



User Guide:

# Intel Cloud Integrity Technology 3.2 **Deployment Wizard**

---

# User Guide

## Cloud Integrity Technology Quick Start

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Intel products are not intended for use in medical, life-saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined."

Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Intel® Cloud Integrity Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Copyright © 2015 Intel Corporation. All rights reserved.

# Table of Contents

Quick Start.....	6
Introduction.....	5
Purpose.....	5
Definitions, Acronyms, Abbreviations.....	5
Acronyms.....	5
References.....	5
Overview.....	6
Installation .....	7
Standard.....	7
Custom.....	8
Upgrade .....	9
Uninstallation.....	10
Browser.....	11
Start.....	11
Environment .....	12
Features - Private Network.....	13
Features - Cloud Service Provider.....	14
Features - Enterprise.....	15
Layout.....	17
Settings - Private Network, VM Integrity, All-in-one.....	18
Settings - Private Network, VM Encryption with Barbican, All-in-one .....	19
Settings - Private Network, VM Encryption with KMIP, All-in-one.....	20
Credentials - Private Network, VM Integrity, All-in-one .....	21
Preview - Private Network, VM Integrity, All-in-one .....	22
Deploying.....	23
Summary .....	23

User Guide  
**Cloud Integrity Technology Quick Start**

## **Introduction**

This document contains the user guide for the Cloud Integrity Technology 3.2 Deployment Wizard server. The Deployment Wizard is an installable service that will automatically deploy CIT components in a variety of configurations.

### **Purpose**

The purpose of the Quick Start server is to simplify the deployment of Cloud Integrity Technology components into a specified environment.

The intended audience is developers, system engineers, product marketing team, and managers.

## **Definitions, Acronyms, Abbreviations**

### **Acronyms**

CIT - Cloud Integrity Technology

KMIP - Key Management Interoperability Protocol

SSH - Secure Shell

VM - Virtual Machine

CSP - cloud service provider

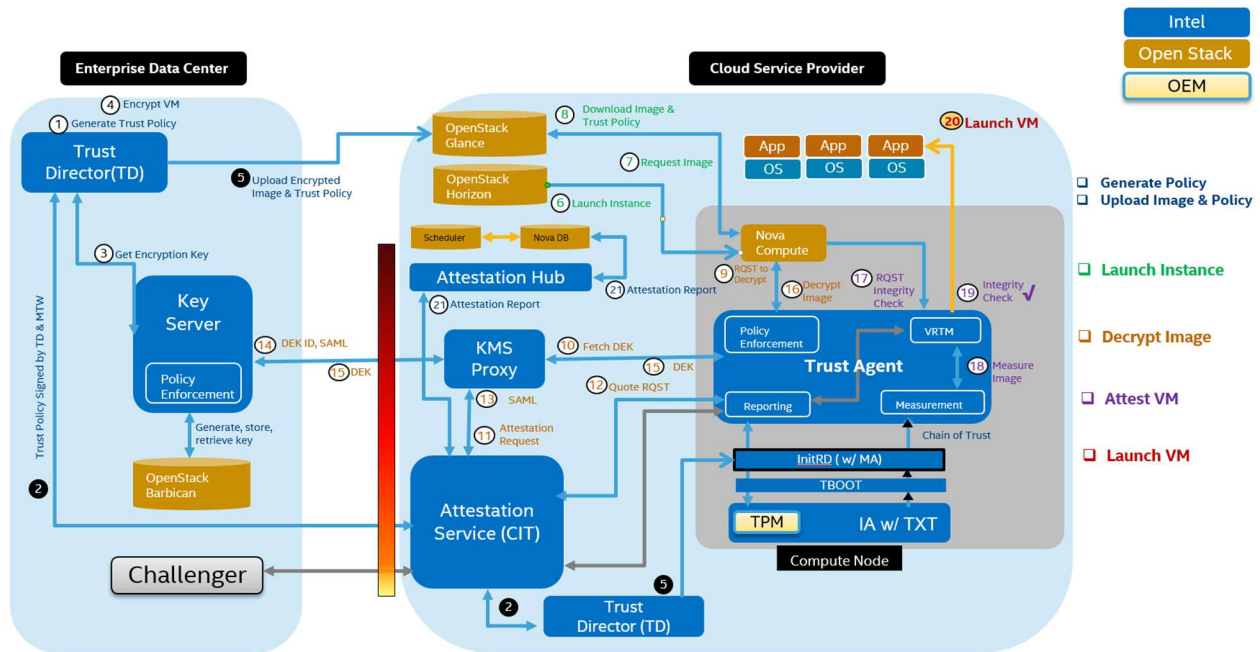
CSC - cloud service consumer (the enterprise customer that is using the CSP), this term is used only to refer to an enterprise in situations when it is acting specifically as a customer of a CSP

### **References**

Cloud Integrity Technology 3.2 Product Guide

User Guide  
Cloud Integrity Technology Quick Start

## Cloud Integrity Technology 3.2 Component Architecture



Intel Cloud Integrity Technology 3.2 consists of multiple components (see the CIT 3.2 Product Guide for a full description of each component and its purpose). These components can be deployed by the Deployment Wizard in different ways to support different use cases. Some components (such as the Key Broker Server) are only deployed to support specific use cases, and may not be used in all CIT installations.

