User Guide

for

Intel Cloud Integrity Technology 3.0

**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 4](#_Toc442707135)

[Introduction 5](#_Toc442707136)

[Purpose 5](#_Toc442707137)

[Definitions, Acronyms, Abbreviations 5](#_Toc442707138)

[Acronyms 5](#_Toc442707139)

[References 5](#_Toc442707140)

[Overview 5](#_Toc442707141)

[Installation 5](#_Toc442707142)

[Standard 6](#_Toc442707143)

[Custom 6](#_Toc442707144)

[Upgrade 8](#_Toc442707145)

[Uninstallation 8](#_Toc442707146)

[Teletype 8](#_Toc442707147)

[Browser 10](#_Toc442707148)

[Start 10](#_Toc442707149)

[Environment 11](#_Toc442707150)

[Features - Private Network 12](#_Toc442707151)

[Features - Cloud Service Provider 13](#_Toc442707152)

[Features - Enterprise 14](#_Toc442707153)

[Layout 15](#_Toc442707154)

[Settings - Private Network, VM Integrity, All-in-one 16](#_Toc442707155)

[Settings - Private Network, VM Encryption with Barbican, All-in-one 17](#_Toc442707156)

[Settings - Private Network, VM Encryption with KMIP, All-in-one 18](#_Toc442707157)

[Credentials - Private Network, VM Integrity, All-in-one 19](#_Toc442707158)

[Preview - Private Network, VM Integrity, All-in-one 21](#_Toc442707159)

[Deploying 22](#_Toc442707160)

[Summary 22](#_Toc442707161)

# Quick Start

To install the Cloud Integrity Technology Quick Start:

1. Copy the installer cit-quickstart-3.0.bin to the target system CIT\_QUICKSTART\_HOST
2. Run the installer ./cit-quickstart-3.0.bin
3. Browse to https://CIT\_QUICKSTART\_HOST

# Introduction

This document contains the user guide for the Cloud Integrity Technology 3.0 Quick Start server.

## 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 3.0 User Guide

## Overview

The user guide is organized into sections covering installation and operation. The operation sections cover teletype (SSH or virtual console) and browser (web) interfaces.

# Installation

The quick start server is packaged as a Linux self-extracting executable.

## Standard

A standard installation of the Cloud Integrity Technology Quick Start 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

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

Table 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 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 quick start 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 quick start server, find the component installer under CIT\_HOME/repository/packages and replace it with the new installer.

## Uninstallation

NOTE: the uninstallation procedure removes the Quick Start 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

# Teletype

How to initiate a deployment using the command line:

1. Prepare a JSON-format file in a world-readable location such as /tmp/order.json containing the deployment specification
2. Run the command:

cit deploy --json=/tmp/order.json

NOTE: the /root home directory is generally not world-readable, so running cit deploy --json=/root/order.json will result in a “File not found” message because the cit user cannot read files in the /root directory.

Example content of /tmp/order.json:

{

"features": [

"attestation\_host"

],

"network\_role": "PRIVATE",

"targets": [

{

"host": "198.51.100.77",

"port": 22,

"username": "root",

"password": "\*\*\*\*\*\*\*\*",

"public\_key\_digest": "22952a72e24194f208200e76fd3900da",

"packages": [

"attestation\_service"

]

}

]

