



# **CLOUD COLLECTOR**

## **INSTALLATION GUIDE**

**WITH MANAGED COMMUNICATIONS BROKER**

FireEye and the FireEye logo are registered trademarks of FireEye, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

FireEye assumes no responsibility for any inaccuracies in this document. FireEye reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Copyright © 2020 FireEye, Inc. All rights reserved.

This product is part of the Helix platform.

Cloud Collector Installation Guide

Software Release 2.4.17

Revision 1

**FireEye Contact Information:**

Website: [www.fireeye.com/company/contact-us.html](http://www.fireeye.com/company/contact-us.html)

Technical Support: [www.fireeye.com/support/contacts.html](http://www.fireeye.com/support/contacts.html)

**Phone (US):**

1.408.321.6300

1.877.FIREEYE

# Contents

<b>Introduction</b>	<b>5</b>
Choosing Between Cloud Collector and Comm Broker	5
About Cloud Collector	6
Network Traffic Collection	6
Full Packet Capture	6
Enriched File Analysis	6
About Standalone Managed Communications Broker Sender	7
<b>Requirements</b>	<b>9</b>
Server Requirements	9
Network Firewall Requirements	10
Network Requirements	10
Configuration Information Requirements	12
<b>Sensor Placement</b>	<b>13</b>
Cloud Collector Installation	13
Communications Broker Sender Installation	14
Traffic Management	14
Multiple Comm Brokers and Cloud Collectors	14
Load Balancers	15
Domain Name Servers (DNS)	15
<b>Cloud Collector Installation</b>	<b>17</b>
Preinstallation	17
Installing the Cloud Collector	17
Configuring the Cloud Collector	18

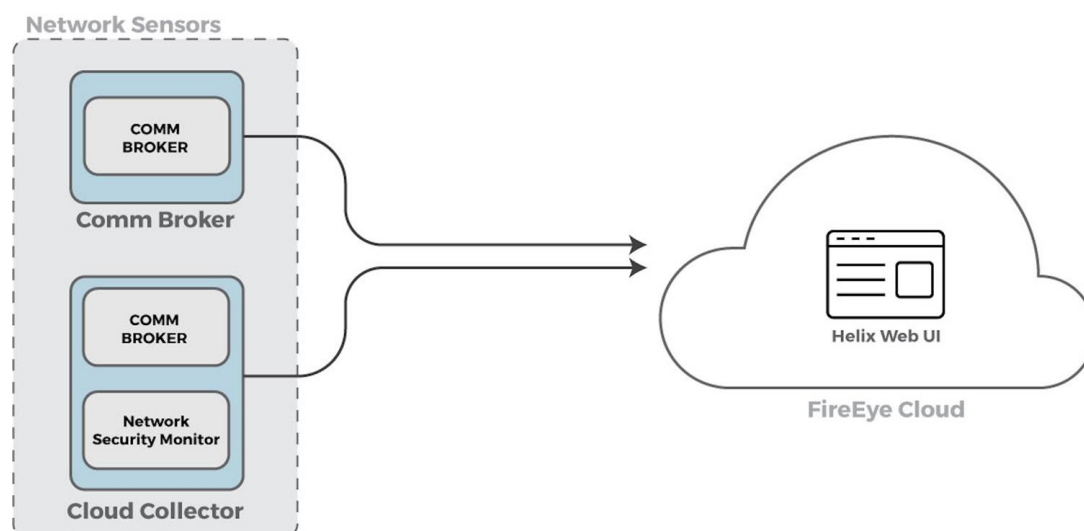
<b>Comm Broker Installation .....</b>	<b>23</b>
Preinstallation .....	23
Installing the Comm Broker .....	23
Configuring the Comm Broker .....	24
 <b>Creating a Bootable USB from an ISO Image .....</b>	 <b>27</b>
 <b>Technical Support .....</b>	 <b>31</b>
Documentation .....	31

# Introduction

This document provides installation instructions for FireEye Cloud Collector network sensor and managed Communications Broker Sender (Comm Broker) using the downloaded ISO image. Before you install Cloud Collector or Comm Broker, review this entire document to familiarize yourself with the products, the requirements, and the installation process.

## Choosing Between Cloud Collector and Comm Broker

A common question, especially for new customers who are deciding where to place network sensors is, "What is the difference between a Cloud Collector and a Comm Broker?" Since you can install either type of appliance from the same ISO image, it is important to understand why you might use one type versus the other.



As you can see in the figure above, the Comm Broker component exists in both the Comm Broker and the Cloud Collector. The Comm Broker component collects logs from network

sources through the management interface. If you are only interested in collecting log data from a particular segment of your network, you can install a Comm Broker.

By contrast, if you want your network sensor to run some analysis on the data before sending it to Helix, install the Cloud Collector. In addition to the log collection performed by the on-board Comm Broker, the Cloud Collector has a network security monitor that provides protocol analysis and packet capture.