The Deployment Wizard can install those components needed by the Cloud Service Provider (CSP), the components needed by the Enterprise Customer, or both. These components can be installed on a single host, or a separate host can be used for each component.

In any scenario where the CSP and Enterprise Customer components will be installed separately, the CSP components must be installed first. Information from the CSP (user authentication information, etc.) will need to be provided to the Enterprise Customer before the customer installs their own CIT components.

### Overview

This user guide is organized into sections covering installation and operation.

## Quick Start

To install the Cloud Integrity Technology Quick Start:

1. Copy the CIT Quick Start installer to the target system `CIT_QUICKSTART_HOST`

## User Guide

### Cloud Integrity Technology Quick Start

2. Run the installer
3. Browse to `https://CIT_QUICKSTART_HOST`

## Installation

The Deployment Wizard server is packaged as a Linux self-extracting executable.

### Standard

A standard installation of the Cloud Integrity Technology Deployment Wizard does not require any configuration. The software will be installed in `/opt/cit` and the server will be available on standard http port 80 and https port 443 by default. Simply run the executable and enter the server's IP address or hostname into a browser window to access the deployment tool.

Example output from a successful installation:

```
Verifying archive integrity... All good.
Uncompressing cit-quickstart-linux-3.0-SNAPSHOT.....
Installing Cloud Integrity Technology (R)...
=====>100%
http://198.51.100.18
```

Example output from a failed installation:

```
Verifying archive integrity... All good.
Uncompressing cit-quickstart-linux-3.0-SNAPSHOT.....
Installing Cloud Integrity Technology (R)...
=====>23%
Installation failed; log file is at /tmp/cit/monitor/install-quickstart/stdout
```

## Custom (Optional)

The following environment variables can be exported or defined in `~/cit.env` before installation in order to customize the installation:

**Table 1** Environment variables to customize installation

Name	Default	Notes
CIT_HOME	/opt/cit	Directory path. Directory where bin, configuration, env, logs, and repository are going to be installed.
CIT_USERNAME	cit	Linux username. The non-root user to run the quick start server
CIT_CONFIGURATION	CIT_HOME/configuration	Directory path. Alternate location: /etc/cit
CIT_REPOSITORY	CIT_HOME/repository	Directory path. Alternate location: /var/opt/cit
CIT_LOGS	CIT_HOME/logs	Directory path. Alternate location: /var/log/cit
CIT_BIN	CIT_HOME/bin	Directory path. Executable scripts and binaries are stored here
CIT_JAVA	CIT_HOME/java	Directory path. Application Java libraries are stored here
CIT_PID_FILE	CIT_LOGS/cit.pid	File path. Alternate location: /var/run/cit.pid
CIT_LOG_LEVEL	INFO	Possible values: DEBUG, INFO, WARN, ERROR. Set to DEBUG to write more details into log; set to WARN or ERROR to write less to the log
JAVA_REQUIRED_VERSION	1.7	Java version. Sets the minimum required Java version for using a pre-installed Java runtime; if one is not found the installer will install this Java version which is included
JETTY_PORT	80	Port number. The server's http port
JETTY_SECURE_PORT	443	Port number. The server's https port
MTWILSON_EXTENSIONS_FILEINCLUDEFILTER_CONTAINS	mtwilson,cit,jersey-media-multipart	Format is comma-separated without spaces. Controls which Jar files are scanned for auto-detecting extensions. Jar files in CIT_JAVA that contain any of



User Guide  
**Cloud Integrity Technology Quick Start**

		these terms in the filename will be included.
MTWILSON_EXTENSIONS_PACKAGEINCLUDEFILTER_STARTSWITH	com.intel,org.glassfish.jersey.media.multipart	Format is comma-separated without spaces. Controls which Java packages are scanned for auto-detecting extensions. Within scanned jar files, Java packages that start with any of these terms will be included.
CIT_NOSETUP	N/A	Undefined, empty, or any value. Normally is not defined; set to any non-empty value such as "1" or "true" to skip generating master password, configuring the application, and running setup tasks during installation.

If present, the `cit.env` file is "sourced" by the shell so it can use any available shell variables and expressions in order to define the variables described in the above table.

