root/ directory.
2. Create the attestation-hub.env installation answer file. See the sample file below.

```
ATTESTATION_HUB_PORT_HTTP=19082
ATTESTATION_HUB_PORT_HTTPS=19445
MTWILSON_API_URL="https://<Verification Service IP or hostname>:8443/mtwilson/v2"
MTWILSON_TLS=<sha384 of Verification Service TLS certificate>
MTWILSON_USERNAME=<username of Verification Service account with attestations:retrieve permissions>
MTWILSON_PASSWORD=<password for Verification Service user account>
MTWILSON_SERVER=<IP address or hostname of the Verification Service>
ATTESTATION_HUB_DB_NAME="attestation_hub_pu"
ATTESTATION_HUB_DB_HOSTNAME="localhost"
ATTESTATION_HUB_DB_PORTNUM="5432"
ATTESTATION_HUB_DB_DRIVER="org.postgresql.Driver"
ATTESTATION_HUB_POLL_INTERVAL=2
ATTESTATION_HUB_TENANT_CONFIGURATIONS_PATH=/opt/tenantconfig
ATTESTATION_HUB_DB_USERNAME=<Database administrative username>
ATTTESTATION_HUB_DB_PASSWORD=<Database password>
```

**Note:** The MTWILSON_TLS value can be retrieved from the Verification Service using the command:

```
cat /opt/mtwilson/configuration/https.properties
```

from the Verification Service command line.

3. Execute the installer binary.

4. Create an administrative user. On the command line while logged in as root, run the following:

```
attestation-hub password admin password --permissions "*"
```

This will create a new user named "admin" with password "password" that will be used to make REST API requests to the Hub.

### 3.13 Installing the Key Broker Service

#### 3.13.1 Required For

The KBS is REQUIRED for the following use cases:

- Workload Confidentiality (both VMs and Docker Containers)
3.13.2 **Prerequisites**

The following must be completed before installing the Key Broker:

- The Verification Service must be installed and available

3.13.3 **Package Dependencies**

3.13.4 **Supported Operating Systems**

The Intel® Security Libraries Key Broker Service supports Red Hat Enterprise Linux 7.4 and later.

3.13.5 **Recommended Hardware**

3.13.6 **Installation**

Create the kms.env installation answer file:

```bash
MTWILSON_API_URL=https://<Verification Service IP or hostname>:8443/mtwilson/v2
MTWILSON_TLS_CERT_SHA384=<SHA384 hash of the Verification Service TLS cert>
MTWILSON_API_USERNAME=<Verification Service user with the certificates:retrieve permission>
MTWILSON_API_PASSWORD=<password for Verification Service user>
JETTY_PORT=80
JETTY_SECURE_PORT=443
```

Execute the KBS installer.

3.14 **Installing the Workload Policy Manager**

3.14.1 **Required For**

The WPM is REQUIRED for the following use cases.

- Workload Confidentiality (both VMs and Docker Containers)

3.14.2 **Package Dependencies**

3.14.3 **Supported Operating Systems**

The Intel® Security Libraries Workload Policy Manager supports Red Hat Enterprise Linux 7.4 and later.
3.14.4 **Recommended Hardware**

3.14.5 **Installation**

Create the wpm.env answer file:

```bash
KMS_API_URL="https://<IP address or hostname of the KBS>:443/v1/"
KMS_API_USERNAME=<Username for KBS account>
KMS_API_PASSWORD=<Password for KBS account>
KMS_TLS_SHA256=<Sha256 hash of the KBS TLS certificate>
ENVELOPE_PUBLIC_KEY_LOCATION="/etc/workload-policy-manager/envelopePublicKey.pub"
ENVELOPE_PRIVATE_KEY_LOCATION="/etc/workload-policy-manager/envelopePrivateKey.pem"
CMS_BASE_URL=https://<IP address or hostname for CMS>:8445/cms/v1/
BEARER_TOKEN=<bearer token from CMS installation>
```

For Docker Container Encryption only, add the following line to the wpm.env installation answer file:

```
WPM_WITH_CONTAINER_SECURITY="yes"
```

Execute the WPM installer.

Commented [KTE7]: Need permissions
4 Deployment Using Containers

The Intel® SecL-DC services can also be deployed as containers. There are a few important notes to consider:

- Each physical Linux server must run a dedicated Trust Agent container. This container must run in privileged mode so that it has access to host resources, including the physical TPM. The storage volume for the Trust Agent must stay with the host; the Agent and its configuration files are intrinsically linked to the physical TPM on the host when the initial installation happens.
- The Verification Service and Integration Hub services can be moved and run anywhere with no hardware restrictions.
- Several of the application commands (<servicename> start/stop/restart, uninstall, etc) are not supported in the containerized deployment. To restart services, simply stop the container and then start it again. To uninstall, simply delete the configuration volume.

The Intel® SecL-DC services are not distributed as ready-made containers, so deployment includes building the initial container image. To make this process easier, Intel distributes premade docker-compose and dockerfile files. These files can be modified for environment-specific settings.

4.1 Building the ISecL Service Docker Images

4.1.1 Prerequisites for Building Docker Images

- Some packages may require packages not available on the regular RHEL repositories. Install the following repos:
  

  RDO ([https://download.docker.com/linux/centos/docker-ce.repo](https://download.docker.com/linux/centos/docker-ce.repo))

  Docker-CE ([https://download.docker.com/linux/centos/docker-ce.repo](https://download.docker.com/linux/centos/docker-ce.repo))

- Docker-ce 1.18 must be installed (from [https://download.docker.com/linux/centos/docker-ce.repo](https://download.docker.com/linux/centos/docker-ce.repo))

- Docker-compose 1.23.1 or later must be installed
• this version may not be available on the RHEL repositories; use PIP for installation of the supported version

- Container-selinux must be installed
- The Docker daemon must be installed and running
- Locations must be identified for persistent data volumes for container configuration files and the database
- (Optional) An external Postgres 9.4 database server may be used. The provided files will automatically configure a Postgres 9.4 Docker container by default.

### 4.1.2 Verification Service

To build the Verification Service Docker image:

1) Download and extract the `host-verification-service-docker.zip` archive to `/root/` on a Docker host server (this may be a physical or virtual server with the prerequisites installed)

2) If custom repositories will be needed, place the `.repo` definition files in the extracted `yum.repos.d/` folder.

3) Run `docker-compose` to build the image. Use build arguments to set proxies if proxies are necessary for your network.
   a) Without Proxies:
      ```bash
      docker-compose build verification-service
      ```
   b) With Proxies:
      ```bash
      docker-compose build --build-arg http_proxy=http_proxy_server \  
      --build-arg https_proxy=https_proxy_server \ 
      --build-arg no_proxy=repo_and_other_local_servers \ 
      verification-service
      ```

After the build process completes, the image should appear when the “docker images” command is executed:

```bash
# docker images
```
The "Dockerfile" file contains the definition for the initial image creation. The build process will use the service installation binary to partially install the Verification Service, without generation of any deployment-specific secrets or keys. The remaining installation tasks will be performed when the container is launched the first time, and a persistent storage volume will be used to maintain the configuration when the container is restarted.

4.1.3 Integration Hub

To build the Integration Hub Docker image:

4) Download and extract the attestation-hub-docker.zip archive to /root/ on a Docker host server (this may be a physical or virtual server with the prerequisites installed)
5) If custom repositories will be needed, place the .repo definition files in the extracted yum.repos.d/ folder.
6) Run docker-compose to build the image. Use build arguments to set proxies if proxies are necessary for your network.

    docker-compose build --build-arg http_proxy=<http_proxy_server> \
    --build-arg https_proxy=<https_proxy_server> \n    --build-arg no_proxy=<repo_and_other_local_servers> \n    attestation-hub

After the build process completes, the image should appear when the "docker images" command is executed:

    # docker images
    REPOSITORY          TAG       IMAGE ID
    isecl-attestation-hub latest 1a9dd20e97e3
The "Dockerfile" file contains the definition for the initial image creation. The build process will use the service installation binary to partially install the Integration Hub, without generation of any deployment-specific secrets or keys. The remaining installation tasks will be performed when the container is launched the first time, and a persistent storage volume will be used to maintain the configuration when the container is restarted.

### 4.1.4 Trust Agent

To build the Trust Agent Docker image:

7) Download and extract the trustagent-linux-docker.zip archive to /root/ on a Docker host server (this may be a physical or virtual server with the prerequisites installed)
8) If custom repositories will be needed, place the .repo definition files in the extracted yum.repos.d/ folder.
9) Run docker-compose to build the image. Use build arguments to set proxies if proxies are necessary for your network.

```
docker-compose build --build-arg http_proxy=<http_proxy_server>
                  --build-arg https_proxy=<https_proxy_server>
                  --build-arg no_proxy=<repo_and_other_local_servers>
                  iseclv1-agent
```

After the build process completes, the image should appear when the "docker images" command is executed:

```
# docker images

<table>
<thead>
<tr>
<th>REPOSITORY</th>
<th>TAG</th>
<th>IMAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>isecl-trustagent</td>
<td>latest</td>
<td>9ec70e88e186</td>
</tr>
</tbody>
</table>
```

The "Dockerfile" file contains the definition for the initial image creation. The build process will use the service installation binary to partially install the Trust Agent, without generation of any deployment-specific secrets or keys. The remaining installation tasks will be performed when the container is launched the first time, and a persistent storage volume will be used to maintain the configuration when the container is restarted.
4.2 Deploying the Intel® SecL Service Containers

4.2.1 Verification Service

When the Verification Service container is first run, it will perform setup and configuration tasks. By default, this includes using a Postgres database container that will automatically be created.

The container uses several persistent storage volumes that contain configuration files, logs, secrets, and keys. If the Verification Service is restarted, the configuration in the storage volumes will be retained so that the initial setup does not need to be repeated, and so that secrets and keys do not change on container restart.

4.2.1.1 Container Configuration

Configuration settings can be changed by modifying the following files:

mtwilson.env

At minimum, this must define the Admin Username and password. This defines the initial administrative user created during installation. Additional variables can be set here as per the same mtwilson.env answer file options supported for the non-container based installer.

MC_FIRST_USERNAME=<Admin user>
MC_FIRST_PASSWORD=<Admin password>

docker-compose.yml

This file defines the container configuration for the Verification Service, and additionally a Postgres database container for the Verification Service to use. An external Postgres 9.4 database server may optionally be used instead of the container, in which case the Postgres portion can be commented out of this file. Be sure to set the appropriate database options in the Verification
Service environment definition in this file if an alternative database server will be used.

This file can be modified to change configuration options for the container, but can be used as-is for a default installation. Be sure that the container hostname is resolvable from all Trust Agent nodes.

```yaml
version: "3.6"

services:
  hvs-pg-db:
    image: postgres:9.4
    command: postgres -c 'max_connections=400' -c 'shared_buffers=400MB'
    secrets:
      - db.password
    volumes:
      - hvs-pgdata-volume:/var/lib/postgresql/data
      - hvs-pg-password: hvs_db
      - POSTGRES_USER: hvs_user
      - POSTGRES_PASSWORD_FILE: /run/secrets/db.password

verification-service:
  image: isecl-verification-service:latest
  build: .
  hostname: verification-service
  depends_on:
    - "hvs-pg-db"
  ports:
    - 8443:8443
  secrets:
    - source: mtwilson_env
      target: mtwilson.env
    - db.password
  environment:
    DATABASE_HOSTNAME: hvs-pg-db
    DATABASE_PORTNUM: 5432
    POSTGRES_DB: hvs_db
    POSTGRES_USER: hvs_user
  volumes:
    - hvs-config-volume:/opt/mtwilson/configuration
    - hvs-logs-volume:/opt/mtwilson/logs

volumes:
  hvs-pgdata-volume:
  hvs-config-volume:
  hvs-logs-volume:

secrets:
  mtwilson_env:
    file: ./mtwilson.env

db.password
```
Update the file to set the Postgres password. This will be used by the Postgres database server, and also will be used by the Verification Service to connect to the database server.

### 4.2.1.2 Persistence Volume Creation

The Verification Service container uses the following persistence volumes:

- hvs-config-volume
- hvs-logs-volume

Additionally, by default the Verification Service docker-compose.yml defines a separate Postgres database container for the Verification Service to use. This database container requires a storage volume to retain database information.

- hvs-pgdata-volume

These volumes are created automatically from the definitions in the docker-compose.yml file. To change the path where these volumes will be stored, edit the docker-compose file.

### 4.2.1.3 Starting the Container

To start the Verification Service and associated Postgres database containers, run the following:

```bash
docker-compose up --remove-orphans --abort-on-container-exit
```

Once the container is down/stopped (docker-compose down), the containers no longer need the .env files and db.password to restart, since the setup activities are done during the first launch and the configurations are stored as part of the volumes.

The container status can be confirmed using the “docker ps” command:
```bash
$ docker ps
CONTAINER ID        IMAGE                               COMMAND
747472d6666c        isecl-verification-service:latest
"/root/start_hvs"
7523fc0e7c83        postgres:9.4
"docker-
entrypoint.s...
```

To stop the containers, use the following:

```
docker-compose down
```

## 4.2.2 Integration Hub

When the Integration Hub container is first run, it will perform setup and configuration tasks. By default, this includes using a Postgres database container that will automatically be created.

The container uses several persistent storage volumes that contain configuration files, logs, secrets, and keys. If the Hub is restarted, the configuration in the storage volumes will be retained so that the initial setup does not need to be repeated, and so that secrets and keys do not change on container restart.

### 4.2.2.1 Prerequisites

- The Verification Service must be installed and running

### 4.2.2.2 Container Configuration

Configuration settings can be changed by modifying the following files:

`attestation-hub.env`

At minimum, this must define the connection details for the Verification Service, and the Integration Hub initial administrator user credentials, which will be created during setup. Additional variables can be set here as per the same `attestation-hub.env` answer file options supported for the non-container based installer.
MTWILSON_HOSTNAME=verification-service
MTWILSON_USERNAME=username
MTWILSON_PASSWORD=password
MTWILSON_TLS_CERT_SHA384=2c8b3d29bd64de927fc66568ee67c8fb36895c440f8455c19c1b2f9949d23b8f6656efc4a47217da3c43d28ddc5f5a4
AHUB_USER_NAME=username
AHUB_USER_PASSWORD=password

docker-compose.yml

This file defines the container configuration for the Integration Hub, and additionally a Postgres database container for the Integration Hub to use. An external Postgres 9.4 database server may optionally be used instead of the container, in which case the Postgres portion can be commented out of this file. Be sure to set the appropriate database options in the Integration Hub environment definition in this file if an alternative database server will be used.

This file can be modified to change configuration options for the container, but can be used as-is for a default installation. Be sure that the MTWILSON_HOSTNAME value is resolvable to the Verification Service from the container.
Update the file to set the Postgres password. This will be used by the Postgres database server, and also will be used by the Integration Hub to connect to the database server.
4.2.2.3 Persistence Volume Creation

The Verification Service container uses the following persistence volumes:

ahub-pgdata-volume:
ahub-config-volume:
ahub-logs-volume:
ahub-tenant-config-volume:

Additionally, by default the Integration Hub `docker-compose.yml` defines a separate Postgres database container for the Integration Hub to use. This database container requires a storage volume to retain database information.

ahub-pgdata-volume

These volumes are created automatically from the definitions in the `docker-compose.yml` file. To change the path where these volumes will be stored, edit the `docker-compose.yml` file.

4.2.2.4 Starting the Container

To start the Integration Hub and associated Postgres database containers, run the following:

docker-compose up --remove-orphans --abort-on-container-exit

Once the container is down/stopped (docker-compose down), the containers no longer need the .env files and db.password to restart, since the setup activities are done during the first launch and the configurations are stored as part of the volumes.

The container status can be confirmed using the "docker ps" command:

```
# docker ps
CONTAINER ID        IMAGE
escbc6c46aee        isecl-attestation-hub:latest
b5037f373ccc        postgres:9.4
```

To stop the containers, use the following:
4.2.3 Trust Agent

When the Trust Agent container is first run, it will perform setup and configuration tasks. This includes taking ownership of the TPM, generating a new AIK, and creation of other secrets and keys. After this setup is performed, the persistent data in the storage volume will be intrinsically tied to the physical TPM of the host, and cannot be used on any other host. Note that this requires that the Trust Agent also be run in privileged mode.

The container uses several persistent storage volumes that contain configuration files, logs, secrets, and keys. If the Trust Agent is restarted, the configuration in the storage volumes will be retained so that the initial setup does not need to be repeated, and so that secrets and keys do not change on container restart.

4.2.3.1 Prerequisites
- The Verification Service must be installed and running
- TPM ownership must be clear and the TPM must be activated
- Tboot must be installed on the host, and the host must be booted to a tboot boot option (TXT-enabled deployments with UEFI SecureBoot not enabled only; if UEFI SecureBoot is enabled, or if TXT is not enabled, tboot must not be installed)

4.2.3.2 Container Configuration
Configuration settings can be changed by modifying the following files:

trustagent.env

At minimum, this must define the connectivity details for the Verification Service. Additional variables can be set here as per the same attestation-hub.env answer file options supported for the non-container based installer. Using the PROVISION_ATTESTATION=yes option and the TRUSTAGENT_LOGIN_REGISTER=yes option are strongly recommended.

MTWILSON_HOSTNAME=verification-service
MTWILSON_API_USERNAME=admin
docker-compose.yml

This file defines the container configuration for the Trust Agent.

This file can be modified to change configuration options for the container, but can be used as-is for a default installation. Be sure that the container hostname is resolvable and unique for each host – this will define the hostname seen in the Verification Service after registration.

```
version: "3.1"
services:
  iseclv1-agent:
    image: isecl-trustagent:latest
    build: .
    hostname: trustagent
    network_mode: host
    privileged: true
    environment:
      - TRUSTAGENT_DOCKER_HOST_MOUNT=/root/host_root
    secrets:
      - source: trustagent_env
        target: trustagent.env
    volumes:
      - tagent-config-volume:/opt/trustagent/configuration
      - tagent-logs-volume:/opt/trustagent/logs
      - /var/lib/tpm:/var/lib/tpm
      - /:/root/host_root
    extra_hosts:
      - "verification-service:<hostname or IP address>"

volumes:
  tagent-config-volume:
  tagent-logs-volume:

secrets:
  trustagent_env:
    file: trustagent.env
```
4.2.3.3 Persistence Volume Creation

The Verification Service container uses the following persistence volumes:

- trustagent-config-volume:/opt/trustagent/configuration
- trustagent-logs-volume:/opt/trustagent/logs
- /var/lib/tpm:/var/lib/tpm
- /:/root/host_root

These volumes are created automatically from the definitions in the docker-compose.yml file. To change the path where these volumes will be stored, edit the docker-compose file. Note that for the Trust Agent specifically, the / and /var/lib/tpm volumes must not be changed, as they allow the container access to the TPM and host information required for trust attestation.

4.2.3.4 Starting the Container

To start the Trust Agent container, run the following:

docker-compose up --remove-orphans --abort-on-container-exit

Once the container is down/stopped (docker-compose down), the containers no longer need the .env files and db.password to restart, since the setup activities are done during the first launch and the configurations are stored as part of the volumes.

The container status can be confirmed using the "docker ps" command:

```
# docker ps
CONTAINER ID        IMAGE
582bfd3da5ee        isecl-trustagent:latest
```

To stop the containers, use the following:

docker-compose down
5 Authentication

NOTE: The Change to AAS-based authentication is currently only partially completed in the Intel® SecL 1.6 BETA. Currently only requests to the CMS, AAS, and WLS use the AAS-based token authentication and authorization. Other services still use the "legacy" HTTP BASIC auth method with each service maintaining their own auth layers with fully independent user access and permissions. In the 1.6 GA release, the HTTP BASIC authentication will be fully deprecated and replaced with AAS-based token authentication. This section is written for the AAS-based token authentication method that will be present in the GA release.

5.1 Token Authentication

Beginning in the Intel® SecL-DC 1.6 release, authentication is centrally managed by the Authentication and Authorization Service (AAS). This service uses a Bearer Token authentication method, which replaces the previous HTTP BASIC authentication. This service also centralizes the creation of roles and users, allowing much easier management of users, passwords, and permissions across all Intel® SecL-DC services.

To make an API request to an Intel® SecL-DC service, an authentication token is now required. API requests must now include an Authorization header with an appropriate token:

"Authorization: Bearer $TOKEN"

The token is issued by the AAS and will expire after a set amount of time. This token may be used with any Intel® SecL-DC service, and will carry the appropriate permissions for the role(s) assigned to the account the token was generated for.

5.1.1 Create Token

To request a new token from the AAS:

POST https://<AAS IP or hostname>:8444/aas/token

| "username" : "<username>",
| "password" : "<password>" |

The response will be a token that can be used in the Authorization header for other requests. The length of time for which the token will be valid is configured on the AAS using the key AASJWT_TOKEN_DURATION_MINS (in the
installation answer file during installation) or `aas.jwt.token.duration.mins` (configured on the AAS after installation). In both cases the value is the length of time in minutes that issued tokens will remain valid before expiring.

5.2 **User Management**

Users in Intel® SecL-DC are no longer restrained to a specific service, as they are now centrally managed by the Authentication and Authorization Service. Any user may now be assigned roles for any service, allowing user accounts to be fully defined by the tasks needed.

5.2.1 **Create User**

```plaintext
POST https://<IP or hostname of AAS>:8444/aas/users
Authorization: Bearer <token>

{
  "username" : "<username>",
  "password" : "<password>"
}
```

5.2.2 **Search User**

```plaintext
GET https://<IP or hostname of AAS>:8444/aas/users
Authorization: Bearer <token>
```

5.2.3 **Delete User**

```plaintext
DELETE https://<IP or hostname of AAS>:8444/aas/users/<User ID>
Authorization: Bearer <token>
```

5.3 **Roles and Permissions**

Permissions in Intel® SecL-DC are managed by Roles. Roles are a set of predefined permissions applicable to a specific service. Any number of Roles may be applied to a User. While new Roles can be created, each Intel® SecL service defines permissions that are applicable to specific predetermined Roles. This means that only pre-defined Roles will actually have any permissions. Role creation is intended to allow Intel® SecL-DC services to define their permissions while allowing role and user management to be centrally managed on the AAS. When a new service is installed, it will use the Role creation functions to define roles applicable for that service in the AAS.
5.3.1  Role Definitions

5.3.1.1  Workload Service

### WLS:Administrator
- Has access to all REST endpoints on WLS

### WLS:FlavorsImageRetrieval
- Allows access to retrieve specified Image Flavors from the WLS

### WLS:ReportsCreate
- Allows access to create new Image Reports

5.3.1.2  Authentication and Authorization Service

AAS:RoleManager
- Has access to create new Roles. Note that Roles must correspond to actual predefined Roles on each service; while "custom" roles can be created, they will not have any actual permissions unless the Role is predefined in a service with assigned permissions.

AAS:UserManager
- Has access to create, search, and delete Users

AAS:UserRoleManager
- Has access to assign Roles to Users. Any number of Roles may be assigned to a single User.

5.3.2  Create Role

POST https://<AAS IP or Hostname>:8444/aas/roles
Authorization: Bearer <token>

```
|
  "service": "<Service name>",
  "name": "<Role Name>
```

5.3.3  Search Roles

GET https://<AAS IP or Hostname>:8444/aas/roles?=value
Authorization: Bearer <token>

Search parameters supported:
Service=<name of service>
Name=<role name>
Context=<context>
contextContains=<partial "context" string>
allContexts=<true or false>
filter=false

5.3.4 Delete Role

DELETE https://<AAS IP or Hostname>:8444/aas/roles/<role ID>
Authorization: Bearer <token>

5.3.5 Assign Role to User

POST https://<AAS IP or Hostname>:8444/aas/users/<user ID>/roles
Authorization: Bearer <token>

| "role_ids": ["comma-separated list of role IDs"] |

5.3.6 List Roles Assigned to User

GET https://<AAS IP or Hostname>:8444/aas/users/<user ID>/roles
Authorization: Bearer <token>

5.3.7 Remove Role from User

DELETE https://<AAS IP or Hostname>:8444/aas/users/<user ID>/roles/<role ID>
Authorization: Bearer <token>
6 User Management

NOTE: This section refers to the authentication and authorization methods used in Intel® SecL-DC prior to the 1.6 release. It is included because several services still use this authentication method in the 1.6 BETA release. This method will be fully deprecated and replaced by the new AAS-based token authentication and authorization mechanism for all services in the 1.6 GA release.

6.1 Permissions

Each REST API in ISecL has specific permission requirements; these are defined for each API resource in the Javadoc. Permissions are defined as a domain:permission key/value pair.

For example, “hosts:create” defines a permission that would allow a user to create host objects. This would correspond to host registration.

Wildcards are also acceptable. The permissions “hosts:*” would allow all permissions on the hosts resource, allowing the user to create, update, and delete hosts.

Permissions can be used for users on the Verification Service, the Trust Agent, and the Integration Hub. However, permissions and users are not shared across these services. A user with permissions on the Verification Service will not have any permissions on the Integration Hub, for example.

6.2 Roles

Roles are collections of permissions that can be applied to a user. Roles are applicable only for the Verification Service.

Several roles are included by default.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
</table>
| trustagent_provisioner | host_aiks:certify
|                  | tpm_endorsements:create
|                  | tpm_endorsements:search
|                  | tpm_passwords:create
|                  | tpm_passwords:retrieve
|                  | tpm_passwords:search
|                  | tpm_passwords:store
|                  | tpm: endorse
|                  | host_signing_key_certificates:create
|                  | store_host_pre_registration_details:create
| administrator     | *:*                                                                         |
### Roles and Permissions

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>auditor</td>
<td>*:search,retrieve</td>
</tr>
<tr>
<td>asset_tag_manager</td>
<td>tag_certificate_requests:*</td>
</tr>
<tr>
<td></td>
<td>tag_selection_kv_attributes:*</td>
</tr>
<tr>
<td></td>
<td>tag_certificates:*</td>
</tr>
<tr>
<td></td>
<td>tag_kv_attributes:*</td>
</tr>
<tr>
<td></td>
<td>tag_selections:*</td>
</tr>
<tr>
<td>flavor_manager</td>
<td>host_tls_policies:create, search, retrieve</td>
</tr>
<tr>
<td></td>
<td>flavorgroup:*</td>
</tr>
<tr>
<td></td>
<td>flavors:*</td>
</tr>
<tr>
<td>host_manager</td>
<td>hosts:*</td>
</tr>
<tr>
<td></td>
<td>host_attestations:*</td>
</tr>
<tr>
<td></td>
<td>host_tls_policies:search,retrieve</td>
</tr>
<tr>
<td></td>
<td>host_status:search,retrieve</td>
</tr>
<tr>
<td>reports_manager</td>
<td>reports:*</td>
</tr>
<tr>
<td>host_unique_flavor_creator</td>
<td>host_unique_flavors:create</td>
</tr>
<tr>
<td>host_based_flavor_creator</td>
<td>host_based_flavor:create</td>
</tr>
</tbody>
</table>

Custom roles can be created using REST APIs:

1. **Create a role:**
   ```
   POST https://host-verification-server.com:8443/mtwilson/v2/roles
   
   Input: {"role_name":"role_sample"}
   ```

2. **Assign permissions to the role:**
   ```
   https://host-verification-server.com:8443/mtwilson/v2/roles/<role ID>/permissions
   
   Input: {"permit_domain":"hosts", "permit_action":"create,delete", "permit_selection":"*"}
   ```

Roles can now be assigned using the new custom role.

