

# Carbon Black Cloud Workload Guide

05 July 2024

VMware Carbon Black Cloud Workload 1.3

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

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

**VMware by Broadcom**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2020-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to <https://www.broadcom.com>. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

# Contents

Carbon Black Cloud Workload Guide	6
<b>1 Carbon Black Cloud Workload Overview</b>	<b>7</b>
<b>2 Preparing to Enable Carbon Black in Your vSphere Environment</b>	<b>11</b>
Download the Carbon Black Cloud Workload Appliance OVA	11
Accessing Carbon Black Cloud	12
<b>3 Enabling Carbon Black in Your vSphere Environment</b>	<b>13</b>
Deploy and Configure Carbon Black Cloud Workload Appliance	13
Deploy the Carbon Black Cloud Workload Appliance in the vCenter Server	14
Register Carbon Black Cloud Workload Appliance with vCenter Server	15
Generate an API ID and API Secret Key	20
Register the Carbon Black Cloud Workload Appliance with Carbon Black Cloud	21
Register the Carbon Black Cloud Workload Appliance with NSX-T	25
Preparing VMs with Carbon Black Launcher	27
Carbon Black Launcher for Windows VMs	28
Carbon Black Launcher for Linux VMs	28
Install Sectigo Certificates	29
Enable Carbon Black Cloud on Virtual Machines	30
Customize the Configuration File	32
<b>4 View the Carbon Black Cloud Workload Plug-in in the vCenter Server</b>	<b>34</b>
Sensor Status and Details	34
Overview of Vulnerability Assessment	35
Working with OS Level Vulnerabilities	36
Working with Application Level Vulnerabilities	37
<b>5 Automatically Install Carbon Black Cloud Host User World</b>	<b>38</b>
<b>6 Manually Install Carbon Black Cloud Host User World</b>	<b>40</b>
<b>7 Using the Carbon Black Cloud Workload Appliance</b>	<b>43</b>
Manage Appliance Users	43
Configure NTP Server Settings	44
View and Update Network Settings	45
Configure Proxy Settings for an Appliance	46
Appliance Health Status	47

- Maintaining the Appliance Password 48
  - Reset Appliance Password 48
  - Extend Password Expiration Time for Appliance 50
  - Disable the Admin Password Expiration 50
- Reboot Appliance 51
- Redeploy a Carbon Black Cloud Workload Appliance 51
- Appliance Logs 51
  
- 8 Updating Carbon Black in your vSphere Environment 54**
  - Update Carbon Black Sensors on Virtual Machines 54
  - Upgrade the Carbon Black Cloud Workload Appliance 55
    - Upgrade an Appliance To 1.0.2 56
  
- 9 Disable Carbon Black from your vSphere Environment 60**
  - Uninstall and Delete Carbon Black Sensors 60
  - Delete Appliance from vCenter Server 61
  
- 10 VM Clones and Carbon Black Workloads 62**
  - Reregister Windows VM Clone and Golden Image 62
  - Reregister Linux VM Clone 63
  
- 11 Carbon Black Sensor Gateway User Guide 65**
  - Sensor Gateway Overview 66
  - Set up your OVA Environment for Sensor Gateway 66
  - Provision Sensor Gateway API Key 67
  - Carbon Black Cloud API Access 69
  - Sensor Gateway Certificates 70
  - Create a Certificate Chain File 71
  - Install Sensor Gateway as an Appliance 72
    - Reconfigure the Sensor Gateway Appliance 78
    - Update Sensor Gateway Appliance Certificate 80
    - Update HTTPS Proxy Certificate 81
  - Installing Carbon Black Cloud Sensors for Sensor Gateway 82
    - Locate a Sensor Gateway Instance 83
    - Generate a Company Code 83
    - Install Carbon Black Cloud Linux Sensor for Sensor Gateway 84
    - Install Carbon Black Cloud Windows Sensor for Sensor Gateway 85
  - Manage Connectivity to Carbon Black Cloud 86
  - Sensor Gateway Notifications 87
    - Subscribe to Receive Sensor Gateway Notifications 88
  - Upgrade a Sensor Gateway Appliance 89

Troubleshooting Sensor Gateway	90
Installing Sensor Gateway on a Linux Server	90
Configure Your Linux Server for Sensor Gateway Installation	91
Install Sensor Gateway on a Linux Server	93
Upgrade a Linux Server Sensor Gateway	97

# Carbon Black Cloud Workload Guide

This guide provides information about how to install, configure, and use the Carbon Black Cloud Workload Plug-in for vCenter Server to secure your VM workloads.

This information is intended for anyone who wants to install, configure, and use Carbon Black Cloud Workload Plug-in.

## Intended Audience

This information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. This manual assumes familiarity with VMware vSphere®, including VMware ESXi™, VMware vCenter Server®, VMware Tools™, and VMware NSX-T Data Center™ .

# Carbon Black Cloud Workload Overview

# 1

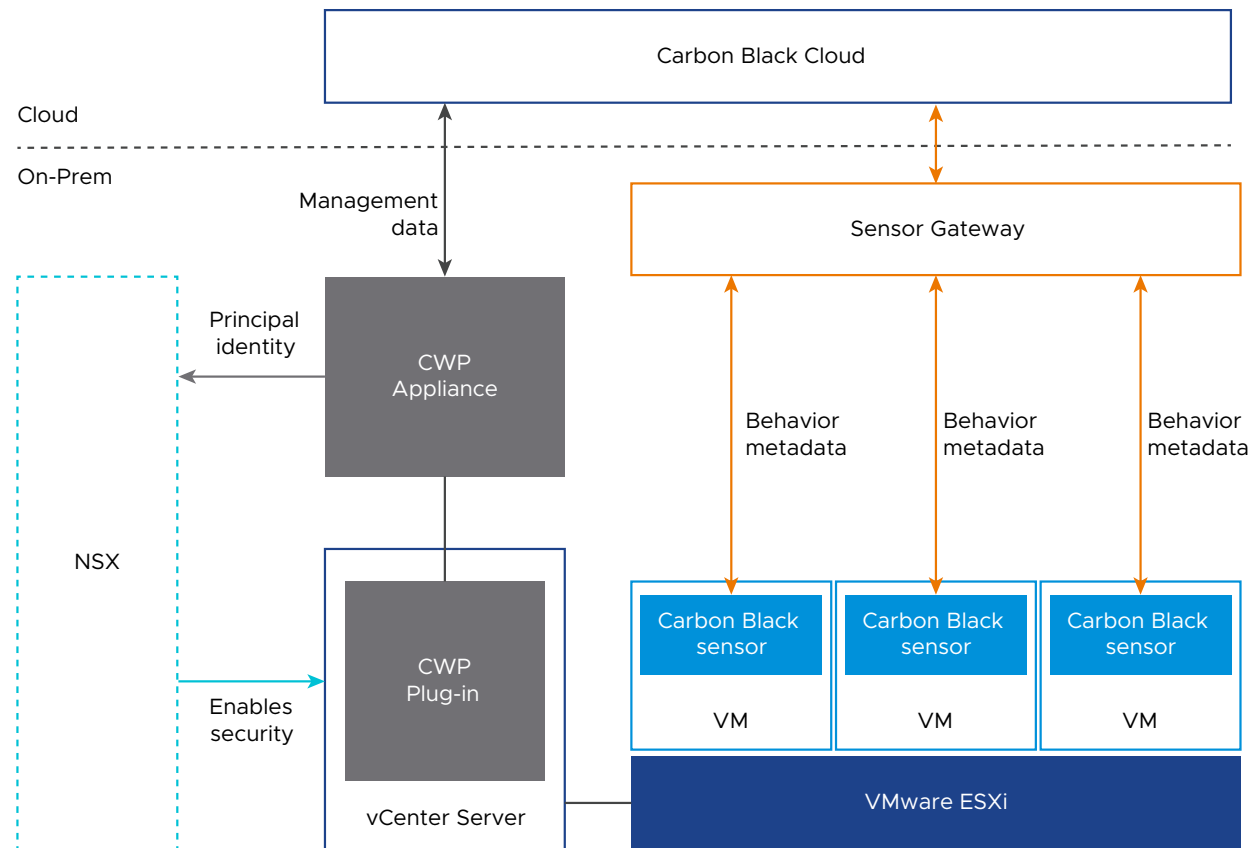
Carbon Black Cloud™ Workload is a data center security product that protects your workloads running in a virtualized environment. Carbon Black Cloud Workload ensures that security is intrinsic to the virtualization environment by providing built-in protection for virtual machines.

After enabling the Carbon Black in vCenter Server, you can view the inventory protected by Carbon Black Cloud Workload and view the inventory and risk assessment dashboard that Carbon Black Cloud Workload Plug-in provides.

You can monitor and protect the data center workloads through the Carbon Black Cloud console. The Carbon Black Cloud Workload Plug-in provides deep visibility into your data center inventory and end-to-end lifecycle management for the components.

Starting with release 1.1, an integration between the Carbon Black Cloud Workload and VMware NSX-T Data Center™ allows you to trigger NSX remediation policies based on observed behaviors in Carbon Black Cloud. Any Carbon Black Cloud alert that triggers remediation on protected Virtual Machines (VMs), allows you to remediate threats using NSX-T Distributed Firewall (DFW) policies.

Carbon Black Cloud Workload consists of a few key components that interact with each other.



To enable Carbon Black Cloud Workload for use with vCenter Server:

- 1 Deploy an on-premises OVF or OVA template for the Carbon Black Cloud Workload Appliance that connects the Carbon Black Cloud to the vCenter Server through a registration process.

After the registration is complete, the Carbon Black Cloud Workload Appliance deploys the Carbon Black Cloud Workload Plug-in and collects the inventory from the vCenter Server. The collected inventory data is displayed on the plug-in **Inventory** tab and is also communicated to the Carbon Black Cloud console.

- 2 Enable Carbon Black on the virtual machines where your application workloads are running. After you enable Carbon Black, you can view and monitor inventory data and processes from the Carbon Black Cloud Workload Plug-in and from the **VMs > Monitor** tab.
- 3 Open the Carbon Black Cloud console and create sensor groups and set policies to meet your organization's security needs.