## About Cloud Collector

FireEye Cloud Collector is a managed *network sensor* that runs on a physical or virtual server in your environment. The Cloud Collector collects network traffic from a network TAP or SPAN port. A built-in *network security monitor* provides protocol analysis and packet capture on the network traffic, while the on-board Comm Broker collects log data. Cloud Collector transmits all data to a dedicated receiver in the Helix virtual private cloud (VPC), where it is accessible in the Helix Web UI.

Cloud Collector performs the following functions.

### Network Traffic Collection

Cloud Collector begins collecting all observed network traffic as soon as you complete the installation, and generates metadata based off of the traffic. Protocol analyzers built into the Cloud Collector ensure that the generated metadata contains the specific information needed for the observed protocol to be presented to Helix.

### Full Packet Capture

The Cloud Collector also has the ability to store full packet captures (PCAPs) of all observed traffic. In Helix, you can generate PCAPs, review the transcript, and download PCAP files for further investigation.



Before you can work with PCAPs in Helix, you must generate an API key and provide the key to FireEye. See the "PCAPs" section of the *Helix Administration Guide* for details.

### Enriched File Analysis

The Cloud Collector performs some basic analysis on each executable file it observes. This analysis is performed locally on the Cloud Collector. MD5 hashes, import hashes, and strings are collected from the file and forwarded to Helix for hunting and further analysis.

# About Standalone Managed Communications Broker Sender

Each Cloud Collector includes Comm Broker, but you can also install Comm Broker as a standalone device. Comm Broker receives third-party log data and sends it to the dedicated receiver in the Helix VPC. The Comm Broker should be deployed when a Cloud Collector cannot be deployed or when you only want to collect logs in a given segment of the network. As with the Cloud Collector, the Comm Broker is managed by FireEye.





# Requirements

The following sections describe the server, network firewall, network, and configuration information requirements for installing Cloud Collector or Communications Broker Sender on a physical or virtual server in your environment.

- [Server Requirements](#) below
- [Network Firewall Requirements](#) on the next page
- [Network Requirements](#) on the next page
- [Configuration Information Requirements](#) on page 12

## Server Requirements

The hardware requirements for a Cloud Collector / Comm Broker depend on network utilization, expressed in terms of peak capacity (Mbps/Gbps) at the network egress.



Cloud Collector / Comm Broker is supported on on-premises virtual machines only. Cloud Collector / Comm Broker is not supported on cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

The following table shows the hardware requirements for Comm Broker and for three different utilization rates for Cloud Collector.

	Comm Broker	Cloud Collector 100 Mbps	Cloud Collector 500 Mbps	Cloud Collector 2 Gbps
<b>CPU (Cores)</b>	8	8	16	24
<b>Memory</b>	8GB	16GB	64GB	128GB
<b>Disk</b>	100GB	100GB	100GB	100GB

	Comm Broker	Cloud Collector 100 Mbps	Cloud Collector 500 Mbps	Cloud Collector 2 Gbps
<b>Required Interfaces</b>	One 1-Gbps	Two 1-Gbps	Two 1-Gbps	One 1-Gbps (Management)  One 10-Gbps (Monitoring)



100GB of disk storage is the minimum storage needed for installation and operation of the Cloud Collector. If you wish to take advantage of stored packet captures (PCAP), allocate more space based on your monitored network traffic rate and desired retention.

## Network Firewall Requirements

The following firewall changes are necessary to allow communication between the Cloud Collector or Comm Broker and FireEye.

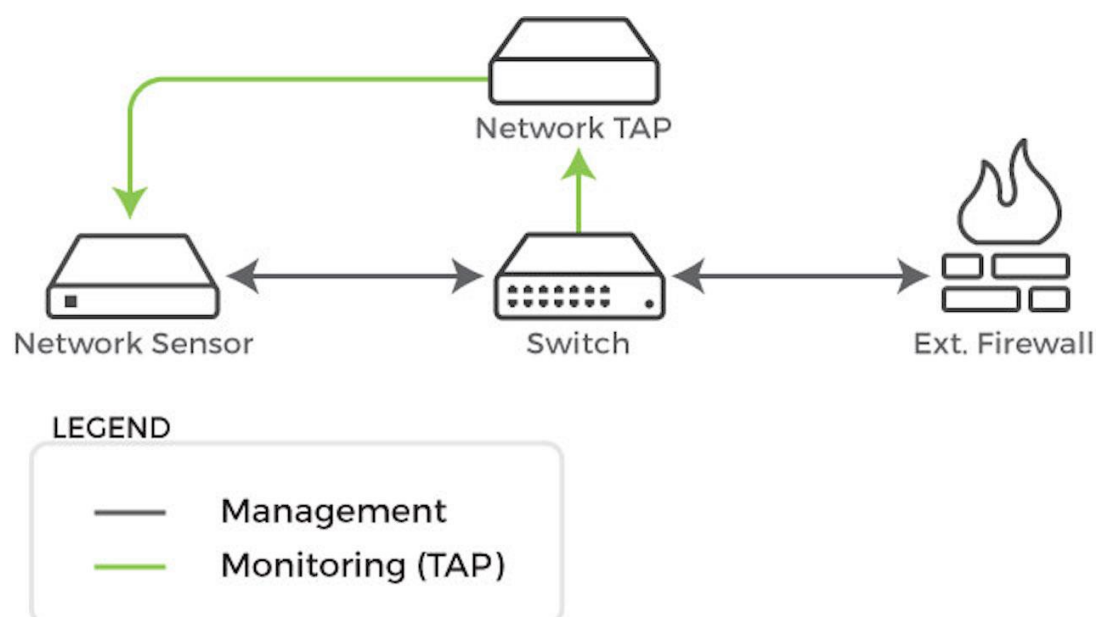
Source	Destination	Action	Protocol	Port
Cloud Collector or Comm Broker	<b>Cloud Collector Manager FQDNs:</b> <ul style="list-style-type: none"> <li>ccmaster01.map.mandiant.com or</li> <li>ccmaster02.map.mandiant.com</li> </ul>	Allow	TCP	80, 4505, 4506
Cloud Collector or Comm Broker	All <sup>1</sup>	Allow	TCP	443