### 6.3 Creating a User for HTTP Basic Authentication

User creation can be performed via the command line (for all ISecL services), or via REST API (Verification Service only).

**Note:** ISecL does not currently integrate with other authentication providers like Keystone or LDAP.

ISecL passwords do not expire automatically, and cannot be changed. To change a password, delete the existing password for the user, and create a new password.
Note: Integration Hub and Trust Agent users cannot be deleted without reinstalling.

6.3.1 Creating a User – CLI

6.3.1.1 Verification Service

mtwilson login-password <username> <password> --permissions <permission1>,<permission2>,...

6.3.1.2 Trust Agent

tagent password <username> <password> --permissions *:*

6.3.1.3 Integration Hub

attestation-hub password <username> <password> --permissions *:*

6.3.2 Creating a User – REST API

Creating a user via the REST API involves three steps:

1. Creating a new user request
2. Creating a new user password
3. Approving the new user password and applying permissions

Note: A single username can have more than one password. Permissions and roles are attached to the password, so a given user could have one password that allows only "hosts:search", but another password that allows "hosts:*".

1. Creating a new user request

```
POST https://host-verification-server.com:8443/mtwilson/v2/users

Input: {"username":"User1","locale":"en-US","comment":"Access needed for Project1"}
```

2. Creating a new user password

The "password_hash" value should be the SHA384 digest of the password in base64 encoded format. The "salt" should be a random 8 bytes in base64 encoded format. The "iterations" value determines the number of iterations used to generate the password_hash from the original password. If the password was hashed only once, this value should be set to "1". Currently only the SHA256 algorithm is supported.

```
POST https://host-verification-server.com:8443/mtwilson/v2/users/<userID>/login-passwords
```
3. Approving the new user password and applying permissions

New user passwords cannot be used until approved by an administrator. The same call used to approve a new user/password request is used to assign permissions to that user by applying one or more roles. Permissions cannot be directly applied via this API. To use a set of permissions not provided by an existing role, create a new custom role with the needed permissions, and use that role for the user password.

https://host-verification-server.com:8443/mtwilson/v2/users/<User ID>/login-passwords/<Password ID>

Input: {"status":"APPROVED","enabled":true,"roles": ["<Role 1>", "<Role 2>"]}

6.4 Certificate Authentication

As an alternative to HTTP Basic authentication, the ISeCL VerificatioN Servie also supports cert0f0cate-based authentication when using the ISeCL Verification Service API Client.

Certificate authentication requires a user-generated keypair. The public key is registered to the Verification Service in x509 certificate form and associated to a user. The login certificate can then be activated and assigned roles by an administrator.

**Note:** A single user may have any number of login passwords and login certificates, each with their own permissions. For example, a user may have additional permissions when logging on using a secure API client using certificate authentication, but have read-only access to fewer resources when logging on with a password via a browser.

ISeCL certificate authentication is a custom implementation. Requests using certificate authentication must include the following header:

`authorization: x509 <string of signed data>`

The signed data includes informative request data and the base64 encoded signature of the request body and all headers. The body of the request and all headers are concatenated into a string and then signed using the user's private key. The following must be included in the signed data string:

- HTTP method (GET, POST, etc.)
- Request URL
- Shiro authentication realm
- The Base64 encoded sha-384 fingerprint of the login certificate containing the RSA public key
- Full request body (if any)
- Signature algorithm (Currently SHA256withRSA or RSA-SHA256 are supported)
- HTTP headers
- A 24-byte X-Nonce consisting of 8 bytes of the current time in milliseconds and 16 bytes of random data
- The current date in the following format: “EEE, d MMM yyyy HH:mm:ss z”

**Note:** The ISecL Verification Service API Client is required for using certificate authentication due to the custom implementation.

### 6.4.1 Creating a Login Certificate

1. Creating a new user request

   POST https://host-verification-server.com:8443/mtwilson/v2/users

   Input: {
   "username": "User1", "locale": "en-US", "comment": "Access needed for Project1"
   }

2. Creating a new user login certificate

   The user should create a new RSA keypair, and include the public key in x509 format in the "certificate" field of the request body.

   POST https://host-verification-server.com:8443/mtwilson/v2/users/<user ID>/login-certificates

   Input: {
   "certificate": "MIICrzCCAZegAwIB.....LX+vzkAQDdqf1SkV+Bw==",
   "comment": "Need to manage user accounts."
   }

3. Approving the new user password and applying permissions

   New user passwords cannot be used until approved by an administrator. The same call used to approve a new user/certificate request is used to assign permissions to that user by applying one or more roles. Permissions cannot be directly applied via this API. To use a set of permissions not provided by an existing role, create a new custom role with the needed permissions, and use that role for the user password.


   Input: {
   "status": "APPROVED", "enabled": true, "roles": ["<Role 1>", "<Role 2>"
   ]}
7 Connection Strings

Connection Strings define a remote API resource endpoint that will be used to communicate with the registered host for retrieving TPM quotes. Connection Strings differ based on the type of host.

7.1 Trust Agent (Windows and Linux)

The Trust Agent connection string connects directly to the Trust Agent on a given host. If the Trust Agent is installed or provisioned with the option to pre-register the Trust Agent credentials in the Verification Service (TRUSTAGENT_LOGIN_REGISTER=true), no authentication details are needed; the Verification Service will use the credentials already stored in its database to make the connection. If the credential pre-registration option was not selected, the credentials for the Trust Agent will need to be provided in the connection string.

intel:https://<HostNameOrIp>:1443

If the "TRUSTAGENT_LOGIN_REGISTER" option was not used during installation, or if it was set to "false," credentials will need to be supplied as part of the connection string:

intel:https://<HostNameOrIp>:1443;u=<username>;p=<password>

7.2 VMware ESXi

The VMware ESXi connection string is actually directed to vCenter, not the actual ESXi host. Many ESXi hosts managed by the same vCenter server will use the same connection string. The username and password specified are vCenter credentials, and the vCenter "Validate Session" privilege is required for access.

vmware:https://<vCenterHostNameOrIp>:443/sdk;h=<hostname of ESXi host>;u=<username>;p=<password>
8 **Platform Integrity Attestation**

Platform attestation is the cornerstone use case for ISecL. Platform attestation involves taking measurements of system components during system boot, and then cryptographically verifying that the actual measurements taken matched a set of expected or approved values, ensuring that the measured components were in an acceptable or "trusted" state at the time of the last system boot.

ISecL leverages the Trusted Compute Group specification for a trusted boot process, extending measurements of platform components to registers in a Trusted Platform Module, and securely generating quotes of those measurements from the TPM for remote comparison to expected values (attestation).

This section includes basic REST API examples for these workflows. See the Javadoc for more detailed documentation on REST APIs supported by ISecL.

Typical workflows in the datacenter might include:

- Creating a set of acceptable flavors for attestation with automatic flavor matching that represent the known-good measurements for acceptable BIOS and OS versions in the datacenter
- Registering hosts for attestation with automatic flavor matching
- Upgrading hosts in the datacenter to a new BIOS or OS version
- Removing hosts from the Verification Service
- Removing flavors
- Provisioning asset tags to hosts
- Invalidating asset tags
- Retrieving current attestation reports
- Retrieving current host state information
- Remediating an untrusted attestation
8.1 **Host Registration**

Registration creates a host record with connectivity details and other host information in the Verification Service database. This host record will be used by the Verification Service to retrieve TPM attestation quotes from the Trust Agent to generate an attestation report.

8.1.1 **Trust Agent**

8.1.1.1 **Registration via Trust Agent Command Line**

The Trust Agent can register the host with a Verification Service by running the following command:

```
tagent create-host <Verification Service base URL> <username> <password>
```

*Note:* Because VMware ESXi hosts do not use a Trust Agent, this method is not applicable for registration of ESXi hosts.

8.1.2 **Registration via Verification Service API**

Any Trust Agent or VMware ESXi host can be registered using a Verification Service API request. Registration can be performed with or without a set of existing Flavors. Rules for Flavor matching can be set by using the Flavor Group in the request; if no Flavor Group is specified, the "mtwilson_automatic" Flavor Group will be used. See the Flavor Management section for additional details on Flavors, Flavor Groups, and Flavor matching.

8.1.2.1 **Sample Call**

```json
POST https://verification.service.com:8443/mtwilson/v2/hosts
{
    "host_name": "<hostname of host to be registered>",
    "tls_policy_id": "TRUST_FIRST_CERTIFICATE",
    "connection_string": "<connection string>",
    "flavorgroup_name": "",
    "description": "<description>"
}
```

Requires the permission “hosts:create”
8.2 Flavor Creation for Automatic Flavor Matching

Flavor creation is the process of adding one or more sets of acceptable measurements to the Verification Service database. These measurements correspond to specific system components, and are used as the basis of comparison to generate trust attestations.

Flavors can be created manually, or can be imported from an example host.

Flavors are automatically matched to hosts based on the Flavorgroup used by the host and the Flavors, and the Flavor Match Policies of the Flavorgroup. The ISeCl Verification Service creates a default Flavorgroups during installation called “automatic.” This Flavorgroup is configured to be used as a pool of all acceptable Flavors in a given environment, and will automatically match the appropriate Flavor parts to the correct host. This Flavorgroup is used by default and is expected to be useful for the majority of deployments. If no Flavorgroup is specified when creating a Flavor, it will be placed in the "automatic" Flavorgroup.

Flavors are also divided into Flavor parts, which correspond to the PLATFORM, OS, HOST_UNIQUE, SOFTWARE, and ASSET_TAG measurements. These can be created and maintained separately (so that users can manage acceptable OS and BIOS versions, rather than entire host configurations). By default, if not specified, the Verification Service will import Flavors as separate Flavor parts, as appropriate for the host type.

By using individual Flavor parts, individual versions of OS or PLATFORM measurements can be managed and automatically mapped. Whenever a host changes states (Untrusted, Connected, etc.) the Verification Service will attempt to match appropriate Flavors to that host. If a Flavor is removed or added, all appropriate hosts will be updated to use the new Flavor, or to no longer use the deleted Flavor. Hosts that are currently using a BIOS where that BIOS versions’ PLATFORM Flavor was deleted will now appear Untrusted, for example. This can be used to easily flag as Untrusted hosts that are using software that has been End-Of-Lifed, or perhaps an OS kernel with a known security vulnerability.

Note: See the Flavor Management section for additional details on how flavors can be managed, and how the Flavor matching engine works. The sample workflow provided here is intended to be an introduction only.
8.2.1 Importing a Flavor from a Sample Host

POST https://server.com:8443/mtwilson/v2/flavors
input:
{ "connection_string": "<connection string>",
"partial_flavor_types": ["PLATFORM", "OS", "HOST_UNIQUE"],
"flavorgroup_name": 
,"tls_policy_id": "TRUST_FIRST_CERTIFICATE"}

Requires the permission "flavors:create"

Note: The HOST_UNIQUE Flavor parts, used by Red Hat Enterprise Linux and VMWare ESXi host types, MUST be created for each registered host of that type, and should in general be imported from that host. This means that importing the HOST_UNIQUE flavor should always be done for each host registered (except for Windows hosts, which do not have HOST_UNIQUE measurements).

To import ONLY the HOST_UNIQUE Flavor part from a host:

POST https://server.com:8443/mtwilson/v2/flavors
input:
{ "connection_string": "<connection string>",
"partial_flavor_types": ["HOST_UNIQUE"],
"flavorgroup_name": 
,"tls_policy_id": "TRUST_FIRST_CERTIFICATE"}

Requires the permission "flavors:create"

8.2.2 Creating a Flavor Manually

Flavors can be directly created (rather than importing from a sample host) if the required information is known. If no Flavorgroup is specified, the Flavor will be placed in the "automatic" group. Note that the "label" is a required field and must be unique.

POST https://server.com:8443/mtwilson/v2/flavors
input:
{ "connection_string": "",
"tls_policy_id": "",
"flavor_collection": 
{ "flavors": []
"meta": 
{ "vendor": "INTEL",
"description": 
{ "flavor_part": "PLATFORM"},
"flavor_part": "PLATFORM",
8.3 Creating the Default SOFTWARE Flavor (Linux Only)

As part of the new Application Integrity feature added in Intel® SecL-DC version 1.5, a new default SOFTWARE Flavor part is provided so that the Linux Trust Agent itself can be measured and included in the attestation process. The default SOFTWARE Flavor includes a manifest for the static files and folders in the Trust Agent. The manifest is automatically deployed to each Linux Trust Agent during the provisioning step.

**Note:** The Linux Trust Agent must be rebooted after the Provisioning step is completed (typically Provisioning happens during installation, based on whether all of the required variables are set in the trustagent.env file). Rebooting allows the default SOFTWARE Flavor manifest to be measured and extended to the TPM PCRs. If the reboot is not performed, the system will require a SOFTWARE Flavor, but the...
measurements will not exist, and the system will appear Untrusted. If an un-rebooted host is used to create the SOFTWARE Flavor, the Flavor will be created based on measurements that do not exist, and will fail.

The SOFTWARE Flavor part should be created separately from the other Flavor parts. Only one default SOFTWARE Flavor needs to be created for each version of the Linux Trust Agent. If the SOFTWARE Flavor for the same Trust Agent version is imported multiple times, subsequent imports will fail as the Flavor already exists.

To import the SOFTWARE Flavor part from a host:

POST https://server.com:8443/mtwilson/v2/flavors
input:
{
"connection_string": "<connection string>",
"partial_flavor_types": ["SOFTWARE"],
"flavorgroup_name": "",
"tls_policy_id": "TRUST_FIRST_CERTIFICATE"
}
Requires the permission "flavors:create"

8.4 Creating and Provisioning Asset Tags

Asset Tags represent a set of key/value pairs that can be associated with a host in hardware. This enables usages around restricting workflows to specific hosts based on tags, which could include location information, compliance tags, etc.

ISEcL creates Asset Tags by creating a certificate containing the list of key/value pairs to be tagged to the host, with the host’s hardware UUID as the certificate subject. A hash of this certificate is then written to an NVRAM index in the host’s TPM. This value is included in TPM quotes, and can be attested using an Asset Tag flavor that matches up the expected value and the actual key/value pairs.

8.4.1 Creating Asset Tag Certificates

Asset Tag certificates can be created with a single REST API call, with any number of key/value pairs. Note that one certificate must be created for each host to be tagged, even if they will all be tagged with identical key/value pairs.
POST https://verification.server.com:8443/mtwilson/v2/tag-certificates
{"hardware_uuid": "<hardware UUID of host to be tagged>",
"selection_content": [
{
   "name": "<key>",
   "value": "<value>"
},
{
   "name": "<key>",
   "value": "<value>"
},
{
   "name": "<key>",
   "value": "<value>"
}
]}

8.4.2 Deploying Asset Tags

8.4.2.1 Windows and Red Hat Enterprise Linux

Asset Tags can be provisioned to a Windows or RHEL host via a REST API request on the Verification Service that will in turn make a request to the Trust Agent on the host to be tagged.

POST https://verification.server.com:8443/mtwilson/v2/rpc/deploy-tag-certificate
{
   "certificate_id": "<certificate ID>",
   "host": "<Hostname of host to be tagged>"
}

8.4.2.2 VMWare

Since VMWare ESXi hosts do not use a Trust Agent, the process for writing Asset Tags to a VMWare host is different from RHEL or Windows. A new interface has been added to ESXi via a new "esxcli" command starting in vSphere 6.5 Update 2 that allows the Asset Tag information to be written to the TPM via a command-line command. The older process is also described below.

The high-level workflow for using Asset Tags with VMWare ESXi is:

1. Create the Asset Tag Certificate for the host.
2. Calculate the Certificate Hash value.
3. Provision the Certificate Hash value to the host TPM and reboot.
4. Create the Asset Tag Flavor.

**Note:** Asset Tag is currently not supported for VMWare hosts using TPM 2.0.

### 8.4.2.2.1 Calculate the Certificate Hash Value

Only the hash value of the Asset Tag Certificate can be provisioned to the TPM, due to the low size of the NVRAM.

1. Retrieve the Asset Tag Certificate. The Asset Tag Certificate can be retrieved either from the response when the Asset Tag certificate is created, or by using a GET API request to retrieve the certificate:

   ```
   GET https://verification.server.com:8443/mtwilson/v2/tag-certificates?subjectEqualTo=<HardwareUUID>
   ```

2. Copy only the "certificate" value (this will be the certificate in encoded format) and write the data to a file on a Linux system. Remove any line breaks and save the file. Assuming the filename used is "tag-cert," use the following to generate the correct hash:

   ```
   cat tag-cert | base64 --decode | openssl dgst -sha1 | awk -F " " '{print $2}''
   ```

   This hash value will be what is actually written to the TPM NVRAM.

### 8.4.2.2.2 Provision the Certificate Hash to the Host TPM

Due to a new feature added in vSphere 6.5 Update 2, the process for provisioning Asset Tags on VMWare ESXi hosts has been significantly improved. Both the old and new process for provisioning Asset Tags is documented below. Intel recommends using vSphere 6.5 Update 2 or later due to the significant difference in the process.

**vSphere 6.5 Update 2 or Later**

Starting in ESXi 6.5u2, you can now use SSH to write Asset Tags directly with no need for TPM clears, reboots, PXE, or BIOS access. SSH to the ESXi host using root credentials. Then use the command:

```
1. esxcli hardware tpm tag set -d <hash>
```

You can use the following command to verify that the tag was written:

```
esxcli hardware tpm tag get
```

4. Reboot the host. After rebooting, the TPM PCR 22 will have the measured value of the hash.
vSphere 6.5 Update 1 or Older

There is no direct interface from VMWare vCenter or ESXi previous to vSphere 6.5 Update 2 that will write the Tag information to the host TPM.

Writing Asset Tag information to a TPM requires TPM ownership; VMWare ESXi takes TPM ownership with a secret password at boot time. This means that the process for writing Asset Tags to a VMWare host requires:

1. Clear TPM ownership.
   a. This can be done via the system BIOS, or using One Touch Activation through the IPMI interface (if enabled by the server OEM).
2. Reactivate TPM/TXT.
   a. This can be done via the system BIOS, or using One Touch Activation through the IPMI interface (if enabled by the server OEM).
3. Booting to an OS that has the ability to issue TPM commands
   a. Typically the provisioning OS used is Ubuntu or RHEL, booted temporarily using PXE.
4. Writing the Tag information
   a. The TPM index 0x40000010 must be defined, and the hash of the Asset Tag certificate must be written to that index.
5. Clear TPM ownership.
   a. This can be done via the system BIOS, or using One Touch Activation through the IPMI interface (if enabled by the server OEM).
6. Reactivate TPM/TXT.
   a. This can be done via the system BIOS, or using One Touch Activation through the IPMI interface (if enabled by the server OEM).
7. Boot back to VMWare ESXi.

When the system is rebooted to ESXi, the Trusted Boot process will extend the value to PCR22, and this value can be used during attestation.

8.4.2.2.3 Creating the Asset Tag Flavor (VMWare ESXi Only)

While for RHEL and Windows hosts the Asset Tag Flavor is automatically created during the Tag Provisioning step, for VMWare ESXi hosts the Flavor must be created by importing it from the host after the Tag has been provisioned.

POST https://verification.server.com:8443/mtwilson/v2/flavors
"connection_string": "<VMware vCenter connection string>",
"tls_policy_id": "TRUST_FIRST_CERTIFICATE"
"partial_flavor_types": ["ASSET_TAG"]
}

Once the Asset Tag Flavor is imported, the host can be attested including Asset Tags as normal.

8.5 Retrieving Current Attestation Reports
GET https://verification.service.com:8443/mtwilson/v2/reports?latestPerHost=true

8.6 Retrieving Current Host State Information
GET https://verification.service.com:8443/mtwilson/v2/host-status?latestPerHost=true

8.7 Upgrading Hosts in the Datacenter to a New BIOS or OS Version
Software and firmware updates are a common occurrence in the datacenter. Automatic Flavor matching makes this process relatively simple:
1. Create a new Flavor for the new version. This may be manually created or imported directly from a sample host that has already received the upgrade. Be sure to create new Flavors for each TPM version represented in your datacenter.

POST https://server.com:8443/mtwilson/v2/flavors
input:
{ "connection_string": "<connection string>",
"partial_flavor_types": ["PLATFORM", "OS", "HOST_UNIQUE"],
"flavorgroup_name": "",
"tls_policy_id": "TRUST_FIRST_CERTIFICATE"}

2. Update the hosts to the new software or firmware version as normal. On the next attestation attempt, the Verification Service will automatically match the updated hosts to the new Flavor.

3. (Optional) If desired, delete the Flavor for the older version after the update is completed. This will cause any hosts that are still using the old version to attest as Untrusted. Which can easily flag hosts that missed the upgrade for remediation.

DELETE https://verification.service.com:8443/mtwilson/v2/flavors/<Flavor ID>

8.8 Removing Hosts From the Verification Service
Hosts can be deleted at any time. Reports for that host will remain in the Verification Service database for audit purposes.

DELETE https://verification.service.com:8443/mtwilson/v2/hosts/<host ID>

The Host ID can be retrieved either at the time the host is created, or by searching hosts using the host's hostname.

8.9 Removing Flavors

Flavors can be deleted; this will cause any hosts that match the deleted Flavor to evaluate as Untrusted. This can be done if, for example, an old BIOS version needs to be retired and should no longer exist in the datacenter. By deleting the PLATFORM Flavor, hosts with the old BIOS version will attest as Untrusted, flagging them for easy remediation.

DELETE https://verification.service.com:8443/mtwilson/v2/flavors/<Flavor ID>

8.10 Invalidating Asset Tags

Asset Tags can be deleted in two ways.

Deleting the ASSET_TAG Flavor part will retain the Asset Tag certificate in the database, but will cause the host using this Tag to no longer use the Asset Tag for attestation (the Tag result will be disregarded and no tags will be exposed in the attestation Reports).

DELETE https://verification.service.com:8443/mtwilson/v2/flavors/<Asset Tag Flavor ID>

Deleting the actual Asset Tag certificate will remove the certificate from the database, but will not actually affect attestation results (the authority for attestation results is the Flavor).

DELETE https://verification.service.com:8443/mtwilson/v2/tag-certificates/<Asset Tag Certificate ID>

8.11 Remediating an Untrusted attestation

Hosts can become Untrusted for a wide variety of causes. The first clue to finding the root cause for an Untrusted attestation is the attestation Report itself – the Report will show Trust results for the PLATFORM, OS, HOST_UNIQUE, and ASSET_TAG Flavor parts individually, along with the OVERALL trust. If the Report shows that the PLATFORM Flavor part trust is “false” for example, it means that the PLATFORM measurements did not match any Flavors in the host’s Flavorgroup.

Untrusted attestation Reports will contain “faults” that describe the specific attestation rules that were not satisfied. This often shows enough information to describe the cause of the Untrusted status. A fault like
“RequiredButNotDefined” means that a Flavor part is required by the Flavorgroup policy, but no Flavors for that Flavor part exist in the Flavorgroup (for example, generally Flavorgroups should always require a PLATFORM Flavor part; if no PLATFORM Flavors are in the Flavorgroup, hosts in the Flavorgroup will attest with this fault).

Other faults include:

“PcrMatchesConstant” - describes a rule that evaluates whether a TPM PCR has a specific value

“PcrEventLogIntegrity” - the module event log is replayed during attestation to verify that the resulting measurement matches the actual value in the module PCR. If the replay does not match, it indicates the event log cannot itself be trusted.

“AikCertificateTrusted” – This rule evaluates whether the TPM quote was signed by the TPM associated with this host. As part of host registration, the public half of the Attestation Identity Keypair is captured, and this public key is used to verify the signature on TPM quotes from that host.

See the Appendix for a full list of the rules evaluated during Attestation.

The Flavor matching engine will use the most-similar Flavor for the attestation Report in the case of an Untrusted result.

The fault will explain in a general sense what rule the host attestation violated. To remediate, the rule will need to be satisfied. This could mean creating a new Flavor to match the actual observed values, or it could mean that the host has been tampered with and should have its BIOS flashed or OS reloaded.

8.12 Attestation Reporting

Attestation results are delivered in the form of Host Reports. A Report can delivered in several different formats, which can change the type of data returned.

The preferred format for Host Reports is a SAML attestation. A SAML-formatted report includes a chain or signatures that provides auditability for the Report. The SAML attestation will include the base trust status of the host, as well as the overall trust for each individual Flavor used in the attestation. The Report will also contain host information, such as TPM version, Operating System name and version, BIOS version, etc. The SAML Report will not, however, contain individual measurements and comparisons of values. This format of the Report is ideal for securely communicating the trust status of a host and for audit history.

Attestation Reports can also be retrieved in JSON or XML format. These formats will not include the signature chain provided in the SAML format, but
will contain the actual measurement values and expected Flavor values used for comparison. These reports are typically used for remediation, because they will show specifically why a given Host attested as Untrusted.

The format for a Report is determined by the “Accept” header in the request.

Attestations are automatically generated in the Verification Service by a repeating scheduled background process. This process looks for Attestation Reports that are close to expiration, and triggers a new Attestation Report. By default, Attestation Reports are valid for 90 minutes, and the background refresh process will trigger a new attestation when a Report is found to be within 3 minutes of expiration.

A user can either retrieve the most recent currently valid Attestation Report for a given host, or may trigger a new Attestation Report to be generated. Typically, it is best to retrieve an existing Report for performance reasons. Generating a new Attestation Report requires the generation of a new TPM quote from the TPM of the host being attested; TPM performance differs greatly between vendors, and a quote can take anywhere between 2-7 seconds to generate.