You can identify, investigate, and remediate potential threats from the Carbon Black Cloud console. See the [Carbon Black Cloud User Guide](#).

## Carbon Black Cloud Workload Appliance



The Carbon Black Cloud Workload Appliance is an on-premise control point that acts as a liaison between vCenter Server and Carbon Black Cloud. The appliance collects the workload inventory data from the vCenter Server and shares the data with Carbon Black Cloud.

The appliance provides the channel for communication between Carbon Black Cloud and NSX Manager. The strong data analysis capabilities of Carbon Black Cloud pair with the firewall protection capabilities of NSX. You can use the appliance to register an NSX integration with your Carbon Black Cloud organization. The appliance registers to the NSX through principal identity. It provides a certificate-based authentication — you do not need to maintain Admin user credentials. For adding a role assignment or principal identity, see [VMware NSX-T Data Center Product Documentation](#).

## Carbon Black Cloud Workload Plug-In

The Carbon Black Cloud Workload Plug-in provides improved life-cycle management and real-time visibility in the vCenter Server. The plug-in provides direct visibility into processes and network connections running on a given virtual machine. The Carbon Black Cloud Workload Plug-in works in concert with the Carbon Black Cloud to provide visibility and control for the security team.

## vCenter Server

vCenter Server gathers inventory data from your data center. The collected inventory data is used for security assignments. The Carbon Black Cloud Workload Plug-in is made available in your vCenter Server for direct visibility.

## Carbon Black Cloud

Carbon Black Cloud is a cloud-native service that consolidates multiple workload security capabilities using a single console. Teams such as Infrastructure and InfoSec can have a single, shared source of truth to improve security.

The Carbon Black Cloud console shows alerts based on Next Generation Anti-Virus (NGAV) detections and behavioral analytics. You can use the console to view any Carbon Black Cloud alerts on the protected VMs and apply tags of certain NSX-T Distributed Firewall (DFW) policies for remediation.

## Carbon Black Launcher

To minimize your deployment efforts, a lightweight Carbon Black launcher is available in VMware Tools. When you enable Carbon Black in your data center, the silent installation is triggered whereby the launcher downloads and installs the Carbon Black sensor on the virtual machine.

You can enable Carbon Black on Windows and Linux VMs.

- **Windows Virtual Machines:** For Windows VMs, the Carbon Black launcher is packaged together with VMware Tools. To receive the launcher for workloads, you must install or upgrade VMware Tools to version 11.2+.
- **Linux Virtual Machines:** For Linux VMs, you must manually install the launcher that is available in VMware Tools Operating System Specific Packages (OSPs). Download and install Carbon Black launcher from the [Broadcom Support Portal](#). For details, see [Carbon Black Launcher for Linux VMs](#).

## NSX Manager

The NSX Manager application provides a web-based user interface for administering your NSX environment. For information on installing, administering, and security capabilities of the NSX Manager, see the *VMware NSX Product Documentation*.

## Carbon Black® Sensor Gateway™

The Carbon Black® Sensor Gateway™ is an on-prem component that acts as a bridge for all inbound and outbound communication between the sensors deployed on vSphere workloads and the Carbon Black Cloud.

# Preparing to Enable Carbon Black in Your vSphere Environment

# 2

Before you enable Carbon Black in your vSphere environment, make sure that your environment is prepared and you can access the Carbon Black Cloud console.

See [Carbon Black Cloud™ Workloads Operating Environment Requirements](#).

Read the following topics next:

- [Download the Carbon Black Cloud Workload Appliance OVA](#)
- [Accessing Carbon Black Cloud](#)

## Download the Carbon Black Cloud Workload Appliance OVA

The Carbon Black Cloud Workload Appliance with the software for Carbon Black Cloud Workload Plug-in is bundled in a single Open Virtualization Appliance (OVA) that is used for the complete installation. You must download the Carbon Black Cloud Workload Appliance OVA.

### Procedure

- 1 To get the Carbon Black Cloud Workload Appliance OVA, go to the [Broadcom Support Portal](#) page:
  - a Go to **My Downloads - Cyber Security Software**.
  - b Search for **VMware Carbon Black Cloud Workload**.
  - c Select the latest release.

- 2 Download the OVA to a local datastore or local web server.

The OVA filename has the following format: `cwp-va-<release-number>-<build-number>_OVF10.ova`. For example, `cwp-va-1.3.0-21602657_OVF10.ova`.

- 3 Copy the file path of the Carbon Black Cloud Workload Appliance OVA file.

For example, if you downloaded the OVA file to a local web server: `http://<local-web-server>/cwp-va-1.3.0-21602657_OVF10.ova`. You will provide this path when you deploy the appliance.

## Results

The Carbon Black Cloud Workload Appliance OVA file is available.

## What to do next

[Deploy and Configure Carbon Black Cloud Workload Appliance](#)

# Accessing Carbon Black Cloud

You must have connectivity with the Carbon Black Cloud.

When you sign up for the Carbon Black Cloud service, or when someone invites you to join a service, you receive an email invitation to confirm your registration. The email contains a link and instructions to activate and set up your Carbon Black Cloud console account. If your organization already has an established instance of Carbon Black Cloud, simply log in to the console using your credentials.

If you do not receive the invitation email or if you require any help with the Carbon Black Cloud service, contact Broadcom Carbon Black Support. If you need any help related to vSphere, contact the VMware Support team.

# Enabling Carbon Black in Your vSphere Environment

# 3

Carbon Black Cloud Workload Appliance is deployed as a virtual appliance (packaged as an OVA file) on an ESXi host in a vCenter Server environment.

## Summary of Steps

- 1 Deploy and Configure Carbon Black Cloud Workload Appliance
  - a Deploy the Carbon Black Cloud Workload Appliance in the vCenter Server
  - b Register Carbon Black Cloud Workload Appliance with vCenter Server
  - c Generate an API ID and API Secret Key
  - d Register the Carbon Black Cloud Workload Appliance with Carbon Black Cloud
  - e Register the Carbon Black Cloud Workload Appliance with NSX-T
- 2 Preparing VMs with Carbon Black Launcher
- 3 Enable Carbon Black Cloud on Virtual Machines

Read the following topics next:

- [Deploy and Configure Carbon Black Cloud Workload Appliance](#)
- [Preparing VMs with Carbon Black Launcher](#)
- [Enable Carbon Black Cloud on Virtual Machines](#)

## Deploy and Configure Carbon Black Cloud Workload Appliance

Carbon Black Cloud Workload Appliance pairs with vCenter Server. You must deploy one Carbon Black Cloud Workload Appliance per vCenter Server.

First, deploy the Carbon Black Cloud Workload Appliance and register the appliance with the vCenter Server. After the appliance is deployed, you must generate an API ID and Secret Key from the Carbon Black Cloud console.

Next, configure the Carbon Black Cloud Workload Appliance and establish a connection between the Carbon Black Cloud Workload Appliance and Carbon Black Cloud.

## Deploy the Carbon Black Cloud Workload Appliance in the vCenter Server

Deploy the Carbon Black Cloud Workload Appliance on-premises in the management cluster. After obtaining the OVA file, you can deploy the appliance using the vSphere Client.

---

**Note** You must implement network controls to limit appliance interface access to authorized administrators only. Unrestricted network access to the appliance interface is not required.

---

### Prerequisites

- Verify the system requirements. See [Carbon Black Cloud Workload Operating Environment Requirements](#).
- Verify that you have the Carbon Black Cloud Workload Appliance OVA file available. See [Download the Carbon Black Cloud Workload Appliance OVA](#).

### Procedure

- 1 Log in to the vSphere Client.
- 2 Right-click the host on which to install the Carbon Black Cloud Workload Appliance and click **Deploy OVF Template**.
- 3 On the **Deploy OVF Template** page, configure the following values and click **Next**.

Option	Description
Select an OVF Template	<ul style="list-style-type: none"> <li>■ <b>URL:</b> Enter the Carbon Black Cloud Workload Appliance <b>URL</b> to a remote Web server. Supported URL sources are HTTP and HTTPS.  Example: <code>http://&lt;local-web-server&gt;/cwp-va-1.0.0.0-17066560_OVF10.ova</code>.</li> <li>■ <b>Local file:</b> Click <b>Choose Files</b> and select the downloaded OVA file.</li> </ul>
Select a name and folder	(Optional) Change the name of the OVA file to <b>Workload Appliance</b> .
Select a compute resource	(Optional) Verify if the selected host is the correct resource to deploy the Carbon Black Cloud Workload Appliance.
Review details	Review the details. The Product must be <b>CBC Workload Appliance VA</b> .
License agreements	To accept the license agreements, click <b>I accept all license agreements</b> .
Select storage	Select how to store the files for the deployed OVA.  Select a datastore to store the deployed OVF or OVA template. The configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine or vApp and all associated virtual disk files.
Select networks	Select the network that has connectivity to vCenter Server.  <b>IP Allocation Settings:</b> Select <b>IP protocol</b> as <b>IPv4</b> or <b>IPv6</b> .

Option	Description
Customize template	<p>a <b>Application:</b></p> <ul style="list-style-type: none"> <li>■ Type passwords for the <i>admin</i> and <i>root</i> user account. You will use these passwords later when you register the appliance with vCenter Server.</li> </ul> <p>The password must meet the following requirements:</p> <ul style="list-style-type: none"> <li>■ At least eight characters</li> <li>■ At least one lowercase character</li> <li>■ At least one numeric character</li> <li>■ At least one special character</li> <li>■ Not more than 20 characters long</li> </ul> <p>b <b>Networking Properties:</b></p> <ul style="list-style-type: none"> <li>■ If you want DHCP to be available while configuring the appliance, leave the configuration values empty.</li> <li>■ If you want to configure a static IP address: <ul style="list-style-type: none"> <li>■ <b>Domain Name and Domain Search Path:</b> Host name of the virtual machine. Example: <code>host.example.local</code>; enter <code>host</code> in the domain name field and enter <code>example.local</code> in the domain search path field.</li> <li>■ Add the following mandatory values: Default Gateway, Domain Name Servers, Network 1 IP Address, Network 1 Netmask.</li> </ul> </li> </ul>
Ready to complete	Verify the details and click <b>Finish</b> .