Here is an example `/root/cit.env` file:

```
CIT_HOME=/opt/cit
CIT_CONFIGURATION=/etc/opt/cit
CIT_REPOSITORY=/var/opt/cit
CIT_LOGS=/var/log/cit
CIT_PID_FILE=/var/run/cit/cit.pid
```

## Upgrade

To upgrade the Deployment Wizard server, simply run the new installer on a host with an existing installation. If the original installation was customized using the `cit.env` file, that file does not need to be present when upgrading. Customizations such as directory layout will be detected from the existing installation. An upgrade should not be used to change directory layouts - data will not be migrated.

To upgrade individual components deployed by the Deployment Wizard server, find the component installer under `CIT_HOME/repository/packages` and replace it with the new installer.

Note that upgrading the CIT Deployment Wizard does not upgrade any CIT components installed by the wizard.

## Uninstallation

NOTE: the uninstallation procedure removes the Deployment Wizard server, **not** any deployed components.

There are two modes of uninstallation. The first mode ("uninstall") leaves configuration, logs, and data intact. The second mode ("uninstall --purge") completely removes the application and all its configuration, logs, and data.

Run the uninstall command that preserves configuration, logs, and data:

```
cit uninstall
```

Run the uninstall command that also removes configuration, logs, and data:

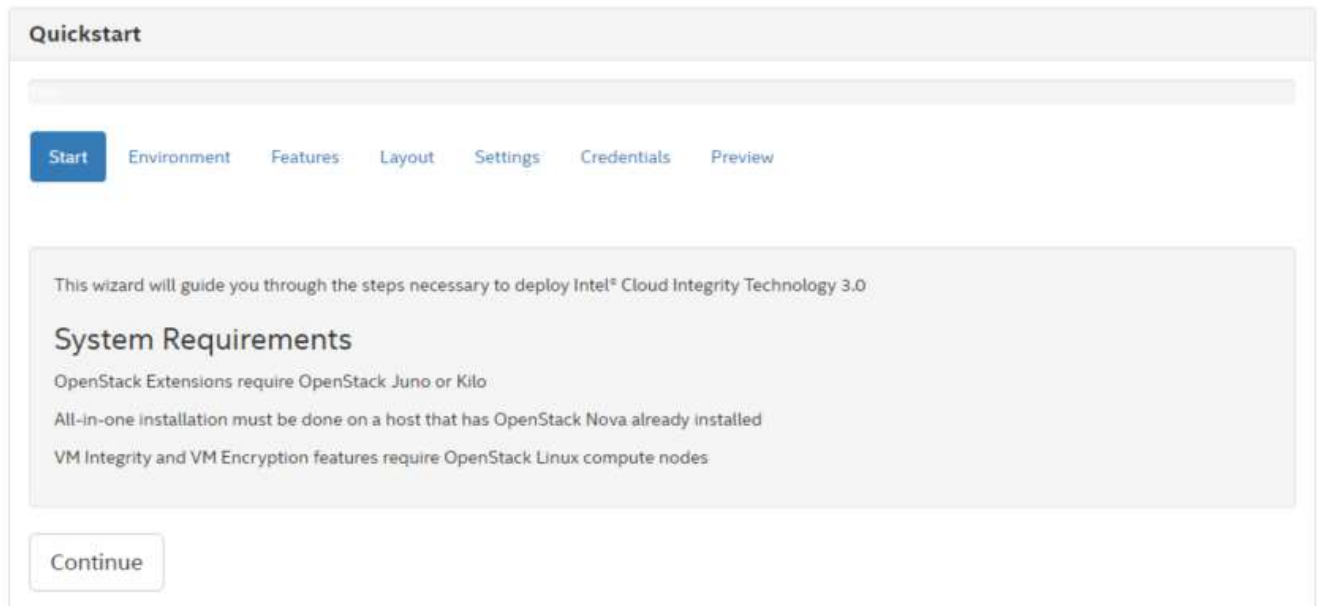
```
cit uninstall --purge
```

## Browser

This section describes the browser user interface in detail. Each section describes one screen and may have one or more screenshots as a visual aid. Actual screens may differ from the screenshots shown here as we continuously improve the software.

### Start

The start screen is an introductory screen that may include some release notes and system requirements for this version of Cloud Integrity Technology.



User Guide  
**Cloud Integrity Technology Quick Start**

## Environment

The environment screen presents a choice that affects which components of Cloud Integrity Technology will be installed and which configuration settings will be required. In a private network, all components will be installed and minimal configuration will be required. In a cloud service provider, all components except the Key Broker will be installed and minimal configuration will be required. In an enterprise, only Trust Director and Key Broker will be installed, and configuration settings will be required to connect to the Cloud Service Provider's OpenStack image service (Glance) and Attestation Service.

The default selection requires the least amount of configuration.