### 8.12.1 Sample Call – Generating a New Attestation Report

**POST** https://server.com:8443/mtwilson/v2/reports

input: {"host_name":"host-1"}

Requires the permission "reports:create"

### 8.12.2 Sample Call – Retrieving an Existing Attestation Report

**GET** https://server.com:8443/mtwilson/v2/reports?hostName=HostName.server.com

Below are the supported criteria options in order of precedence. If no host filter criteria is specified, then results are returned for all active hosts.

- **id** - unique UUID of the report entry in the database
- **hostId** - unique UUID of the host entry in the database
- **hostName** - name of the host
- **hostHardwareId** - hardware UUID of the host
- **hostStatus** - current state of the host, which supports the following options:
  - **CONNECTED** - host is in connected state
  - **QUEUE** - host is in queue to be processed
  - **CONNECTION_FAILURE** - connection failure
— UNAUTHORIZED - unauthorized
— AIK_NOT_PROVISIONED - AIK certificate is not provisioned
— EC_NOT_PRESENT - endorsement certificate is not present
— MEASURED_LAUNCH_FAILURE - TXT measured launch failure
— TPM OWNERSHIP_FAILURE - TPM ownership failure
— TPM_NOT_PRESENT - TPM is not present
— UNSUPPORTED_TPM - unsupported TPM version
— UNKNOWN - unknown host state

Requires the permissions "reports:search"

Other search criteria may also be used. By default, the most recent currently valid attestation is returned. However, different query parameters can be used to retrieve all attestations for a specific host over the last 30 days, for example.

### 8.13 Integration

Intel® SecL can be integrated with scheduler services (or potentially other services) to provide additional security controls. For example, by integrating Intel® SecL with the OpenStack scheduler service, the OpenStack placement service can incorporate the Intel® SecL security attributes into VM scheduling.

#### 8.13.1 Integration Hub

The Integration Hub acts as the central integration point between the Verification Service and any number of third party services. The primary purpose of the Hub is to collect and maintain up-to-date attestation information, and to “push” that information to the external services. The secondary purpose is to allow for multitenancy. The Verification Service does not allow for permissions to be applied for specific hosts; a user with the “attestation” role can access all attestations for all hosts. The Integration Hub allows hosts to be associated with specific tenants; the tenants do not have direct access to the Verification Service, and the Hub will push attestations only for the associated hosts to a given tenant’s integration endpoints.

For example, Tenant A is using hosts 1-10 for an OpenStack environment. Tenant B is using hosts 11-15 for a Docker environment. The Attestation Hub can push the information for hosts 1-10 to Tenant A’s OpenStack endpoint, and hosts 11-15 to Tenant B’s Docker endpoint. Neither tenant will have access to the Verification Service, and will not be able to see attestation or other host details regarding infrastructure used by other tenants.

Different integration endpoints can be added to the Integration Hub through a plugin architecture. By default, the Attestation Hub includes a plugin for OpenStack.
8.13.2 Integration with OpenStack

Starting in the Rocky release, OpenStack can now use "Traits" to provide qualitative data about Nova Compute hosts, and to establish Trait requirements for VM instances. The updated scheduler will place VMs requiring a given Trait on Nova Compute nodes that meet the Trait requirements.

Intel SecL-DC uses the Integration Hub to continually push platform integrity and Asset Tag information to the OpenStack Traits resources. This means the OpenStack scheduler natively supports workload scheduling incorporating Intel SecL-DC security attributes, including attestation report Trust status and Asset Tags. The OpenStack Placement Service will automatically attempt to place images with Trait requirements on compute nodes that have those Traits.

NOTE: This control only applies to instances launched using the OpenStack scheduler, and the Traits functions will not affect manually-launched instances where a specific Compute Node is defined (since this does not use the scheduler at all). Intel SecL-DC uses existing OpenStack interfaces and does not modify OpenStack code. The datacenter owner or OpenStack administrator is responsible for the security of the OpenStack workload scheduling process in general, and Intel recommends following published OpenStack security best practices.

8.13.2.1 Prerequisites

- Verification Service must be installed and running.
- OpenStack* Rocky Nova, Glance, Horizon, and Keystone services must be installed and running
- The Integration Hub must be installed and running.

8.13.2.2 Setting Image Traits

Image Traits define the policy for which Traits are required for that Image to be launched on a Nova Compute node. By setting these Traits to "required," the OpenStack scheduler will require these same Traits to be present on a Nova Compute node in order to launch instances of the image.

To set the Image Traits for Intel SecL-DC, a specific naming convention is used. This naming convention will match the Traits that the Integration Hub will automatically push to OpenStack. Two types of Traits are currently supported – one Trait is used to require that the Compute Node be Trusted in the Attestation Report, and the other Trait is used to require specific Asset Tag key/value pairs.

To require a "Trusted" Attestation Report:
The naming convention for Asset Tags is more flexible, and any number of these Traits can be used simultaneously.

**Note:** All of the Traits must be present on the Compute Node for the scheduler to allow instances to land, so be sure not to set mutually exclusive Asset Tag values.

CUSTOM_ISECL_TRUSTED=required

For example, to define a Trait that will require an Asset Tag where "State = CA," use the following:

CUSTOM_ISECL_AT_STATE_CA=required

These Traits can be set using CLI commands for OpenStack Glance:

```bash
openstack image set --property trait:CUSTOM_ISECL_AT_STATE_CA=required <image_name>
openstack image set --property trait:CUSTOM_ISECL_TRUSTED=required <image_name>
```

To remove a Trait so that it is no longer required for an Image:

```bash
openstack image unset --property trait:CUSTOM_ISECL_AT_STATE_CA <image_name>
openstack image unset --property trait:CUSTOM_ISECL_TRUSTED <image_name>
```

### 8.13.2.3 Configuring the Integration Hub for Use with OpenStack

After installation, the Integration Hub will automatically start retrieving Reports from the Verification Service. However, the Hub needs to be configured with endpoint information defining credentials and URLs for the OpenStack environment, and needs to have Hosts assigned to specific Tenants so that the right host info can be pushed to the correct OpenStack.

### 8.13.2.4 Integration Hub Account Creation

From the command line, run the following:

```
attestation-hub password username password --permissions *:*
```

The username and password defined will be the credentials used for API requests.

Only one Hub admin account is needed; this step can be skipped if an administrative user has already been created.
8.13.2.5 Integration Hub Tenant Creation

At least one tenant must be created to receive the attestations. For the Hub, a single tenant is typically a single OpenStack controller. Below is an example using OpenStack where the api.endpoint is Nova and the auth.endpoint is Keystone.

POST https://server.com:19445/v1/tenants

```json
{
    "name": "<Tenant name>",
    "plugins": [
        {
            "name": "nova",
            "properties": [
                {
                    "key": "api.endpoint",
                    "value": "http://<Nova API endpoint>/compute/v2.1"
                },
                {
                    "key": "auth.endpoint",
                    "value": "http://<Keystone API endpoint>:5000/identity"
                },
                {
                    "key": "auth.version",
                    "value": "v3"
                },
                {
                    "key": "user.name",
                    "value": "<Username for Nova API>"
                },
                {
                    "key": "user.password",
                    "value": "<Password for Nova API>"
                },
                {
                    "key": "tenant.name",
                    "value": "<Name of tenant in OpenStack>"
                },
                {
                    "key": "domain.name",
                    "value": "<Name of Domain in OpenStack>"
                },
                {
                    "key": "plugin.provider",
                    "value": "com.intel.attestationhub.plugin.nova.NovaPluginImpl"
                }
            ]
        }
    ]
}
```
8.13.2.6 List Hosts

The Integration Hub periodically queries the Verification Service for the list of all new Reports; only Reports generated after the timestamp of the most recent query are returned. Because host registration will trigger the generation of a new Report, any new hosts added to the Verification Service will be seen in the Hub on the next refresh (determined by the value of the POLL_INTERVAL variable during install).

The list of hosts known to the Integration Hub can be retrieved using the below API sample.

GET https://server.com:19445/v1/hosts

8.13.2.7 Assign Hosts to Tenants

Hosts must be assigned to a tenant before Intel SecL-DC security attributes will be pushed to the OpenStack Traits. Any number of hosts may be assigned to one tenant. Multiple hosts can be assigned to a tenant in a single request by using a comma-separated list of hardware_uuids.

POST https://server.com:19445/v1/host-assignments

{ "tenant_id": "DCC2284A-F525-4094-BA01-E317FE28E15F", "hardware_uuids": [ "D088db98-994d-e411-906e-0017a4403562" ] }

The Hub will "push" Intel SecL-DC attributes as OpenStack Traits to the tenant's configured endpoints (in this case, Nova) every time it looks for new attestations.

8.13.2.8 Scheduling Instances

Once Trait requirements are set for Images and the Integration Hub is configured to push attributes to OpenStack, instances can be launched in OpenStack as normal. As long as the OpenStack Nova scheduler is used to schedule the workloads, only compliant Compute Nodes will be scheduled to run instances of controlled Images.

**NOTE:** This control only applies to instances launched using the OpenStack scheduler, and the Traits functions will not affect manually-launched instances where a specific Compute Node is defined (since this does not use the scheduler at all).

Intel SecL-DC uses existing OpenStack interfaces and does not modify OpenStack code. The datacenter owner or OpenStack administrator is responsible for the security of the OpenStack environment.
workload scheduling process in general, and Intel recommends following published OpenStack security best practices.
8.13.3 Integration with Kubernetes

Through the use of Custom Resource Definitions for the Kubernetes Master, Intel® Security Libraries can make Kubernetes aware of Intel® SecL security attributes and make them available for pod orchestration. In this way, a security-sensitive pod can be launched only on “Trusted” physical worker nodes, or on physical worker nodes that match specified Asset Tag values.

NOTE: This control only applies to pods launched using the Kubernetes scheduler, and these scheduling controls will not affect manually-launched instances where a specific worker node is defined (since this does not use the scheduler at all). Intel SecL-DC uses existing Kubernetes interfaces and does not modify Kubernetes code, using only the standard Custom Resource Definition mechanism to add this functionality to the Kubernetes Master. The datacenter owner or Kubernetes administrator is responsible for the security of the Kubernetes workload scheduling process in general, and Intel recommends following published Kubernetes security best practices.

8.13.3.1 Prerequisites

- Verification Service must be installed and running.
- Kubernetes Master Node must be installed and running
- Kubernetes Worker Nodes must be configured as physical hosts and attached to the Master Node
- The Integration Hub must be installed and running.

8.13.3.2 Installing the Intel® SecL Custom Resource Definitions

Intel® SecL uses Custom Resource Definitions to add the ability to base orchestration decisions on Intel® SecL security attributes to Kubernetes. These CRDs allow Kubernetes administrators to configure pods to require specific security attributes so that the Kubernetes Master Node will schedule those pods only on Worker Nodes that match the specified attributes.

Perform the following steps on the Kubernetes Master Node:

1) Add a mount path to the kube-scheduler.yaml file for the Intel SecL scheduler extension:

   - mountPath: /opt/isecl-k8s-extensions/bin/
     name: extendedsched
     readOnly: true
2) Add a volume path to the kube-scheduler.yaml file for the Intel SecL scheduler extension:

   - hostPath:
     path: /opt/isecl-k8s-extensions/bin/
     type: ""  
   name: extendedsched

3) Copy the isecl-k8s-extensions.bin installer to the Kubernetes Master and execute the installer

   ./isecl-k8s-extensions.bin

4) The installer will output a set of keystores upon completion into .attestation-hub-keystores/. These contain keys that will be used by the Integration Hub to communicate with this Kubernetes Master. Copy the contents of this directory to the Integration Hub:

   scp -r /root/attestation-hub-keystores/* root@integration-hub.server.com:/opt/attestation-hub/configuration/

   Note that the Integration Hub can manage multiple Kubernetes Master environments at the same time, but the keystores must be kept separate. To do this, create subfolders in the Hub configuration directory for each separate Kubernetes environment, and copy the appropriate keystores to the matching subfolder.

5) Copy the Integration Hub public key to the Kubernetes Master:

   scp attestation-hub.server.com:/opt/attestation-hub/configuration/hub_public_key.pem /etc/kubernetes/pki/

6) Run the command systemctl restart kubelet to restart all the control plane container services, including the base scheduler.

7) (Optional) Verify that the Intel ® SecL Custom Resource Definitions have been started:

   kubectl get crds
   kubectl get -o json hostattributes.isecl.intel.com

8.13.3.3 Integration Hub Account Creation

   From the command line, run the following:

   attestation-hub password username password --permissions *:*

   The username and password defined will be the credentials used for API requests.

   Only one Hub admin account is needed; this step can be skipped if an administrative user has already been created.
8.13.3.4 Integration Hub Tenant Creation

At least one tenant must be created to receive the attestations. For the Hub, a single tenant is typically a single OpenStack controller. Below is an example using OpenStack where the api.endpoint is Nova and the auth.endpoint is Keystone.

POST https://server.com:19445/v1/tenants

```json
{
  "name": "TenantName",
  "plugins": [
    {
      "name": "kubernetes",
      "properties": [
        {
          "key": "api.endpoint",
          "value": "https://kubernetes-master.server.com:6443"
        },
        {
          "key": "tenant.name",
          "value": "TenantName"
        },
        {
          "key": "plugin.provider",
          "value": "com.intel.attestationhub.plugin.kubernetes.KubernetesPluginImpl"
        },
        {
          "key": "kubernetes.client.keystore",
          "value": "/opt/attestation-hub/configuration/root_k8s_client.jks"
        },
        {
          "key": "kubernetes.server.keystore",
          "value": "/opt/attestation-hub/configuration/root_k8s_trust.jks"
        },
        {
          "key": "kubernetes.client.keystore.password",
          "value": "<Keystore password>"
        },
        {
          "key": "kubernetes.server.keystore.password",
          "value": "<Keystore Password>"
        }
      ]
    }
  ]
}
```

**NOTE:** the value of `kubernetes.client.keystore` and `kubernetes.server.keystore` must be the filesystem path on
the Integration Hub that contains the Kubernetes Master keystores output from the scheduler extensions for this tenant. The value of `kubernetes.server.keystore.password` and `kubernetes.server.keystore.password` must be the keystore passwords output by the scheduler extensions installer.

### 8.13.3.5 List Hosts

The Integration Hub periodically queries the Verification Service for the list of all new Reports; only Reports generated after the timestamp of the most recent query are returned. Because host registration will trigger the generation of a new Report, any new hosts added to the Verification Service will be seen in the Hub on the next refresh (determined by the value of the `POLL_INTERVAL` variable during install).

The list of hosts known to the Integration Hub can be retrieved using the below API sample.

```
GET https://server.com:19445/v1/hosts
```

### 8.13.3.6 Assign Hosts to Tenants

Hosts must be assigned to a tenant before Intel SecL-DC security attributes will be pushed to Kubernetes. Any number of hosts may be assigned to one tenant. Multiple hosts can be assigned to a tenant in a single request by using a comma-separated list of `hardware_uids`.

```
POST https://server.com:19445/v1/host-assignments
{
  "tenant_id": "DC02284A-F525-4094-B401-E317FE28E15F",
  "hardware_uids": [
    "00886b98-994d-e411-906e-0017a4403562"
  ]
}
```

The Hub will “push” Intel SecL-DC attributes as OpenStack Traits to the tenant’s configured endpoints (in this case, Nova) every time it looks for new attestations.

### 8.13.3.7 Configuring Pods to Require Intel® SecL Attributes

1) (Optional) Verify that the worker nodes have had their Intel® SecL security attributes populated:

```
kubectl get nodes --show-labels
```

The output should show the Trust status and any Asset Tags applied to all of the registered Worker Nodes.

2) Add the following to any Pod creation files:
spec:
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
          - matchExpressions:
              - key: isecl.trusted
                operator: In
                values:
                  - "true"
              - key: TAG_Country
                operator: In
                values:
                  - CA
                  - US
              - key: TAG_Customer
                operator: In
                values:
                  - Coke
                  - Pepsi
              - key: TAG_State
                operator: In
                values:
                  - CA

The "isecl.trusted" key defines the requirement for a Trusted host. Only one of these keys should be used. The "TAG_" keys indicate Asset Tags; if the workload should only launch on hosts with the "COUNTRY=US" Asset Tag, the pod should be launched with the matchExpression key "TAG_COUNTRY" with the value "US".

All of the matchExpression definitions must be true for a given worker node to launch the pod – in the example above, the host must be attested as Trusted with Asset Tags "Country=US," "Customer=Customer1," and "State=CA." If the worker node has additional Asset Tags beyond the ones required, the pod will still be able to be launched on that node. However, if one of the specified Tags is missing or has a different value, that worker node will not be used for that pod.
Workload Confidentiality builds upon Platform Attestation to protect data in virtual machine and container images. At its core, this feature is about allowing an image owner to set policies that define the conditions under which their image will be allowed to run; if the policy conditions are met, the decryption key will be provided, and if the conditions are not met, the image will remain encrypted and inaccessible. This provides a level of enforcement beyond integration with orchestrators, and protects sensitive data when the image is at rest.

Workload Encryption relies on Platform Attestation to define the security attributes of hosts. When a protected image is launched, the Workload Agent on the host launching the VM or container image will detect the attempt (using either Libvirt hooks for VMs, or as a function of the Docker Secure Overlay Driver in the case of containers) and use the Image ID to find the Image Flavor on the Workload Service. The Workload Service will retrieve the current trust report for the host launching the image, and use that report to make a key retrieval request to the key transfer URL retrieved from the image flavor. The key transfer URL refers to the URL to the image owner’s Key Broker Service, along with the ID of the key needed.

In a typical production deployment, a Cloud Service Provider would enable Intel® Secl-DC security controls by installing the Intel® Secl-DC applications (with the exception of the Key Broker and Workload Policy Manager), and configuring each workload host to be Trusted (as per the Platform Integrity Attestation use case).

The owner of the workload image(s) to be protected (for example, the end customer of the CSP) must install a Key Broker Service (which must be available for network communication from the Workload Service hosted on the CSP), the Workload Policy Manager, and their own Authentication and Authorization Service and Certificate Management Service (these will manage authentication and certificates for the KBS and WPM).

Any number of image owner customers with their own unique KBS/WPM/AAS/CMS deployments may protect images that can be run by a single CSP deployment.

The image owner will use the WPM to encrypt any image(s) to be protected; the WPM will automatically create a new image encryption key using the KBS, and will output the encrypted image and an Image Flavor. The image owner can then upload the encrypted image to the CSP’s image storage service, and then upload the Image Flavor to the CSP-hosted WLS.

When a compute host at the CSP attempts to launch a protected image, the WLA on the host will detect the launch request, and will issue a key transfer
request to the WLS. The WLS will use the image ID to retrieve the Image Flavor, which contains the key retrieval URL for that image. This URL is hosted on the KBS of the image owner (which is why the KBS must be available to network requests from the WLS). The WLS will access the HVS to retrieve the current Platform Integrity Attestation report for the host, and will use this report to make a key transfer request to the KBS at the key transfer URL.

The KBS will receive the request, verify that the Platform Integrity Attestation report is signed using a known SAML signing key (verifying that the report comes from a known and trusted HVS), and will then verify that the report shows that the host is trusted.

If these requirements are met, the KBS will use the host’s Binding Key (the public half of an asymmetric keypair generated by the host’s TPM and included in the attestation report) as a Key Encryption Key to seal the Image Encryption Key to the TPM of the host that was attested.

When the host receives the response to the key request, it will unseal the Image Encryption Key using its TPM. Because the Key Encryption Key is unique to this host’s TPM, only the actual host that was attested will be able to gain access to the image.

With the Image Encryption Key, the host’s WLA will create the appropriate encrypted volume(s) for the image and begin the launch as normal.

The WLA does not retain the key on disk; if/when the host is rebooted or the WLA is restarted, restarting the workloads based on protected images will trigger new key requests based on new Platform Integrity Attestation reports. In this way, if a host is compromised in a method detectable by the Platform Integrity feature, protected images will be unable to launch on this server.

### 9.1 Virtual Machine Confidentiality

#### 9.1.1 Prerequisites

To enable Virtual Machine Confidentiality, the following Intel® SecL-DC components must be installed and available:

- Authentication and Authorization Service
- Certificate Management Service
- Key Broker Service
- Host Verification Service
- Workload Service
- Trust Agent + Workload Agent (on each virtualization host)
- Workload Policy Manager

See the Installation subsection on Recommended Service Layout for recommendations on how/where to install each service.

It is strongly recommended to use a VM orchestration solution (for example, OpenStack) with the Intel® SecL-DC Integration Hub to schedule encrypted workloads on compute hosts that have already been pre-checked for their Platform Integrity status. See the Platform Integrity Attestation subsection on Integration with OpenStack for an example.

You will need at least one QCOW2-format virtual machine image (for quick testing purposes, a very small minimal premade image like CirrOS is recommended; a good place to look for testing images is the OpenStack Image Guide found here: https://docs.openstack.org/image-guide/obtain-images.html).

One or more hypervisor compute nodes running QEMU/KVM is required. Each of these nodes must have the Intel® SecL-DC Trust Agent and Workload Agent installed, and they must be registered with the Verification Service. Each of these servers should show as “trusted;” see the Platform Integrity Attestation section for details. You should have Flavors that match the system configuration for these hosts, and attestation reports should show all Flavor parts as “trusted=true.” Hosts that are not trusted (including servers where there is no trust status, like hosts with no Trust Agent) will fail to launch any encrypted workloads.

9.1.2 Workflow

9.1.2.1 Encrypting Images

wpm create-image-flavor -i <user-friendly unique label> -l <path to image file> -e <output path and filename for encrypted image> -o <output path for JSON image flavor>

After generating the encrypted image with the WPM, the encrypted image can be uploaded to the Image Storage service of choice (for example, OpenStack Glance). Note that the ID of the image in this Image Storage service must be retained and used for the next steps.

9.1.2.2 Uploading the Image Flavor

POST https://<Workload Service IP or Hostname>:5000/wls/flavors

Use the above API request to upload the Image Flavor to the WLS. The Image Flavor will tell other Intel® SecL-DC components the Key Transfer URL for this image.
9.1.2.3 Creating the Image Flavor to Image ID Association

The WLS needs to know the ID of the image as it exists in the image storage service used by the CSP (for example, OpenStack Glance). Use the below API request to create an association between the Image Flavor created in the previous step and the image ID.

POST https://<Workload Service IP or Hostname>:5000/wls/images
{
    "id": "<image ID on image storage>",
    "flavor_ids": [<"<Image Flavor ID>"]
}

9.1.2.4 Launching Encrypted VMs

Instances of the protected images can now be launched as normal. Encrypted images will only be accessible on hosts with a Platform Integrity Attestation report showing the host is trusted.

If the VM is launched on a host that is not trusted, the launch will fail, as the decryption key will not be provided.

9.2 Docker Container Confidentiality

9.2.1 Prerequisites

To enable Docker Container Confidentiality, the following Intel® SecL-DC components must be installed and available:

- Authentication and Authorization Service
- Certificate Management Service
- Key Broker Service
- Host Verification Service
- Workload Service
- Trust Agent + Workload Agent (on each Docker host)
- Workload Policy Manager

See the Installation subsection on Recommended Service Layout for recommendations on how/where to install each service.

It is strongly recommended to use a container orchestration solution (for example, Kubernetes) with the Intel® SecL-DC Integration Hub to
schedule encrypted Docker containers on compute hosts that have already been pre-checked for their Platform Integrity status. See the Platform Integrity Attestation subsection on Integration with Kubernetes for an example.

You will need at least one Docker container image (for quick testing purposes.)

One or more Docker container worker nodes running Docker 19.03 is required. Each of these nodes must have the Intel® SecL-DC Trust Agent and Workload Agent installed, and they must be registered with the Verification Service. Each of these servers should show as “trusted;” see the Platform Integrity Attestation section for details. You should have flavors that match the system configuration for these hosts, and attestation reports should show all flavor parts as “trusted=true.” Hosts that are not trusted (including servers where there is no trust status, like hosts with no Trust Agent) will fail to launch any encrypted workloads.

**Important Note:** Docker version 19.03 is specifically required, and other versions are not supported. Installation of the Workload Agent for Docker Container Confidentiality will replace the existing Docker binaries (the client and daemon, in /usr/bin/dockerd and /usr/bin/docker) with a recompiled Docker engine that includes the Secure Overlay Driver. This is what allows the launch of encrypted containers to be intercepted and decrypted. The Docker runtime must not be upgraded or downgraded to any other version; doing so will cause encrypted Docker Containers to fail to launch.

In the future, the Container Encryption feature will be modified to use OCI-standard container encryption without the need for recompilation or file replacement.

### 9.2.2 Workflow

#### 9.2.2.1 Encrypting Docker Container Images

The first step is encryption of a Docker Container image. The WPM is a command-line utility that will perform the actual image encryption, and allow the resulting encrypted image to be uploaded to a Docker Registry.

```bash
wpm create-container-image-flavor -1 <container image name> -t <tag name> -e -o <output path for JSON image flavor>
```

After generating the encrypted image with the WPM, the encrypted image can be uploaded to a local Docker Registry.
9.2.2.2 Uploading the Image Flavor

POST https://<Workload Service IP or Hostname>:5000/wls/flavors
{
  <Image Flavor content from WPM output>
}

Use the above API request to upload the Image Flavor to the WLS. The Image Flavor will tell other Intel® SecL-DC components the Key Transfer URL for this image.

9.2.2.3 Creating the Image Flavor to Image ID Association

For Docker images stored in a Docker Registry, the ID is typically an MD5 hash. This format must be converted for use with the Workload Service. To get the non-truncated ID of the image, use the Docker command:

```
docker images --no-trunc
```

Next, convert this to a UUID that can be used by ISecL:

```
wpm get-container-image-id <image-full-md5id>
```

The output will be a UUID, which will be considered the ID of the image for the WLS.

Use the below API request to create an association between the Image Flavor created in the previous step and the image ID.

POST https://<Workload Service IP or Hostname>:5000/wls/images
{
  "id": "<image ID on image storage>",
  "flavor_ids": ["<Image Flavor ID>"
}

9.2.2.4 Launching Encrypted Docker Containers

Containers of the protected images can now be launched as normal. Encrypted images will only be accessible on hosts with a Platform Integrity Attestation report showing the host is trusted.