The OVA begins to import and deploy. It can take some time, depending on the public network download speed.

- 4 After the deployment is complete, go to the Carbon Black Cloud Workload Appliance virtual machine (VM), and power on the VM.

The Carbon Black Cloud Workload Appliance time zone is UTC and cannot be changed.

- 5 Note the Carbon Black Cloud Workload Appliance IP address.

## Results

The Carbon Black Cloud Workload Appliance is deployed.

## What to do next

[Register Carbon Black Cloud Workload Appliance with vCenter Server](#)

## Register Carbon Black Cloud Workload Appliance with vCenter Server

After the Carbon Black Cloud Workload Appliance is deployed, you must register the appliance with the vCenter Server.

You can register either with:

- The on-premises vCenter Server. See [Register the Carbon Black Cloud Workload Appliance with On-Premises vCenter Server](#).

- The vCenter Server in your VMware Cloud on AWS software-defined data center (SDDC). See [Register Carbon Black Cloud Workload Appliance With vCenter Server In Your VMware Cloud on AWS SDDC](#).

**What to do Next:** [Generate an API ID and API Secret Key](#)

## Register the Carbon Black Cloud Workload Appliance with On-Premises vCenter Server

After the Carbon Black Cloud Workload Appliance is deployed, register the new appliance with the on-premises vCenter Server.

### Prerequisites

- You have deployed the Carbon Black Cloud Workload Appliance.
- The Carbon Black Cloud Workload Appliance VM is powered-on.
- Appliance has HTTPS (443) connectivity to communicate with the vCenter Server.
- The SSO server time and the Carbon Black Cloud Workload Appliance time are in sync. See [Configure NTP Server Settings](#).

---

**Important** Time must be synchronized between the Carbon Black Cloud Workload Appliance and the vCenter Single Sign-On (SSO) server. NTP server must be specified so that the SSO server time and the Carbon Black Cloud Workload Appliance time are in sync.

---

### Procedure

- 1 From your browser, log in to the Carbon Black Cloud Workload Appliance at `https://<appliance IP address>` using **admin** credentials.
- 2 Go to the **Appliance > Registration** page.
- 3 In the **SSO lookup configuration** section, click **Edit**. Configure the following values:

SSO lookup configuration	Description
SSO Hostname	Enter the IP address or FQDN of the vCenter Single Sign-On (SSO) and click <b>Register</b> .  <b>Note</b> Carbon Black Cloud Workload Appliance uses a service account to interact with vCenter. This service account is created in your SSO server for improved security and manageability. You must have SSO administrator credentials to create this service account. The SSO administrator credentials are only used for this session and do not persist in the Carbon Black Cloud.
Username and Password	Enter the username and password for the vCenter SSO administrator. To add a member to the vCenter SSO administrator group, see <a href="#">vSphere Documentation</a> .
VMware Cloud on AWS	By default, the toggle is <code>OFF</code> . Do not change the setting.
Thumbprint (SHA1)	Verify the SHA1 thumbprint of the SSO server.



- 4 In the **vCenter Server Details** section, click **Register** and configure the following values:

vCenter Server details	Description
vCenter Server hostname	Select the required vCenter Server host name from the list. You can install one Carbon Black Cloud Workload Appliance per vCenter Server.
Plug-in	The version of the registered Carbon Black Cloud Workload Plug-in is available after the registration is complete.
Thumbprint (SHA256)	Verify the SHA256 thumbprint of the vCenter Server.

- 5 Click **Register**.
- 6 To reflect the changes, log out of the Carbon Black Cloud Workload Appliance and log in to the vCenter Server using the same *Administrator* role that you used to register the Carbon Black Cloud Workload Appliance.

Alternatively, refresh the vSphere Client browser.

### Results

The appliance registers successfully with the vCenter Server.

You can view the Carbon Black Cloud Workload Plug-in in the vCenter Server. The Carbon Black



icon appears in the left navigation pane and in the **Shortcuts** menu of the vSphere Client.

### What to do next

Go to the Carbon Black Cloud console and generate the API ID and secret key.

## Register Carbon Black Cloud Workload Appliance With vCenter Server In Your VMware Cloud on AWS SDDC

After the Carbon Black Cloud Workload Appliance is deployed, you can register the appliance with the vCenter Server that is available in your VMware Cloud on AWS software-defined data center (SDDC).

### Prerequisites

- You have deployed the Carbon Black Cloud Workload Appliance.
- The Carbon Black Cloud Workload Appliance VM is powered-on.
- SDDC is deployed and configured in VMware Cloud on AWS.
- Configure firewall rules in your SDDC. See [Configure Firewall Rules in SDDC](#).
- Configure the NAT rule for the appliance IP. See [Create a NAT Rule for Carbon Black Cloud Workload Appliance IP Address](#).

- The SSO server time and the Carbon Black Cloud Workload Appliance time are in sync. See [Configure NTP Server Settings](#).

---

**Important** Time must be synchronized between the Carbon Black Cloud Workload Appliance and the vCenter Single Sign-On (SSO) server. NTP server must be specified so that the SSO server time and the Carbon Black Cloud Workload Appliance time are in sync.

---

#### Procedure

- 1 From your browser, log in to the Carbon Black Cloud Workload Appliance at `https://<appliance IP address>` using the **admin** credentials.
- 2 Go to the **Appliance > Registration** page.
- 3 In the **SSO lookup configuration** section, click **Edit**. Configure the following values.

SSO lookup configuration	Description
SSO Hostname	Enter the IP address or FQDN of the vCenter Single Sign-On (SSO) instance and click <b>Register</b> . The VMC URLs are listed in <code>vmc.vmware.com</code> under <b>SDDCs &gt; Settings</b> . For example, <code>vcenter.sddc-x-x-x-x.vmwarevmc.com</code> . Do not enter the <code>https://</code> header.
VMware Cloud on AWS	Toggle the VMware Cloud on AWS environment <b>ON</b> .
User name and Password	Enter the user name and password for the vSphere Administration in VMware Cloud on AWS. For example, <code>cloudadmin@vmc.local</code> .
Thumbprint (SHA1)	Verify the SHA1 thumbprint of the SSO server.

- 4 In the **vCenter Server Details** section, click **Register** and configure the following values.

vCenter Server details	Description
vCenter Server hostname	Select the required vCenter Server host name from the list. You can install one Carbon Black Cloud Workload Appliance per vCenter Server.
Plug-in	The version of the registered Carbon Black Cloud Workload Plug-in is available after the registration is complete.
Thumbprint (SHA256)	Verify the SHA256 thumbprint of the vCenter Server.

- 5 Click **Register**.

The appliance is registered with the vCenter Server in your VMware Cloud on AWS SDDC.

#### Results

Log out of the Carbon Black Cloud Workload Appliance and log in to the vCenter Server from your SDDC with the same *Cloud Admin* role used during registration.

After the registration is successful, you can view the Carbon Black Cloud Workload Plug-in in



the vCenter Server. The Carbon Black **Shortcuts** menu of the vSphere Client.

### What to do next

Go to the Carbon Black Cloud console and generate the API ID and secret key.

### Configure Firewall Rules in SDDC

After your SDDC is deployed and configured in VMware Cloud on AWS, you must configure firewall rules for secure communication.

#### Procedure

- 1 Log in to the VMC Console.
- 2 On the **Networking & Security** tab, click **Gateway Firewall**.
- 3 Configure the following firewall rules:

Firewall Rule	Source	Destination	Service/Applied To
Go to the <b>Management Gateway</b> tab and add an inbound rule that allows appliance to communicate with the vCenter Server over HTTPS.	Any or appliance IP address	vCenter	HTTPS
Go to the <b>Management Gateway</b> tab and add an outbound rule that allows the vCenter Server to communicate with the appliance.	vCenter	Any or appliance IP address	Any
Go to the <b>Compute Gateway</b> tab and add an uplink rule that allows appliance and VMs to communicate with the Carbon Black Cloud.	Any	Any	Any

**Note** You can narrow rules for specific URLs based on network settings of your organization. Make sure that the appliance has external connectivity with the Carbon Black Cloud.

### Create a NAT Rule for Carbon Black Cloud Workload Appliance IP Address

After you deploy Carbon Black Cloud Workload Appliance, the IP address of the appliance is a private IP address that is only accessible from inside the SDDC network.

To make the IP address securely accessible, you must generate a publicly accessible IP address for the appliance and map the public IP address with the private IP address of the appliance by using Network Address Translation (NAT).

## Procedure

- 1 Log in to the VMC Console.
- 2 On the **Networking & Security** tab, click **Public IPs**.
- 3 Generate a publicly accessible IP address for the appliance. To request or release a public IP address, see *VMware Cloud on AWS Networking and Security* documentation.
- 4 Create a NAT rule to map the new public IP with the private IP of the appliance.

NAT Rule	Public IP	Service	Public and Internal Port	Internal IP	Firewall
Provide a name to your NAT rule	Add the public IP address that you generated	All Traffic	Any	Add IP address of the Carbon Black Cloud Workload Appliance	Match Internal IP Address

See also *VMware Cloud on AWS Networking and Security*.

## Generate an API ID and API Secret Key

Generate an API key from the Carbon Black Cloud console and use the generated API key to establish a connection between the Carbon Black Cloud console and the Carbon Black Cloud Workload Appliance that is deployed in the vCenter Server. You can configure one appliance per vCenter Server. You can configure multiple appliances for your organization. If you are configuring multiple appliances, you must generate a separate API key for each appliance.

Use the pre-defined custom access level, and generate an API key for that appliance. You can use the same custom access level to configure multiple appliances for your organization.