The screenshot shows the 'Quickstart' interface for the Cloud Integrity Technology installation. At the top, a green bar indicates 'Step 1 of 6'. Below this, a horizontal navigation bar contains seven tabs: 'Start', 'Environment' (which is highlighted with a blue background), 'Features', 'Layout', 'Settings', 'Credentials', and 'Preview'. The main content area displays three radio button options for the deployment environment:

- ☒ **Private Network (Enterprise or Datacenter)**  
All components will be installed for an stand-alone deployment
- ☐ **Cloud Service Provider**  
Installs Intel® Cloud Integrity Technology attestation server, Trust Director (for host attestation), OpenStack integration (if applicable), Key Broker Proxy (if applicable)
- ☐ **Enterprise**  
Installs Trust Director (for workload attestation), Key Broker (if applicable)

At the bottom of the form is a 'Continue' button.

## Features - Private Network (Enterprise or Datacenter)

The features screen presents a choice that affects which components will be installed and which configuration settings will be required. The items available in the features screen depend on the choice made in the environment screen. In a private network, all features are available.

The default selections require the least amount of configuration.

The “Private Network” selection will install all CIT components automatically. This is intended for a private cloud datacenter, as opposed to a Cloud Service Provider with one or more Enterprise Customers.

**Quickstart**

Step 2 of 6

Start Environment **Features** Layout Settings Credentials Preview

**Attestation**

- ☒ Host BIOS, kernel, hypervisor  
Verifies Linux KVM, Xen, or VMware® ESXi hypervisor. Verifies asset tags
- ☒ Host operating system, applications, drivers, configuration  
Additional verification for static files such as executables, libraries, and configuration

**Workload Protection**

- ☒ VM integrity  
Measure and enforce trust policy for VMs before launching on a trusted host
- ☐ VM encryption  
Encrypted workloads run only on trusted hosts
- ☐ Container integrity (Docker)  
Measure and enforce trust policy for containers before launching via Docker Engine on a trusted host

**Integrations**

- ☒ OpenStack Nova & Horizon  
Nova trust scheduler and patches to Horizon to expose trust in dashboard
- ☒ OpenStack Glance  
Nova trust scheduler and patches to Horizon to expose trust in dashboard

Continue

## Features - Cloud Service Provider

The features screen presents a choice that affects which components will be installed and which configuration settings will be required. The items available in the features screen depend on the choice made in the environment screen. In a cloud service provider, Key Broker related features are omitted such as integration with OpenStack Barbican or a KMIP-enabled key server.

See the Cloud Integrity Technology Component Architecture diagram to see which components are part of a Cloud Service Provider deployment.

The default selections require the least amount of configuration.

The screenshot shows the 'Quickstart' interface, specifically the 'Features' step (Step 2 of 6). The navigation bar includes 'Start', 'Environment', 'Features' (highlighted), 'Layout', 'Settings', 'Credentials', and 'Preview'. The main content area is divided into three sections: 'Attestation', 'Workload Protection', and 'Integrations'. Each section contains a list of features with checkboxes and descriptive text.

**Quickstart**

Step 2 of 6

Start Environment **Features** Layout Settings Credentials Preview

**Attestation**

- ☒ Host BIOS, kernel, hypervisor  
Verifies Linux KVM, Xen, or VMware® ESXi hypervisor. Verifies asset tags
- ☒ Host operating system, applications, drivers, configuration  
Additional verification for static files such as executables, libraries, and configuration

**Workload Protection**

- ☒ VM integrity  
Measure and enforce trust policy for VMs before launching on a trusted host
- ☐ VM encryption  
Encrypted workloads run only on trusted hosts
- ☐ Container integrity (Docker)  
Measure and enforce trust policy for containers before launching via Docker Engine on a trusted host

**Integrations**

- ☒ OpenStack Nova & Horizon  
Nova trust scheduler and patches to Horizon to expose trust in dashboard
- ☒ OpenStack Glance  
Nova trust scheduler and patches to Horizon to expose trust in dashboard

Continue

## **Features - Private Network (Enterprise or Datacenter)**

The features screen presents a choice that affects which components will be installed and which configuration settings will be required. The items available in the features screen depend on the choice made in the environment screen.

In an enterprise network, workload protection and various integration features are available. No Enterprise Customer deployment is needed if only Platform Attestation will be provided (all components needed for this are on the Cloud Service Provider side).

All selections will require some configuration because the enterprise installation is not a stand-alone installation and is intended to integrate with a cloud service provider's offering. To install all components locally with minimal configuration, choose the private network option in the environment screen.

Note that the Key Broker Server will not be installed if VM Encryption is not selected. If the VM Encryption will be selected for deployment, an existing KMIP or Barbican key management service must be installed and available before running the Enterprise Customer deployment.