If the Docker Container is launched on a host that is not trusted, the launch will fail, as the decryption key will not be provided.
10 Flavor Management

10.1 Flavor Format Definitions

A Flavor is a standardized set of expectations that determines what platform measurements will be considered "trusted." Flavors are constructed in a specific format, containing a metadata section describing the Flavor, and then various other sections depending on the Flavor type or Flavor part.

10.1.1 Meta

The first part of a Flavor is the "meta" section:

```
"meta": {
  "vendor": "INTEL",
  "description": {
    "flavor_part": "PLATFORM",
    "bios_name": "Intel Corporation",
    "bios_version": "SE5C620.868.00.01.0004.071220170215",
    "tpm_version": "2.0"
  }
},
```

This section defines the Flavor part and any versioning information.

Note: Even when the BIOS or OS version remains the same, the actual measurements in the measured boot process will be different between TPM 1.2 and TPM 2.0, and so the TPM version is captured here as well. The attributes in the Meta section are used by the Flavor matching engine when matching Flavors to Hosts.

10.1.2 Hardware

The "hardware" section is unique to PLATFORM flavor parts:

```
"hardware": {
  "processor_info": "54 06 05 00 FF FB EB BF",
  "processor_flags": "fpu vme de _",
  "feature": {
    "tpm": {
      "enabled": true,
      "pcr_banks": [
        "SHA1",
        "SHA256"
      ]
    }
  }
},
```
This part of the Flavor defines expected hardware attributes of the host, and contains processor and TPM-related attributes.

10.1.3 PCRs

The last section of a Flavor is the "PCRs" section, which contains the actual expected measurements for any PCRs. This section will contain PCR measurements for each applicable algorithm supported by the TPM (SHA1 only for TPM 1.2, SHA256 and SHA1 sections for TPM 2.0).

Some PCRs simply have a value and nothing else. Other PCRs, however, contain different "event" measurements. This indicates that separate individual platform or OS components are independently measured and extended to the same PCR. PCRs with event measurements will contain an "Event" array that lists, in the correct order, all of the events in the measurement event log that are extended to this PCR. When the Verification Service attests a host against a given Flavor, each measurement event is compared to the Flavor value, and all of the events are replayed to confirm that a replay of all of the measurement extensions do in fact result in the hash seen in the PCR value. In this way, the Verification Service can ensure that the measurement event log contents are secure, and the individual measurements can be attested so that the cause for an Untrusted attestation can easily be seen.

The full PCRs section is not shown here due to length; see the sample Flavor sections for a full sample.

```
"pcrs": {"SHA1": { "pcr_0": {"value": "d2ed12594276641a7260c4f92fdefbb67d531a0def"},
"pcr_17": {
"value": "1ec12004b371e3af47d04155abde7476a3794f4s", "event": [
{ "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1", "value": "2fb7d57d5455af9ac08d82bd2f155bce59a044", "label": "HASH_START", "info": [
{ "ComponentName": "HASH_START", "EventName": "OpenSource.EventName"}}
```
10.1.4 Sample PLATFORM Flavor

The PLATFORM Flavor part encompasses measurements that are unique to a specific platform, including the server OEM, BIOS version, etc. A PLATFORM Flavor can be “shared” across all hosts of the same model that have the same BIOS version.

```json
{
    "flavor_collection": {
        "flavors": [{
            "meta": {
                "vendor": "INTEL",
                "description": {
                    "flavor_part": "PLATFORM",
                    "bios_name": "Intel Corporation",
                    "bios_version": "SSE5C620.86B.00.01.0004.071220170215",
                    "tpm_version": "2.0"
                }
            },
            "hardware": {
                "processor_info": "54 06 05 00 FF FB EB BF",
                "processor_flags": "fpu vme de ..",
                "feature": {
                    "tpm": {
                        "enabled": true,
                        "pcr_banks": [
                            "SHA1",
                            "SHA256"
                        ]
                    },
                    "txt": {"enabled": true}
                }
            },
            "pcrs": {
                "SHA1": {
                    "pcr_0": {"value": "d2ed125942726641a7260c4f592bab575d531a0def"},
                    "pcr_1": {
                        "value": "lec12004d371e3af43d04155ahde7476a3794fa",
                        "event": {
                            "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
                            "value": "2fbd57dec5455af9ac08d82bf315d4bc59a044",
                            "label": "HASH_START",
                            "info": {
                                "ComponentName": "HASH_START",
                                "EventName": "OpenSource.EventName"
                            }
                        }
                    }
                }
            }
        }
    }
}
```
{
  "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
  "value": "ffb1806465d2de1b7531fd5a2afad7c5a047",
  "label": "BIOSAC_REG_DATA",
  "info": {
    "ComponentName": "BIOSAC_REG_DATA",
    "EventName": "OpenSource.EventName"
  }
},
{
  "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
  "value": "3c585604e87f855973731fefa83e21f930d22fc",
  "label": "CPU_SCRM_STAT",
  "info": {
    "ComponentName": "CPU_SCRM_STAT",
    "EventName": "OpenSource.EventName"
  }
},
{
  "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
  "value": "9069ca78a7450258134186525c259a473",
  "label": "LCP_CONTROL_HASH",
  "info": {
    "ComponentName": "LCP_CONTROL_HASH",
    "EventName": "OpenSource.EventName"
  }
},
{
  "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
  "value": "5ba93c9db0c93c9f52b521d7420e43f6eda2784f",
  "label": "LCP_DETAILS_HASH",
  "info": {
    "ComponentName": "LCP_DETAILS_HASH",
    "EventName": "OpenSource.EventName"
  }
},
{
  "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
  "value": "5ba93c9db0c93c9f52b521d7420e43f6eda2784f",
  "label": "STMHASH",
  "info": {
    "ComponentName": "STMHASH",
    "EventName": "OpenSource.EventName"
  }
},
{
  "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
  "value": "3c585604e87f855973731fefa83e21f930d22fc",
  "label": "OSSINITDATA_CAP_HASH",
  "info": {
    "ComponentName": "OSSINITDATA_CAP_HASH",
    "EventName": "OpenSource.EventName"
  }
}
<table>
<thead>
<tr>
<th>ComponentName</th>
<th>EventName</th>
<th>SHA256</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLE_HASH</td>
<td>OpenSource.EventName</td>
<td></td>
</tr>
<tr>
<td>NV_INFO_HASH</td>
<td>OpenSource.EventName</td>
<td></td>
</tr>
<tr>
<td>tb_policy</td>
<td>OpenSource.EventName</td>
<td></td>
</tr>
<tr>
<td>vmlinuz</td>
<td>OpenSource.EventName</td>
<td></td>
</tr>
<tr>
<td>initrd</td>
<td>OpenSource.EventName</td>
<td></td>
</tr>
</tbody>
</table>
"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value": "9301981c093654d5aa3430ba05c880a5e2eb2eb3e18248f5f93e1f6dab1cb947",
"label": "HASH_START",
"info": {
  "ComponentName": "HASH_START",
  "EventName": "OpenSource.EventName"
}
},

"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value": "2785d1ed65f6b3b55dc24ce5a68a44ce8740fe77e1e15a10b1ff6cca90",
"label": "BIOSAC_REG_DATA",
"info": {
  "ComponentName": "BIOSAC_REG_DATA",
  "EventName": "OpenSource.EventName"
}
},

"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value": "67abdd721024f0ff4e0b3f4c2fc13bc5bad42d0b7851d456d88d203d15aaa450",
"label": "CPU_SCRTM_STAT",
"info": {
  "ComponentName": "CPU_SCRTM_STAT",
  "EventName": "OpenSource.EventName"
}
},

"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value": "df3f619804a92db405792dc433d746e2778aadc524e984e08524c014b81119",
"label": "LCP_CONTROL_HASH",
"info": {
  "ComponentName": "LCP_CONTROL_HASH",
  "EventName": "OpenSource.EventName"
}
}

10.1.5 Sample OS Flavor

An OS Flavor encompasses all of the measurements unique to a given OS. This includes the OS kernel and other measurements.

| "flavor_collection": |
| "flavors": [ |
| "meta": |
| "vendor": "INTEL",
| "description": |
| "flavor_part": "OS",}
"os_name": "RedHatEnterpriseServer",
"os_version": "7.3",
"vmm_name": "",
"vmm_version": "",
"tpm_version": "2.0"
}
",
"pcrs": {
"SHA1": {
"value": "1ec12004b371e3af43d04155abde7476a3794fa",
"event": {
"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "2fb7d57dce545a3f9ac08d808df315dbcc59a044",
"label": "HASH_START",
"info": {
"ComponentName": "HASH_START",
"EventName": "OpenSource.EventName"
}
},
"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "ffb18064652de1b7531f5a2a6e6fa7c5a047",
"label": "BIOSAC_REG_DATA",
"info": {
"ComponentName": "BIOSAC_REG_DATA",
"EventName": "OpenSource.EventName"
}
},
"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "3c585604e87f855973731f6a83e21eaf9392d2fc",
"label": "CPU_SCRM_STAT",
"info": {
"ComponentName": "CPU_SCRM_STAT",
"EventName": "OpenSource.EventName"
}
},
"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "9069ca7e6a650b28517363b3e525c2529e473",
"label": "LCP_CONTROL_HASH",
"info": {
"ComponentName": "LCP_CONTROL_HASH",
"EventName": "OpenSource.EventName"
}
},
"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "5ba93c9db0c9f3f2b521d7420e43f6eda2784f"}
"label": "LCP_DETAILS_HASH",
"info": {
  "ComponentName": "LCP_DETAILS_HASH",
  "EventName": "OpenSource.EventName"
}
},

"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "5ba93c9db6cfff93f2b521d7420e43f6eda2784f",
"label": "STM_HASH",
"info": {
  "ComponentName": "STM_HASH",
  "EventName": "OpenSource.EventName"
}
},

"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "3c585604e87f88559733f1e89321fab9392d24c",
"label": "OSSINITDATA_CAP_HASH",
"info": {
  "ComponentName": "OSSINITDATA_CAP_HASH",
  "EventName": "OpenSource.EventName"
}
},

"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "3d42560dcf165a5557b3156a21583f2c6dbef10e",
"label": "MLE_HASH",
"info": {
  "ComponentName": "MLE_HASH",
  "EventName": "OpenSource.EventName"
}
},

"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "274f929dbab8b98a7031bbcd9e6a5613c2a86e6",
"label": "NV_INFO_HASH",
"info": {
  "ComponentName": "NV_INFO_HASH",
  "EventName": "OpenSource.EventName"
}
},

"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "ca96de412b4e8c662e570d3013d2fccc4b20d0a",
"label": "tb_policy",
"info": {
  "ComponentName": "tb_policy",
  "EventName": "OpenSource.EventName"
}
"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "d123e2f2b30f1effa8d9522667af9dad4f48cfd",
"label": "vmlinuz",
"info": {
  "ComponentName": "vmlinuz",
  "EventName": "OpenSource.EventName"
}
},
{
"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
"value": "f3742133e1a0deb8177a74ed225418e5cf73fd1",
"label": "initrd",
"info": {
  "ComponentName": "initrd",
  "EventName": "OpenSource.EventName"
}
}
],
"SHA256": {
"pcr_17": {
  "value": "50bd58407a1893056eacff493245cfe785f045b2c0e1cc3e6e9eb5812d8d91bd",
  "event": [
    {
      "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
      "value": "9301981c093654d5aa3430ba05c880a52eb22b9e8e1824f5f93e1f1dab1cb947",
      "label": "HASH_START",
      "info": {
        "ComponentName": "HASH_START",
        "EventName": "OpenSource.EventName"
      }
    },
    {
      "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
      "value": "2785d1ed65f6b5d55255dc24ce5e068a44ce8740fe77e0e15a10b1ff66c6a90",
      "label": "BIOSAC_REG_DATA",
      "info": {
        "ComponentName": "BIOSAC_REG_DATA",
        "EventName": "OpenSource.EventName"
      }
    },
    {
      "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
      "value": "67abdd7212024f0ff4e0b3f4c2fc13bc5ba4d20b7851d456d88d203d15aa450",
      "label": "CPU_SCRMT_STAT",
    }
  ]
}
"info":
  
  "ComponentName": "CPU_SCRMT_STAT",
  "EventName": "OpenSource.EventName"
}
},

"digest_type":
"com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value":
"df3f619004a92f6b405192d43d748ea775a2c498cbe80524c014b81119",
"label": "LCP_CONTROL_HASH",
"info":
  
  "ComponentName": "LCP_CONTROL_HASH",
  "EventName": "OpenSource.EventName"
}
),

"digest_type":
"com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value":
"6e340b9ccf87a989c544e6bb70a2c78901d3fb3373876851a30617af01d",
"label": "LCP_DETAILS_HASH",
"info":
  
  "ComponentName": "LCP_DETAILS_HASH",
  "EventName": "OpenSource.EventName"
}
),

"digest_type":
"com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value":
"6e340b9ccf87a989c544e6bb70a2c78901d3fb3373876851a30617af01d",
"label": "STM_HASH",
"info":
  
  "ComponentName": "STM_HASH",
  "EventName": "OpenSource.EventName"
}
),

"digest_type":
"com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value":
"67abdd721024f0ff4e6b3f4c2fc13bc5bad42d9b7851d456d88d203d15a5a450",
"label": "OSSINITDATA_CAP_HASH",
"info":
  
  "ComponentName": "OSSINITDATA_CAP_HASH",
  "EventName": "OpenSource.EventName"
}
),

"digest_type":
"com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value":
"26e1d98742f79c950dc637f8c067b0b72a1b0e8ff75db4e609c7e17321acfd3f4",
"label": "MLE_HASH",}
"info":
  {
    "ComponentName": "MLE_HASH",
    "EventName": "OpenSource.EventName"
  },
  {
    "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
    "value": "0f6e0c7a5944963d788ea494ddff1e9afa689a148e39f684db06578869ea38b",
    "label": "NV_INFO_HASH",
    "info":
      {
        "ComponentName": "NV_INFO_HASH",
        "EventName": "OpenSource.EventName"
      }
  },
  {
    "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
    "value": "27808f64e6383982cd3bccc10cfc9457c0b66f465f779d89bb668839eaf263a67",
    "label": "tb_policy",
    "info":
      {
        "ComponentName": "tb_policy",
        "EventName": "OpenSource.EventName"
      }
  },
  {
    "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
    "value": "c89ad1d1e9adaa7ecf62abc7e63b92472685f7d1b9f3799bf49974b66ed9638",
    "label": "vmlinuz",
    "info":
      {
        "ComponentName": "vmlinuz",
        "EventName": "OpenSource.EventName"
      }
  },
  {
    "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
    "value": "81b88e268e697ccf799d24db9dea748a8f395acfb47aa67c9845479d4e8456f77",
    "label": "initrd",
    "info":
      {
        "ComponentName": "initrd",
        "EventName": "OpenSource.EventName"
      }
  }
}
10.1.6 Sample HOST_UNIQUE Flavor

Host-Unique flavors define measurements for a specific host. This can be either a single large flavor that incorporates all of the host measurements into a single flavor document used only to attest a single host, or can be a small subset of measurements that are specific to a single host. For example, some VMWare module measurements will change from one host to the next, while most others will be shared assuming the same ESXi build is used. The full Flavor requirement for such a host would include Host-Unique flavors to cover the measurements that are unique to only this one host, and would still use a generic PLATFORM and OS flavor for the other measurements that would be identical for other similarly configured hosts.

Note: The HOST_UNIQUE Flavors are unique to a specific host, and should always be imported directly from the specific host. Windows hosts do not require a HOST_UNIQUE flavor part.

```json
{"flavors": [{
  "meta": {
    "id": "4d387cbd-f72b-4742-b4e5-c5b0ffed59e0",
    "vendor": "INTEL",
    "description": {
      "flavor_part": "HOST_UNIQUE",
      "source": "Purley11",
      "bios_name": "Intel Corporation",
      "bios_version": "SE5C620.86B.00.01.0004.071220170215",
      "os_name": "RedHatEnterpriseServer",
      "os_version": "7.4",
      "tpm_version": "2.0",
      "hardware_uuid": "00448C61-46F2-E711-906E-001560A04062"
    }
  },
  "pcrs": {
    "SHA256": {
      "pcr_17": {
        "value": "f9ef8c53ddfce89636eda55064363c52b4bfa2bd451a89aaa102f03181722176",
        "event": {
          "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
          "value": "df3f619804a2f2db4057192dc43dd74eaa778adc52bc498ce80524c014b88119",
          "label": "LCP_CONTROL_HASH",
          "info": {
            "ComponentName": "LCP_CONTROL_HASH",
            "EventName": "OpenSource.EventName"
          }
        }
      }
    }
  }
},
{"digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
"value": "4d387cbd-f72b-4742-b4e5-c5b0ffed59e0",
"label": "HOST_UNIQUE",
"info": {
  "ComponentName": "HOST.Unique",
  "EventName": "OpenSource.EventName"
}]
```
"value": "09f468dfc1d98a1fee86eb7297a56b0e097d57be66db4eae539061332da2e723",
  "label": "initrd",
  "info": {
    "ComponentName": "initrd",
    "EventName": "OpenSource.EventName"
  }
}

,"pcr_18": {
  "value": "c1f7bfdae5f270d9f13aa9620b8977951d6b759f1131fe9f9289317f3a56ef1a",
  "event": [
    {
      "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha256",
      "value": "df3f6198b4a92f3db4057192dc43dd748a778a02fc498ce80524c014b81119",
      "label": "LCP_CONTROL_HASH",
      "info": {
        "ComponentName": "LCP_CONTROL_HASH",
        "EventName": "OpenSource.EventName"
      }
    }
  ]
}

,"SHA1": {
  "pcr_17": {
    "value": "48695f747a3d494710bd14d20cb0a93c78a485cc",
    "event": [
      {
        "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
        "value": "90e9ca78e7450a285173431b3e652c5c25299e473",
        "label": "LCP_CONTROL_HASH",
        "info": {
          "ComponentName": "LCP_CONTROL_HASH",
          "EventName": "OpenSource.EventName"
        }
      },
      {
        "digest_type": "com.intel.mtwilson.lib.common.model.MeasurementSha1",
        "value": "b1f8db37e396b12820821b7e0ac54a5ec2791",
        "label": "initrd",
        "info": {
          "ComponentName": "initrd",
          "EventName": "OpenSource.EventName"
        }
      }
    ]
  }
}

,"pcr_18": {
  "value": "983ec7db975ed31e2c85ef8e375c038d6d307efb",
  "event": [
    {
      "repositories": {
        "value": "09f468dfc1d98a1fee86eb7297a56b0e097d57be66db4eae539061332da2e723",
        "label": "initrd",
        "info": {
          "ComponentName": "initrd",
          "EventName": "OpenSource.EventName"
        }
      }
    }
  ]
}
10.1.7 Sample ASSET_TAG Flavor

Asset Tag flavor parts are unique to Asset Tag attestation. These flavors verify that the Asset Tag data in the host’s TPM correctly matches the most recently created, currently valid Asset Tag certificate that has been deployed to that host.

```json
{
  "meta": {
    "id": "b3e0c056-5b6c-4b6b-95c4-de5f1473cac0",
    "description": {
      "flavor_part": "ASSET_TAG",
      "hardware_uuid": "<Hardware UUID of the server to be tagged>",
    }
  },
  "external": {
    "asset_tag": {
      "tag_certificate": {
        "encoded": "<Tag certificate in base64 encoded format>",
        "issuer": "CN=assetTagService",
        "serial_number": 1519153541461,
        "subject": "<Hardware UUID of the server to be tagged>",
        "not_before": "2018-02-20T11:05:41-0800",
        "not_after": "2019-02-20T11:05:41-0800",
        "fingerprint_sha256": "2YjKiugUM4kgk2Nh34vydXxurfMfewfIpYUiUz4c",
        "attribute": {
          "attr_type": "id": "2.5.4.789.2",
          "attribute_values": [{"objects": {}}]
        },
        "attr_type": "id": "2.5.4.789.2",
        "attribute_values": [{"objects": {}}]
      },
      "attribute": {
        "attr_type": "id": "2.5.4.789.2",
        "attribute_values": [{"objects": {}}]
      }
    }
  }
}
```
10.2 Flavor Matching

Flavors are matched to host by objects called “Flavor Groups.” A Flavor Group represents a set of rules to satisfy for a set of flavors to be matched to a host for attestation. For example, a Flavor Group can require that a PLATFORM Flavor and an OS Flavor be used for attestation. Without this level of association, a host that matches measurements for only a PLATFORM flavor, for example, can be attested as Trusted, even though the OS Flavor would attest the host as Untrusted.

Flavor matching can be automatic (the default), or can explicitly specify a host to which the Flavor Group must apply.

Automatic flavor matching allows for more ease in datacenter lifecycle management with updates and patches that may cause the appropriate flavors to change over time. Automatic flavor matching will trigger a new matching action when a new flavor is added, when an existing flavor is deleted, or when a host is initially attested as Untrusted. The system will automatically attempt to find a new set of flavors that match the Flavor Group rules that will attest the host as Trusted. For example, if a host in your datacenter has recently had a BIOS update, the next attestation will cause the host to appear Untrusted (because the PLATFORM measurements will now differ). Using automatic flavor matching, the Verification Service will automatically search for a new PLATFORM flavor that matches the actual BIOS version and measurement seen on the host. If a new BIOS version is successfully found, the Verification Service will use the new version for attestation, and the host will appear Trusted. If no matching PLATFORM flavor is found, the host will appear Untrusted. When automatic flavor matching is used, think of the various flavors in the Verification Service as a collection of valid configurations, and an attested host matching any combination of those configurations (within the confines of the Flavor Group requirements for which flavor types must be present) will be attested as Trusted.

Host-based flavor matching explicitly maps a specific host to a flavor. Host-based attestation requires that a host saves its entire configuration in a composite flavor document in the system, and then later validates against this flavor to detect any changes. In this case, if a host received a BIOS upgrade, the host will attest as Untrusted, and no attempt will be made to re-match a new flavor. An administrator will need to explicitly specify a new flavor to be used for that host.

10.2.1 When Does Flavor Matching Happen?

Generally speaking, a new Flavor match operation is triggered whenever a host is registered, whenever a host is attested and would be untrusted, and whenever a Flavor is added to or removed from a Flavor group.
When a new host is registered, the Verification Service will retrieve the Host Report and derive the platform information needed for Flavor matching (BIOS version, server OEM, OS type and version, TPM version, etc.). The Verification Service then searches through the Flavors in the same Flavor group that the host is in, and finds any Flavors that match the platform information.

If a Flavor is deleted, the Verification Service finds any hosts that are currently associated with that Flavor, and attempts to match them to alternative Flavors.

If a Flavor is added, the Verification Service looks for any hosts in the same Flavor group that are not currently matched to a Flavor of the appropriate Flavor part, and checks to see whether those hosts should be mapped to the new Flavor.

If a new Report is generated for a host and would not result in a Trusted attestation, the Verification Service will first repeat the Flavor matching process to be sure that no matching Flavors exist in the host's Flavor group that would result in a Trusted attestation. If the Service still finds no matching Flavors, the host will appear as Untrusted.

### 10.2.2 Flavor Matching Performance

Flavor matching causes affected hosts to be moved into the "QUEUE" state while the host and Flavor are evaluated to determine whether the host and Flavor should be linked. Hosts can remain in the QUEUE state for varying amounts of time based on the extent of the Flavor match required. This means that the trust status of a host will not be actually updated to reflect a new Flavor until after the process finishes, which may take a few seconds or minutes depending on the number of registered hosts, Flavors in the same Flavorgroup, etc.

If a new host is registered, only that host will be added to the queue, and other hosts will be unaffected. The Verification Service will look for only the HOST_UNI flavor part applicable to that specific host, and then will look at all PLATFORM and OS Flavors in the same Flavorgroup has the host, using the Flavor metadata and host info to narrow the results. The Service will match the new host to the most similar Flavors, and then move the host to the "CONNECTED" state and generate a new trust report.

When a new PLATFORM or OS Flavor is created, the Service will instead add all hosts in the same Flavorgroup as the new Flavors to the queue. Each host in the queue will then be re-evaluated against every PLATFORM and OS Flavor in the Flavorgroup to determine the closest match.

This means that adding a new Flavor can cause more hosts to each spend more time in the QUEUE state, as compared to adding a new host. For this reason, as a best practice for initial population of Flavors and hosts for a new deployment, it is suggested that Flavors be created before registering hosts. This is not a concern after the initial population of Flavors and hosts.
10.2.3 **Flavor Groups**

Flavor Groups represent a collection of one or more Flavors that are possible matches for a collection of one or more hosts. Flavor Groups link to both Flavors and hosts – a host in Flavor Group "ABC" will only be matched to Flavors in Flavor Group "ABC."

10.2.4 **Default Flavor Group**

By default the Verification Service includes a Flavor Group named "automatic" and another named "unique." During host registration, the "automatic" Flavor Group is used as a default selection if no other Flavor Group is specified.

10.2.4.1 **automatic**

The automatic Flavor Group is used as the default Flavor Group for all hosts and all Flavor parts. If no other Flavor Groups are specified when creating Flavors or Hosts, all Hosts and Flavors will be added to this group. This is useful for datacenters that want to manage a single set of acceptable configurations for all hosts.

10.2.4.2 **unique**

The unique Flavor Group is used to contain HOST_UNIQUE Flavors. This Flavor group is used by the backend software and should not be managed manually.

10.2.5 **Flavor Match Policies**

Flavor Match Policies are used to define how the Flavor Match engine will match Flavors to hosts for attestation for a given Flavor Group. Each Flavor part can have defined Flavor Match Policies within a given Flavor Group.

i.e.,

```
"PLATFORM": { "any_of", "required" } 
"OS": { "all_of", "required_if_defined" } 
"HOST_UNIQUE": { "latest","required_if_defined"} 
"ASSET_TAG": {"latest","required_if_defined"} 
"SOFTWARE": {"all_of","required_if_defined"} 
```

The sample Policy above would require that a PLATFORM Flavor part be matched, but any PLATFORM Flavor part in the Flavor Group may be matched. The OS Flavor Part will only be required if there is an OS Flavor part in the Flavor Group; if there are no OS Flavor parts in the Group, the match will not be required. If more than one OS Flavor part exists in the Group, all of those OS parts will be required to match for a host to be Trusted.
10.2.5.1 Default Flavor Match Policy

The “automatic” Flavor Group, and any Flavor Group created without explicitly defining a Flavor Match Policy, will be created using the following Flavor Match Policy. This is the default behavior for Flavor Matching:

```
"PLATFORM": { "any_of", "required" }
"OS": { "any_of", "required" }
"HOST_UNIQUE": { "latest", "required_if_defined" }
"ASSET_TAG": { "latest", "required_if_defined" }
"SOFTWARE": { "all_of", "required_if_defined" }
```

10.2.5.2 ANY_OF

The ANY_OF Policy allows any Flavor of the specified Flavor part to be matched. If the Flavor Group contains OS Flavor 1 and OS Flavor 2, a host will be Trusted if it matches either OS Flavor 1 or OS Flavor 2.