### Prerequisites

- [Deploy the Carbon Black Cloud Workload Appliance in the vCenter Server.](#)
- Use the `CWP Appliance` custom access level for appliances in your organization. Starting with version 1.2, the pre-defined custom access level for your appliance holds all necessary permissions.
- [Register Carbon Black Cloud Workload Appliance with vCenter Server](#)

### Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 In the left navigation pane, go to the **Settings > API Access** page.
- 3 Click the **API Keys** tab and click **Add API Key**.

The **Add API Key** window displays.

- 4 Enter a unique name for the appliance API key.
- 5 From the **Access Level type** dropdown menu, select **Custom**.
- 6 From the **Custom Access Level** dropdown menu, find and select the `CWP Appliance` custom access level for the appliance.
- 7 Click **Save**.

The Carbon Black Cloud console generates the API ID and API secret key.

- 8 Copy the API ID and API secret key values and paste them into a plain text editor.  
You will use these values later to establish a connection between the appliance and the Carbon Black Cloud console.

---

**Important** You can use only one API ID and secret key per appliance.

---

#### What to do next

[Register the Carbon Black Cloud Workload Appliance with Carbon Black Cloud.](#)

---

**Tip** To retrieve the keys at a later time, perform the following steps.

- 1 In the left navigation pane, click **Settings > API Access > API Keys**.
- 2 Go to the appliance API name and click the down arrow next to the Edit icon.
- 3 Click **API Credentials**.

The **API Credentials** dialog box appears. Copy the keys.

---

## Register the Carbon Black Cloud Workload Appliance with Carbon Black Cloud

After you register the Carbon Black Cloud Workload Appliance with the vCenter Server and generate credentials, you must register the appliance with Carbon Black Cloud.

**Before you begin:** [Generate an API ID and API Secret Key](#)

**What to do next:** [Connect the Carbon Black Cloud Workload Appliance with Carbon Black Cloud](#)

## Connect the Carbon Black Cloud Workload Appliance with Carbon Black Cloud

After generating the authentication credentials from the Carbon Black Cloud console, configure the Carbon Black Cloud Workload Appliance to establish connection with Carbon Black Cloud.

### Prerequisites

- Verify that the Carbon Black Cloud Workload Appliance VM is powered on.
- Verify that the API keys are generated and copied from the Carbon Black Cloud console. See [Generate an API ID and API Secret Key](#).
- The appliance must have HTTPS (443) connectivity to communicate with the vCenter Server and the Carbon Black Cloud.

### Procedure

- 1 Log in to the vSphere Client.
- 2 To verify that the Carbon Black Cloud Workload Appliance VM is powered on, open the VM console and note the IP address of the appliance.
- 3 From your browser, log in to the Carbon Black Cloud Workload Appliance at **https://<appliance IP address>** using **admin** credentials.
- 4 Go to the **Appliance > Registration** page.
- 5 In the Carbon Black Cloud section, click **Edit**.
- 6 Select a Carbon Black Cloud environment from the **CB Cloud Environment** dropdown menu.

VMware Carbon Black Cloud (Refer to the User Guide) ✓

CB Cloud Environment:	<input type="text" value="https://defense-prod05.conferdeploy.net"/>
API ID:	<input type="text" value="API ID"/>
API Secret Key:	<input type="text" value="API Secret Key"/>

- 7 Optional: If the Carbon Black Cloud environment is not listed, select **Other** from the **CB Cloud Environment** dropdown menu, and enter the **CBC URL**.

VMware Carbon Black Cloud (Refer to the User Guide) ✓

CB Cloud Environment:	Other
CBC URL:	https://defense-prod05.conferdeploy.net
CSP URL:	CSP URL
API ID:	API ID
API Secret Key:	API Secret Key

**Note** VMware Cloud services is integrated into the Carbon Black Cloud Workload Appliance. Thus, it is not mandatory to specify the **CSP URL**.

- 8 Configure the following mandatory values:
- CB Cloud Environment:** Enter the Carbon Black Cloud console URL as per your hosted Carbon Black Cloud location.
  - API ID:** Paste the 10 digit *API ID* copied from the Carbon Black Cloud console.
  - API secret key:** Paste the *API secret key* copied from the Carbon Black Cloud console.
- 9 Click **Save**.

### Results

When you see a green check mark, the connection between the vCenter Server, Carbon Black Cloud Workload Appliance, and Carbon Black Cloud is established.

After successful registration:

- If the registered Carbon Black Cloud Workload Appliance is with version 1.2+, you will see the Org Key.
- If the registered Carbon Black Cloud Workload Appliance is with version 1.1, you will see the Org Name.
- If the registered Carbon Black Cloud Workload Appliance is with version earlier then 1.1, you will see the Org Key.

VMware Carbon Black Cloud (Refer to the User Guide) ✓

CB Cloud Environment:	https://defense-dev01.cbdtest.io
Appliance Name:	anant_test
Org Key:	QWYTZY4W
API ID:	U9ARHBBHPB

## What to do next

After the connection is successfully established, you can view data in the Carbon Black Cloud



Workload Plug-in from the vCenter Server. When you click the Carbon Black icon in the left navigation pane, the **Summary** tab displays appliance health and inventory status.

[Verify Connection between Carbon Black Cloud Workload Appliance and Carbon Black Cloud](#)

## Verify Connection between Carbon Black Cloud Workload Appliance and Carbon Black Cloud

Verify that the connection between the Carbon Black Cloud Workload Appliance and the Carbon Black Cloud is successfully established.

### Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 From the left navigation pane, click **Settings > API Access > API Keys**.
- 3 Go to the appliance API. You can see the appliance name with a link next to the appliance API name.
- 4 Click the appliance name. You can view appliance health and connection status.
- 5 From the left navigation pane, click **Inventory > Workloads > Not Enabled**. You can view VM data.
- 6 You can also verify connectivity using the following `curl` commands:

```
curl -v telnet://<carbonblack_prod_url>:443
* Rebuilt URL to: <carbonblack_prod_url>:443/
* Trying xx.00.xx.x...
* TCP_NODELAY set
* Connected to carbonblack_prod_url (xx.00.xx.x) port 443 (#0)

curl -v telnet://<vcsa_on_vc>:443
* Rebuilt URL to: telnet://<vcsa_on_vc>:443/
* Trying xx.0.0.xx...
* TCP_NODELAY set
* Connected to vcsa_on_vc (xx.0.0.xx) port 443 (#0)
```

### Results

The connection is established and the troubleshooting logs are shared with VMware.

## What to do next

To opt-out, go to the **Troubleshooting > Logs** page and toggle **OFF** the log export feature. See [Appliance Logs](#).



## View Inventory in the Carbon Black Cloud Workload Plug-in and the Carbon Black Cloud Console

After you successfully connect your appliance with the Carbon Black Cloud, you can view your inventory in the Carbon Black Cloud Workload Plug-in and the Carbon Black Cloud console.

### Prerequisites

- 1 [Connect the Carbon Black Cloud Workload Appliance with Carbon Black Cloud](#)
- 2 [Verify Connection between Carbon Black Cloud Workload Appliance and Carbon Black Cloud](#)

### Procedure

- 1 View your inventory in the Carbon Black Cloud Workload Plug-in:
  - a Go to the Carbon Black Cloud Workload Plug-in in the vCenter Server.
  - b Navigate to the **Inventory > Not Enabled** tab.
  - c To secure your workloads, see [Enable Carbon Black Cloud on Virtual Machines](#) .
- 2 View your inventory in the Carbon Black Cloud console:
  - a From the left navigation pane, click **Inventory > Workloads > Not Enabled**.
  - b Refresh the **Not Enabled** tab.

The virtual inventory appears within a few minutes after your appliance is connected.

### What to do next

[Register the Carbon Black Cloud Workload Appliance with NSX-T](#)

## Register the Carbon Black Cloud Workload Appliance with NSX-T

After you register the Carbon Black Cloud Workload Appliance with the vCenter Server and the Carbon Black Cloud, you can register an NSX integration with your Carbon Black Cloud organization.

This is an onboarding workflow that sets up a trust between the Carbon Black Cloud Workload Appliance and the NSX Manager appliance. After the onboarding completes, the Carbon Black Cloud Workload Appliance creates one or more pre-defined Distributed Firewall (DFW) policy templates for use by the Carbon Black Cloud, and instantiates them as a part of the initial authentication and configuration process. It creates the following NSX DFW policies and associated tags.

- `CB-NSX-Quarantine` – The VM workload is quarantined from the network. This is a read-only policy for NSX administrators. The policy allows the following network flows:
  - DHCP for IP addresses and DNS traffic for name resolution.
  - HTTPS traffic to a list of FQDNs required by sensor to remain connected to Carbon Black Cloud.

- `CB-NSX-Isolate` – The VM workload is completely isolated from the network. This is a read-only policy for NSX administrators.
- `CB-NSX-Custom` – Customizable by the NSX security admin. Advanced users can use such a policy to create a custom security posture.

After NSX-T integration, you can use the newly created NSX policies to remediate VM workloads in the Carbon Black Cloud console or you can remove applied NSX policies from VM workloads.

### Prerequisites

- Verify the Carbon Black Cloud Workload Appliance VM is powered-on.
- Verify the SSO registration is valid.
- The Carbon Black Cloud Workload Appliance must have a valid registration with both vCenter Server and Carbon Black Cloud.
- Communication between Carbon Black Cloud and Carbon Black Cloud Workload Appliance is over HTTPS.
- Communication between NSX and Carbon Black Cloud Workload Appliance is over HTTPS, and uses certificate-based authentication with NSX principal identity. For information on adding a role assignment or principal identity, see [VMware NSX-T Data Center Product Documentation](#).
- The supported NSX-T version is 3.1.3+.
- [Register the Carbon Black Cloud Workload Appliance with Carbon Black Cloud](#)

### Procedure

- 1 Log in to the Carbon Black Cloud Workload Appliance at `https://<appliance IP address>` using `admin` credentials.
- 2 Go to the **Appliance > Registration** page.
- 3 In the **NSX details** section, select the NSX Manager IP address from the **NSX hostname** dropdown menu.  
The **Register** button becomes active.
- 4 To initiate NSX on-boarding, click **Register**.
- 5 Enter the NSX administrator user name and password and click **Register**.