For Barbican deployments, you will need the following information:

- Barbican ID
- Barbican URL
- Keystone URL
- Username
- Password
- Barbican Tenant Name

For KMIP deployments, you will need the following information:

- KMIP Server URL

See the Cloud Integrity Technology Component Architecture diagram to see which components are part of an Enterprise Customer deployment.

The following information will need to be provided by your Cloud Service Provider before installing the Enterprise Customer components:

**Attestation Service Info:**

- Host Name or IP Address
- Port Number
- TLS Certificate SHA-1 Fingerprint
- Username: *(Attestation Server user created by CSP)*
- Password: *(Attestation Server user password created by CSP)*

User Guide  
**Cloud Integrity Technology Quick Start**

OpenStack Glance Integration:

- Glance Server URL
- Keystone Server URL
- Glance Username (*User created by CSP*)
- Glance Password (*User password created by CSP*)
- OpenStack Tenant Name (*Tenant name created by CSP*)

**Quickstart**

Step 2 of 6

[Start](#) [Environment](#) **[Features](#)** [Layout](#) [Settings](#) [Credentials](#) [Preview](#)

**Attestation**

- ☒ **Host BIOS, kernel, hypervisor**  
Verifies Linux KVM, Xen, or VMware® ESXi hypervisor. Verifies asset tags
- ☒ **Host operating system, applications, drivers, configuration**  
Additional verification for static files such as executables, libraries, and configuration

**Workload Protection**

- ☒ **VM integrity**  
Measure and enforce trust policy for VMs before launching on a trusted host
- ☐ **VM encryption**  
Encrypted workloads run only on trusted hosts
- ☐ **Container integrity (Docker)**  
Measure and enforce trust policy for containers before launching via Docker Engine on a trusted host

**Integrations**

- ☒ **OpenStack Nova & Horizon**  
Nova trust scheduler and patches to Horizon to expose trust in dashboard
- ☒ **OpenStack Glance**  
Nova trust scheduler and patches to Horizon to expose trust in dashboard

Continue



## Layout

The layout screen presents a choice that will affect which configuration settings and login credentials will be required.

An “all-in-one” installation will result in all software components being installed in the same host, so only one host address and root password will be required in the credentials screen.

A “one package per remote host” installation will result in each software component being installed in a separate host, so the credentials screen will require multiple host addresses and root passwords.

The default selection requires the least amount of configuration.

**Quickstart**

Step 3 of 6

Start Environment Features **Layout** Settings Credentials Preview

Choose how to deploy the software:

**Preset Layouts**

- ☒ All-in-one, remote host  
All components will be installed on a single host or VM. This is the simplest option, but not recommended for production.
- ☐ One package per remote host  
Each component will be installed on a separate host or VM.

**Layout Options**

- ☐ OpenStack Glance installed separately  
Configure Trust Director to use an existing OpenStack Glance.

Continue

## Settings - Private Network, VM Integrity, All-in-one

The settings screen presents required and optional settings that affect the configuration of the deployed software components. Selections made in the environment, features, and layout screens affect which settings are required or optional.

Quickstart

Step 4 of 6

[Start](#) [Environment](#) [Features](#) [Layout](#) [Settings](#) [Credentials](#) [Preview](#)

Attestation

**Attestation Service Cache Duration**

15 min ▾

Controls how often host attestations must be refreshed

Continue

User Guide  
Cloud Integrity Technology Quick Start

## Settings - Private Network, VM Encryption with Barbican, All-in-one

The settings screen presents required and optional settings that affect the configuration of the deployed software components. Selections made in the environment, features, and layout screens affect which settings are required or optional.

Note: this is the same as just VM Integrity, because OpenStack Barbican is setup automatically on the OpenStack host.

**Quickstart**

Step 4 of 6

Start Environment Features Layout **Settings** Credentials Preview

**Attestation**

**Attestation Service Cache Duration**

15 min ▾

Controls how often host attestations must be refreshed

**Key Server: OpenStack Barbican Integration**

**Barbican Project ID**

Example: 12345

**Barbican Server URL**

Example: http://openstack.example.com:9311

**Keystone Server URL**

Example: http://keystone.example.com:5000

**Username**

**Password**

**Barbican Tenant Name**

Continue

## Settings - Private Network, VM Encryption with KMIP, All-in-one

The settings screen presents required and optional settings that affect the configuration of the deployed software components. Selections made in the environment, features, and layout screens affect which settings are required or optional.

The all-in-one layout applies to CIT 3.2 components, and the URL to the KMIP interface of the key server must be entered in this page.