<sup>1</sup> The Helix VPC uses the Amazon AWS address space. If you would like to be more restrictive than allowing 443 traffic to all destinations, refer to AWS documentation found here: <http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>.

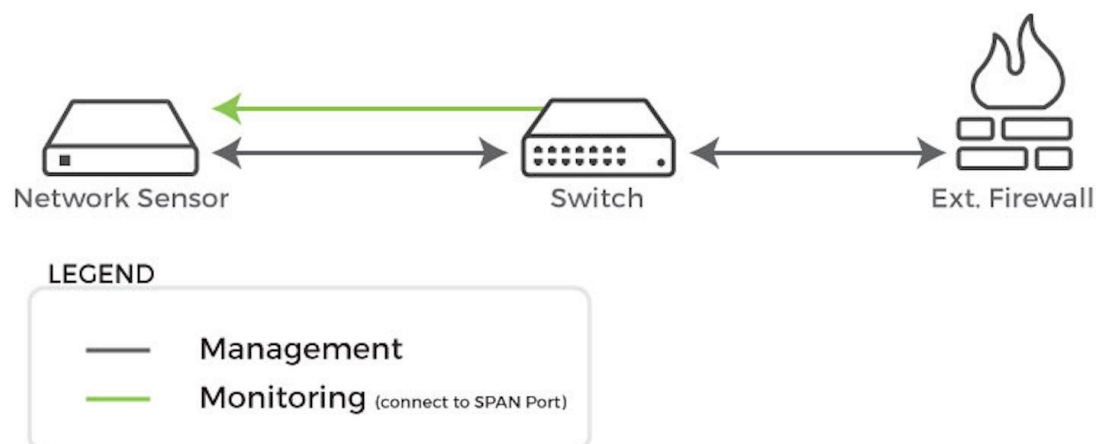
## Network Requirements

FireEye recommends that the monitoring interface of the network sensor be attached to a network TAP. A network TAP is a hardware device placed at a specific network point that

allows you to connect a third device to monitor the network traffic. If you use a network TAP, connect the monitoring interface of your network sensor to the network TAP and connect the management interface to a network segment that meets the previously outlined network firewall requirements.



Alternatively, you can attach the monitoring interface to a SPAN port on a network switch. Be aware that with a SPAN port packet loss will most likely occur due to pressure on the switch's backplane as a result of traffic mirroring. Attach the management interface to a network segment that meets the previously outlined network firewall requirements.



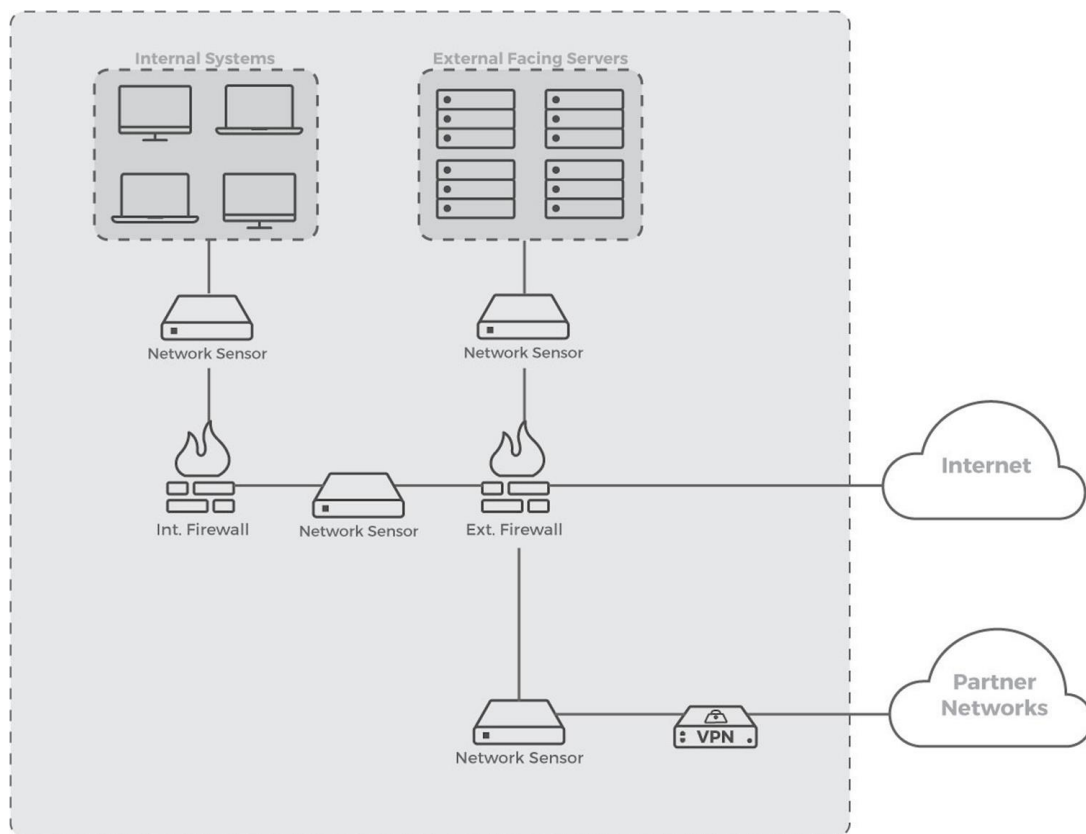
For more information, see [Sensor Placement](#) on page 13.