It can take up to 15 seconds for the process to complete. A green check mark confirms a successful registration.

- 6 Verify all objects are created in the NSX Manager:
  - a Log in to the NSX Manager with **admin** credentials.
  - b Navigate to the **Inventory > Groups** page and check if the following groups exist:
    - CB-NSX-Custom-Group
    - CB-NSX-Isolate-Group
    - CB-NSX-Quarantine-Group
  - c Navigate to the **Security > Distributed Firewalls > CATEGORY SPECIFIC RULES** page and check if the following default policies exist:
    - CB-NSX-Custom
    - CB-NSX-Isolate
    - CB-NSX-Quarantine
  - d Navigate to the **Inventory > Context Profiles > Context Profiles** page and check if the CB-NSX-Quarantine-Context-Profile exists with valid FQDNs.

#### What to do next

[Preparing VMs with Carbon Black Launcher](#)

## Preparing VMs with Carbon Black Launcher

You can enable Carbon Black in your data center. Carbon Black launcher is available on the Windows and Linux VMs.

**Before you begin:** [Register the Carbon Black Cloud Workload Appliance with NSX-T](#)

### Before you begin

[Register the Carbon Black Cloud Workload Appliance with NSX-T](#)

When you enable Carbon Black from the Carbon Black Cloud Workload Plug-in, the silent installation is triggered and the launcher downloads and installs the Carbon Black sensor on the virtual machine.

Carbon Black launcher is available for Windows and Linux VMs as follows:

- **Windows Virtual Machines:** For Windows VMs, the Carbon Black launcher is packaged with VMware Tools.

To receive the launcher for your workloads, you must install or upgrade VMware Tools to version 11.2+.

- **Linux Virtual Machines:** For Linux VMs, you must manually install the launcher available at VMware Tools Operating System Specific Packages (OSPs).

Download and install Carbon Black launcher from the [Broadcom Support Portal](#). For details, see [Carbon Black Launcher for Linux VMs](#).

## What to do next

[Enable Carbon Black Cloud on Virtual Machines](#)

### Carbon Black Launcher for Windows VMs

For Windows VMs, the Carbon Black launcher is packaged with VMware Tools. To receive the launcher for your workloads, you must install or upgrade VMware Tools to version 11.2+.

For more information, refer to [VMware Tools documentation](#).

---

**Note** The VM must have Internet connectivity.

---

You can find the launcher logs at the following locations.

- On the ESXi host: The log file is available at the `/vmfs/volumes/datastore_name/VM_NAME/vmware.log` location when you install or upgrade VMware Tools to version 11.2+.
- On the Windows VM: The logs are created at `C:\Windows\Temp\Cbinstall*.log` or `SystemTemp\Cbinstall*.log` when you trigger the Carbon Black installation.
- On the Windows VM: The logs are created at `C:\Windows\Temp\cb-install*.log` or `SystemTemp\Cb-install*.log` after the Carbon Black installation is complete.

### Carbon Black Launcher for Linux VMs

To enable the Carbon Black launcher on Linux virtual machines (VMs) where your workloads are running, you must first install the launcher.

#### Procedure

- 1 Go to the Linux VM.
- 2 Download the launcher from the [Broadcom Support Portal](#).
  - a Go to **My Downloads - Cyber Security Software**.
  - b Search for **VMware Carbon Black Cloud Workload**.
  - c Select the latest release and click the **Open Source** tab.

A `.tar.gz` file for Carbon Black CBLauncher for Linux Sensor is available (for example, `cbclinux-cblauncher-1.3.0.tar.gz`). This file contains both `cblauncher_1.3.0-21602657_amd64.deb` and `cblauncher-1.3.0-21602657.x86_64.rpm`.

---

**Note** The exact file names vary depending on the release version.

---

- 3 Download the Carbon Black CBLauncher for the Linux sensor by clicking the HTTPS download icon on the right.
- 4 Extract the `.tar.gz` file on the Linux VM.

## 5 Install the CBLauncher.

Linux Distribution	Command to Use for Installation
Ubuntu	<ul style="list-style-type: none"> <li> <pre>dpkg -i cblauncher_<i>[version]</i>-<i>[build number]</i>_amd64.deb</pre> </li> </ul> <p>For example:</p> <pre>dpkg -i cblauncher_1.3.0-2160265_amd64.deb</pre>
RHEL/SUSE/CentOS/Oracle/Amazon Linux	<ul style="list-style-type: none"> <li> <pre>rpm -Uvh cblauncher-<i>[version]</i>-<i>[build number]</i>.x86_64.rpm</pre> </li> </ul> <p>For example:</p> <pre>rpm -Uvh cblauncher-1.3.0-2160265.x86_64.rpm</pre>

## 6 To start the Carbon Black launcher daemon, run the following command with root privilege.

- For CentOS/RHEL/Oracle 6.x, issue the following command: `service cblauncher start`.
- For all other distributions, issue the following command: `systemctl start cblauncher`.

## 7 To stop the Carbon Black launcher daemon, run the following command with root privilege.

- For CentOS/RHEL/Oracle 6.x, issue the following command: `service cblauncher stop`.
- For all other distributions, issue the following command: `systemctl stop cblauncher`.

## 8 To verify the Carbon Black launcher status, run the following command with root privilege:

- For CentOS/RHEL/Oracle 6.x, issue the following command: `service cblauncher status`.
- For all other distributions, issue the following command: `systemctl status cblauncher`.

The status must be `Running`.

### What to do next

After the launcher is installed, enable Carbon Black on the Linux VMs from the Carbon Black Cloud Workload Plug-in. See [Enable Carbon Black Cloud on Virtual Machines](#).

## Install Sectigo Certificates

Carbon Black Cloud sensor installs on Windows Server 2008 R2 and Windows 7 can fail to verify signature information if the Sectigo signing certificate is not added to the trust store of the operating system.

Perform the following procedure to download and install the Sectigo signing certificates.

### Procedure

- 1 Go to the [Sectigo Intermediate Certificates](#) page and locate the **Root Certificates** section.
- 2 Click the **Download** link for **AAA Certificate Services**.
- 3 Click the **Download** link for the **SHA-2 Root: USERTrust RSA Certification Authority**.
- 4 To install the certificates, double click the `.crt` files and accept the default options.

---

**Note** When prompted, you must install the certificates for both options under **Store Location - Local Machine** and **Current User**.

---

### What to do next

You can now enable Carbon Black on your Windows Server 2008 R2 and Windows 7 machines.

## Enable Carbon Black Cloud on Virtual Machines

You must enable Carbon Black on the virtual machines (VM) where your application workloads are running.

### Prerequisites

- You have deployed and configured the Carbon Black Cloud Workload Appliance.
- Verify the operating system where you want to enable Carbon Black. For details, see [Chapter 2 Preparing to Enable Carbon Black in Your vSphere Environment](#).
- If you have older operating systems such as Windows 2008 R2 or Windows 7, you must use Sectigo certificates for signing the Carbon Black sensor MSI. Verify you installed the Sectigo certificates in your certificate store under `Trusted Root Certification Authorities`. For more information, see [Install Sectigo Certificates](#).
- Verify that a Carbon Black launcher is available.

### Procedure

- 1 Log in to the vSphere Client using your administrator credentials.
- 2 In the left navigation pane, click **Carbon Black**.
- 3 Open the **Inventory > Not Enabled** tab.

- 4 Verify the VM eligibility in the **Status** column. You can enable Carbon Black on the eligible VMs.

Status	Description
Eligible	A correct version of the VMware Tools and the Carbon Black launcher is available on the VMs. You can go ahead and enable Carbon Black on the VMs.
Not Eligible	<p>VMs might not be eligible to enable Carbon Black. For example:</p> <ul style="list-style-type: none"> <li>■ VM is powered off.</li> <li>■ The required version of the VMware Tools or Carbon Black launcher is not available.</li> <li>■ The <code>isolation.tools.setinfo.disable</code> parameter for the VM is set to <code>true</code>.</li> </ul> <p>To make a VM eligible, you can perform any of the following actions based on the non-eligibility criteria:</p> <ul style="list-style-type: none"> <li>■ Power on the VM.</li> <li>■ For Windows VMs: Install or upgrade VMware Tools to version 11.2+.</li> <li>■ For Linux VMs: Install the Carbon Black launcher manually. See <a href="#">Carbon Black Launcher for Linux VMs</a>.</li> <li>■ Set the <code>isolation.tools.setinfo.disable</code> parameter to <code>false</code>. See <a href="#">vSphere documentation</a>.</li> </ul>
Not Supported	Carbon Black Cloud Workload does not support the OS or the OS version. Upgrade to the supported OS and version. For details, see <a href="#">Chapter 2 Preparing to Enable Carbon Black in Your vSphere Environment</a> .

- 5 Select one or more eligible VMs for which to enable Carbon Black and click **Enable**.

Option	Description
To enable Carbon Black with the latest available version.	Proceed to the next step. Carbon Black is enabled with the latest available sensor version.
To enable Carbon Black with a particular version.	<ol style="list-style-type: none"> <li>1 Click <b>Advanced</b>. A list of available version appears for each OS.</li> <li>2 Only the supported sensor versions are listed. Select the required version from the dropdown menu.</li> <li>3 (Optional) You can preconfigure Carbon Black Cloud settings using the <code>configuration</code> file. You can upload the configuration file in an <code>.ini</code> file format. Click <b>Upload File</b>. Browse and select the <code>configuration</code> file.</li> </ol> <p>To view the sample configuration file and the parameter details, see <a href="#">Customize the Configuration File</a>.</p>

- 6 A confirmation dialog box opens. Click **OK**.

## Results

Carbon Black is enabled.

- Go to the **VM > Summary > Carbon Black** widget. You can view the installed version.
- Go to the **Carbon Black > Inventory > Enabled** tab. VM status is `Active`.