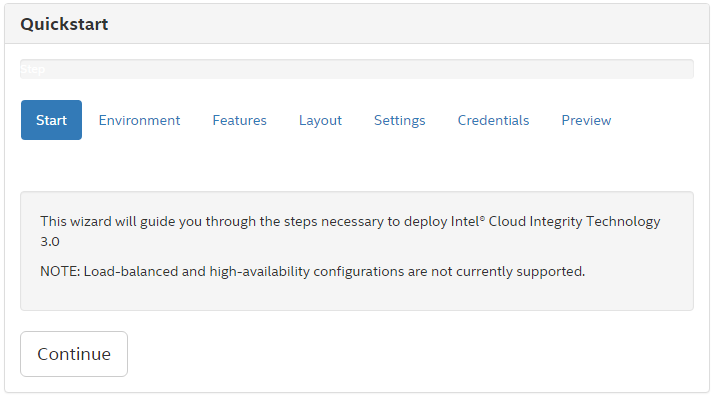
}

# 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

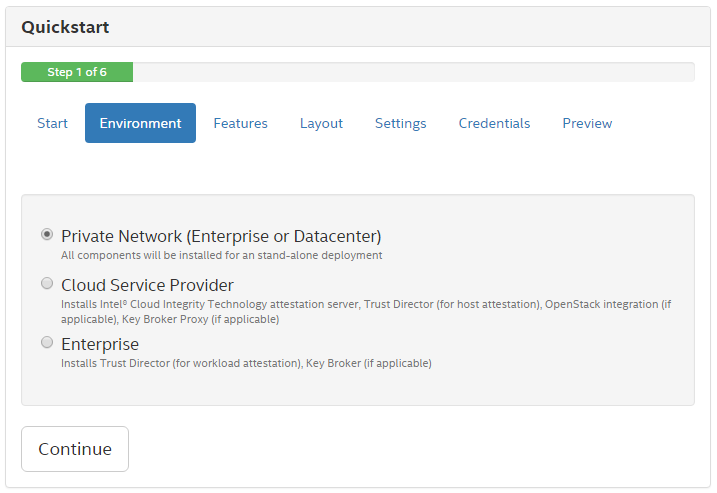
The start screen is an introductory screen that may include some release notes and system requirements for this version of Cloud Integrity Technology.



## 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.

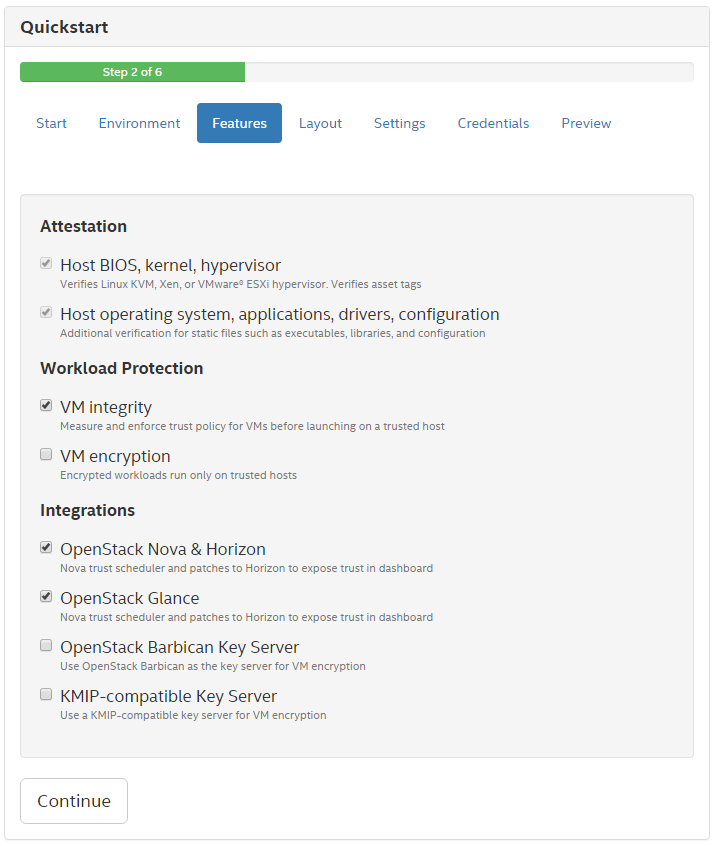
The default selection requires the least amount of configuration.



## Features - Private Network

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.