# Configuration Information Requirements

Before you install the ISO image, download the Cloud Collector Planning Worksheet from <https://docs.fireeye.com/docs/helix.html>. Complete the requested information and email it to FireEye at [support@fireeye.com](mailto:support@fireeye.com). Then continue with your installation, as described in [Cloud Collector Installation](#) on page 17.

## Sensor Placement

The following figure illustrates some of the areas in your network where you may want to place a Cloud Collector or Comm Broker, collectively referred to as network sensors. FireEye will provide you with the fully-qualified domain names (FQDN) of the dedicated receivers that your network sensors will use to send data to the Helix VPC.



## Cloud Collector Installation

Each FireEye Cloud Collector requires two network interfaces.



For more diagrams that show connected interfaces, see [Network Requirements](#) on page 10.

The first interface, referred to as the *monitor interface*, collects data about your network traffic, and does not require a dedicated IP address. The monitor interface is connected to a network TAP (preferred) or SPAN port (for example, on the trusted side of an egress firewall) so it can monitor all incoming and outgoing network traffic.

The second interface, referred to as the *management interface*, connects to your internal network and is responsible for sending data to the Communications Broker Receiver in the Helix VPC, as well as allowing FireEye to remotely manage the server. The management interface connects to your internal network. You will configure this interface with an IP address for the subnet to which it is connected. Both static and dynamic IP addresses are supported.

## Communications Broker Sender Installation

The FireEye Comm Broker requires a management interface only, as it does not actively monitor network traffic. It accepts logs from current log sources.

## Traffic Management

To manage large streams of data both to the Comm Broker Sender or Cloud Collector (also called *network sensors*), and between the Comm Broker Sender or Cloud Collector and the Comm Broker Receiver, Helix supports multiple options.

### Multiple Comm Brokers and Cloud Collectors

You can deploy multiple Comm Brokers or Cloud Collectors in your network. A single Comm Broker Receiver (in the Helix VPC) can receive traffic from multiple Cloud Collectors or Comm Brokers in your network. Each Cloud Collector and Comm Broker Sender operates independently.

Installing these network sensors closer to the data source conserves bandwidth. If your environment includes data centers that are regional, you can deploy one or more network sensors within each data center.

## Load Balancers

Comm Brokers can be deployed behind load balancers for redundancy and load sharing. Load balancers can also be used to detect when systems are unavailable.

## Domain Name Servers (DNS)

A DNS round robin can be used to provide redundancy. Some systems may not be capable of sending syslog to a DNS, however, and are limited to an IP destination only. You can also use low TTL DNS to help automatically fail over devices that use FQDN destinations for syslog.





# Cloud Collector Installation

## Preinstallation

1. Download the `FireEye-CCCB-v2.4.17.iso` image.
2. Use the ISO image to create one of the following types of bootable media:
  - [USB drive](#)
  - virtual DVD in virtualization systems such as VMware
  - physical CD or DVD

See [Creating a Bootable USB from an ISO Image](#) on page 27.
3. Connect the network cables to their appropriate interfaces. See [Sensor Placement](#) on page 13.
4. Mount the media you created from the provided ISO, and boot the server for the first time.

## Installing the Cloud Collector

1. From the **Boot** menu, use the arrow and Enter keys to select **Install Cloud Collector Sensor Software Appliance**, and then press **Enter**.



2. If you are installing the Cloud Collector Sensor Software Appliance and have provisioned your hardware with additional hard drives to provide more storage for network PCAPs, you will be prompted to select the drive on which you would like to install the operating system. Enter the drive label and press **Enter**.

```
Multiple hard drives detected. Beginning hard drive provisioning.
Device  Size
sda     104GB
sdb     252GB
There are 2 available disk(s)
Which device would you like to use as the operating system filesystem (must be larger than 60GB):
sda
```

3. You will then be asked if you would like to use the same device for PCAP storage. You will not typically store PCAPs on the same drive as the operating system. Type **no** and press **Enter**.
4. Enter the drive label of the device you want to use for PCAP storage and press **Enter**.
5. Type **Yes** and press **Enter** to acknowledge that continuing will destroy all data on this device and will perform a new OS installation.
6. When installation is complete, press **Enter** to reboot.