10.2.5.3 ALL_OF

The ALL_OF Policy requires all Flavors of the specified Flavor Part in the Flavor Group to be matched. For example, if Flavor Group X contains PLATFORM Flavor Part 1 and PLATFORM Flavor Part 2, a host in Flavor Group X will need to match both PLATFORM Flavor 1 and PLATFORM Flavor 2 to attest as Trusted. If the host matches only one of the Flavors, or neither of them, the host will be attested as Untrusted.

10.2.5.4 LATEST

The LATEST Policy requires that the most recently created Flavor of the specified Flavor part be used when matching to a host. For example:

```
"ASSET_TAG": { "latest", "required_if_defined" }
```

ASSET_TAG Flavor parts by default use the above Policy. This means that if Asset Tag Flavors are in the Flavor Group, the most recently created Asset Tag Flavor will be used. If no Asset Tag Flavors are present in the Flavor Group, then this Flavor part will be ignored.
10.2.5.5 REQUIRED

The REQUIRED Policy requires a Flavor of the specified part to be matched. For example:

"PLATFORM": { "any_of", "required" }

This policy means that a PLATFORM Flavor part must be used; if the Flavor Group contains no PLATFORM Flavor parts, hosts in this Flavor Group will always count as Untrusted.

10.2.5.6 REQUIRED_IF_DEFINED

The REQUIRED_IF_DEFINED Policy requires that a Flavor part be used if a Flavor of that part exists. If no Flavor part of this type exists in the Flavor Group, the Flavor part will not be required.

"ASSET_TAG": { "latest", "required_if_defined" }

ASSET_TAG Flavor parts by default use the above Policy. This means that if Asset Tag Flavors are in the Flavor Group, the most recently created Asset Tag Flavor will be used. If no Asset Tag Flavors are present in the Flavor Group, then this Flavor part will be ignored.

10.2.6 Flavor Match Event Triggers

Several events will cause the background queue service to attempt to re-match Flavors and hosts:

1. Host registration
   This event is the first time a host will be attempted to be matched to appropriate Flavors in the same Flavor Group, and affects only the host that was added (other hosts will not be re-matched to Flavors when you add a new host).

2. Flavor creation
   When a new Flavor is added to a Flavor Group, the queue system will repeat the Flavor match operation for all hosts in the same Flavor Group as the new Flavor.

3. Flavor deletion
   When a Flavor is deleted, the queue system will repeat the Flavor match operation for all hosts in the same Flavor Group as the deleted Flavor.

4. Creation of a new Attestation Report
   When a new Attestation Report is generated, if the host would attest as Untrusted with the currently-matched Flavors, the host being attested will be re-matched as part of the Report generation process. This ensures that Reports are always generated using the best possible Flavor matches available in the database.
10.2.7 Sample Flavorgroup API Calls

10.2.7.1 Create a New Flavor Group

POST https://server.com:8443/mtwilson/v2/flavorgroups

Input:
{
    "flavorgroup_name":"firstTest",
    "flavor_match_policy_collection":{
        "flavor_match_policies":{
            "flavor_part":"PLATFORM",
            "match_policy":{
                "match_type":"ANY_OF",
                "required":"REQUIRED"
            }
        }
    }
}

Output:
{"id": "a0950923-596b-41f7-b9ad-09f525929ba1",
"flavorgroup_name":"firstTest",
"flavor_match_policy_collection":{
    "flavor_match_policies":{
        "flavor_part":"PLATFORM",
        "match_policy":{
            "match_type":"ANY_OF",
            "required":"REQUIRED"
        }
    }
}}

10.3 SOFTWARE Flavor Management

10.3.1 What is a SOFTWARE Flavor?

A SOFTWARE Flavor part defines the measurements expected for a specific application, or a specific set of files and folders on the physical host. SOFTWARE Flavors can be used to attest the boot-time integrity of any static files or folders on a physical server.

A single server can have multiple SOFTWARE Flavors associated. Intel® SecLDAC provides a "default" SOFTWARE Flavor that is deployed to each Trust
Agent server during the provisioning step. This default Flavor includes the static files and folders of the Trust Agent itself, so that the Trust Agent is measured during the server boot process, and its integrity is included in the attestation of the other server measurements.

Using SOFTWARE Flavors consists of two parts – creating the actual SOFTWARE Flavor, and deploying the SOFTWARE Flavor manifest to the host.
10.3.2 Creating a SOFTWARE Flavor part

Creating a new SOFTWARE Flavor requires creating a manifest of the files and folders that need to be measured.

There are three different types of entries for the manifest: Directories, Symlinks, and Files.

10.3.2.1 Directories

A Directory defines measurement rules for measuring a directory. Effectively this involves listing the contents of the directory and hashing the results; in this way, a Directory measurement can verify that no files have been added or removed from the directory specified, but will not measure the integrity of individual files (i.e., files can change within the directory, but cannot be renamed, added, or removed).

Directory entries can use regular expressions to define explicit Include and Exclude filters. For example, "Exclude=*.log" would exclude all files ending with .log from the measurement, meaning files with the .log extension can be added or removed from the directory.

```
<Dir Type="dir" Include=".*" Exclude="" Path="/opt/trustagent/hypertext/WEB-INF" />
```

10.3.2.2 Symlinks

A Symlink entry defines a symbolic link that will be measured. The actual symbolic link is hashed, not the file or folder the symlink points to. In this way, the measurement will detect the symbolic link being modified to point to a different location, but the actual file or folder pointed to can have its contents change.

```
<Symlink Path="/opt/trustagent/bin/tpm_nvinfo" />
```

10.3.2.3 Files

Individual files can be explicitly specified for measurement as well. Each file listed will be hashed and extended separately. This means that if any file explicitly listed this way changes its contents or is deleted or moved, the measurement will change, and the host will become Untrusted.

```
<File Path="/opt/trustagent/bin/module_analysis_da.sh" />
```

10.3.3 Sample SOFTWARE Flavor Creation Call

Creating a new SOFTWARE Flavor requires specifying a sample host where the application, files or folders that will be measured are currently present. The measurements specified in the manifest will be captures when this call is
executed, and the Verification Service will communicate with the Trust Agent and create a SOFTWARE Flavor based on the file measurements.

The Connection String must point to the sample Trust Agent host. The Label defines the name of the new Flavor (ideally this should be the name of the application being measured for easier management).

POST https://server.com:8443/mtwilson/v2/flavor-from-app-manifest

Input:
<ManifestRequest xmlns="lib:wml:manifests-req:1.0">
  <connectionString>intel:https://trustagent.server.com:1443;u=trustagentUsername;p=trustagentPassword</connectionString>
  <Manifest xmlns="lib:wml:manifests:1.0" DigestAlg="SHA384" Label="Tomcat" Uuid="">
    <Dir Type="dir" Include=".*" Exclude="" Path="/opt/trustagent/hypertext/WEB-INF" />
    <Symlink Path="/opt/trustagent/bin/tpm_nvinfo" />
    <File Path="/opt/trustagent/bin/module_analysis_da.sh" />
  </Manifest>
</ManifestRequest>

### 10.3.4 Deploying a SOFTWARE Flavor Manifest to a Host

Once the SOFTWARE Flavor has been created, it can be deployed to any number of Trust Agent servers. This requires the Flavor ID (returned from Flavor creation) and the Host ID (returned from host registration). The Verification Service will send a request to the appropriate Trust Agent and create the manifest.

**Note:** After the SOFTWARE Flavor manifest is deployed to a host, the host must be rebooted. This will allow the measurements specified in the Flavor to be taken and extended to the TPM. Until the host is rebooted, the host will now appear Untrusted, as it now requires measurements from a SOFTWARE Flavor that have not yet been extended to the TPM.

POST https://server.com:8443/mtwilson/v2/rpc/deploy-software-manifest

Input:
```json
{   "flavor_id":"a6544ff4-6dc7-4c74-82be-578592e7e3ba",   "host_id":"a6544ff4-6dc7-4c74-82be-578592e7e3ba" }
```
10.3.5 SOFTWARE Flavor Matching

The default Flavor Match Policy for SOFTWARE Flavor parts is "ALL_OF","REQUIRED_IF_DEFINED". This means that all Software Flavors defined in a Flavorgroup must match to all hosts in that Flavorgroup. If no SOFTWARE Flavors are in the Flavorgroup, then hosts can still be considered Trusted.

Because the default uses the "ALL_OF" Policy, it's recommended to use Flavorgroups dedicated to specific software loadouts. For example, if a number of hosts will act as virtualization hosts and will have SOFTWARE Flavors for the hypervisor and VM management applications, those hosts should be placed in their own Flavorgroups as they will all run similar or identical application loadouts. If another group of servers in the datacenter will act as container hosts, these hosts might need SOFTWARE Flavors that include attestation of container runtimes and management applications, and will have a very different application loadout from the VM-based hosts. These should be placed in their own Flavorgroup, so that the VM hosts are attested using the hypervisor-related SOFTWARE Flavors, and the container hosts are attested using the container-related SOFTWARE Flavors.

As with other Flavor parts, hosts will be matched to Flavors in the same Flavorgroup that the host is added to, and will not be matched to Flavors in different Flavorgroups. Flavor matching will happen on the same events as for other Flavor parts.

10.3.6 Kernel Upgrades

Because the Application Integrity functionality involves adding a measurement agent (tbootXM) to initrd, an additional process must be followed when updating the OS kernel to ensure the new initrd also contains the measurement agent. This is not required if Application Integrity will not be used.

1) Update grub to have the boot menu-entry created for the new kernel version in grub.cfg
   (grub2-mkconfig -o <path to grub file>)
2) Reboot the host and boot into new kernel menu-entry.
3) Generate a new initrd with tbootXM. (/opt/tbootxm/bin/generate_initrd.sh)
4) Copy the generated initrd to the boot directory. (cp /var/tbootxm/<generated initrd file name> /boot/)
5) Update the "TCB protection" menu-entry with the new kernel version. (edit /etc/grub.d/40_custom)
6) Update the default boot menu-entry to have new kernel version. (edit /etc/default/grub)
7) Update the grub to reflect the updates. (grub2-mkconfig -o <path to grub file>)
8) Reboot the host and boot into TCB protection menu-entry.)
After updating the system with the new initrd, the Software Flavor should attest as Trusted. Note that changing grub and initrd does result in a new OS Flavor measurements, so an updated OS Flavor should be imported after updating the kernel and regenerating initrd.
11 Scalability and Sizing

11.1 Configuration Maximums

11.1.1 Registered Hosts

The Intel® Secl Verification Service can support a maximum of 2000 registered hosts with a single Verification Service instance with default settings.

11.1.2 HDD Space

The HDD space recommendations below represent expected log and database growth using default settings. Altering the database or log rotation settings, or the SAML expiration setting, may change the amount of disk space required. For default settings, 100 GB of disk space is recommended.

11.2 Database Rotation Settings

The Intel® Secl Verification Service database will automatically rotate the audit log table after one million records, and will retain up to ten total rotations. These settings are user-configurable if a longer retention period is needed.

mtwilson.audit.log.num.rotations - defines the maximum number of rotations before the oldest rotation is deleted to make space for a new rotation.

mtwilson.audit.log.max.row.count - defines the maximum number of rows in the audit log table before a rotation will occur.

11.3 Log Rotation

The Intel® Secl services (the Verification Service, Trust Agent, and Integration Hub) use Logrotate to rotate logs automatically during a daily cron job.

By default, logs are rotated once per month or when they exceed 1 GB in size, whichever comes first, and 12 total rotations will be retained.
## 12 Intel Security Libraries Configuration Settings

### 12.1 Verification Service

#### 12.1.1 Installation Answer File Options

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTWILSON_SERVER</td>
<td>192.168.1.1</td>
<td>Hostname or Ip address of the Verification Service</td>
</tr>
<tr>
<td>MTWILSON_API_BASEURL</td>
<td>https://&amp;{MTWILSON_SERVER}:8443/mtwilson/v1</td>
<td>v1 baseurl for the Verification Service. Generally this should not be changed.</td>
</tr>
<tr>
<td>MC_FIRST_USERNAME</td>
<td>administrator</td>
<td>Username for a new administrator-level user to be created during installation.</td>
</tr>
<tr>
<td>MC_FIRST_PASSWORD</td>
<td>mypassword123</td>
<td>Password for the new administrator-level user to be created during installation.</td>
</tr>
<tr>
<td>INSTALL_PKGS</td>
<td>&quot;logrotate&quot;</td>
<td>Defines the optional Verification Service components that will be installed. logrotate: the installer will automatically install and configure logrotate. This is optional.</td>
</tr>
<tr>
<td>LOG_SIZE</td>
<td>50M</td>
<td>Defines the log rotation size threshold for the Verification Service log. This is required if logrotate is installed.</td>
</tr>
<tr>
<td>LOG_OLD</td>
<td>3</td>
<td>Defines the number of rotated logs to be retained by logrotate before deletion. Required if logrotate is installed.</td>
</tr>
<tr>
<td>LOG_ROTATION_PERIOD</td>
<td>daily</td>
<td>Defines time interval. Log files are rotated when they grow bigger than size bytes, but not before the additionally specified time interval. Required if logrotate is installed.</td>
</tr>
<tr>
<td>LOG_COMPRESS</td>
<td>compress</td>
<td>Defines to compress log files. Old versions of log files are compressed with gzip(1) by default. Required if logrotate is installed.</td>
</tr>
<tr>
<td>LOG_DELAYCOMPRESS</td>
<td>delaycompress</td>
<td>Defines to postpone compression of the previous log file to the next rotation cycle. This is used with compress. Required if logrotate is installed.</td>
</tr>
<tr>
<td>LOG_COPYTRUNCATE</td>
<td>copytruncate</td>
<td>Defines to truncate the original log file in place after creating a copy, instead of moving the old log file and optionally creating a new one. Required if logrotate is installed.</td>
</tr>
<tr>
<td>MTWILSON_TLS_POLICY_ALLOW</td>
<td>certificate,certificate-digest,public-key,public-key-digest,TRUST_FIRST_CERTIFICATE,</td>
<td>Defines the TLS policies that will be allowed by the Verification Services. Policies not included in this list will not be created. See the TLS Policy Management section for details on TLS Policy types.</td>
</tr>
<tr>
<td><strong>Key</strong></td>
<td><strong>Sample Value</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>MTWILSON_DEFAULT_TLS_POLICY_ID</td>
<td>TRUST_FIRST_CERTIFICATE</td>
<td>Defines the default TLS policy to be used if no TLS policy is specified. Note that only TRUST_FIRST_CERTIFICATE can be specified here, because no other TLS policies exist at the time of installation. This setting is optional; if not used, there will be no default TLS Policy, and all API calls that require a TLS Policy will require the desired TLS Policy to be explicitly specified in the call.</td>
</tr>
<tr>
<td>DATABASE_HOSTNAME</td>
<td>127.0.0.1</td>
<td>Defines the database server IP address or hostname. This should be the loopback address for local database server installations, but should be the IP address or hostname of the database server if a remote database will be used.</td>
</tr>
<tr>
<td>DATABASE_PORTNUM</td>
<td>5432</td>
<td>Defines the port number for communication with the database server. By default with a local database server installation, this port will be set to 5432.</td>
</tr>
<tr>
<td>DATABASE_SCHEMA</td>
<td>mw_as</td>
<td>Defines the schema name of the database. If a remote database connection will be used, this schema must be created in the remote database before installing the Verification Service.</td>
</tr>
<tr>
<td>DATABASE_USERNAME</td>
<td>root</td>
<td>Username for accessing the database. If a remote database connection will be used, this user/password must be created and granted all permissions for the database schema before installing the Verification Service.</td>
</tr>
<tr>
<td>DATABASE_PASSWORD</td>
<td>dbpassword</td>
<td>Password for accessing the database. If a remote database connection will be used, this user/password must be created and granted all permissions for the database schema before installing the Verification Service.</td>
</tr>
<tr>
<td>MTWILSON_AUDIT_LOG_MAX_ROW_COUNT</td>
<td>1000000</td>
<td>Optional; uses a default of 1000000 if not specified during installation. Defines the maximum number of rows for a single rotation of the audit log table in the database. After reaching this number of records, the table will rotate.</td>
</tr>
<tr>
<td>MTWILSON_AUDIT_LOG_NUM_ROTATIONS</td>
<td>10</td>
<td>Optional; uses a default of 10 if not specified during installation. Defines the maximum number of rotations for the database audit table. After this number of rotations have occurred, subsequent rotations will result in the deletion of the oldest rotation to make room for the newest one.</td>
</tr>
<tr>
<td>POSTGRESQL_KEEP_PGPASS</td>
<td>TRUE</td>
<td>If set to &quot;TRUE,&quot; the Postgres database connectivity information will be stored in plaintext in the hidden file /opt/mtwilson/configuration/.pgpass. This prevents the user from being prompted for database credentials whenever the Hoist Verification Service starts.</td>
</tr>
<tr>
<td>ADD_POSTGRESQL_REPO</td>
<td>yes</td>
<td>This setting instructs the installer to add the Postgresql repository to the repository list.</td>
</tr>
<tr>
<td>TAG_VALIDITY_SECON DS</td>
<td>31536000</td>
<td>This value defines in seconds the length of time Asset Tag Certificates will remain valid.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>JETTY_TLS_CERT_DN</td>
<td>CN=Mt Wilson</td>
<td>Defines the Distinguished Name for the TLS Certificate</td>
</tr>
<tr>
<td>JETTY_PORT</td>
<td>8442</td>
<td>Insecure (http) Jetty port. This port must match the port defined in the endpoint.url value. Secure (https) Jetty port. This port must match the port defined in the mtwilson.api.url value.</td>
</tr>
<tr>
<td>JETTY_SECURE_PORT</td>
<td>8443</td>
<td>Secure (https) Jetty port. This port must match the port defined in the mtwilson.api.url value.</td>
</tr>
<tr>
<td>JAVAX_NET_SSL_KEYSTORE</td>
<td>/opt/mtwilson/configuration/keystore.jks</td>
<td>Defines the location of the Jetty webserver SSL keystore.</td>
</tr>
<tr>
<td>JETTY_TLS_CERT_DNS</td>
<td>devops5,localhost</td>
<td>Comma-separated list of hostnames to be added as Subject Alternative Names to the TLS certificate. Only connections to an IP address or hostname in the Subject Alternative Names list will be accepted; other connections will be rejected.</td>
</tr>
<tr>
<td>JETTY_TLS_CERT_IP</td>
<td>192.168.1.1,127.0.0.1</td>
<td>Comma-separated list of IP addresses to be added as Subject Alternative Names to the TLS certificate. Only connections to an IP address or hostname in the Subject Alternative Names list will be accepted; other connections will be rejected.</td>
</tr>
<tr>
<td>QUEUE_EXECUTION_INTERVAL</td>
<td>3</td>
<td>Defines the frequency in seconds at which the background queue process is executed</td>
</tr>
<tr>
<td>ESXHOSTS_AUTOUPDATE_INTERVAL</td>
<td>120</td>
<td>Defines the frequency in seconds at which ESXi host information is retrieved from configured vCenters and updated in the database</td>
</tr>
<tr>
<td>MTWILSON_TELEMETRY_INTERVAL</td>
<td>86400</td>
<td>Defines the frequency in seconds at which telemetry data is collected. Telemetry data includes a simple count of all hosts currently registered.</td>
</tr>
</tbody>
</table>

### 12.1.2 Configuration Options

The Verification Service configuration is encrypted and stored in the file /opt/mtwilson/configuration/mtwilson.properties. To view or change any configuration settings, use the following commands:

**View Configuration:**

```
mtwilson export-config --stdout
```

To change the value of any configuration setting in mtwilson.properties, use the following command:

```
mtwilson config <key> <value>
```
<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtwilson.queue.execution.interval</td>
<td>3</td>
<td>Defines in seconds the length of time between background queue operations. The background queue is the process that automatically matches Flavors to Hosts that share the same Flavorgroup.</td>
</tr>
<tr>
<td>mtwilson.queue.max.threads</td>
<td>32</td>
<td>The number of threads that the background queue will allocate for concurrent task execution.</td>
</tr>
<tr>
<td>mtwilson.queue.execution.timeout</td>
<td>60</td>
<td>The amount of time in seconds an individual background queue task is allowed to take before throwing a timeout exception.</td>
</tr>
<tr>
<td>mtwilson.telemetry.interval</td>
<td>86400</td>
<td>Defines in seconds the length of time between checks for the number of hosts registered in the Verification Service. By default this checks once every 24 hours. A report of the last 90 days of host counts can be retrieved through a REST API (see the Javadoc for details).</td>
</tr>
<tr>
<td>mtwilson.esxihosts.autoupdate.interval</td>
<td>120</td>
<td>Defines in seconds the length of time between checks to see if any changes have occurred in vCenter for any VMWare vCenter Cluster objects that have been registered with the Verification Service. If a new host has been added or removed from the Cluster in vCenter, the host will be added or removed respectively in the Verification Service as well.</td>
</tr>
<tr>
<td>saml.validity.seconds</td>
<td>3600</td>
<td>Defines in seconds the length of time a Report will remain valid. The Verification Service automatically checks for Reports that are nearing expiration and refreshes them; lowering this value will increase the frequency of automatic background Report generation.</td>
</tr>
<tr>
<td>mtwilson.tls.policy.allow</td>
<td>certificate,certificate-digest,public-key,public-key-digest,TRUST_FIRST_CERTIFICATE</td>
<td>Defines the TLS policies that will be allowed. TLS policies not in this list will be denied. This list is based off of the MTWILSON_TLS_POLICY_ALLOW list provided at installation time in the mtwilson.env answer file. See the TLS Policy section for information on TLS Policies.</td>
</tr>
<tr>
<td>mtwilson.default.tls.policy.id</td>
<td>TRUST_FIRST_CERTIFICATE</td>
<td>Defines the default TLS policy to be used if no TLS policy is specified. This value is based off of the MTWILSON_DEFAULT_TLS_POLICY_ID value provided at installation time in the mtwilson.env answer file. Note that only TRUST_FIRST_CERTIFICATE and INSECURE can be specified during installation, because no other TLS policies exist at the time of installation. This can be changed to a new TLS policy, however, by setting the ID of the TLS policy to be used as a default. This setting is optional.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>mtwilson.extensions.packageIncludeFilter.startsWith</code></td>
<td>com.intel.org.glassfish.jersey.media.multipart</td>
<td>Do not change this value. Java code package name string to include for classpath jar loading optimization.</td>
</tr>
<tr>
<td><code>mtwilson.extensions.fileIncludeFilter.contains</code></td>
<td>mtwilson, jersey-media-multipart</td>
<td>Do not change this value. Java jar filename string identifier to include for classpath jar loading optimization.</td>
</tr>
<tr>
<td><code>mtwilson.extensions.packageExcludeFilter.startsWith</code></td>
<td>java,javax</td>
<td>Do not change this value. Java code package name string to exclude for classpath jar loading optimization.</td>
</tr>
<tr>
<td><code>mtwilson.host</code></td>
<td>192.168.1.1</td>
<td>The IP address or hostname of the Verification Service. This is configured at installation time by the MTWILSON_SERVER value specified in the mtwilson.env answer file at installation time.</td>
</tr>
<tr>
<td><code>mtwilson.api.url</code></td>
<td><a href="https://192.168.1.1:8443/mtwilson/v1">https://192.168.1.1:8443/mtwilson/v1</a></td>
<td>Defines the baseurl the Verification Service v1 APIs. Note that this will need to be updated if the Jetty secure port is changed.</td>
</tr>
<tr>
<td><code>dbcp.validation.query</code></td>
<td>select 1</td>
<td>Query used to verify that the database is accessible</td>
</tr>
<tr>
<td><code>dbcp.validation.on.return</code></td>
<td>false</td>
<td>This property determines whether or not the pool will validate objects before they are borrowed from the pool.</td>
</tr>
<tr>
<td><code>dbcp.validation.on.borrow</code></td>
<td>true</td>
<td>This property determines whether or not the pool will validate objects before they are borrowed from the pool.</td>
</tr>
<tr>
<td><code>mtwilson.locales</code></td>
<td>en-US</td>
<td>Do not change this value.</td>
</tr>
<tr>
<td><code>mtwilson.db.user</code></td>
<td>root</td>
<td>Defines the database user</td>
</tr>
<tr>
<td><code>mtwilson.db.password</code></td>
<td>dbpassword</td>
<td>Defines the database password</td>
</tr>
<tr>
<td><code>mtwilson.db.driver</code></td>
<td>org.postgresql.Driver</td>
<td>Defines the database driver to be used. Do not change this value.</td>
</tr>
<tr>
<td><code>mtwilson.db.schema</code></td>
<td>mw_as</td>
<td>Defines the database schema name.</td>
</tr>
<tr>
<td><code>mtwilson.db.port</code></td>
<td>5432</td>
<td>Defines the database connection port. The default port for a locally installed PostgreSQL database server is 5432.</td>
</tr>
<tr>
<td><code>mtwilson.db.host</code></td>
<td>127.0.0.1</td>
<td>Defines the IP or hostname of the database server. By default for a locally installed PostgreSQL database server this will be 127.0.0.1.</td>
</tr>
<tr>
<td><code>mtwilson.audit.log.max.row.count</code></td>
<td>1000000</td>
<td>Defines the maximum number of rows for a single rotation of the audit log table in the database. After reaching this number of records, the table will rotate.</td>
</tr>
<tr>
<td><code>mtwilson.audit.log.num.rotations</code></td>
<td>10</td>
<td>Defines the maximum number of rotations for the database audit table. After this number of rotations have occurred, subsequent rotations will result in the deletion of the oldest rotation to make room for the newest one.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mtwilson.privacyca.ek.p12.password</td>
<td></td>
<td>Defines Endorsement CA password</td>
</tr>
<tr>
<td>mtwilson.privacyca.aik.p12.password</td>
<td></td>
<td>Defines Privacy CA password</td>
</tr>
<tr>
<td>mtwilson.as.dek</td>
<td></td>
<td>Decryption key used for sensitive data encrypted in the database.</td>
</tr>
<tr>
<td>saml.key.alias</td>
<td>samlkey1</td>
<td>Alias for the SAML signing certificate. Do not change this value.</td>
</tr>
<tr>
<td>saml.keystore.file</td>
<td>SAML.jks</td>
<td>Keystore that contains the SAML signing key.</td>
</tr>
<tr>
<td>jetty.tls.cert.dn</td>
<td>CN=Mt Wilson</td>
<td>Defines the Distinguished Name for the TLS Certificate</td>
</tr>
<tr>
<td>jetty.port</td>
<td>8442</td>
<td>Insecure (http) Jetty port. This port must match the port defined in the endpoint.url value.</td>
</tr>
<tr>
<td>jetty.secure.port</td>
<td>8443</td>
<td>Secure (https) Jetty port. This port must match the port defined in the mtwilson.api.url value.</td>
</tr>
<tr>
<td>javax.net.ssl.keyStore</td>
<td>/opt/mtwilson/configuration/keystore.jks</td>
<td>Defines the location of the Jetty webserver SSL keystore.</td>
</tr>
<tr>
<td>jetty.tls.cert.dns</td>
<td>devops5,localhost</td>
<td>Comma-separated list of hostnames to be added as Subject Alternative Names to the TLS certificate. Only connections to an IP address or hostname in the Subject Alternative Names list will be accepted; other connections will be rejected.</td>
</tr>
<tr>
<td>jetty.tls.cert.ip</td>
<td>192.168.1.1,127.0.0.1</td>
<td>Comma-separated list of IP addresses to be added as Subject Alternative Names to the TLS certificate. Only connections to an IP address or hostname in the Subject Alternative Names list will be accepted; other connections will be rejected.</td>
</tr>
<tr>
<td>mtwilson.ca.dn</td>
<td>CN=mtwilson-ca,OU=mtwilson</td>
<td>CA distinguishable name</td>
</tr>
</tbody>
</table>

### 12.1.3 Command-Line Options

The Verification Service supports several command-line commands that can be executed only as the Root user:

Syntax:

```
mtwilson <command>
```

#### 12.1.3.1 Help

```
mtwilson help
```
Displays the list of available CLI commands.

12.1.3.2 Start
mtwilson start
Starts the services.

12.1.3.3 Stop
mtwilson stop
Stops the services.

12.1.3.4 Restart
mtwilson restart
Restarts the services.

12.1.3.5 Status
mtwilson status
Reports whether the service is currently running.

12.1.3.6 Uninstall
mtwilson uninstall
Uninstalls the service, including the deletion of all files and folders. Database content is not removed. See section 14.1 for additional details.