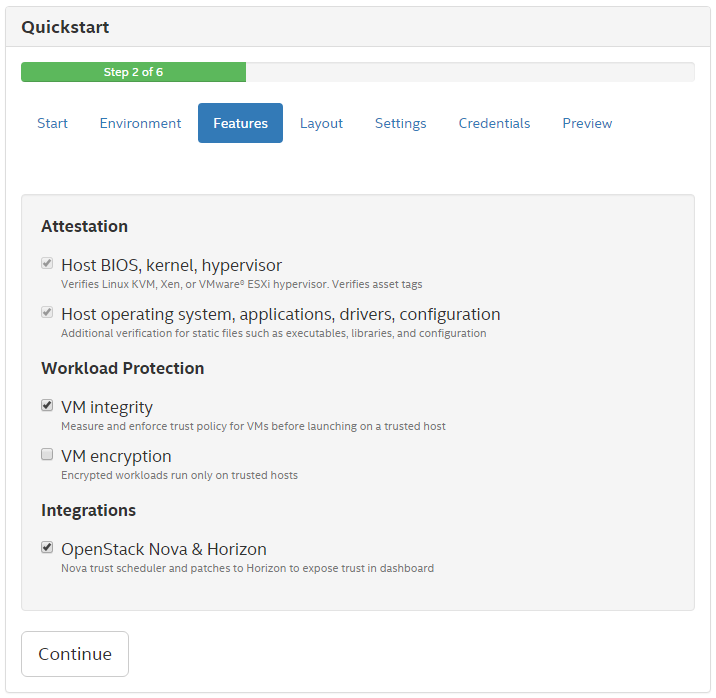
The default selections require the least amount of configuration.



## 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.

The default selections require the least amount of configuration.

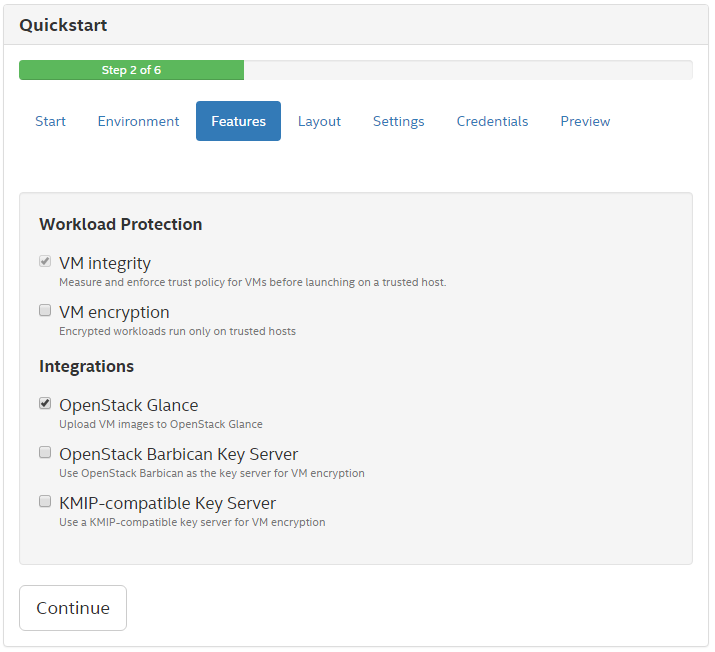


## Features - Enterprise

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.

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.



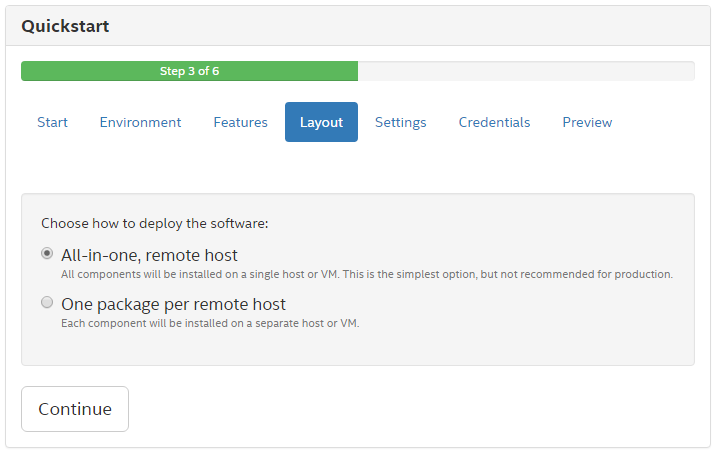
## Layout

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.