## Configuring the Cloud Collector

1. After rebooting, log into the server using the default credentials.

**Username:** fireeye

**Password:** flre3ye

```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.10.1.el7.x86_64 on an x86_64

localhost login:
```

2. Create a new user account to replace and disable the default account. You will need to use the credentials you are creating now to log into the server.

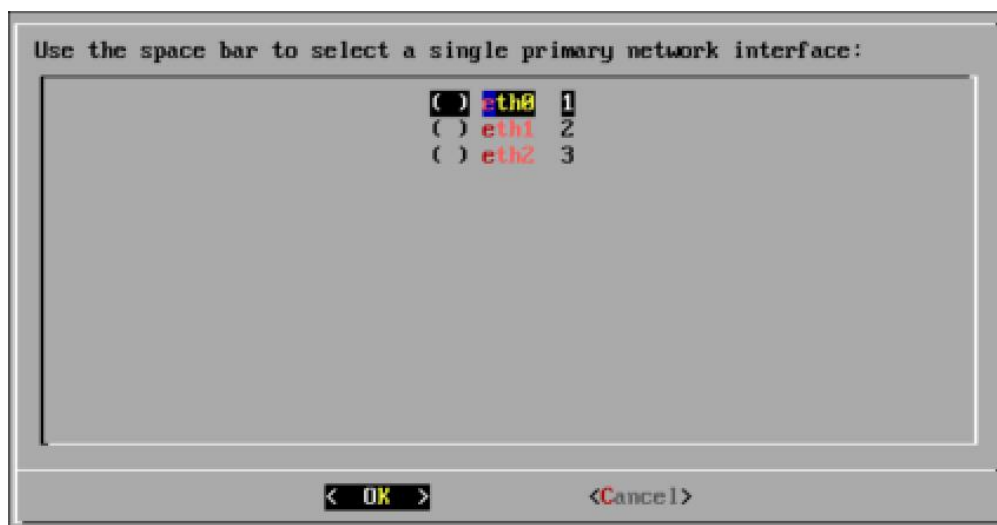


3. Enter a password for this account. Reenter the password for confirmation.

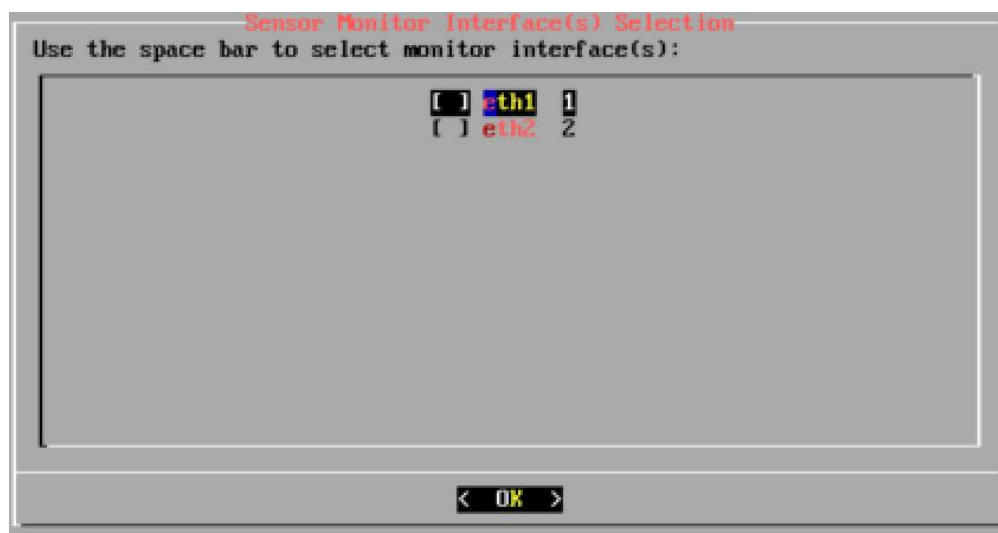


Create a strong password, not a weak one that is easy to crack.

4. Specify whether you will be using DHCP to configure your management interface.
5. Enter the hostname for this device. This will be the name that you provided in the Cloud Collector ISO Planning Worksheet.
6. Using the space bar, select the interface to be used as the Management Interface, and press **Enter**.



7. If you have chosen to use DHCP for the management interface configuration, skip to step 8. If you have *not* chosen to use DHCP, enter the following:
  - IP address you would like to assign to the management interface
  - Netmask appropriate for this IP address
  - Gateway IP address for this network
  - DNS search domain appropriate for this host
  - Primary DNS server's IP address
8. Using the space bar, select one or more devices to be used for the Monitor Interfaces, and press **Enter**.