## What to do next

After enabling Carbon Black on VMs where workloads are running, you can start using the Carbon Black Cloud Workload Plug-in in the vSphere Client to monitor inventory in your data center. You can perform life-cycle management with a direct visibility in the vCenter Server.

The Carbon Black Summary page in the vSphere Client shows a summary of the VMs where Carbon Black is enabled.

You can open the Carbon Black Cloud console and create sensor groups and policies to meet your organization's security needs. You can identify, investigate, and remediate potential threats from the Carbon Black Cloud console.

## Customize the Configuration File

To enable Carbon Black with a specific sensor version, upload a *configuration* file. You can preconfigure the Carbon Black Cloud settings in the configuration file. By default, VMs are assigned to the Standard policy in the Carbon Black Cloud. You can define an alternate policy in the configuration file based on your organization requirements.

---

**Important** The configuration file is used for Carbon Black Cloud Workload Appliance only. It does not apply to other installations, and is primarily used for proxy settings.

---

### Sample Configuration File

```
[customer]
EncodedCompanyCode = 7X2KTWJQHO@RUO
CompanyCode = NBEA2
BackendServer = prod01.xyz.io
```

---

**Note** You can add additional parameters into the configuration file as described in [Install Sensors on VM Workloads](#).

---

*EncodedCompanyCode*, *CompanyCode*, and *BackendServer* are mandatory parameters in the configuration file.

### Procedure

- 1 In the left navigation pane, click **Inventory > VM Workloads**.



- 2 Click **Sensor Options**, click **View Company Codes**, and then click **Show**.

### View Company Codes ✕

---

[Registration](#) | [Deregistration](#) [Regenerate registration codes](#)

Use your registration code to install sensors by distribution system or imaging

Registration Code

**WX29KRLEHMSZYMSZ4FB1UMW** Copy

Windows v1.x - 2.x | macOS v1.x - 2.x [Hide](#)

**DBEFA** Copy

---

Close

- 3 Take note of the generated codes. The long string code is the **EncodedCompanyCode** and the short string code is the **CompanyCode**. Copy and paste the codes into a plain text editor.
- 4 For the *BackendServer* parameter, enter the device services URL for Carbon Black Cloud based on your region. For example, **https://devices.confer.net**.


# View the Carbon Black Cloud Workload Plug-in in the vCenter Server

# 4

After the Carbon Black Cloud Workload Appliance is deployed and configured, you can view the Carbon Black Cloud Workload Plug-in in the vCenter Server.

## Procedure

- 1 Log in to the vSphere Client using your administrator credentials.

- 2 Click the Carbon Black  icon in the left navigation pane or in the **Shortcuts** menu of the vSphere Client.

The Carbon Black Cloud Workload Plug-in dashboard or the **Summary** tab displays different widgets for a quick overview of the health and inventory status. Depending on your configuration, you can also view vulnerabilities affecting your assets and critical product vulnerabilities.

- 3 Go to the **Inventory > Not Enabled** tab to enable Carbon Black for your data center inventory.
- 4 Use the **Inventory > Enabled** tab to view the list of inventory protected by Carbon Black, and to update or disable Carbon Black for a selection of your data center inventory.

## What to do next

You can go to the individual VMs **Summary** or **Configure** tab and enable or update Carbon Black. You can go to the individual VMs **Monitor** tab and view VM-specific OS or application level vulnerabilities (if applicable).

## Sensor Status and Details

The **Status** column on the Carbon Black Cloud Workload Plug-in **Inventory > Enabled** tab indicates the installation or active state of the sensor and any admin actions taken on the sensor.

Sensor Status	Description
Active	Sensors are properly communicating to the Carbon Black Cloud.
Inactive	Sensors have not communicated to the Carbon Black Cloud for last 30 days.

Sensor Status	Description
Registered	Sensors are registered.
Deregistered	<p>Sensors are deregistered or uninstalled. Sensors persist on the <b>Inventory &gt; Not Enabled</b> tab in the <i>Deregistered</i> status until removed from the Carbon Black Cloud console.</p> <hr/> <p><b>Note</b> The sensor gets deleted when VM is deleted or VM is moved to another vCenter Server. The deleted sensors are displayed as <i>Deregistered</i> on the Carbon Black Cloud console. The workload sensors that are inactive for three or more days and have received a <i>delete</i> action from the vCenter Server are automatically <b>Deregistered</b>.</p>
Errors	Sensors are reporting errors.
Eligible for update	Sensors can be updated to the most current, available sensor version.
Bypass	<p>Sensors have been put into the <i>Bypass</i> mode by the Carbon Black Cloud administrator. All policy enforcement on the asset is disabled and the sensor does not send data to the Carbon Black Cloud.</p> <hr/> <p><b>Note</b> Sensors can momentarily enter <i>Bypass</i> mode during a sensor update.</p>
Quarantined	Sensors have been put into Quarantine mode by the Carbon Black Cloud administrator and are isolated from the network to mitigate spread of potentially malicious activity.

## Overview of Vulnerability Assessment

As a vCenter Server administrator, you need visibility of known vulnerabilities in your environment to understand your security posture and schedule maintenance windows for patching and remediation. With the help of vulnerability assessment, you can proactively minimize the risk in your environment. You can monitor known vulnerabilities from the Carbon Black Cloud Workload Plug-in. You can discover vulnerabilities from the **Summary** tab or from the **Vulnerabilities** tab and coordinate with your teams to schedule maintenance windows for patches or updates. To view the vulnerability assessment feature, you must enable Carbon Black in your data center. After enabling Carbon Black, you can typically view vulnerability data within a few minutes.

Carbon Black discovers vulnerabilities related to:

- Operating System (OS) of a virtual machine.
  - **Windows OS:** Displays OS-level vulnerabilities for Windows VMs. The system looks for OS details and the security patches applied on each VM. When the security patch associated with the vulnerability is not applied, the VM is flagged as vulnerable.
  - **Linux OS:** Displays OS-level vulnerabilities for Linux VMs. The system looks for OS details with the list of all installed packages. System determines the vulnerable packages installed on the VM and reports the CVEs against those packages.

- Applications installed on the virtual machine.
  - **Windows Apps:** Displays application-level vulnerabilities for Windows VMs.
  - **Linux Apps:** Displays application-level vulnerabilities for Linux VMs.

## Vulnerabilities Tab



- In the left navigation pane, click the Carbon Black icon.
- On the Carbon Black Cloud Workload Plug-in dashboard, click the **Vulnerabilities** tab.

Critical severity is the default filter. To display a list of all vulnerabilities available on the **Vulnerabilities** tab, click **All**. The total vulnerabilities are the count of all vulnerabilities across all monitored assets and products (OS, applications, versions).

You can either view the **Asset View** tab or the **Vulnerability View** tab. Use the **Asset View** tab to view which assets have known vulnerabilities. Use the **Vulnerability View** tab to view the list of all vulnerabilities on all the assets.

To export all data on the page to a CSV file, click **Export**.

---

**Note** The **Export** functionality is blocked in vCenter Server 6.7 and 7.0 due to a known vCenter Server issue. The issue is fixed in 7.0 U1 or later versions.

---

On the **Asset View** tab, the data is filtered on Windows and Linux. To view more details about the risk score and the Common Vulnerability Scoring System (CVSS), click the **Vulnerability Count** number. Expand the row to view further details. To view details of CVE on the external National Vulnerability Database website, click the [National Vulnerability Database](#) link. Click the asset name of the affected VM to open the **VM > Monitor > Carbon Black > Vulnerabilities** tab.

On the **Vulnerabilities** tab, the data is filtered based on the OS-level vulnerabilities and App-level vulnerabilities for Windows and Linux systems.

Vulnerability data for each virtual machine is refreshed automatically every 24 hours. To immediately view the updated vulnerability data, click **Reassess**.

---

**Note** Vulnerability data for the VMs newly added to your inventory is typically collected within minutes, but under certain circumstances it can take up to 24 hours.

---


## Working with OS Level Vulnerabilities

You can view all OS-level vulnerabilities from the Carbon Black Cloud Workload Plug-in **Vulnerabilities** tab.

The **Windows OS** tab displays a list of vulnerabilities for the virtual machines that have a Windows operating system. The **Linux OS** tab displays list of vulnerabilities for the virtual machines that have a Linux operating system.

You can view OS-level vulnerabilities for a particular virtual machine.

- 1 Go to the **VM > Monitor > Carbon Black > Vulnerabilities** tab.
- 2 Click the **OS** tab.

All the OS-level vulnerabilities related to that particular VM are listed. You can filter the columns using the filter  icon. You can also view the external National Vulnerability Database (<https://nvd.nist.gov/>) website.

To resolve the vulnerability for the Windows OS, look at the *CVE-ID*, and apply the suggested KB patch.

For Linux OS, vulnerability is associated at the package level. The **Version** and **Fixed By** column display the version and the build number in which the listed vulnerability is fixed.

To resolve the vulnerability for the Linux OS, upgrade to the listed version and the build number.


## Working with Application Level Vulnerabilities

You can view all application-level vulnerabilities from the Carbon Black Cloud Workload Plug-in **Vulnerabilities** tab.

The **Windows Apps** tab displays a list of application-level vulnerabilities for virtual machines that have a Windows operating system. The **Linux Apps** tab displays a list of application-level vulnerabilities for virtual machines that have a Linux operating system. The **VM > Monitor > Carbon Black > Vulnerabilities** tab of the virtual machine displays a list of application-level vulnerabilities for that virtual machine.

To view application-level vulnerabilities for a particular virtual machine:

- 1 Open the **VM > Monitor > Carbon Black > Vulnerabilities** tab.
- 2 Click the **App** tab.

Vulnerabilities for the actively running applications are displayed. You can filter the columns using the filter  icon.

Vendor and product information are provided. The **Version** and **Fixed By** column display the version and the build number in which the listed vulnerability is fixed. You must upgrade to the listed version and the build number to resolve the vulnerability. You can also look at the *CVE-ID* and view the external National Vulnerability Database (<https://nvd.nist.gov/>) website.