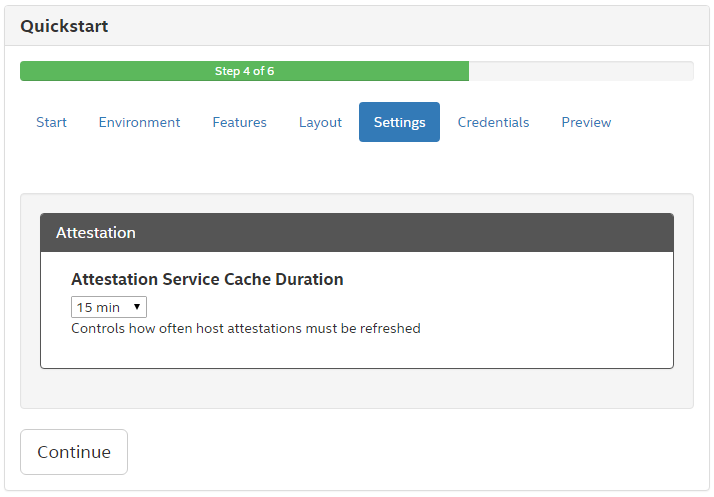
A “one package per remote host” installation will result in each software component being installed in a separate host, so the credentials screen will require multiple host addresses and root passwords.

The default selection requires the least amount of configuration.



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

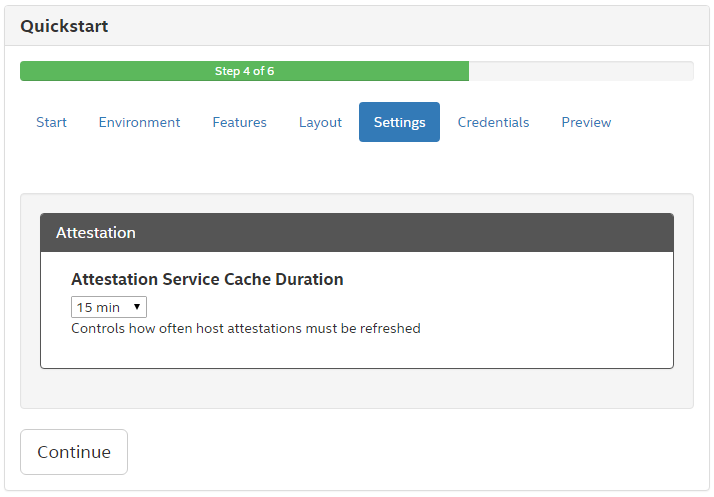
The settings screen presents required and optional settings that affect the configuration of the deployed software components. Selections made in the environment, features, and layout screens affect which settings are required or optional.



## 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.

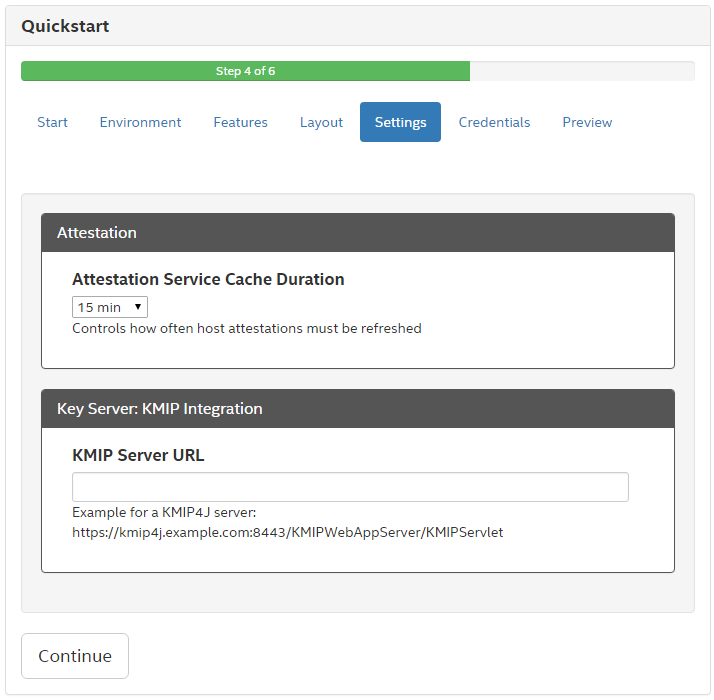
Note: this is the same as just VM Integrity, because OpenStack Barbican is setup automatically on the OpenStack host.