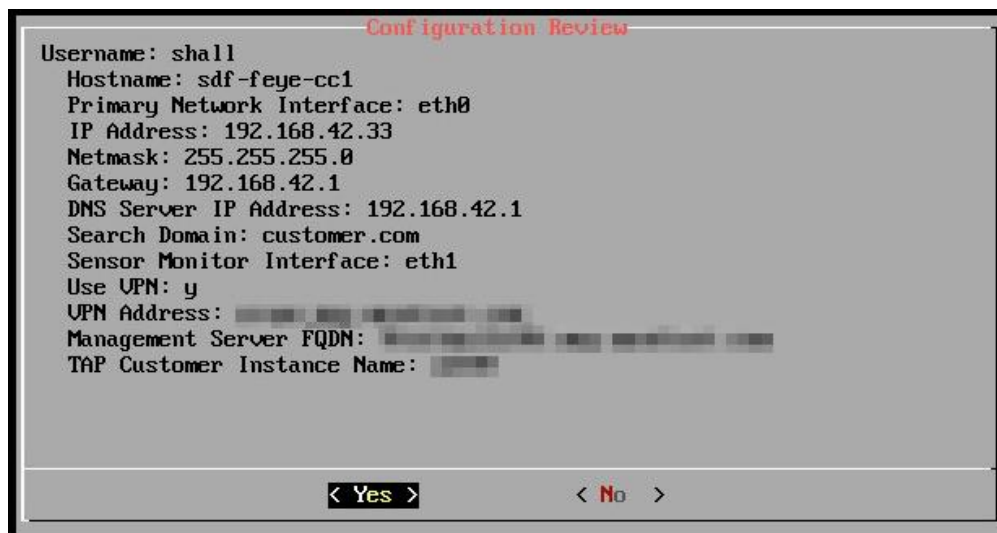
9. Enter the fully qualified domain name (FQDN) of the Cloud Collector management server.
  - ccmaster01.map.mandiant.com or
  - ccmaster02.map.mandiant.com



10. Enter your Helix ID, which you can obtain from the Helix Web UI.

11. Review your entries. If any of the items are incorrect, use the arrow or tab key to select either **Yes** or **No**.

Selecting **No** will restart the configuration process and allow you to make necessary changes. Selecting **Yes** will confirm the information you have entered and commit the configuration changes.



12. When prompted, select **OK** to reboot the device. Be sure to remove the installation media when finished.

After the reboot has completed, send an email to [support@fireeye.com](mailto:support@fireeye.com) with the hostname of the Cloud Collector host you have just configured. Your key will then be accepted on the management server, and the Cloud Collector management team will perform the final post-installation configuration of the device. Please allow one business day for this to be completed.



# Comm Broker Installation

## Preinstallation

1. Download the `FireEye-CCCB-v2.4.16.iso` image from the FireEye Customer Support Portal.
2. Use the ISO image to create one of the following types of bootable media:
  - [USB drive](#)
  - virtual DVD in virtualization systems such as VMware
  - physical CD or DVD

See [Creating a Bootable USB from an ISO Image](#) on page 27.
3. Connect the network cables to their appropriate interfaces. See [Sensor Placement](#) on page 13.
4. Mount the media you created from the provided ISO, and boot the server for the first time.

## Installing the Comm Broker

1. From the Boot menu, use the arrow and enter keys to select **Install Cloud Collector Comm Broker Software Appliance** and press **Enter**.



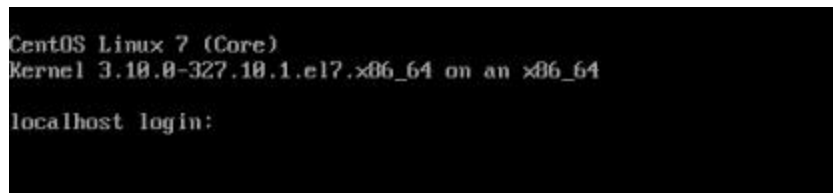
2. Type **Yes** and press **Enter** to acknowledge that continuing will destroy all data on this device and will perform a new OS installation.
3. When installation is complete, press **Enter** to reboot.

## Configuring the Comm Broker

1. After rebooting, log into the server using the default credentials.

**Username:** fireeye

**Password:** flre3ye



2. Create a new user account to replace and disable the default account. You will need to use the credentials you are creating now to log into the server.