The **Fixed By** column might be empty if there is no update available from the product to fix the vulnerability or if Carbon Black does not have enough information to point to a specific resolution.

# Automatically Install Carbon Black Cloud Host User World

# 5

Carbon Black Cloud Host Module runs on the ESXi as a host user world process and provides unique identity information to the VMs. To save time from manual installation and configuration of a host user world on every host in your vCenter Server, you can use an automatic installation and configuration workflow.

You can install the host user world on a single host or on many hosts in a cluster.

## Prerequisites

- Host with ESXi 6.7 or later.
- vCenter Server 6.7 or later.
- Carbon Black Cloud Workload Appliance 1.1 or later.
- The host must be powered on and connected to the vCenter Server.

## Procedure

- 1 Log in to the vSphere Client with administrator credentials.
- 2 Select a host from the inventory tree and click the **Configure** tab.
- 3 Navigate to the **Carbon Black > Security** page and click **Enable Host Module**.

This action takes up to 5 minutes.

After the installation completes, the status changes from **Installable** to **Up to date**. You can see the host user world version and its general status as connected.

- 4 To upgrade the host user world to its latest version, click **Upgrade Host Module**.  
After the upgrade completes, the status changes from **Upgradable** to **Up to date**.
- 5 Optional: To install the Carbon Black Cloud Host Module on all hosts in a cluster:
  - a Select the cluster from the inventory tree and click the **Configure** tab.
  - b Navigate to the **Carbon Black > Security** page, and click **Enable Host Module**.
  - c Select **Confirm** in the **Carbon Black Cloud** popup window.

### **What to do next**

Install Carbon Black Cloud sensors on Linux or Windows VMs in a vCenter Server environment to enable the automatic identification and registration of VDI clones.

# Manually Install Carbon Black Cloud Host User World

## 6

You can install the Carbon Black Cloud Host User World module on ESXi hosts by remediating individual hosts or all hosts in a cluster collectively through the vSphere Lifecycle Manager service. This service lets you use a vSphere Lifecycle Manager single image as an alternative way to install and manage the lifecycle of the ESXi hosts.

To install the Host User World module, you first must add your third-party download source under the **Settings** tab. The download sources are online depots for downloading software.

Next, update your local vSphere Lifecycle Manager depot immediately by initiating synchronization between the vSphere Lifecycle Manager depot and the download source. As a result, the component that must download (the VMware Carbon Black component for ESX) displays under the **Image Depot** tab. When vSphere Lifecycle Manager synchronizes to online depots, it downloads only the update metadata. The actual payload will download during staging or remediation.

Check the compliance status of the ESXi hosts against the ESXi image hosted in the depot, and remediate the hosts against that image under the **Updates** tab.

### Prerequisites

- Hosts must be running ESXi 7.0+.
- You must power on your hosts and connect them to the vCenter Server.
- You must own the required privileges for using vSphere Lifecycle Manager images. For more information, see *Managing Host and Cluster Lifecycle*, which is part of the *vSphere 7.0 → ESXi and vCenter Server* documentation.

### Procedure

- 1 Log into the vSphere Client using your administrator credentials.
- 2 Click **Menu > Lifecycle Manager**.
- 3 On the **Settings** tab, select **Administration > Patch Setup**.

The Internet is the default download source for vSphere Lifecycle Manager.



- 4 To download a third-party component, such as the Carbon Black component for ESX, click **New** and enter the URL address for the download source.

Option	Description
<code>https:// prod.cwp.carbonblack.io/ cbhost/us/online-depot/ index.xml</code>	Depot URL for the United States region.
<code>https:// prod.cwp.carbonblack.io/ cbhost/au/online-depot/ index.xml</code>	Depot URL for the Africa Union region.
<code>https:// prod.cwp.carbonblack.io/ cbhost/ap/online-depot/ index.xml</code>	Depot URL for the Asia-Pacific region.
<code>https:// prod.cwp.carbonblack.io/ cbhost/eu/online-depot/ index.xml</code>	Depot URL for the Europe region.

The description is optional.

- 5 To keep the changes, click **Save**.

The source URL appears at the bottom of the list of download sources.

- 6 To update your local vSphere Lifecycle Manager depot immediately, locate the **Actions** dropdown menu, and click **Sync Updates**.

The vSphere Lifecycle Manager downloads the software from the online depot that you configured it to use. The Carbon Black component is available in the **Image Depot > Components** table.

- 7 To make the hosts in your cluster manageable by a single image, you must set up the image.
- From the **vSphere Client** dropdown menu, click **Hosts and Clusters** and select the cluster to manage using the image.
  - On the **Updates** tab, select **Hosts > Image**, and click the **Setup Image** button.
  - To define the image in Step 1, select the ESXi version from the related dropdown menu, click **Add Components**, and select the **VMware Carbon Black** component.  
The Carbon Black component shows in the **Additional components** table.
  - Click **Validate**, and after the image shows as **Valid**, click **Save**.

- e To check the compliance of your hosts with the defined image in Step 2, select a host, and click **Check Compliance**.
- f When all hosts in your cluster are compliant with the newly defined image, click **Finish Image Setup** and confirm the action.

The **Image** and **Image Compliance** panels show summary of the image setup.

**8** Remediate all your hosts in the cluster:

- a In the **Image Compliance** panel, click the **Remediate All** button.

The **Review Remediation Impact** screen displays.

- b Accept the terms of the end user license agreement and click **Start Remediation**.

The **Image Compliance** panel notifies you when the remediation process completes successfully. The remediation installs only the VIBs on the hosts and does not configure the Host User World module.

**9** On the **Configure** tab, click **Configuration > Security**.

The **Host status** displays as `Needs install`.

**10** Click the **Enable Host Module** button.

After the operation completes successfully, the **Host status** displays as `Latest sensor installed`.

**11** Optional: Select a host from the cluster, navigate to the **Configure > Security** page, and view the Carbon Black Cloud summary.

**What to do next**

Select the managed cluster, navigate to the **Updates > Hosts > Image** page, and click **Check Compliance**.

The image remains compliant with all the hosts in the cluster. Change in the image (due to other components), do not remove the Host User World module from the hosts because the component is included in the image.

# Using the Carbon Black Cloud Workload Appliance

# 7

You can view the overall status of the Carbon Black Cloud Workload Appliance using the appliance dashboard. You can also register to vCenter Server, connect to Carbon Black Cloud, configure NTP server settings, and view the network settings.

---

**Note** You must implement network controls to limit the appliance interface access to authorized administrators only. Unrestricted network access to the appliance interface is not required.

---

You can log in to the Carbon Black Cloud Workload Appliance console at **https://<appliance IP address>** using the **admin** credentials. The appliance dashboard appears as a default home page. The dashboard displays the overall health status of the appliance. By default, the session timeout for the appliance is five minutes.

Read the following topics next:

- [Manage Appliance Users](#)
- [Configure NTP Server Settings](#)
- [View and Update Network Settings](#)
- [Configure Proxy Settings for an Appliance](#)
- [Appliance Health Status](#)
- [Maintaining the Appliance Password](#)
- [Reboot Appliance](#)
- [Redeploy a Carbon Black Cloud Workload Appliance](#)
- [Appliance Logs](#)

## Manage Appliance Users

As an appliance administrator, you can manage the users in the Carbon Black Cloud Workload appliance. You can add new system users, assign them to different groups, or remove them. You can also set a password for a new user account or update the password for an already existing user.

### Prerequisites

Make sure your user belongs to the wheel group with **root** and **admin** privileges.

### Procedure

- 1 Log in to the appliance using root credentials.
- 2 To create a new user with a specified home directory and a group, to which the user belongs to, issue the command `useradd -m -G <group-name> <user-name>`.

Run the command `useradd -m -G group1,group2 user1`.

The example command creates a new user - `user1`, which is part of two groups - `group1` and `group2`.

- 3 To set a new password for a newly created user, use the command `passwd <user-name>`.

Run the command `passwd user1`.

The example command creates a new password for `user1`.

---

**Note** You can also use the `passwd` command to change the password for a user.

---

## Configure NTP Server Settings

You must configure the NTP server to synchronize the SSO server time and the Carbon Black Cloud Workload Appliance time.

### Prerequisites

You have deployed the Carbon Black Cloud Workload Appliance.

### Procedure

- 1 Log in to the vCenter Server at `https://<vCenter IP/Domain address>` using admin credentials.
- 2 To configure the time synchronization settings with the vCenter Server, click the **Appliance > General** tab.

- 3 In the **Time Settings** section, click **Edit** and add the following details:

**Note** A time difference between the appliance and the vCenter Server results in a clock skew error. Set the NTP synchronization between the appliance and ESXi host as described in [Knowledge Base Article 2012069](#).

Time Settings	Description
NTP server	A Network Time Protocol (NTP) server is used for synchronizing the time. Enter the same NTP server that is used to set up the vCenter Server configuration. For example, <code>pool.ntp.org</code> . When entering the multiple NTP servers, use a comma-separated list followed by a space between the entries.
Fallback NTP server	Enter details for an alternative NTP server.
Date and Time	Verify that the date and time are synchronized with the vCenter Server.

- 4 Click **Save**.

## View and Update Network Settings

To view network settings of the appliance VM, open the **Network** page . You can view details about an IP address of the appliance, the network gateway, and the DNS-related details. To update the network settings, use the virtual appliance management interface (VAMI). You cannot modify the network settings from the appliance user interface.

### Procedure

- 1 Log in to the appliance using root credentials.
- 2 Run the VAMI CLI command `/opt/vmware/share/vami`.

Verify the list of options available for network settings using the `/opt/vmware/share/vami/vami_set_network --help` command.

- 3 Update the desired network configuration parameters.