## 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 3.0 components, and the URL to the KMIP interface of the key server must be entered in this page.

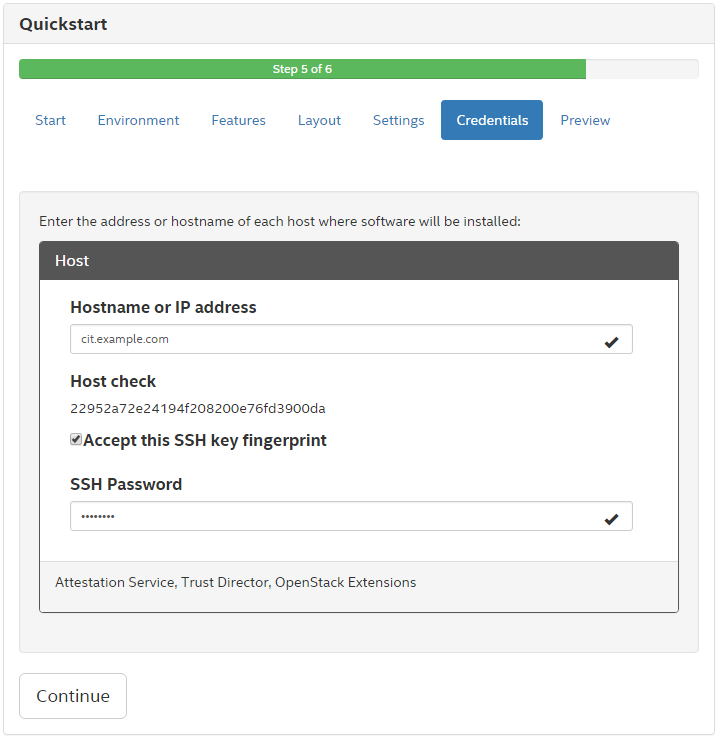


## Credentials - Private Network, VM Integrity, All-in-one

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.

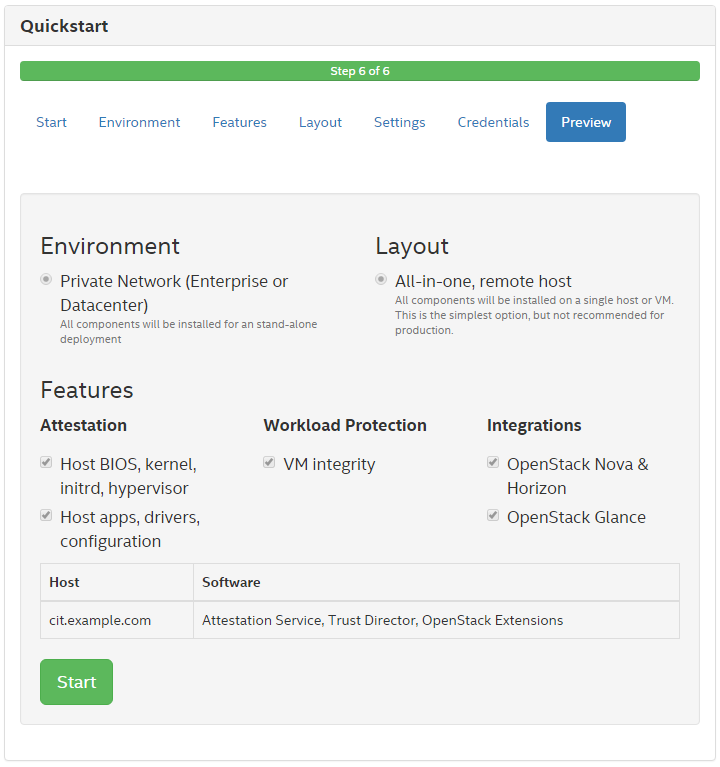
Each host for which credentials are required is shown in a separate box. When a hostname or IP address is entered, the host’s SSH public key is retrieved and displayed in the “Host check” area. If the host cannot be reached an error message will be shown. The SSH public key must be accepted in order 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.