12.1.3.7 Version
mtwilson version
Reports the version of the service.

12.1.3.8 Fingerprint
mtwilson fingerprint
Displays the TLS certificate information.

12.1.3.9 Java-detect
mtwilsopn java-detect
Displays the detected path and installed version of Java.

**12.1.3.10 Erase-data**

mtwilson erase-data

Deletes all non-user information from the database.

**12.1.3.11 Erase-users**

mtwilson erase-users [--all]

Deletes all users from the database, except for the default administrative user. If the "--all" option is used, the administrative user will be deleted as well.

**12.1.3.12 Zeroize**

mtwilson zeroize

Shreds all secrets, keys, and configurations.

**12.1.3.13 Login-password**

mtwilson login-password [username] [password] [--permissions] [permission1] [permission2]...

Creates a new user with the specified username and password. If the --permissions option is used, the user can be directly assigned permissions.

*Note:* This command only allows the assignment of individual permissions, not roles. Permissions are defined in a domain:permission format. For example, hosts:create would allow the user to create new hosts, but not modify or delete existing hosts. Any number of permissions may be applied to a single user. Wildcards are also acceptable; the permissions *:* grants all permissions on all domains, effectively creating an administrative user.

**12.1.3.14 Export-config**

mtwilson export-config <outfile|--in=infile|--out=outfile|--stdout>

Exports the current configuration. Configuration settings are stored in the encrypted file /opt/mtwilson/configuration/mtwilson.properties; this command allows the configuration to be decrypted or output to the console.

**12.1.3.15 Config**

mtwilson config [key] [value]
Configures a specified configuration setting to a specified value. Changing settings may require a service restart to take effect.

12.1.3.16 Setup

mtwilson setup [--force|--noexec] [task1 task2 ...]

Re-runs the installation setup tasks, or the specific tasks listed.

12.1.3.17 Replace-tls-key-pair

mtwilson replace-root-key-pair [--private-key=newprivatekey.pem] [--cert-chain=]

Replaces the TLS key pair and certificate. See the Certificate and Key Management section for more details.

12.1.4 Directory Layout

The Verification Service installs by default to /opt/mtwilson with the following folders.

12.1.4.1 Backup

This folder contains backup copies of the Service configuration files, generated at installation with a timestamp.

12.1.4.2 Bin

This folder contains executable scripts.

12.1.4.3 Configuration

This folder contains certificates, keys, and configuration files.

12.1.4.4 Env

This folder contains environment variable files.

12.1.4.5 Features

This folder contains utility scripts and files for specific features.

12.1.4.6 Java

This folder contains application Java libraries.
12.1.4.7 Logs

This folder contains log files.

12.1.4.8 Monit

This folder contains the configuration files for the Monit process monitoring application.

12.1.4.9 Repository

12.1.4.10 Share

12.2 Trust Agent

12.2.1 Installation Answer File Options

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTWILSON_API_URL</td>
<td>https://&lt;Verification Service IP or hostname&gt;:8443/mtwilson/v2</td>
<td>Defines the base URL for the Verification Service API.</td>
</tr>
<tr>
<td>MTWILSON_TLS_CERT_SHA384</td>
<td>SHA384 hash of the Verification Service TLS certificate.</td>
<td>This can be retrieved from the Verification Service in the file /opt/mtwilson/configuration/https.properties</td>
</tr>
<tr>
<td>MTWILSON_API_USERNAME</td>
<td>admin</td>
<td>Defines the username that will be used for authentication to the Verification Service API.</td>
</tr>
<tr>
<td>MTWILSON_API_PASSWORD</td>
<td>password</td>
<td>Defines the password that will be used for authentication to the Verification Service API.</td>
</tr>
<tr>
<td>REGISTER_TPM_PASSWORD</td>
<td>y</td>
<td>If this is set to &quot;y,&quot; the Trust Agent will attempt to store the TPM owner secret with the Verification Service. This is used for &quot;Pull&quot; Asset Tag provisioning so that the TPM ownership does not need to be cleared (which reduces the number of needed reboots). Pull provisioning for Asset Tags is not recommended.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AUTOMATIC_REGISTRATION</td>
<td>no</td>
<td>If set to &quot;yes&quot; this will cause the Trust Agent installer to attempt to register the host with the Verification Service. Requires that &quot;PROVISION_ATTESTATION&quot; be set to &quot;y&quot;. If this is set to &quot;no&quot;, the registration will not happen after installation, and can be performed either using the trust agent command line commands, or using a REST API for the Verification Service.</td>
</tr>
<tr>
<td>TRUSTAGENT_LOGIN_REGISTRATION</td>
<td>true</td>
<td>If this is set to true,&quot; the Trust Agent will attempt to register the Trust Agent API credentials with the Verification Service. This will allow the Verification Service to accept connection strings to connect to this host without explicitly specifying the Trust Agent username and password. If this is set to &quot;false&quot; or not specified, the Verification Service will require the connection string to include the username and password. Setting this to &quot;true&quot; is recommended if the Trust Agent credentials will be randomly generated during installation.</td>
</tr>
<tr>
<td>PROVISION_ATTESTATION</td>
<td>y</td>
<td>If set to &quot;y,&quot; the Trust Agent will attempt to perform the Provisioning steps after installation completes. See the Trust Agent installation section of the Product Guide for details on Provisioning. If not specified or set to &quot;n,&quot; the Trust Agent will install but will not attempt to perform the Provisioning steps.</td>
</tr>
<tr>
<td>TRUSTAGENT_ADMIN_USERNAME</td>
<td>&lt;username&gt;</td>
<td>Defines the initial Trust Agent API user that will be created during Trust Agent installation. If this is not specified, the username and password will be randomly generated.</td>
</tr>
<tr>
<td>TRUSTAGENT_ADMIN_PASSWORD</td>
<td>&lt;password&gt;</td>
<td>Defines the initial Trust Agent API user that will be created during Trust Agent installation. If this is not specified, the username and password will be randomly generated.</td>
</tr>
<tr>
<td>CURRENT_IP</td>
<td>&lt;IP address&gt;</td>
<td>This IP is used for Attestation registration.</td>
</tr>
<tr>
<td>TPM_OWNER_SECRET</td>
<td>20 hex-encoded bytes. This can be used to preserve the TPM Owner Secret between installations so that TPM ownership does not need to be reset for a re-installation. Note: If the OS is re-installed, the file /var/lib/tpm/system.data contains sealed persistent TPM secrets unique to the TPM owner and needs to be preserved from just before the old OS is wiped and replaced immediately after trousers is re-installed in the new OS.</td>
<td></td>
</tr>
<tr>
<td>AIK_SECRET</td>
<td>20 hex-encoded bytes, Secret to generate AIK</td>
<td></td>
</tr>
<tr>
<td>JAVA_REQUIRED_VERSION</td>
<td>1.8</td>
<td>Defines the required Java version. Do not change this value.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TPM_QUOTE_IPV4</td>
<td>Default: true</td>
<td>When enabled (not set or set to true) causes the challenger's nonce to be extended with the IP Address of the trusted host for quoting to prevent quote relay attacks.</td>
</tr>
<tr>
<td>TPM_SRK_SECRET</td>
<td>Example: 0000000000000000000000000000000000000000</td>
<td>Many tools assume this well-known SRK comprised of 20 zero bytes.</td>
</tr>
<tr>
<td>TRUSTAGENT_KEYSTORE_PASSWORD</td>
<td>Generated automatically. Example: 9JF7+HpMUM_</td>
<td>The password used to access the trustagent.jks file with the keytool.</td>
</tr>
<tr>
<td>TRUSTAGENT_PASSWORD</td>
<td>No default value.</td>
<td>The password used to encrypt and decrypt the trustagent.properties file. This password must be exported in an environment variable for the Trust Agent to use it.</td>
</tr>
<tr>
<td>TRUSTAGENT_TLS_CERT_DN</td>
<td>CN=trustagent,OU=DCG, O=Intel, L=Folsom, C=US</td>
<td>Determines the subject name of the trust agent's TLS certificate. These names are added as subject alternative names on the Trust Agent's TLS certificate. By default, all names in /etc/hosts corresponding to local IP Addresses are used. If not specified, the installer performs a reverse DNS lookup for all IP Addresses found in the ifconfig output. In some environments this can cause a delay during installation. Manually specifying the subject names can eliminate this delay.</td>
</tr>
<tr>
<td>TRUSTAGENT_TLS_CERT_DNS</td>
<td>Generated automatically. Comma-separated list of all hostnames used by the host</td>
<td>Comma-separated list of DNS names to be added as Subject Alternative Names to the TLS certificate. Only connections to an IP address or hostname in the Subject Alternative Names list will be accepted; other connections will be rejected.</td>
</tr>
<tr>
<td>TRUSTAGENT_TLS_CERT_IP</td>
<td>Possible values: Comma-separated list of IP Addresses.</td>
<td>Comma-separated list of IP addresses to be added as Subject Alternative Names to the TLS certificate. Only connections to an IP address or hostname in the Subject Alternative Names list will be accepted; other connections will be rejected.</td>
</tr>
<tr>
<td>INSTALL_WORKLOAD_AGENT</td>
<td>Y or n</td>
<td>Determines whether the Workload Agent will be installed. The WLA is only needed for Workload Encryption use cases. Use &quot;y&quot; to install the WLA, and &quot;n&quot; to install only the Trust Agent.</td>
</tr>
<tr>
<td>WLS_API_URL</td>
<td>https://&lt;IP or hostname of the Workload Service&gt;:5000/wls/</td>
<td>Defines the base URL for access to the Workload Service. This is needed only for Workload Confidentiality use cases.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WLS_API_USERNAME</td>
<td></td>
<td>Defines credentials for a machine service account used for access to the WLS. This is needed only for Workload Confidentiality use cases.</td>
</tr>
<tr>
<td>WLS_API_PASSWORD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WLA_NOSETUP</td>
<td>false</td>
<td>Allows the installation of the WLA without running setup. Most installations should set to &quot;false&quot;.</td>
</tr>
<tr>
<td>AAS_API_URL</td>
<td>https://&lt;IP or hostname of the AAS&gt;:8444/aas</td>
<td>Defines the base URL for the AAS. Used to get authentication tokens for access to other services.</td>
</tr>
<tr>
<td>CMS_BASE_URL</td>
<td></td>
<td>Defines the base URL for the CMS</td>
</tr>
<tr>
<td>WA_WITH_CONTAINER_SECURITY</td>
<td>Y or n</td>
<td>Determines whether the WLA will be configured for Docker Container Confidentiality. If Container Confidentiality will be used, set this to &quot;y&quot;. If VM Confidentiality will be used, set this to &quot;n&quot;. If neither Workload Confidentiality use case will be used, do not install the WLA.</td>
</tr>
<tr>
<td>INSECURE_SKIP_VERIFY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO_PROXY</td>
<td></td>
<td>Defines a proxy exception list, if applicable</td>
</tr>
<tr>
<td>REGISTRY_SCHEME_TYPE</td>
<td>https</td>
<td></td>
</tr>
</tbody>
</table>

Commented [KTE9]: Need to define

Commented [KTE10]: Need to define
### 12.2.2 Configuration Options

The Trust Agent configuration .properties file is encrypted during installation. To view the contents of the trustagent.properties file, use the following commands:

**View Configuration:**

tagent export-config --stdout

**Change a Setting:**

tagent config <property_name> <new_value>

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustagent.keystore.password</td>
<td>Generated automatically</td>
<td>Password for the trustagent.jks keystore</td>
</tr>
<tr>
<td>trustagent.tls.cert.ip</td>
<td>Comma-separated list of IP addresses</td>
<td>These addresses are added as subject alternative names on the Trust Agent's TLS certificate. By default, all IP Addresses shown in the ifconfig output are used. Connections to the Trust Agent using an IP or hostname not in this list will be rejected.</td>
</tr>
<tr>
<td>trustagent.tls.cert.dns</td>
<td>Comma-separated list of hostnames</td>
<td>These names are added as subject alternative names on the Trust Agent's TLS certificate. By default, all names in /etc/hosts corresponding to local IP Addresses are used. If not specified, the installer performs a reverse DNS lookup for all IP Addresses found in the ifconfig output. In some environments this can cause a delay during installation. Manually specifying the subject names can eliminate this delay. Connections to the Trust Agent using an IP or hostname not in this list will be rejected.</td>
</tr>
<tr>
<td>mtwilson.tls.cert.sha384</td>
<td></td>
<td>SHA384 hash of the Verification Service TLS certificate. Obtain this from the Verification Service server, in /opt.mtwilson/configuration/https.properties</td>
</tr>
<tr>
<td>mtwilson.api.username</td>
<td>User specified</td>
<td>Verification Service username used for any REST calls from the Trust Agent to the VS. This includes Trust Agent Provisioning tasks, and optionally may include host registration and/or importing the HOST_UNIQUE flavor part.</td>
</tr>
<tr>
<td>hardware.uuid</td>
<td></td>
<td>Hardware UUID of the host</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>tpm.srk.secret</td>
<td>00000000000000000000000000000000</td>
<td>Storage Root Key secret. Many tools assume the SRK secret to be a &quot;well-known&quot; secret of twenty bytes of zero.</td>
</tr>
<tr>
<td>trustagent.admin.username</td>
<td>User specified, or randomly generated</td>
<td>Username of the Trust Agent administrative user created during installation. This is inherited from the TRUSTAGENT_ADMIN_USERNAME value in trustagent.env during installation if specified. If not specified, this value will be generated randomly during installation. This user is used by external services (including the Verification Service) when making REST API calls to the Trust Agent.</td>
</tr>
<tr>
<td>mtwilson.api.password</td>
<td>User specified</td>
<td>Verification Service password used for any REST calls from the Trust Agent to the VS. This includes Trust Agent Provisioning tasks, and optionally may include host registration and/or importing the HOST_UNIQUE flavor part.</td>
</tr>
<tr>
<td>aik.secret</td>
<td>Generated automatically as 20 hex-encoded bytes.</td>
<td>20 hex-encoded bytes, Secret to generate AIK</td>
</tr>
<tr>
<td>current.ip</td>
<td>10.105.167.121</td>
<td>This IP address or hostname value is used as the hostname field when automatically registering the host when using the &quot;tagent attestation-registration&quot; command.</td>
</tr>
<tr>
<td>mtwilson.extensions.packag eExcludeFilter.startsWith</td>
<td>java, javax</td>
<td>Do not change this value.</td>
</tr>
<tr>
<td>mtwilson.api.url</td>
<td>https://&lt;IP or hostname&gt;:8443/mtwilson/v2</td>
<td>Baseurl for the Verification Service API.</td>
</tr>
<tr>
<td>mtwilson.extensions.packag eIncludeFilter.startsWith</td>
<td>com.intel</td>
<td>Do not change this value.</td>
</tr>
<tr>
<td>tpm.owner.secret</td>
<td>User specified or randomly generated, 20 hex-encoded bytes.</td>
<td>Password used to assert ownership of the host TPM. Inherited from TPM_OWNER_SECRET in trustagent.env if specified during installation of the Trust Agent. Randomly generated if not specified.</td>
</tr>
<tr>
<td>trustagent.tls.cert.dn</td>
<td>CN=trustagent</td>
<td>Defines the subject name of the Trust Agent's TLS certificate.</td>
</tr>
<tr>
<td>trustagent.tls.cert.sha384</td>
<td>SHA384 hash of the TLS certificate. Do not change this value.</td>
<td></td>
</tr>
<tr>
<td>aik.secret</td>
<td>Generated automatically.</td>
<td>20 hex-encoded bytes, Secret to generate Attestation Identity Key</td>
</tr>
<tr>
<td>binding.key.secret</td>
<td>20 hex-encoded bytes, Secret to generate Binding Key</td>
<td></td>
</tr>
<tr>
<td>hardware.uuid</td>
<td>Host hardware UUID. Do not change this value.</td>
<td></td>
</tr>
<tr>
<td>signing.key.secret</td>
<td>20 hex-encoded bytes, Secret to generate Signing key</td>
<td></td>
</tr>
<tr>
<td>tpm.srk.secret</td>
<td>0</td>
<td>Many tools assume this well-known SRK comprised of 20 zero bytes.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>trustagent.keystore.password</td>
<td>Generated automatically. Example: 9JF7+HpMUM_</td>
<td>The password used to access the trustagent.jks file with the keytool.</td>
</tr>
<tr>
<td>trustagent.tls.cert.dns</td>
<td>Generated automatically Comma- separated list of all hostnames used by the host.</td>
<td>These names are added as subject alternative names on the Trust Agent’s TLS certificate. By default, all names in /etc/hosts corresponding to local IP Addresses are used. If not specified, the installer performs a reverse DNS lookup for all IP Addresses found in the ifconfig output. In some environments this can cause a delay during installation. Manually specifying the subject names can eliminate this delay.</td>
</tr>
<tr>
<td>trustagent.tls.cert.ip</td>
<td>Generated automatically Comma-separated list of IP Addresses.</td>
<td>These addresses are added as subject alternative names on the Trust Agent’s TLS certificate. By default, all IP Addresses shown in the ifconfig output are used.</td>
</tr>
</tbody>
</table>

### 12.2.3 Command-Line Options

#### 12.2.3.1 Available Commands

#### 12.2.3.1.1 Help

tagent help

Displays the list of available CLI commands.

#### 12.2.3.1.2 Start

tagent start

Starts the services.

#### 12.2.3.1.3 Stop

tagent stop

Stops the services.

#### 12.2.3.1.4 Restart

tagent restart

Restarts the services.

#### 12.2.3.1.5 Status

tagent status
Reports whether the service is currently running.

12.2.3.1.6 Uninstall
tagent uninstall
Uninstalls the service, including the deletion of all files and folders. See section 14.2 for additional information.

12.2.3.1.7 Version
tagent version
Reports the version of the service.

12.2.3.1.8 Fingerprint
tagent fingerprint
Displays the TLS certificate information.

12.2.3.1.9 Java-detect
agent java-detect
Displays the detected path and installed version of Java.

12.2.3.1.10 Zeroize
tagent zeroize
Shreds all secrets, keys, and configurations.

12.2.3.1.11 Password
tagent password [username] [password] --permissions *:* 
Creates a new user with the specified username and password. Because the Trust Agent does not have granular user permissions, the --permissions *:* is necessary and assigns all permissions to the created user.

12.2.3.1.12 Export-config
tagent export-config <outfile|--in=infile|--out=outfile|--stdout>
Exports the current configuration. Configuration settings are stored in the encrypted file /opt/trustagent/configuration/trustagent.properties; this command allows the configuration to be decrypted or output to the console.
12.2.3.1.13  Config

tagent config [key] [value]

Configures a specified configuration setting to a specified value. Changing
settings may require a service restart to take effect.

12.2.3.1.14  Setup

tagent setup [--force|--noexec] [task1 task2 ...]

Re-runs the installation setup tasks, or the specific tasks listed.

12.2.4  Directory Layout

12.2.4.1  Windows

12.2.4.2  Linux

The Linux rust Agent installs by default to /opt/trustagent, with the following
subfolders:

Bin
Configuration
Env.d
Features
Hypertext
Logs
Repository
Share
Var

12.3  Integration Hub

12.3.1  Installation Answer File

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTESTATION_HUB_PORT_HTTP</td>
<td>19082</td>
</tr>
<tr>
<td>ATTESTATION_HUB_PORT_HTTPS</td>
<td>19443</td>
</tr>
</tbody>
</table>
### Configuration Options

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jetty.tls.cert.dns</td>
<td>server.com,localhost</td>
<td>Subject Alternative Names</td>
</tr>
<tr>
<td>attestation-hub.db.schema</td>
<td>attestation_hub_pu</td>
<td>Defines the database schema name.</td>
</tr>
<tr>
<td>attestation-hub.poll.interval</td>
<td>2</td>
<td>Defines in minutes how long the Hub will wait before sending a new polling request to the Verification Service to retrieve new reports.</td>
</tr>
<tr>
<td>mtwilson.api.password</td>
<td>HubPassword</td>
<td>Defines the Verification Service user that will be used by the Integration Hub for API requests. This user must be created with at minimum the reports:search permission or the reports_manager or auditor roles.</td>
</tr>
<tr>
<td>mtwilson.api.url</td>
<td><a href="https://server.com:8443/mtwilson/v2">https://server.com:8443/mtwilson/v2</a></td>
<td>Defines the base URL for the Verification Service API.</td>
</tr>
<tr>
<td>javax.net.ssl.keyStore</td>
<td>/opt/attestation-hub/configuration/keystore.jks</td>
<td>Defines the SSL keystore file path.</td>
</tr>
<tr>
<td>mtwilson.extensions.packageExcludeFilter</td>
<td>startsWith.java,javax</td>
<td>Do not change this value.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mtwilson.username</td>
<td>hubadmin</td>
<td>Defines the Verification Service user that will be used by the Integration Hub for API requests. This user must be created with at minimum the reports_search permission or the reports_manager or auditor roles.</td>
</tr>
<tr>
<td>jetty.tls.cert.ip</td>
<td>192.168.1.1,127.0.0.1</td>
<td>Defines the IP addresses that are listed in the Integration Hub TLS Certificate as Subject Alternative Names. These addresses are used to validate connections to the Hub.</td>
</tr>
<tr>
<td>attestation-hub.db.password</td>
<td>dbpassword</td>
<td>Defines the database connection password.</td>
</tr>
<tr>
<td>attestation-hub.db.driver</td>
<td>org.postgresql.Driver</td>
<td>Defines the database connection driver. Do not change this value.</td>
</tr>
<tr>
<td>mtwilson.extensions.fileIncludeFilter.contains</td>
<td>mtwilson,attestation-hub</td>
<td>Do not change this value.</td>
</tr>
<tr>
<td>mtwilson.api.tls.policy.certificat e.sha384</td>
<td>20 hex-encoded bytes. Obtain this from the Verification Service server, in /opt/mtwilson/configuration/https.properties</td>
<td></td>
</tr>
<tr>
<td>jetty.port</td>
<td>19082</td>
<td>Defines the webserver insecure (http) port.</td>
</tr>
<tr>
<td>mtwilson.server</td>
<td>hvs.server.com</td>
<td>Defines the IP address or hostname of the Verification Service from which the Hub will poll new attestation reports.</td>
</tr>
<tr>
<td>jetty.secure.port</td>
<td>19445</td>
<td>Defines the webserver secure (https) port.</td>
</tr>
<tr>
<td>attestation-hub.db.name</td>
<td>attestation_hub_pu</td>
<td>Defines the database schema name.</td>
</tr>
<tr>
<td>password.vault.file</td>
<td>/opt/attestation- hub/configuration/password- vault.jck</td>
<td>Information about keystore path, default would be configuration.</td>
</tr>
<tr>
<td>attestation-hub.db.username</td>
<td>root</td>
<td>Defines the database connection credentials.</td>
</tr>
<tr>
<td>mtwilson.extensions.packageInc ludeFilter.startsWith</td>
<td>com.intel.org.glassfish.jersey. media.multipart</td>
<td>Do not change this value.</td>
</tr>
<tr>
<td>tenant.configuration.path</td>
<td>/opt/tenantconfig</td>
<td>Defines the path where tenant configurations will be stored. These are also stored in the database.</td>
</tr>
<tr>
<td>attestation-hub.db.portnum</td>
<td>5432</td>
<td>Defines the database connection port.</td>
</tr>
<tr>
<td>mtwilson.api.username</td>
<td>hubadmin</td>
<td>Defines the Verification Service credentials that the Hub will use to access the VS API.</td>
</tr>
<tr>
<td>jetty.tls.cert.dn</td>
<td>CN=Attestation Hub</td>
<td>Defines the Distinguished Name of the Hub TLS certificate.</td>
</tr>
<tr>
<td>mtwilson.password</td>
<td>HubPassword</td>
<td>Defines the Verification Service credentials that the Hub will use to access the VS API.</td>
</tr>
<tr>
<td>attestation-hub.db.hostname</td>
<td>localhost</td>
<td>Defines the database connection IP address or hostname.</td>
</tr>
</tbody>
</table>
### Key Sample Value Description

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password.vault.type</td>
<td>JCEKS</td>
<td>Defines password for keystore vault.</td>
</tr>
<tr>
<td>attestation-hub.db.url</td>
<td>jdbc:postgresql://localhost:5432/attestation_hub_pu</td>
<td>Defines the complete database connection URL.</td>
</tr>
<tr>
<td>mtwilson.server.port</td>
<td>8443</td>
<td>Defines the Verification Service API port.</td>
</tr>
</tbody>
</table>

#### 12.3.3 Command-Line Options

#### 12.3.3.1 Available Commands

**12.3.3.1.1 Help**

```bash
attestation-hub help
```

Displays the list of available CLI commands.