The screenshot shows a 'Quickstart' wizard interface. At the top, a green progress bar indicates 'Step 4 of 6'. Below the progress bar is a navigation menu with tabs: 'Start', 'Environment', 'Features', 'Layout', 'Settings' (which is highlighted in blue), 'Credentials', and 'Preview'. The main content area is divided into two sections. The first section, titled 'Attestation', contains a setting for 'Attestation Service Cache Duration' with a dropdown menu set to '15 min' and a description: 'Controls how often host attestations must be refreshed'. The second section, titled 'Key Server: KMIP Integration', contains a setting for 'KMIP Server URL' with a text input field. Below the input field is an example URL: 'https://kmip4j.example.com:8443/KMIPWebAppServer/KMIPServlet'. At the bottom of the form is a 'Continue' button.

**Quickstart**

Step 4 of 6

Start Environment Features Layout **Settings** Credentials Preview

**Attestation**

**Attestation Service Cache Duration**

15 min ▼

Controls how often host attestations must be refreshed

**Key Server: KMIP Integration**

**KMIP Server URL**

Example for a KMIP4J server:  
https://kmip4j.example.com:8443/KMIPWebAppServer/KMIPServlet

Continue

## Credentials - Private Network, VM Integrity, All-in-one

The credentials screen is the final configuration step for the Cloud Integrity Technology deployment. Selections made in the environment, features, and layout screens affect how many credentials are required here.

Each host for which credentials are required is shown in a separate box. When a hostname or IP address is entered, the host's SSH public key is retrieved and displayed in the "Host check" area. If the host cannot be reached an error message will be shown. The SSH public key must be accepted in order to enter the SSH password for the host. When a password is entered, the password will be verified. This verification ensures that the deployment tool will be able to access all designated hosts when deploying the software.

Note that even when deploying to localhost, the root password will be required. This is because the deployment tool itself does not run as root, but in order to install the software components root access is required. So when deploying to localhost the deployment tool still uses SSH to login as root and install the software.

The screenshot shows the 'Quickstart' interface at 'Step 5 of 6'. The navigation bar includes 'Start', 'Environment', 'Features', 'Layout', 'Settings', 'Credentials' (highlighted), and 'Preview'. The main content area is titled 'Enter the address or hostname of each host where software will be installed:'. It features an 'Edit Host' section with a 'Hostname or IP address' input field and a 'Check' button. Below this, a list of services is shown: 'Attestation Service, Trust Director, OpenStack Extensions'. At the bottom of the host configuration area is a '+ Add compute node' button. A 'Continue' button is located at the bottom of the screen.

## Preview - Private Network, VM Integrity, All-in-one

The preview screen summarizes the deployment choices and shows what software packages will be installed on each host. No action will be taken until the “Start” button is clicked.

### Quickstart

Step 6 of 6

[Start](#) [Environment](#) [Features](#) [Layout](#) [Settings](#) [Credentials](#) [Preview](#)

#### Environment

- ☐ Private Network (Enterprise or Datacenter)  
All components will be installed for an stand-alone deployment

#### Layout

- ☐ All-in-one, remote host  
All components will be installed on a single host or VM. This is the simplest option, but not recommended for production.

#### Features

##### Attestation

- ☒ Host BIOS, kernel, initrd, hypervisor
- ☒ Host apps, drivers, configuration

##### Workload Protection

- ☒ VM integrity

##### Integrations

- ☒ OpenStack Nova & Horizon
- ☒ OpenStack Glance

Host	Software
cit.example.com	Attestation Service, Trust Director, OpenStack Extensions

[Start](#)

## Deploying

The deploying screen shows a progress bar and a summary of what software will be installed on each host.



Quickstart

15%

### Deploying Intel® Cloud Integrity Technology 3.0...

Host	Software
cit.example.com	<input type="checkbox"/> Attestation Service <input type="checkbox"/> OpenStack Extensions <input type="checkbox"/> Trust Director

[Show/Hide detailed progress](#)

Cancel

## Summary

The summary screen shows a list of the hosts included in the deployment. For each host there is a check list of the software installed and any necessary access information such as URL, username, and password.

For OpenStack Extensions, the Horizon URL and login credentials are shown.

For Trust Agent, the checkmark will not appear. The Trust Agent installer and trustagent.env file are copied to the host but the installer is not run automatically. The administrator must complete the Trust Agent installation by following the directions in the Trust Agent section of the Cloud Integrity Technology User Guide. However, the trustagent.env file that is copied to the host by the deployment tool contains the necessary information for that procedure.