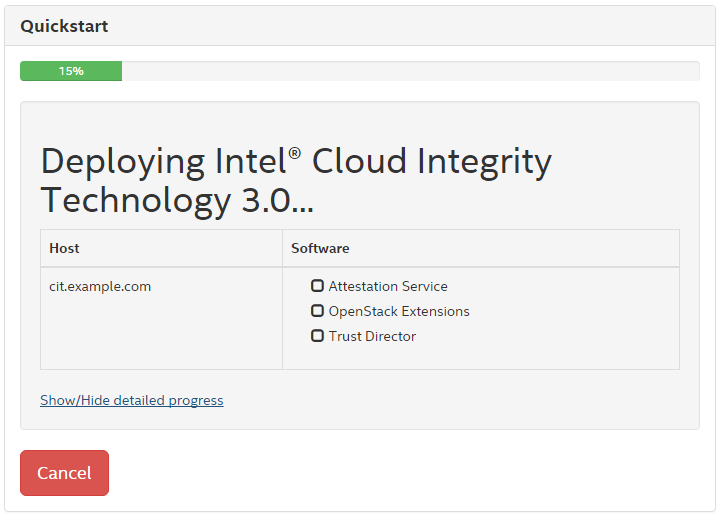
## Preview - Private Network, VM Integrity, All-in-one

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.



## Deploying

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



## Summary

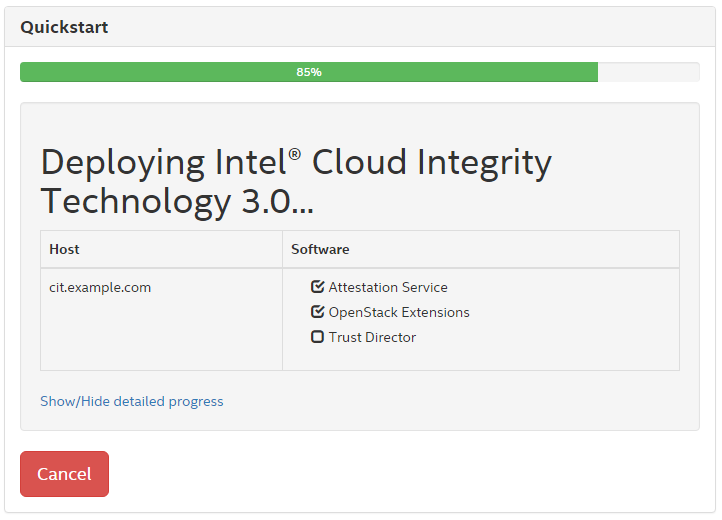
The summary screen shows a list of the hosts included in the deployment. For each host there is a check list of the software installed and any necessary access information such as URL, username, and password.