**12.3.3.1.2 Start**

```bash
attestation-hub start
```

Starts the services.

**12.3.3.1.3 Stop**

```bash
mtwilson stop
```

Stops the services.

**12.3.3.1.4 Restart**

```bash
attestation-hub restart
```

Restarts the services.

**12.3.3.1.5 Status**

```bash
attestation-hub status
```

Reports whether the service is currently running.

**12.3.3.1.6 Uninstall**

```bash
attestation-hub uninstall [--purge]
```

Uninstalls the service, including the deletion of all files and folders. Database content is not removed. If the `--purge` option is used, database content will be removed during the uninstallation.
12.3.1.7 Version

attestation-hub version

Reports the version of the service.

12.3.1.8 Password

attestation-hub password [username] [password] --permissions *::*

Creates a new user with the specified username and password. Because the Hub does not have granular user permissions, the --permissions *::* is necessary and assigns all permissions to the created user.

12.3.1.9 Export-config

attestation-hub export-config <outfile|--in=infile|--out=outfile|--stdout>

Exports the current configuration. Configuration settings are stored in the encrypted file /opt/mtwilson/configuration/mtwilson.properties; this command allows the configuration to be decrypted or output to the console.

12.3.1.10 Config

attestation-hub config [key] [value]

Configures a specified configuration setting to a specified value. Changing settings may require a service restart to take effect.

12.3.1.11 Setup

attestation-hub setup [-force|--noexec] [task1 task2 ...]

Re-runs the installation setup tasks, or the specific tasks listed.

12.3.4 Directory Layout

12.3.4.1 Logs

12.4 Certificate Management Service

12.4.1 Installation Answer File Options
### Configuration Options

#### 12.4.3 Command-Line Options

**12.4.3.1 Help**

```
cms help
```

Displays the list of available CLI commands.

**12.4.3.2 Start**

```
cms start
```

Starts the services.

**12.4.3.3 Stop**

```
cms stop
```

Stops the service.

**12.4.3.4 Restart**

```
cms restart
```

Restarts the services.

**12.4.3.5 Status**

```
cms status
```

---

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS_NOSETUP</td>
<td>false</td>
<td>Determines whether &quot;setup&quot; will be executed after installation. Typically this is set to &quot;false&quot; to install and perform setup in one action. The &quot;true&quot; option is intended for building the service as a container, where the installation would be part of the image build, and setup would be performed when the container starts for the first time to generate any persistent data.</td>
</tr>
<tr>
<td>CMS_PORT</td>
<td>8445</td>
<td>Defines the HTTPS port the service will use.</td>
</tr>
<tr>
<td>AAS_API_URL</td>
<td>https://&lt;Hostname or IP address of the AAS&gt;:8444/aas/</td>
<td>URL to connect to the AAS, used during setup for authentication.</td>
</tr>
<tr>
<td>AAS_TLS_SAN</td>
<td>&lt;Comma-separated list of IPs/hostnames for the AAS&gt;</td>
<td></td>
</tr>
</tbody>
</table>

*Commented [KTE11]: Why is this needed?*
Reports whether the service is currently running.

**12.4.3.6 Uninstall**

`cms uninstall`

Uninstalls the service, including the deletion of all files and folders.

**12.4.3.7 Version**

`cms version`

Reports the version of the service.

**12.4.3.8 TlsCertSha384**

Shows the SHA384 of the TLS certificate.

**12.4.3.9 setup [task]**

Runs a specific setup task.

Available Tasks for setup:

**12.4.3.9.1 cms setup server [--port=<port>]**

- Setup http server on `<port>`
- Environment variable CMS_PORT=<port> can be set alternatively

**12.4.3.9.2 cms setup root_ca [--force]**

- Create its own self signed Root CA keypair in /etc/cms for quality of life
- Option [--force] overwrites any existing files, and always generate new Root CA keypair

**12.4.3.9.3 cms setup tls [--force] [--host_names=<host_names>]**

- Create its own root_ca signed TLS keypair in /etc/cms for quality of life
- Option [--force] overwrites any existing files, and always generate root_ca signed TLS keypair
- Argument <host_names> is a list of host names used by local machine, seperated by comma
- Environment variable CMS_HOST_NAMES=<host_names> can be set alternatively

**12.4.3.9.4 cms setup cms_auth_token [--force]**

- Create its own self signed JWT keypair in /etc/cms/jwt for quality of life
- Option [--force] overwrites any existing files, and always generate new JWT keypair and token
**12.4.4 Directory Layout**

The Certificate Management Service installs by default to /opt/cms with the following folders.

**12.4.4.1 Bin**

This folder contains executable scripts.

**12.4.4.2 Cacerts**

This folder contains the CMS root CA certificate.

**12.5 Authentication and Authorization Service**

**12.5.1 Installation Answer File Options**

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS_BASE_URL</td>
<td>https://&lt;cms IP or hostname&gt;/cms/v1/</td>
<td>Provides the URL for the CMS.</td>
</tr>
<tr>
<td>AAS_API_URL</td>
<td>https://&lt;aas IP or hostname&gt;:8444/aas</td>
<td></td>
</tr>
<tr>
<td>AAS_NOSETUP</td>
<td>false</td>
<td>Determines whether &quot;setup&quot; will be executed after installation. Typically this is set to &quot;false&quot; to install and perform setup in one action. The &quot;true&quot; option is intended for building the service as a container, where the installation would be part of the image build, and setup would be performed when the container starts for the first time to generate any persistent data.</td>
</tr>
<tr>
<td>AAS_DB_HOSTNAME</td>
<td>localhost</td>
<td>Hostname or IP address of the AAS database</td>
</tr>
<tr>
<td>AAS_DB_PORT</td>
<td>5432</td>
<td>Database port number</td>
</tr>
<tr>
<td>AAS_DB_NAME</td>
<td>pgdb</td>
<td>Database name</td>
</tr>
<tr>
<td>AAS_DB_USERNAME</td>
<td>dbuser</td>
<td>Database username</td>
</tr>
</tbody>
</table>
### 12.5.2 Configuration Options

### 12.5.3 Command-Line Options

#### 12.5.3.1 Help

Displays the list of available CLI commands.

#### 12.5.3.2 setup <task>

Executes a specific setup task. Can be used to change the current configuration.

Available Tasks for setup:

##### 12.5.3.2.1 authservice setup all

- Runs all setup tasks
12.5.3.2.2  authservice setup database [-force] [--arguments=<argument_value>]

- Available arguments are:
  - db-host alternatively, set environment variable AAS_DB_HOSTNAME
  - db-port alternatively, set environment variable AAS_DB_PORT
  - db-user alternatively, set environment variable AAS_DB_USERNAME
  - db-pass alternatively, set environment variable AAS_DB_PASSWORD
  - db-name alternatively, set environment variable AAS_DB_NAME
  - db-sslmode <disable|allow|prefer|require|verify-ca|verify-full>
    alternatively, set environment variable AAS_DB_SSLMODE
  - db-sslcert path to where the certificate file of database. Only applicable
    for db-sslmode=<verify-ca|verify-full>. If left empty, the cert
    will be copied to /etc/authservice/tdcertdb.pem
    alternatively, set environment variable AAS_DB_SSLCERT
  - db-sslcertsrc <path to where the database ssl/tls certificate file>
    mandatory if db-sslcert does not already exist
    alternatively, set environment variable AAS_DB_SSLCERTSRC
- Run this command with environment variable AAS_DB_REPORT_MAX_ROWS and AAS_DB_REPORT_NUM_ROTATIONS can update db rotation arguments

12.5.3.2.3  authservice setup server [ --port=<port> ]

- Setup http server on <port>
- Environment variable AAS_PORT=<port> can be set alternatively
authservice setup tls [ --force ] [ --host_names=<host_names> ]
- Use the key and certificate provided in /etc/threat-detection if files exist
- Otherwise create its own self-signed TLS keypair in /etc/authservice for quality of life
- Option [ --force ] overwrites any existing files, and always generate self-signed keypair
- Argument <host_names> is a list of host names used by local machine, seperated by comma
- Environment variable AAS_TLS_HOST_NAMES=<host_names> can be set alternatively

12.5.3.2.4  authservice setup admin [ --user=<username> ] [ --pass=<password> ]

- Environment variable AAS_ADMIN_USERNAME=<username> can be set alternatively
- Environment variable AAS_ADMIN_PASSWORD=<password> can be set alternatively

12.5.3.2.5  authservice setup reghost [ --user=<username> ] [ --pass=<password> ]

- Environment variable AAS_REG_HOST_USERNAME=<username> can be set alternatively
- Environment variable AAS_REG_HOST_PASSWORD=<password> can be set alternatively

12.5.3.2.6  authservice setup download_ca_cert [ --force ]

- Download CMS root CA certificate
- Option [ --force ] overwrites any existing files, and always downloads new root CA cert
- Environment variable CMS_BASE_URL=<url> for CMS API url
12.5.3.2.7 authservice setup download_cert TLS [--force]
- Generates Key pair and CSR, gets it signed from CMS
- Option --force overwrites any existing files, and always downloads newly signed TLS cert
- Environment variable CMS_BASE_URL=<url> for CMS API url
- Environment variable BEARER_TOKEN=<token> for authenticating with CMS
- Environment variable KEY_PATH=<key_path> to override default specified in config
- Environment variable CERT_PATH=<cert_path> to override default specified in config
- Environment variable AAS_TLS_CERT_CN=<TLS CERT COMMON NAME> to override default specified in config
- Environment variable AAS_CERT_ORG=<CERTIFICATE ORGANIZATION> to override default specified in config
- Environment variable AAS_CERT_COUNTRY=<CERTIFICATE COUNTRY> to override default specified in config
- Environment variable AAS_CERT_LOCALITY=<CERTIFICATE LOCALITY> to override default specified in config
- Environment variable AAS_CERT_PROVINCE=<CERTIFICATE PROVINCE> to override default specified in config
- Environment variable SAN_LIST=<san> list of hosts which needs access to service

12.5.3.2.8 authservice setup jwt
- Create jwt signing key and jwt certificate signed by CMS
- Environment variable CMS_BASE_URL=<url> for CMS API url
- Environment variable AAS_JWT_CERT_CN=<CERTIFICATE SUBJECT> AAS JWT Certificate Subject
- Environment variable AAS_JWT_INCLUDE_KEYID=<KEY ID> AAS include key id in JWT Token
- Environment variable AAS_JWT_TOKEN_DURATION_MINS=<DURATION> JWT Token validation minutes
- Environment variable BEARER_TOKEN=<token> for authenticating with CMS

12.5.3.3 Start
Starts the service.

12.5.3.4 Status
Displays the current status of the service.

12.5.3.5 Stop
Stops the service.

12.5.3.6 tlscertsha384
Shows the SHA384 of the TLS certificate.

12.5.3.7 Uninstall
Removes the service. Use the "--purge" flag to also delete all data.
### 12.5.3.8 Version

Shows the version of the service.

### 12.5.4 Directory Layout

The Verification Service installs by default to `/opt/authservice` with the following folders.

#### 12.5.4.1 Bin

Contains executable scripts and binaries.

#### 12.5.4.2 Dbscripts

Contains database scripts.

### 12.6 Workload Service

#### 12.6.1 Installation Answer File Options

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLS_LOGLEVEL</td>
<td>INFO</td>
<td>Alternatives include WARN and DEBUG. Sets the log level for the service.</td>
</tr>
<tr>
<td>WLS_NOSETUP</td>
<td>false</td>
<td>Determines whether &quot;setup&quot; will be executed after installation. Typically this is set to &quot;false&quot; to install and perform setup in one action. The &quot;true&quot; option is intended for building the service as a container, where the installation would be part of the image build, and setup would be performed when the container starts for the first time to generate any persistent data.</td>
</tr>
<tr>
<td>WLS_USER</td>
<td></td>
<td>Defines a new user with the WLS:Administrator role that will be created during setup.</td>
</tr>
<tr>
<td>WLS_PASSWORD</td>
<td></td>
<td>Defines the password for the new WLS user.</td>
</tr>
<tr>
<td>WLS_PORT</td>
<td>5000</td>
<td>Defines the HTTPS port used by the service.</td>
</tr>
<tr>
<td>Key</td>
<td>Sample Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>WLS_DB_HOSTNAME</td>
<td>localhost</td>
<td>Database hostname</td>
</tr>
<tr>
<td>WLS_DB</td>
<td>wlsdb</td>
<td>Database name</td>
</tr>
<tr>
<td>WLS_DB_PORT</td>
<td>5432</td>
<td>Database port number</td>
</tr>
<tr>
<td>WLS_DB_USERNAME</td>
<td>wlsdbuser</td>
<td>Database username</td>
</tr>
<tr>
<td>WLS_DB_PASSWORD</td>
<td>wlsdbuserpass</td>
<td>Database password</td>
</tr>
<tr>
<td>HVS_URL</td>
<td>https://&lt;HVS IP address or hostname&gt;:8443/mtwilson/v2/</td>
<td>Base URL for the HVS</td>
</tr>
<tr>
<td>HVS_USER</td>
<td></td>
<td>Username for machine account used by the WLS to access the HVS to retrieve reports for key transfer requests.</td>
</tr>
<tr>
<td>HVS_PASSWORD</td>
<td></td>
<td>Password for the HVS machine account</td>
</tr>
<tr>
<td>AAS_API_URL</td>
<td>https://&lt;AAS IP address or hostname&gt;:8444/aas</td>
<td>Base URL for the AAS</td>
</tr>
<tr>
<td>SAN_LIST</td>
<td>127.0.0.1,localhost,10.x.x.x</td>
<td>Comma-separated list of IP addresses and hostnames that will be valid connection points for the service. Requests sent to the service using an IP or hostname not in this list will be denied, even if it resolves to this service.</td>
</tr>
<tr>
<td>CMS_BASE_URL</td>
<td></td>
<td>Base URL for the CMS</td>
</tr>
<tr>
<td>BEARER_TOKEN</td>
<td>&lt;token&gt;</td>
<td>Token from the CMS generated during CMS setup that allows the AAS to perform initial setup tasks.</td>
</tr>
</tbody>
</table>

12.6.2 Configuration Options

12.6.3 Command-Line Options

The Workload Service supports several command-line commands that can be executed only as the Root user:

Syntax:

wls <command>
12.6.4 Directory Layout

The Workload Service installs by default to /opt/wls with the following folders.

12.7 Key Broker Service

12.7.1 Installation Answer File Options

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTWILSON_API_URL</td>
<td>https://&lt;IP or hostname of HVS&gt;:8443/mtwilson/v2</td>
<td>Base URL for access to the HVS</td>
</tr>
<tr>
<td>MTWILSON_TLS_CERT_SHA384</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTWILSON_API_USERNAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTWILSON_API_PASSWORD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AAS_API_URL</td>
<td>https://&lt;AAS IP address or hostname&gt;:8444/aas</td>
<td>Base URL for the AAS. Note that this is for the AAS owned by the KBS owner; this may be a different AAS from the one used by other components.</td>
</tr>
<tr>
<td>CMS_BASE_URL</td>
<td>https://&lt;CMS IP address or hostname&gt;:8445/cms/v1</td>
<td>Base URL for the CMS. Note that this is for the CMS owned by the KBS owner; this may be a different CMS from the one used by other components.</td>
</tr>
<tr>
<td>https_proxy</td>
<td>Optional; used to define a proxy if needed</td>
<td></td>
</tr>
<tr>
<td>no_proxy</td>
<td>Optional; used to define proxy exceptions if applicable</td>
<td></td>
</tr>
<tr>
<td>JETTY_TLS_CERT_IP</td>
<td>Comma-separated list of IP addresses that will be valid connection points for the service. Requests sent to the service using an IP not in this list will be denied, even if it resolves to this service.</td>
<td></td>
</tr>
<tr>
<td>JETTY_TLS_CERT_DNS</td>
<td>Comma-separated list of hostnames that will be valid connection points for the service. Requests sent to the service using a hostname not in this list will be denied, even if it resolves to this service.</td>
<td></td>
</tr>
<tr>
<td>JETTY_PORT</td>
<td>80</td>
<td>Defines the HTTP port for the service</td>
</tr>
<tr>
<td>JETTY_SECURE_PORT</td>
<td>443</td>
<td>Defines the HTTPS port for the service</td>
</tr>
</tbody>
</table>

Commented [KTE15]: verify

Commented [KTE16]: This needs to get removed. Should import SAML, not give direct HVS access
12.7.2 Configuration Options

12.7.3 Command-Line Options

The Key Broker Service supports several command-line commands that can be executed only as the Root user:

Syntax:

kms <command>

12.7.3.1 Start

Starts the service

12.7.3.2 Stop

Stops the service

12.7.3.3 Uninstall

Removes the service

12.7.3.4 Version

Displays the version of the service

12.7.3.5 setup

Usage: /usr/local/bin/kms setup [--force|--noexec] [task1 task2 ...]

Available setup tasks:
12.7.3.5.1 kms setup jca-security-providers
12.7.3.5.2 kms setup password-vault
12.7.3.5.3 kms setup jetty-ports
12.7.3.5.4 kms setup jetty-tls-keystore
12.7.3.5.5 kms setup shiro-ssl-port
12.7.3.5.6 kms setup notary-key
12.7.3.5.7 kms setup envelope-key
12.7.3.5.8 kms setup storage-key
12.7.3.5.9 kms setup saml-certificates
12.7.3.5.10 kms setup tpm-identity-certificates

12.7.4 Directory Layout
The Verification Service installs by default to /opt/kms with the following folders.

12.7.4.1 Bin
Contains scripts and executable binaries

12.7.4.2 Configuration
Contains configuration files

12.7.4.3 Env
Contains environment details

12.7.4.4 Features

12.7.4.5 Java
Contains Java artifacts
12.7.4.6 Logs
Contains logs. Primary log file is kms.log

12.7.4.7 Repository
Contains the "keys" subdirectory, which is used for storing image encryption keys.

12.7.4.8 Script
Contains additional scripts

12.8 Workload Agent

12.8.1 Installation Answer File Options
See the Linux Trustagent section. The WLA is installed as part of the Trust Agent installation.

12.8.2 Configuration Options

12.8.3 Command-Line Options
The Workload Agent does not have any CLI commands.

12.8.4 Directory Layout
The Workload Agent installs by default to /opt/workload-agent with the following folders.

12.8.4.1 Bin
Contains scripts and executable binaries.

12.9 Workload Policy Manager

12.9.1 Installation Answer File Options
<table>
<thead>
<tr>
<th>Key</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMS_API_URL</td>
<td>https://&lt;IP address or hostname of the KBS&gt;:443/v1/</td>
<td>Defines the baseurl for the Key Broker Service.  The WPM uses this URL to request new encryption keys when encrypting images.</td>
</tr>
<tr>
<td>KMS_API_USERNAME</td>
<td></td>
<td>Defines a service account for the WPM to access the Key Broker Service. This is used for key creation when encrypting new images.</td>
</tr>
<tr>
<td>KMS_API_PASSWORD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMS_TLS_SHA256</td>
<td></td>
<td>SHA256 hash of the Key Broker TLS certificate</td>
</tr>
<tr>
<td>ENVELOPE_PUBLIC_KEY_LOCATION</td>
<td><em>/etc/workload-policy-manager/envelopePublicKey.pub</em></td>
<td>Defines the location of the envelope key used to secure image keys when transferred from the Key Broker</td>
</tr>
<tr>
<td>ENVELOPE_PRIVATE_KEY_LOCATION</td>
<td><em>/etc/workload-policy-manager/envelopePrivateKey.pem</em></td>
<td>Defines the location of the envelope key used to secure image keys when transferred from the Key Broker</td>
</tr>
<tr>
<td>CMS_BASE_URL</td>
<td>https://&lt;IP address or hostname for CMS&gt;:8445/cms/v1/</td>
<td>Defines the base URL for the CMS owned by the image owner. Note that this CMS may be different from the CMS used for other components.</td>
</tr>
<tr>
<td>BEARER_TOKEN</td>
<td>&lt;token&gt;</td>
<td></td>
</tr>
<tr>
<td>WPM_WITH_CONTAINER_SECURITY</td>
<td>&quot;yes&quot; or &quot;no&quot;</td>
<td>Defines whether the WPM will support Docker Container encryption. If this is set to Yes, the appropriate prerequisites for Docker Container encryption will be installed. If this is set to &quot;no,&quot; the WPM will not be able to encrypt Docker Container images, and will only be usable to encrypt Virtual Machine images.</td>
</tr>
</tbody>
</table>

**12.9.2 Configuration Options**

**12.9.3 Command-Line Options**

The Workload Policy Manager supports several command-line commands that can be executed only as the Root user:

Syntax:

```plaintext
wpm <command>
```

**12.9.3.1 create-image-flavor**

Creates a new image flavor and encrypts a source image. Output is the image flavor in JSON format and the encrypted image.
usage: wpm create-image-flavor [-l label] [-i in] [-o out] [-e encout] [-k key]
-l, --label image flavor label
-i, --in input image file path
-o, --out (optional) output image flavor file path
-e, --encout (optional) output encrypted image file path
-k, --key (optional) existing key ID
if not specified, encryption is skipped
if not specified, a new key is generated

12.9.3.2 create-container-image-flavor

Used to encrypt Docker container images and generate a container image flavor.

-i, --img-name container image name
-t, --tag (optional) container image tag name
-f, --docker-file (optional) container file path
to build the container image
-d, --build-dir (optional) build directory to build the container image
-k, --key-id (optional) existing key ID
-e, --encryption-required if
-s, --integrity-enforced if
-n, --notary-server (optional) specify notary server url
-o, --out-file (optional) specify output file path

12.9.3.3 get-container-image-id

12.9.3.4 create-software-flavor

Not currently supported; intended for future functionality.

12.9.3.5 Uninstall

Removes the WPM.

12.9.3.6 --help

Displays help text

12.9.3.7 --version

Displays the WPM version
12.9.3.8 Setup

usage: wpm setup [<tasklist>]

<tasklist> - space separated list of tasks

12.9.3.8.1 wpm setup

12.9.3.8.2 wpm setup CreateEnvelopeKey

12.9.3.8.3 wpm setup RegisterEnvelopeKey

12.9.3.8.4 wpm setup download_ca_cert [--force]
- Download CMS root CA certificate
- Option [--force] overwrites any existing files, and always downloads new root CA cert
- Environment variable CMS_BASE_URL=<url> for CMS API url

12.9.3.8.5 wpm setup download_cert Flavor-Signing [--force]
- Generates key pair and CSR, gets it signed from CMS
- Option [--force] overwrites any existing files, and always downloads newly signed Flavor-Signing cert
- Environment variable CMS_BASE_URL=<url> for CMS API url
- Environment variable BEARER_TOKEN=<token> for authenticating with CMS
- Environment variable KEY_PATH=<key_path> to override default specified in config
- Environment variable CERT_PATH=<cert_path> to override default specified in config
- Environment variable WPM_FLAVOR_SIGN_CERT_CN=<COMMON NAME> to override default specified in config
- Environment variable WPM_CERT_ORG=<CERTIFICATE ORGANIZATION> to override default specified in config
- Environment variable WPM_CERT_COUNTRY=<CERTIFICATE COUNTRY> to override default specified in config
- Environment variable WPM_CERT_LOCALITY=<CERTIFICATE LOCALITY> to override default specified in config
- Environment variable WPM_CERT_PROVINCE=<CERTIFICATE PROVINCE> to override default specified in config
13 Certificate and Key Management

13.1 Verification Service Certificates and Keys

Each of the certificates and keys used by the Verification Service can be automatically replaced by deleting the certificate or key and running "mtwilson setup". This will re-run the installation setup tasks, which will detect that needed certificates are missing and create new ones. Restart the VS after replacing certificates in this way.

13.1.1 Root Certificate

The VS Root Certificate is used to sign the TLS, SAML and Asset tag certificates, and is generated during installation.

/opt/mtwilson/configuration/cacerts.pem
[opt/mtwilson/configuration/cakey.pem
/opt/mtwilson/configuration/MtWilsonRootCA.crt.pem

The Root Certificate can be replaced using the following command:

mtwilson replace-root-key-pair --private-key=key.pem --cert-chain=cert-chain.pem

This will:
- Replace key pair in /opt/mtwilson/configuration/cakey.pem
- Update /opt/mtwilson/configuration/cacerts.pem with cert chain
- Update /opt/mtwilson/configuration/MtWilsonRootCA.crt.pem with cert chain

This does not require a service restart. However, since the Root Certificate is used to sign the TLS, SAML, and Asset Tag certificates, changing the Root Certificate requires recreation of those certificates as well.

13.1.2 TLS Certificate

The TLS Certificate is created at installation time, and the key pair is stored in a keystore:

/opt/mtwilson/configuration/keystore.jks
When generating a new TLS key pair for the Verification Service, it is recommended to use the RSA algorithm with no restriction on size. The TLS certificate must contain Subject Alternative name entries for any resolvable hostname or IP address for hostname verification.

The TLS Certificate can be replaced with a user-specified keypair and certificate chain using the following command:

```
mtwilson replace-tls-key-pair --private-key=new.key.pem --cert-chain=new.cert-chain.pem
```

This will:

- Replace the key pair in `/opt/mtwilson/configuration/keystore.jks`, alias jetty.
- Updates the values of the following properties in mtwilson.properties:
  - jetty.tls.cert.dn
  - jetty.tls.cert.ip
  - jetty.tls.cert.dns

After replacing the Verification Service TLS certificate, the VS service will need to be restarted:

```
mtwilson restart
```

Additionally, all Trust Agent hosts will need to be updated to trust the new TLS certificate. On each Trust Agent host, update the value of the configuration setting `mtwilson.tls.cert.sha384` with the SHA384 hash of the new TLS certificate.

To retrieve the new SHA384 value, run "mtwilson fingerprint" on the VS.