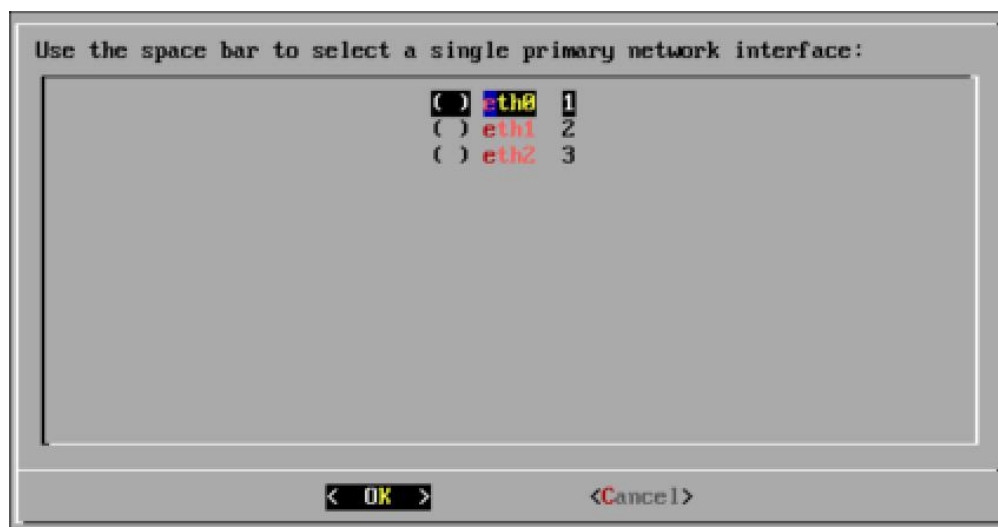


3. Enter a password for this account. Reenter the password for confirmation.



Create a strong password, not a weak one that is easy to crack.

4. Specify whether you will be using DHCP to configure your management interface.
5. Enter the hostname for this device. This is the name that you provided in the Cloud Collector ISO Planning Worksheet.
6. Using the space bar, select the interface to be used as the Management Interface, and press **Enter**.



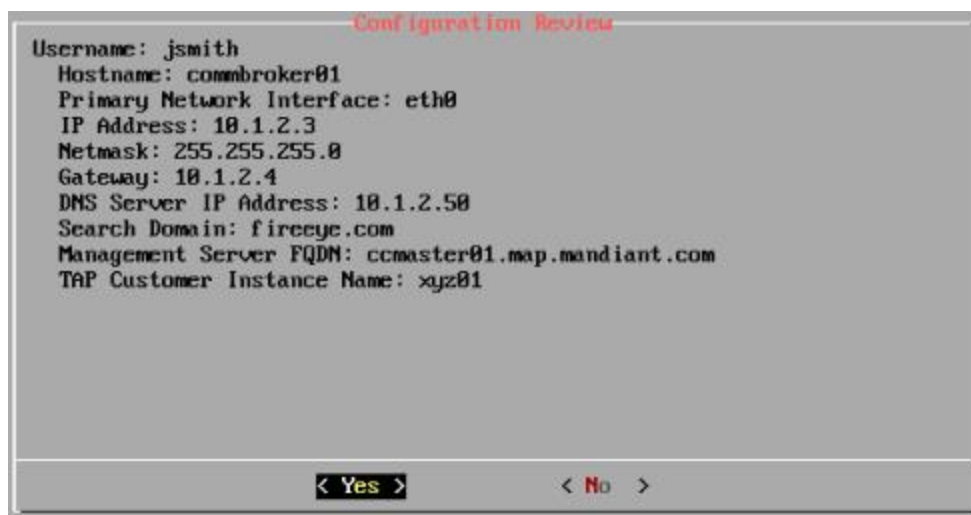
7. If you have chosen to use DHCP for the management interface configuration, skip to step 8; otherwise enter the following:
  - IP address to assign the management interface
  - Netmask for this IP address
  - Gateway IP address for this network
  - DNS search domain appropriate for this host
  - IP address of the primary DNS server

8. Enter the FQDN of the Cloud Collector management server, provided in [Network Firewall Requirements](#) on page 10.



9. Enter your Helix ID, which is visible in the upper right corner of the Helix Web UI.
10. Review your entries.

Use the arrow or tab key to select either **Yes** or **No**. Selecting **No** will restart the configuration process and allow you to make necessary changes. Selecting **Yes** will confirm the information you have entered and commit the configuration changes.



11. Select **OK** to reboot the device. Be sure to remove the installation media.
12. After the reboot has completed, send an email to [support@fireeye.com](mailto:support@fireeye.com) with the hostname of the Comm Broker host you have just configured. Your key will then be accepted on the management server, and the Cloud Collector management team will perform the final post-installation configuration of the device. Please allow one business day for this to be completed.

# Creating a Bootable USB from an ISO Image

Use the instructions corresponding to your operating system to create physical media from the ISO file.

## OS X:

1. Convert the ISO to a DMG file:  

```
hdiutil convert -format UDRW -o /<path-to-output-img>/FireEyeCCB-vx.x.x.img /<path-to-input-iso>/FireEye-CCCBvx.x.x.iso
```
2. List your currently attached disks:  

```
diskutil list
```
3. Insert your USB drive.
4. List your currently attached disks and identify the newly attached USB drive:  

```
diskutil list
```
5. Unmount the USB drive:  

```
diskutil unmountDisk /dev/diskX
```
6. Use `dd` to copy the image to the new USB drive, making sure to specify the USB drive as `/dev/rdiskX` instead of `/dev/diskX`:  

```
sudo dd if=/path/to/input/dmg/FireEye-CC1-vx.x.x.img.dmg of=/dev/rdiskX bs=1m
```
7. Eject the USB drive:  

```
diskutil eject /dev/diskX
```

## Windows:

To create a bootable USB image from the ISO on Windows, you will need an imaging software such as Rufus or Yum.