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

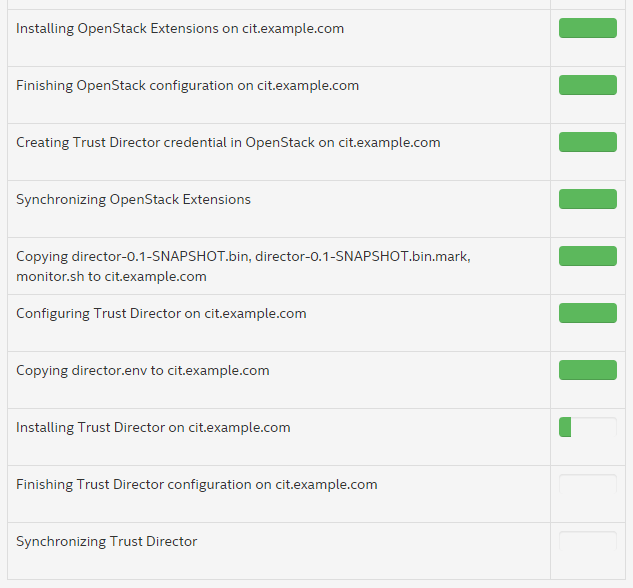
For Trust Agent, the checkmark will not appear. The Trust Agent installer and trustagent.env file are copied to the host but the installer is not run automatically. The administrator must complete the Trust Agent installation by following the directions in the Trust Agent section of the Cloud Integrity 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.



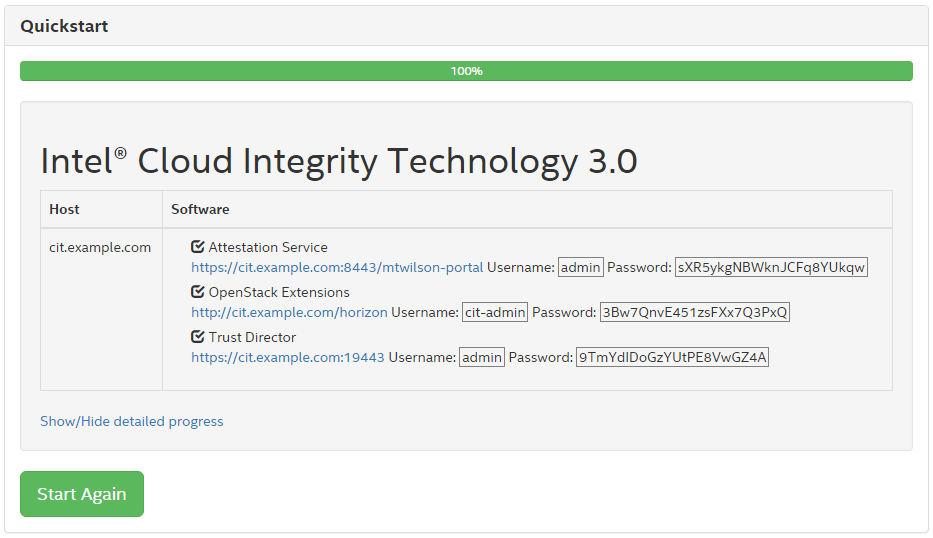
As each software component is installed, the box next to it is checked. Note that there may be some configuration steps after all software has been installed, so it’s possible for all boxes to be checked before the progress bar reaches 100%.



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



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.



# Errors

## CertificateNotYetValidException

You may see a message like this in the log, for example when attempting to import Attestation Service certificates into Key Broker:

[2016-04-27 15:56:46,466] 1107594 [pool-1-thread-1] ERROR c.i.mtwilson.util.task.AbstractTask - Execution failed

javax.ws.rs.ProcessingException: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: Server certificate is invalid: CN=Key Server: java.security.cert.CertificateNotYetValidException: NotBefore: Wed Apr 27 15:57:09 PDT 2016

Note the timestamps on the two lines: the first timestamp 15:56:46 shows the current time on the Quickstart server, the second timestamp 15:57:09 shows the not-before date on the remote certificate (in this case, it was the Key Broker SSL certificate). Because the SSL certificate in question was probably created earlier in the process, this indicates the system clocks are not in sync on the two systems.

To resolve this error, synchronize the clocks among the Quickstart server and all the deployment target hosts.