User Guide  
Cloud Integrity Technology Quick Start

Quickstart

100%

## Intel® Cloud Integrity Technology 3.0

Host	Software
10.1.68.31	<input checked="" type="checkbox"/> Key Broker Proxy
10.1.68.34	<input checked="" type="checkbox"/> Key Broker <a href="https://10.1.68.34:443">https://10.1.68.34:443</a> Username: <input type="text" value="admin"/> Password: <input type="text" value="Ouw7rKz+hN7Z6KrsT2igjA"/>
10.1.68.31	<input checked="" type="checkbox"/> OpenStack Extensions <a href="http://10.1.68.31/horizon">http://10.1.68.31/horizon</a> Username: <input type="text" value="cit-admin"/> Password: <input type="text" value="bQFOzLhMjbZ366KKyf8URQ"/>
10.1.68.31	<input checked="" type="checkbox"/> Attestation Service <a href="https://10.1.68.31:8443/mtwilson-portal">https://10.1.68.31:8443/mtwilson-portal</a> Username: <input type="text" value="admin"/> Password: <input type="text" value="UHGboqJ6cz+VVVmGV5jFw"/>
10.1.68.34	<input checked="" type="checkbox"/> Trust Director <a href="https://10.1.68.34:443">https://10.1.68.34:443</a> Username: <input type="text" value="admin"/> Password: <input type="text" value="3xR5ROsb+Y2vccmMlcK3sA"/>
10.1.71.180	<input type="checkbox"/> Trust Agent

[Show/Hide detailed progress](#)

Start Again



User Guide

## Cloud Integrity Technology Quick Start

As each software component is installed, the box next to it is checked. Note that there may be some configuration steps after all software has been installed, so it's possible for all boxes to be checked before the progress bar reaches 100%.

**Quickstart**

85%

### Deploying Intel® Cloud Integrity Technology 3.0...

Host	Software
cit.example.com	<input checked="" type="checkbox"/> Attestation Service
	<input checked="" type="checkbox"/> OpenStack Extensions
	<input type="checkbox"/> Trust Director

[Show/Hide detailed progress](#)

Cancel

User Guide  
**Cloud Integrity Technology Quick Start**

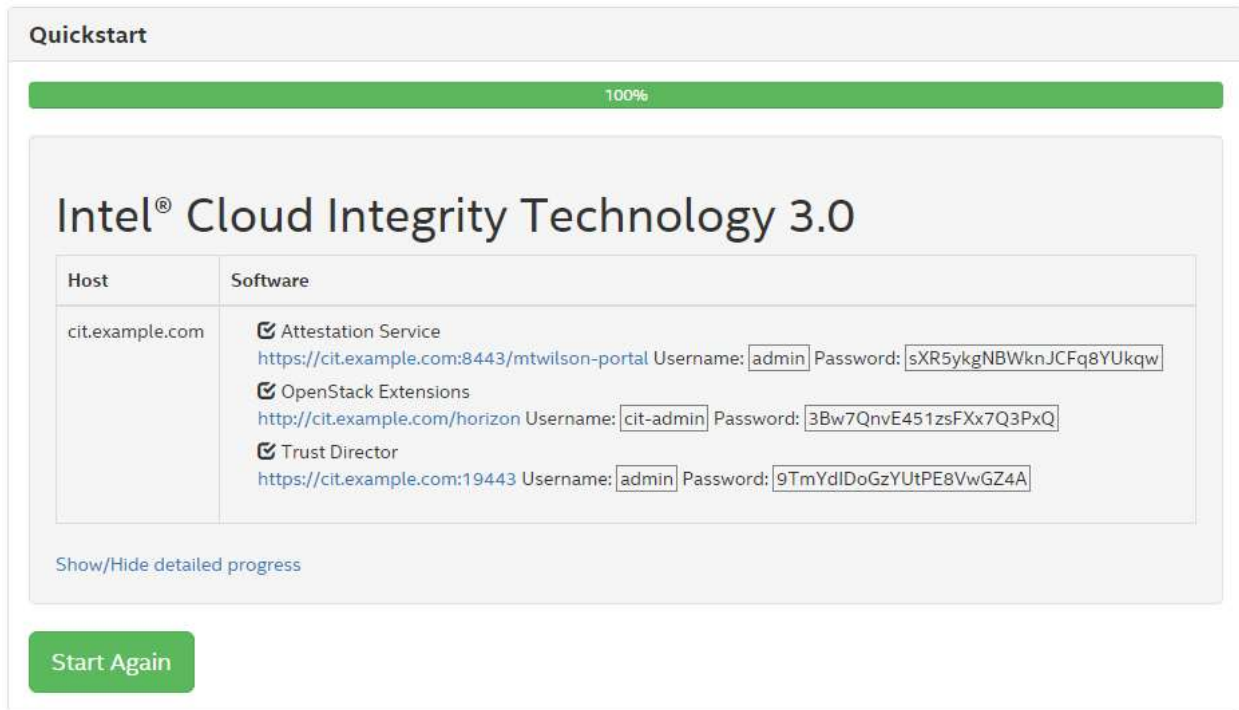
View a more detailed progress report including configuration steps by clicking “Show/Hide detailed progress”.