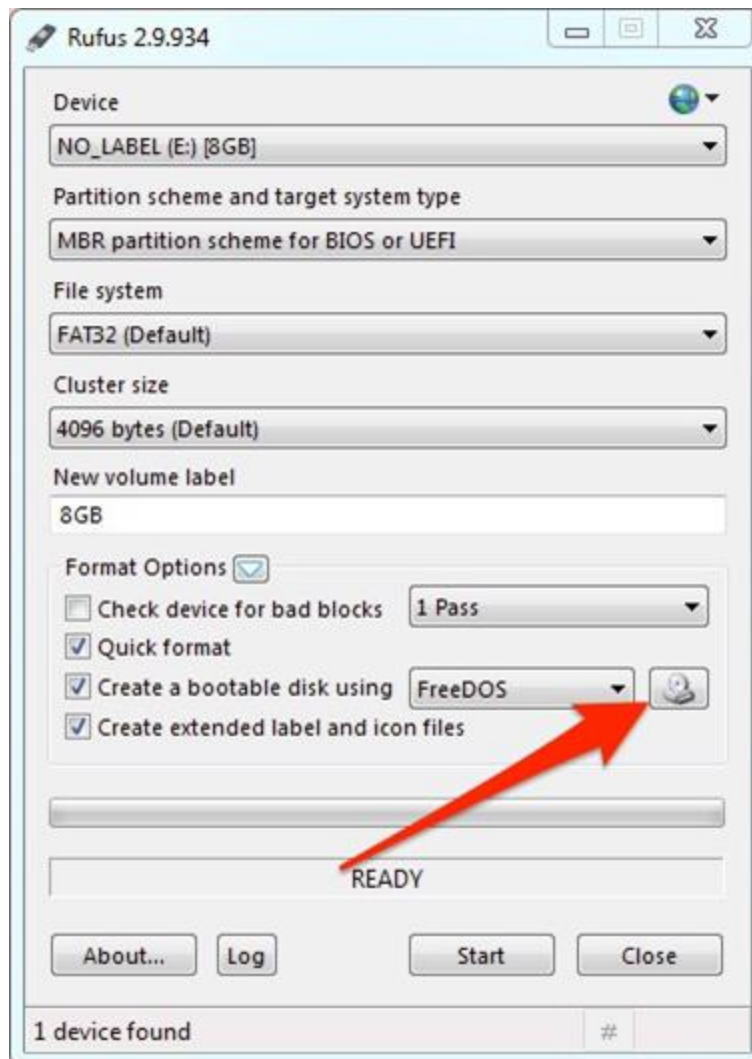


FireEye does not certify or recommend any particular software application for the purpose of creating a bootable USB image.

The following procedure is provided for demonstration purposes only, using Rufus.

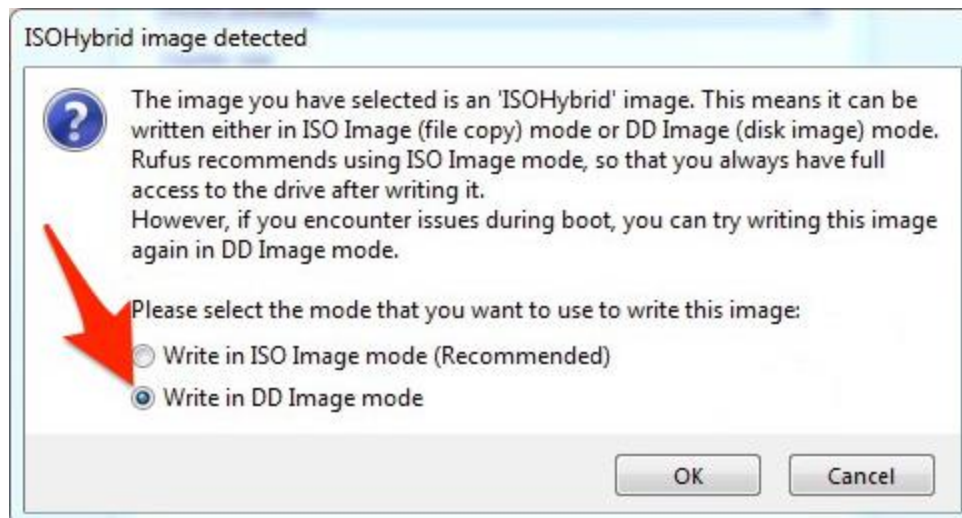
1. Download and run the Rufus imaging tool:  
<https://rufus.akeo.ie/>

2. Click the CD icon to select the ISO from which to create the USB.



3. Click **Start**.

4. Choose **Write in DD Image mode** as the method to create the USB image.



5. Click **OK**.



# Technical Support

For technical support, contact FireEye through the Support website:

[www.fireeye.com/support/contacts.html](http://www.fireeye.com/support/contacts.html)

## Documentation

Documentation for all FireEye products is available on the FireEye Documentation Portal (login required):

<https://docs.fireeye.com/>