To reconfigure the `mtwilson.tls.cert.sha384` value on a Trust Agent host, run the following commands:

```
tagent config mtwilson.tls.cert.sha384 <HVS TLS SHA384>
tagent setup download-mtwilson-tls-certificate
tagent restart
```

No action is required after changing the VS TLS certificate for VMWare hosts.

### 13.1.3 SAML

The SAML Certificate is used to sigh SAML attestation reports, and is itself signed by the Root Certificate.

```
/opt/mtwilson/configuration/saml.crt
```
The SAML Certificate can be replaced with a user-specified keypair and certificate chain using the following command:

```
mtwilson replace-saml-key-pair --private-key=new.key.pem --cert-chain=new.cert.pem
```

This will:

- Replace key pair in `/opt/mtwilson/configuration/SAML.jks`, alias samlkey1
- Update `/opt/mtwilson/configuration/saml.crt` with saml DER public key cert
- Update `/opt/mtwilson/configuration/saml.crt.pem` with saml PEM public key cert
- Update configuration properties:
  - saml.key.password to null
  - saml.certificate.dn
  - saml.issuer

When the SAML certificate is replaced, all hosts will immediately be added to a queue to generate a new attestation report, since the old signing certificate is no longer valid.

If the Integration Hub is being used, the new SAML certificate will need to be imported to the Hub.

### 13.1.4 Asset Tag

The Asset tag Certificate is used to sign all Asset Tag Certificates.

```
mtwilson replace-tag-key-pair --private-key=new.key.pem --cert-chain=new.cert-chain.pem
```

This will:

- Replace key pair in database table `mw_file` (ckey is private and public key pem formatted, cacerts is cert chain)
- Update `/opt/mtwilson/configuration/tag-cacerts.pem` with cert chain
- Update configuration properties:
No service restart is needed. However, all existing Asset Tags will be considered invalid, and will need to be recreated. It is recommended to delete any existing Asset Tag certificates and Flavors, and then recreate and deploy new Tags.

13.1.5 Privacy CA

The Privacy CA certificate is used as part of the certificate chain for creating the Attestation Identity Key (AIK) during Trust Agent provisioning. The Privacy CA must be a self-signed certificate.

The Privacy CA certificate is used by Trust Agent nodes during Trust Agent provisioning; if the Privacy CA certificate is changed, all Trust Agent nodes will need to be re-provisioned.

```
/opt/mtwilson/configuration/PrivacyCA.p12
/opt/mtwilson/configuration/PrivacyCA.pem
```

The Privacy CA Certificate can be replaced with a user-specified keypair and certificate chain using the following command:

```
mtwilson replace-pca-key-pair --private-key=new.key.pem --cert-chain=new.cert-chain.pem
```

This will:
- Replace key pair in /opt/mtwilson/configuration/PrivacyCA.p12, alias 1
- Update /opt/mtwilson/configuration/PrivacyCA.pem with cert
- Update configuration properties:
  - mtwilson.privacyca.aik.issuer
  - mtwilson.privacyca.aik.validity.days

After the Privacy CA certificate is replaced, all Trust Agent hosts will need to be re-provisioned with a new AIK:

```
tagent setup download-mtwilson-privacy-ca-certificate --force
tagent setup request-aik-certificate --force
tagent restart
```

13.1.6 Endorsement CA

The Endorsement CA is a self-signed certificate used during Trust Agent provisioning.

```
/opt/mtwilson/configuration/EndorsementCA.p12
```
/opt/mtwilson/configuration/EndorsementCA.pem

The Endorsement CA Certificate can be replaced with a user-specified keypair and certificate chain using the following command:

```
mtwilson replace-eca-key-pair --private-key=new.key.pem --cert-chain=new.cert-chain.pem
```

This will:

- Replace key pair in /opt/mtwilson/configuration/EndorsementCA.p12, alias 1
- Update /opt/mtwilson/configuration/EndorsementCA.pem with accepted ECs
- Update configuration properties:
  - mtwilson.privacyca.ek.issuer
  - mtwilson.privacyca.ek.validity.days

After the Endorsement CA certificate is replaced, all Trust Agent hosts will need to be re-provisioned with a new Endorsement Certificate:

tagent setup request-endorsement-certificate --force
tagent restart

### 13.2 Trust Agent Certificates and Keys

#### 13.2.1 TLS Certificate

The TLS Certificate is created at installation time, and the key pair is stored in a keystore:

```
/opt/trustagent/configuration/trustagent.jks
```

When generating a new TLS key pair for the Trust Agent, it is recommended to use the RSA algorithm with no restriction on size. The TLS certificate must contain Subject Alternative name entries for any resolvable hostname or IP address for hostname verification.

The TLS Certificate can be replaced with a user-specified keypair and certificate chain using the following command:

```
tagent replace-tls-key-pair --private-key=new.key.pem --cert-chain=new.cert-chain.pem
```

This will:

- Replace key pair in /opt/mtwilson/configuration/trustagent.jks alias tls
• Update configuration properties:
  — trustagent.tls.cert.sha384
  — trustagent.tls.cert.dn
  — trustagent.tls.cert.ip
  — trustagent.tls.cert.dns

The Trust Agent service will need to be restarted after replacing the TLS certificate.

### 13.2.2 Trust Agent Provisioning Process

- aik.blob
- aik.pem
- endorsement.pem
- trustagent.jks

### 13.3 Integration Hub Certificates and Keys

#### 13.3.1 TLS Certificate

The TLS Certificate is created at installation time, and the key pair is stored in a keystore:

```
/opt/attestation-hub/configuration/keystore.jks
```

When generating a new TLS key pair for the Hub, it is recommended to use the RSA algorithm with no restriction on size. The TLS certificate must contain Subject Alternative name entries for any resolvable hostname or IP address for hostname verification.

The TLS Certificate can be replaced with a user-specified keypair and certificate chain using the following command:

```
attestation-hub replace-tls-key-pair --private-key=new.key.pem --cert-chain=new.cert-chain.pem
```

This will:

• Replace key pair in /opt/attestation-hub/configuration/keystore.jks, alias jetty
• Update configuration properties:
  — jetty.tls.cert.dn
— jetty.tls.cert.ip
— jetty.tls.cert.dns

The Integration Hub service will need to be restarted after replacing the TLS certificate.
14 High Availability

To maximize service availability in an environment where hypervisor-level high availability or fault tolerance solutions are impractical, unavailable, or insufficient, Intel recommends using a redundancy model featuring two (or more) ISECL Verification Service instances running on separate hosts accessing the same external database with traffic directed by a reverse-proxy server.

Note: The shared database server should be configured for redundancy as well. However, database server configuration is beyond the scope of this document.

In this configuration, if one of the Verification Services becomes unavailable for any reason, the reverse-proxy automatically fails over to another remaining Verification Service. Since both instances are accessing a shared database, there is no loss of data in the case of a failover, and there is no manual intervention required after the failed server is brought back on-line.

The instructions below define a sample configuration using the NginX reverse proxy and two Verification Service instances. These instructions can be adapted to similar alternative solutions.

The key requirements for redundant Verification Services are:

- A shared database (whether this is external, or a replicated database across the Verification Service servers).
- Some form of reverse proxy or other method of sharing a single IP Address or hostname across all Verification Service instances.
- Identical keys, certificates, and other secrets on all Verification Service instances so that they can all use the same credentials to access the database, and so that the TLS certificate used by the web services remains identical. These include passwords and secrets defined in the various .properties files in the Verification Service configuration directory, all of the certificates and keys in that directory, the TLS certificate for the web server, and the configuration files for the web server.

14.1 Prerequisites

Following are the prerequisites:

- Separate database server (PostgreSQL is supported).
- An additional server running the NginX reverse-proxy service (other solutions are also possible).
14.2 Deployment Instructions

Following are the deployment instructions:

1. Deploy two (or more) separate Attestation Server instances on separate host servers.
   - Use a shared IP Address or hostname for the Attestation Server IP when setting up all Attestation Servers. The first installation performs the configurations of the secrets, certificates, keys, and users that are later copied to all of the other instances. Subsequent installations throw errors during user creation, as they attempt to create users that already exist; this is normal and expected.

2. In the mtwilson.env installation answer file, configure the IP Address, port, and logon credentials for the external database server as well as the port and logon credentials and the database name.
   - The database schema and a valid user with rights over this database must be created on the database server prior to running the Verification Service installation, and must be configured to enable connections from all redundant servers. The Verification Service installer automatically creates the required database tables on the remote server.

3. Copy the entire /opt/mtwilson/configuration directory from the first/Primary VS to all other Verification Services.

4. Restart the Verification Service an all servers.

5. On the reverse-proxy server, run the following command:
   - `$ apt-get install nginx`

6. Create or modify the default.conf configuration file:
   - `$ nano /etc/nginx/conf.d/default.conf`

   Edit the file as follows:

   ```
   upstream mtwilson {
     server <Verification Service 1 IP>:<port> max_fails=1 fail_timeout=30s;
     server <Verification Service 2 IP>:<port> backup;
   }

   server {
     listen <IP Address of NginX Server>:<port> server_name <DNS Name of NginX Server>;
     access_log /var/log/nginx/ISecL-VS-HA.log; error_log /var/log/nginx/ISecL-VS-HA.error.log;
     ## send request back to mtwilson ##
     location / {
       proxy_pass http://mtwilson/;
       proxy_next_upstream error timeout invalid_header http_500 http_502 http_503 http_504;
     }
   }
   ```
The upstream section allows for the declaration of the Verification Services to be used with the reverse proxy, as well as configuration of when each of the servers is used. In this configuration, one server is set to be the primary, and a second server is set to be the backup.

**Note:** All traffic goes to the primary server, and the server labeled backup is only used if the other server has been flagged as failed. This is done to preserve session information.

A failure is triggered when an HTTP request times out. In this case, the max_fails=1 variable sets a single timeout to trigger a failure. This can be set higher, but doing so increases the amount of time before a failure is detected and remediated. The fail_timeout=30s variable tells NginX to leave a server flagged as failed for 30 seconds before trying again. Increasing this value can improve performance slightly when a failover has occurred (as every new request more than 30 seconds since the last failed flag re-attempts the primary server and thus has to wait for a timeout), but also delay the automatic fail-back to the primary server once it is recovered.

As an alternative to the active/passive configuration, the ip_hash line can be added to the beginning of the upstream section. Note that if ip_hash is used, remove the max_fails, fail_timeout, and backup arguments. This causes NginX to direct incoming traffic to a Verification Service in the upstream list based on a hash of the requesting machine's IP Address.

In this way, NginX can perform load balancing. Requests are divided evenly across all servers in the list, or the weight argument can be added to determine load ratios.

The listen and server_name variables tell NginX which specific IP and port to listen on and forward. Requests sent to other ports are not forwarded and receives a default NginX page. This can be configured to be a different page if desired. For more information, refer to the documentation for NginX at http://nginx.org/en/docs/.

The proxy_pass setting tells NginX to forward all requests matching the syntax http://<listening IP/ name and port>//* to the Verification Service setting declared in the upstream section.

7. Restart the NginX service.

   $ service nginx restart

At this point, it should be possible to point a browser to the Attestation Server portal URLs, but substituting the Attestation Server IP/DNS name with the NginX server's IP/DNS name. NginX automatically forwards the URLs to the appropriate Attestation Server, and the services can be used normally.
14.3 Failover

If a failover to the backup server should occur, there is a brief waiting period (approximately 5-10 seconds) as NginX waits for the timeout and flags the primary as failed.
15 TLS Policies

The Intel Security Libraries Verification Service validates the authenticity of connections through the use of various TLS verification policies.

15.1 TLS Policy Types

Intel Security Libraries Verification Service uses six types of TLS policies.

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Behavior</th>
<th>Shared</th>
<th>Per-Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>The certificate policy requires one or more trusted certificates or CA certificates and only connects to a peer whose certificate either is a trusted certificate or is signed by a CA that is trusted. This policy type also performs hostname verification. <strong>Note:</strong> The remote server's hostname must be resolvable from the Mt. Wilson server.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate Fingerprint</td>
<td>This policy stores the SHA384 hash of the certificate for validation rather than the entire certificate itself.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Public Key</td>
<td>The public key policy requires one public key parameter and only connects to a peer using that key. This is similar to SSH public key authentication of clients and hosts. Hostname verification is NOT performed when using Public Key TLS policies.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Public Key Fingerprint</td>
<td>This policy stores the SHA384 hash of the public key for validation rather than the public key itself.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TRUST_FIRST_CERTIFICATE</td>
<td>This policy stores the first certificate encountered when connecting to a host, and uses that certificate for all future TLS validation with that host.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>INSECURE</td>
<td>This policy disables all TLS validation. All connections are accepted regardless of TLS certificates. This policy should be used for troubleshooting and development only, and should never be used in a production environment.</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

15.2 Policy Scope

TLS policies can be per-host or shared across multiple hosts.
15.2.1 Per-Host

A per-host TLS policy is an individual, per-host TLS policy. When the host is deleted, its per-host TLS policy is automatically deleted as well.

15.2.2 Shared

A shared TLS policy may be referenced by multiple host records. When a host that referenced a shared TLS policy is deleted, the shared policy continues to exist regardless if there are any remaining hosts that are referencing it. Shared policies must be explicitly deleted by the user.

The Verification Service requires a TLS policy to be defined for any remote host to which it connects. If no TLS policy is defined, or if the TLS information does not match the TLS policy, the connection fails.

15.3 Default Policy Selection

Any shared-scope policy can be defined as the "default" TLS policy for a given Verification Service environment. For example, if all TLS certificates for all hosts in the attestation environment have been signed by the same CA certificate, that CA certificate can be used to create a shared-scope certificate policy, and this same policy could be used to validate all TLS connections with all attested hosts. By configuring this policy as the default TLS policy, the Verification Service uses this specific policy for all hosts unless another policy is specified.

In the Verification Service UI, this mostly means that the default policy is automatically selected from the drop-down when registering hosts. From an API perspective, it means that, when calling a registration API, if no TLS policy is specifically defined in the call, the default TLS policy is used. Using a shared default policy that is valid across all hosts in the attestation environment can greatly simplify TLS policy and host management.

*Note:* During installation, the only two shared-scope policies that might be available are TRUST_FIRST_CERTIFICATE and INSECURE, and these only if they have actually been enabled. All other policies must be user-created after installation. To define a default TLS policy, edit the mtwilson.properties file and set the value of mtwilson.default.tls.policy.id to either the UUID or the name of the shared-scope TLS policy to be set as the default. Restart Mt. Wilson to affect the change.

15.4 Default TLS Policies

At the time the Verification Service is installed, two TLS policies are created.
15.4.1 TRUST_FIRST_CERTIFICATE

This policy creates a new TLS policy the first time that a new host is registered to the Verification Service, and uses that policy for all future interactions with that host.

15.4.2 INSECURE

This policy turned off all TLS certificate validation entirely (all connections were trusted, regardless of TLS certificates). This policy should only be used for development or troubleshooting, and should never be used in a production environment.

To configure the Verification Service to use TRUST_FIRST_CERTIFICATE as the default TLS Policy (and disallow the use of INSECURE), use the following settings:

mtwilson.tls.policy.allow=TRUST_FIRST_CERTIFICATE

mtwilson.default.tls.policy.id=TRUST_FIRST_CERTIFICATE

This can be done automatically during installation by setting the following variables in mtwilson.env:

export MTW_TLS_POLICY_ALLOW= TRUST_FIRST_CERTIFICATE

export MTW_DEFAULT_TLS_POLICY_ID=TRUST_FIRST_CERTIFICATE
16 Uninstallation

This section describes steps used for uninstalling Intel SecL-DC services.

Note: This section does not apply for containerized deployments. To uninstall a containerized deployment, simply shut down the container and delete the persistence volumes.

16.1 Verification Service

To uninstall the Verification Service, run the following command:

```bash
mtwilson uninstall
```

Removes following directories:
1. `usr/local/bin/mtwilson`
2. `$MTWILSON_HOME/bin`
3. `$MTWILSON_HOME/java`
4. `$MTWILSON_HOME/features`

```bash
mtwilson uninstall --purge
```

Removes following directories:
1. `$MTWILSON_HOME /opt/mtwilson`
2. `$MTWILSON_CONFIGURATION $MTWILSON_HOME/configuration (/opt/mtwilson/configuration)`
3. `$MTWILSON_LOGS $MTWILSON_HOME/logs (/opt/mtwilson/logs)`

The mtwilson uninstall command will not delete any database content. To completely uninstall and delete all database content and user data, run the following:

```bash
mtwilson erase-data

mtwilson erase-users --all

mtwilson uninstall --purge
```

Note: The uninstall command must be issued last, because the uninstall process removes the scripts that execute the other commands, along with all database connectivity info.
16.2 Trust Agent

To uninstall the Trust Agent, run the following command:
tagent uninstall

Backs up the configuration directory and removes all Trust Agent files, except for configuration files which are saved and restored.

Removes following directories:
1. /usr/local/bin/tagent
2. TRUSTAGENT_HOME : /opt/trustagent
3. /opt/tbootxm
4. /var/log/trustagent/measurement.*

**Note:** TPM ownership can be preserved by retaining the TPM owner secret. If the Operating System will also be cleared, Linux systems will also require the /usr/local/var/lib/tpm/system.data file to be preserved. This file must be preserved from after ownership is taken, and then replaced after the OS reload before the Trust Agent attempts to reassert ownership.

If the ownership secret and/or system.data file are not preserved, reinstallation will require clearing TPM ownership.

16.3 Integration Hub

To uninstall the Integration Hub, run the following command:
attestation hub uninstall

Removes the following directories:
1. /usr/local/bin/attestation-hub
2. /usr/bin/attestation-hub
3. /opt/attestation-hub
4. /etc/logrotate.d/attestation-hub

attestation-hub uninstall --purge

Removes the following directories (in addition to directories removed without the --purge option):
1. Drops the database
2. Drops the user
3. Removes attestation hub tenant configuration path
### 17.1 PCR Definitions

#### 17.1.1 Microsoft Windows Server 2016 Datacenter

#### 17.1.1.1 TPM 1.2 and 2.0

<table>
<thead>
<tr>
<th>PCR</th>
<th>Measurement Parameters</th>
<th>Description</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCR 0</td>
<td>BIOS ROM and Flash Image</td>
<td>This PCR is based solely on the BIOS version, and remains identical across all hosts using the same BIOS. This PCR is used as the PLATFORM Flavor.</td>
<td>All</td>
</tr>
<tr>
<td>PCR 12</td>
<td>Data events and highly volatile events</td>
<td>This PCR measures some of the modules which has boot counters in it. It changes on every boot and resume (Microsoft Windows ONLY; do not use for attestation as the values change on reboot)</td>
<td>Microsoft Windows Server</td>
</tr>
<tr>
<td>PCR 13</td>
<td>Boot Module Details</td>
<td>This PCR remains static except major changes such as kernel module update, different device driver for different OEM servers, etc. (Microsoft Windows ONLY)</td>
<td>Microsoft Windows Server</td>
</tr>
<tr>
<td>PCR 14</td>
<td>Boot Authorities</td>
<td>Used to record the Public keys of authorities that sign OS components. Expected not to change often. (Microsoft Windows ONLY)</td>
<td>Microsoft Windows Server</td>
</tr>
</tbody>
</table>

#### 17.1.2 Red Hat Enterprise Linux

#### 17.1.2.1 TPM 2.0

<table>
<thead>
<tr>
<th>PCR</th>
<th>Measurement Parameters</th>
<th>Description</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCR 0</td>
<td>BIOS ROM and Flash Image Initial Boot Block (Intel® BootGuard only)</td>
<td>This PCR is based solely on the BIOS version, and remains identical across all hosts using the same BIOS. This PCR is used as the PLATFORM Flavor. Intel® BootGuard only: Extends measurements based on the Intel® BootGuard profile configuration and production vs non-production ACM flags; ACM signature; BootGuard key manifest hash; Boot Guard Policy Manifest Signature</td>
<td>All</td>
</tr>
<tr>
<td>PCR 7</td>
<td>Intel® BootGuard configuration and profiles</td>
<td>Describes the success of the IBB measurement event.</td>
<td>All (Intel® BootGuard only)</td>
</tr>
</tbody>
</table>
For TA hosts, this PCR includes measurements of the OS, InitRD, and UUID. This changes with every install due to InitRD and UUID change.

For ESXi and Trust Agent hosts, this PCR contains individual measurements of all of the non-Kernel modules.

For Linux hosts, this PCR is a measurement of the OS, InitRD, and UUID.

17.1.3 VMware ESXi

17.1.3.1 TPM 1.2

<table>
<thead>
<tr>
<th>PCR</th>
<th>Measurement Parameters</th>
<th>Description</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCR 0</td>
<td>BIOS ROM and Flash Image</td>
<td>This PCR is based solely on the BIOS version, and remains identical across all hosts using the same BIOS. This PCR is used as the PLATFORM Flavor.</td>
<td>All</td>
</tr>
<tr>
<td>PCR 17</td>
<td>ACM</td>
<td>This PCR measures the SINIT ACM, and is hardware platform-specific. This PCR is part of the PLATFORM Flavor.</td>
<td>VMware ESXi, Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>PCR 18</td>
<td>MLE [Tboot +VMM]</td>
<td>This PCR measures the tboot and hypervisor version. In ESXi hosts, only the tboot version is measured.</td>
<td>VMware ESXi, Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>PCR 19</td>
<td>Description</td>
<td>Operating System</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------------</td>
<td></td>
</tr>
</tbody>
</table>
| OS Specific.  
• ESX and Trust Agent — non Kernel modules  
• Citrix Xen — OS  
• + Init RD + UUID | For ESXi and Trust Agent hosts, this PCR contains individual measurements of all of the non-Kernel modules.  
For Citrix Xen hosts, this PCR is a measurement of the OS, InitRD, and UUID. | • VMware ESXi  
• Red Hat Enterprise Linux |

| PCR 20 | For ESXi only, VM Kernel and VMK Boot | This PCR is used only by ESXi hosts and is blank for all other host types. | • VMware ESXi |

| PCR 22 | Asset Tag | This PCR contains the measurement of the SHA1 of the Asset Tag Certificate provisioned to the TPM, if any. | • VMware ESXi |

### 17.1.3.2 TPM 2.0
VMware supports TPM 2.0 with Intel TXT starting in vSphere 6.7 Update 1. Earlier versions will support TPM 1.2 only.

| PCR 0 | BIOS ROM and Flash Image | This PCR is based solely on the BIOS version, and remains identical across all hosts using the same BIOS. This PCR is used as part of the PLATFORM flavor. | • All |

| PCR 17 | ACM | This PCR measures the SINIT ACM, and is hardware platform-specific. This PCR is part of the PLATFORM Flavor. | • VMware ESXi  
• Red Hat Enterprise Linux |

| PCR 18 | MLE [tboot +VMM] | This PCR measures the boot and hypervisor version. In ESXi hosts, only the tboot version is measured. This PCR is part of the PLATFORM Flavor. | • VMware ESXi  
• Red Hat Enterprise Linux |

| PCR 19 | OS Specific.  
• ESX and Trust Agent — non Kernel modules  
• Citrix Xen — OS  
• + Init RD + UUID | For ESXi this PCR contains individual measurements of all of the non-Kernel modules – this includes all of the VIBs installed on the ESXi host. This is part of the OS flavor. Note that two ESXi hosts with the same version of ESXi installed may require different OS flavors if different VIBs are installed. | • VMware ESXi  
• Red Hat Enterprise Linux |

| PCR 20 | For ESXi only, VM Kernel and VMK Boot | This PCR is used only by ESXi hosts for some host-specific measurements, and is part of the host-unique flavor. | • VMware ESXi |
### A.1 Attestation Rules

<table>
<thead>
<tr>
<th>Platform</th>
<th>TPM</th>
<th>Flavor Type</th>
<th>Rules to be verified</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL</td>
<td>1.2</td>
<td>HARDWARE</td>
<td>PcrMatchesConstant rule for PCR 0, PcrMatchesConstant rule for PCR 17</td>
<td>For all flavor evaluations, verification of the AIK certificate is needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PcrEventLogIncludes rule for PCR 17</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSET_TAG</td>
<td>AssetTagMatches rule</td>
<td>AssetTagMatches rule needs to be updated to verify the key-value pairs after verifying the tag certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HOST_SPECIFIC</td>
<td>PcrEventLogIncludes rule for PCR 19</td>
<td>Only for the host specific modules. Only PCR 19 data is needed in this flavor.</td>
</tr>
<tr>
<td>RHEL</td>
<td>2.0</td>
<td>HARDWARE</td>
<td>PcrMatchesConstant rule for PCR 0, PcrEventLogIncludes rule for PCR 17, PcrEventLogIntegrity rule for PCR 17</td>
<td>Evaluation of PcrEventLogIncludes would not include the host specific module verification. Even though PCR 19 only contains host specific modules, it is still needed in OS flavor for integrity check.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PcrEventLogIntegrity rule for PCR 17</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>HOST_SPECIFIC</td>
<td>PcrEventLogIncludes rule for PCR 17 (initrd &amp; vmlinuz)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSET_TAG</td>
<td>AssetTagMatches rule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>HOST_SPECIFIC</td>
<td>PcrEventLogIncludes rule for PCR 17 (initrd &amp; vmlinuz)</td>
<td></td>
</tr>
</tbody>
</table>

**PCR Measurement Parameters**

| PCR 22 | Asset Tag | Asset Tag is not currently supported for TPM 2.0 with ESXi. | VMware ESXi |

---

**Description**

- PCR 22: Asset Tag is not currently supported for TPM 2.0 with ESXi.
<table>
<thead>
<tr>
<th>Platform</th>
<th>TPM</th>
<th>Flavor Type</th>
<th>Rules to be verified</th>
<th>Comments</th>
</tr>
</thead>
</table>
| VMware ESXi | 1.2  | PLATFORM    | PcrMatchesConstant rule for PCR 0  
PcrMatchesConstant rule for PCR 17       |                                                                          |
| VMWare ESXi | 2.0  | PLATFORM    | NOT SUPPORTED                                                                        |                                                                          |
| Windows   | 1.2  | PLATFORM    | PcrMatchesConstant rule for PCR 0                                                   |                                                                          |
| Windows   | 2.0  | PLATFORM    | PcrMatchesConstant rule for PCR 0                                                   |                                                                          |
| ASSET_TAG |       | AssetTagMatches rule |                                                 | AssetTagMatches rule needs to be updated to verify the key-value pairs after verifying the tag certificate. |

A.2 Intel TXT and the Trusted Boot Process