Installing OpenStack Extensions on cit.example.com	<div><div></div></div>
Finishing OpenStack configuration on cit.example.com	<div><div></div></div>
Creating Trust Director credential in OpenStack on cit.example.com	<div><div></div></div>
Synchronizing OpenStack Extensions	<div><div></div></div>
Copying director-0.1-SNAPSHOT.bin, director-0.1-SNAPSHOT.bin.mark, monitor.sh to cit.example.com	<div><div></div></div>
Configuring Trust Director on cit.example.com	<div><div></div></div>
Copying director.env to cit.example.com	<div><div></div></div>
Installing Trust Director on cit.example.com	<div><div></div></div>
Finishing Trust Director configuration on cit.example.com	<div><div></div></div>
Synchronizing Trust Director	<div><div></div></div>

## User Guide

### Cloud Integrity Technology Quick Start

When installation is complete, the deploying screen will show URLs and login credentials for each installed service that has a browser interface. This information should be saved before clicking the “Start Again” button or closing the quick start browser window.

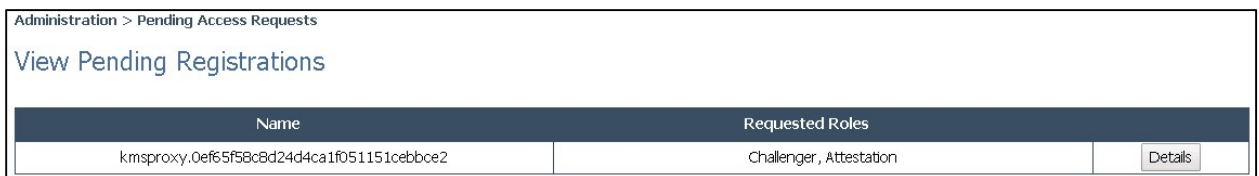


After the setup is complete, (Applies to CSP, Private Cloud options) you should do the following steps:

1. Approve and assign the roles/permissions for the Key Broker Proxy user in the Attestation server

After the setup is complete, (Applies to CSP, Private Cloud options) you should do the following steps:

- a. Navigate to the “Pending Requests” page by clicking on the “Administration” folder tab, then click the “Details” button.



- b. Approve the user “kmsproxy.xxxx” and check the boxes marked in yellow to assign the roles “Attestation” and “Challenger” roles

## User Guide

### Cloud Integrity Technology Quick Start

Administration > Pending Access Requests

### View Pending Registrations

Name: kmsproxy.0ef65f58c8d24d4ca1f051151cebbce2

Fingerprint: db1e0da7e73315a3a21b22c3820e0401d754eb6cc66eb6c4fe7f739f941f0ef8

Issuer: C=US,O=Trusted Data Center,OU=Mt Wilson,CN=kmsproxy.0ef65f58c8d24d4ca

Requested Roles: ?

Roles requested by the user are highlighted.

Mt Wilson 1.x roles for backward compatibility:

☐ Security ☐ Whitelist ☒ Attestation ☐ Report ☐ Audit ☐ AssetTagManagement

Mt Wilson 2.x roles:

☐ Administrator ☐ AssetTagManager ☐ Auditor ☒ Challenger ☐ HostManager ☐ ReportManager ☐ ServerManager ☐ UserManager ☐ WhitelistManager ☐ TlsPolicyManager

Expires: 2026-02-20T03:15:19.000Z

Comments:

Approve Reject

kmsproxy.0ef65f58c8d24d4ca1f051151cebbce2

db1e0da7e73315a3a21b22c3820e0401d754eb6cc66eb6c4fe7f739f941f0ef8

C=US,O=Trusted Data Center,OU=Mt Wilson,CN=kmsproxy.0ef65f58c8d24d4ca

Roles requested by the user are highlighted.

Mt Wilson 1.x roles for backward compatibility:

☐ Security ☐ Whitelist ☒ Attestation ☐ Report ☐ Audit ☐ AssetTagManagement

Mt Wilson 2.x roles:

☐ Administrator ☐ AssetTagManager ☐ Auditor ☒ Challenger ☐ HostManager ☐ ReportManager ☐ ServerManager ☐ UserManager ☐ WhitelistManager ☐ TlsPolicyManager

2. Import the data bundle (certificates of the Attestation server) to Key Broker
  - Log into the Key Broker Portal
  - Select **Settings**
  - Select **Upload Settings**

## User Guide

### Cloud Integrity Technology Quick Start

**Upload Configuration Data Bundle**

Choose a data bundle from your computer and submit this form to upload it to the server and import the data.

**Data Bundle**

No file chosen

Once you have completed the steps above, refer to the Product Guide for use and operations of CIT 3.2.