For example:

```
vami_set_network <interface> (DHCPV4|DHCPV6|AUTOV6|DHCPV4+DHCPV6|DHCPV4+AUTOV6|
DHCPV4+NONEV6)
vami_set_network <interface> (STATICV4|STATICV4+DHCPV6|STATICV4+AUTOV6|STATICV4+NONEV6)
<ipv4_addr> <netmask> <gatewayv4>
vami_set_network <interface> (STATICV6|DHCPV4+STATICV6) <ipv6_addr> <prefix> (<gatewayv6>|
default)
vami_set_network <interface> STATICV4+STATICV6 <ipv4_addr> <netmask> <gatewayv4>
<ipv6_addr> <prefix> (<gatewayv6>|default)
```

- 4 Restart the appliance VM.
- 5 Log in to appliance using admin credentials.

- 6 Verify the updated network settings on the **Configuration > Network > Network details** tab.

## Configure Proxy Settings for an Appliance

configure the proxy server to establish a secure connection with the Carbon Black Cloud. All the outgoing network traffic from the Carbon Black Cloud Workload Appliance to the Carbon Black Cloud can flow through the configured proxy server.

After setting up your proxy server in the Carbon Black Cloud Workload Appliance, you can verify if the Carbon Black Cloud URL is reachable from that proxy server.

### Prerequisites

Register the Carbon Black Cloud Workload Appliance with Carbon Black Cloud, and vCenter Server.

The proxy support for appliance is available for version 1.1 or later.

### Procedure

- 1 Log in to the vCenter Server at **https://<vCenter IP/Domain address>** using admin credentials.
- 2 To configure the proxy settings, open the **Appliance > Network** page.
- 3 Click the **Proxy** tab and click **Edit**.



- a Select the required proxy type as **HTTP**, **HTTPS**, **SOCKS4**, or **SOCKS5**.
  - b Enter the proxy server host name without the HTTP or HTTPS scheme.  
Do not enter the `http://` or `https://` header.
  - c Enter the port that the proxy server listens to.  
Use the correct port value for the selected proxy type. Incorrect combination of a port number and a proxy type leads to Carbon Black Cloud Workload appliance being unable to connect to Carbon Black Cloud through proxy.
  - d Enter the proxy user name and password, if necessary for the proxy.
- 4 Click **Save**.

The proxy server settings are configured. Once configured, the settings are effective immediately.

If the proxy server is not reachable, saving your configuration generates an error message.

- 5 To check whether the appliance VM connects to Carbon Black Cloud through the proxy server, click **Verify**.

The **Verify connection to Carbon Black Cloud** window displays.

- 6 Select the Carbon Black Cloud environment to which you want the appliance to connect and click **Test**.

You get a notification for the status of the connection. If the appliance is unable to connect to the cloud, update your proxy settings.

## Results

The connection status displays in the **Dashboard > Health** and in the **Appliance > Registration > VMware Carbon Black Cloud** panels.

## Appliance Health Status

You can view overall health status of the Carbon Black Cloud Workload Appliance using the Carbon Black Cloud Workload Plug-in. You can view the connectivity status of each appliance service on the Carbon Black Cloud Workload Plug-in, and you can view service-wise health status on the Carbon Black Cloud Workload Appliance dashboard.

Appliance services are:

- Appliance Worker
- vSphere Worker
- Gateway
- Access Control Service

The appliance can have be in of the following health states:

- **Connected:** The appliance is connected.
- **Disconnected:** The appliance is disconnected. If the status is disconnected, make sure that the appliance VM is powered-on. Go to the appliance **Registration** tab and verify the configurations.

---

**Note** During the vCenter Server reboot, the Carbon Black Cloud Workload Appliance can show vCenter Server as unregistered. You must wait until the vCenter Server is up and running before verifying connection with the appliance.

---

- **Unhealthy:** The appliance is connected, but one of the services is down. The individual appliance services can have **Connected** or **Disconnected** status. When the appliance status is **Unhealthy**, look for the individual service status. For the disconnected appliance service, you can restart the service as follows:
  - a SSH to the Carbon Black Cloud Workload Appliance using admin credentials.
  - b Switch to the root user using the `sudo su` command.

- c Use the appropriate command for the service to restart:

```
systemctl restart cwp-appliance-worker
```

```
systemctl restart cwp-access-control-service
```

```
systemctl restart cwp-vsphere-worker
```

```
systemctl restart cwp-appliance-gateway.service
```

- d Reverify the appliance service status.
- e If any appliance service is still down, contact Broadcom Carbon Black Support or the VMware support team.

Log files help the support team to troubleshoot any issues for which you have opened a support ticket.

## Maintaining the Appliance Password

An appliance password is active for a certain amount of time. To maintain the password, reset it or extend the expiration time.

The password for the appliance expires in 90 days after you deploy the appliance for the first time. The appliance interface displays a notification when your password is due to expire. The message appears 15 days before the password expiry. The Carbon Black Cloud Workload Plug-in also shows a notification regarding the appliance's password expiry. You must reset the password before it expires. You can also extend the password expiration time manually or disable the password expiration permanently.

By default, the appliance time zone is UTC.

The Carbon Black Cloud Workload appliance console shows a root password expiration notification. You can also view the appliance root password expiration notification in the Carbon Black Cloud Workload Plug-in, which is part of the vSphere Client.

## Reset Appliance Password

If you are locked out of the Carbon Black Cloud Workload Appliance that has admin privileges, you can reset the password.

### Procedure

- 1 Log in to the vCenter Server at **https://<vCenter IP/Domain address>** using admin credentials.
- 2 Under **Hosts & Clusters**, select the Carbon Black Cloud Workload Appliance.
- 3 In vCenter Server, click the **Summary** tab and click **Launch Web Console**.
- 4 In the **Web Console** window, use the root credential to log in.



- 5 Verify if the admin account is locked using the `pam_tally2 -u admin` command.
- 6 If the admin account is locked, issue the following command to unlock it:

```
pam_tally2 -r -u admin
```

- 7 To change the admin user password:
  - a SSH to the Carbon Black Cloud Workload Appliance using admin credentials.  
For example, SSH `admin@<Appliance_IP_Address>`.
  - b Issue the `passwd admin` command.
  - c Enter the current password and then enter the new password.

---

**Note** Do not use the last five passwords. The password must have at least eight characters. Enter a password that meets basic complexity: at least one number, one lower case letter, one upper case letter, and one special character.

---

- d Re-enter the admin password.  
The Carbon Black Cloud Workload Appliance admin user password is changed.
- 8 The appliance password automatically expires after 90 days. To reset the expired password:
  - a SSH to the Carbon Black Cloud Workload Appliance using admin credentials.
  - b Enter an admin password.

---

**Note** Do not use the last five passwords. The password must have at least eight characters. Enter a password that meets basic complexity: at least one number, one lower case letter, one upper case letter, and one special character.

---

- c Re-enter the admin password.
  - d SSH to the Carbon Black Cloud Workload Appliance to verify that the password change is successful.
  - e Log in to the Carbon Black Cloud Workload Appliance using the admin user name and the updated password.
- 9 To reset the root password.

---

**Note** For security reasons, SSH access for the root user is disabled on the Carbon Black Cloud Workload Appliance by default.

---

- a SSH to the Carbon Black Cloud Workload Appliance using the admin credentials.
  - b Reset the password using the following commands:

```
sudo su
passwd root
```

- c Enter the current password and then the new password.

## Extend Password Expiration Time for Appliance

You can manually extend the password expiration time to the required number of days for the Carbon Black Cloud Workload Appliance. You can also disable the password expiration permanently.

### Procedure

- 1 To extend password expiration time manually:
  - a SSH to the Carbon Black Cloud Workload Appliance using admin credentials.
  - b Run the following commands and extend the password expiration time to the required number of days for both root and admin users. The following example shows 180 days.

```
sudo chage -I -1 -m 0 -M 180 -E -1 admin
sudo chage -I -1 -m 0 -M <number of days> -E -1 admin
sudo chage -I -1 -m 0 -M 180 -E -1 root
sudo chage -I -1 -m 0 -M <number of days> -E -1 root
```

- 2 To disable the password expiration permanently:
  - a SSH to the appliance using admin credentials.
  - b Run the following commands and disable the password expiration permanently for both root and admin users.

```
sudo chage -I -1 -m 0 -M 99999 -E -1 admin
sudo chage -I -1 -m 0 -M 99999 -E -1 root
```

## Disable the Admin Password Expiration

By default, the administrative password for the Carbon Black Cloud Workload appliance expires in 90 days. However, you can disable the password expiry after initial installation and configuration.

If your admin password expires, you cannot log in and manage components. Additionally, any task or API call that requires the admin password to execute results with a failure. To resolve such cases in advance, you can disable the password expiry so the password never expires.

### Procedure

- 1 Log in to the vCenter Server at **https://vCenter IP/Domain address** using admin credentials.
- 2 Open the **Appliance > General > Password Settings** tab.  
By default, the admin password expiry option is enabled.
- 3 To disable the expiration of the admin password, click the related toggle switch.  
The toggle changes its state to **Inactive**.

## Reboot Appliance

For any issues, you can reboot the Carbon Black Cloud Workload Appliance using one of the following methods.

- From the vCenter Server, right-click the Carbon Black Cloud Workload Appliance, and click **Power > Restart Guest OS**.

-OR-

- SSH to the Carbon Black Cloud Workload Appliance and run the `sudo reboot` command.

## Redeploy a Carbon Black Cloud Workload Appliance

If the Carbon Black Cloud Workload Appliance is unreachable and unresponsive, you can redeploy the appliance. You must register the appliance using the original SSO and vCenter Server. You must regenerate the API ID and the key for the appliance from the Carbon Black Cloud console, and use the new API ID and key to establish a connection between the appliance and the Carbon Black Cloud.

### Procedure

- 1 Delete the Carbon Black Cloud Workload Appliance from the vCenter Server. See [Delete Appliance from vCenter Server](#).
- 2 Deploy the Carbon Black Cloud Workload Appliance as described in [Deploy the Carbon Black Cloud Workload Appliance in the vCenter Server](#).

---

**Note** If you cannot access the appliance user interface, clear the web browser SSL certificate cache, and then log in to the appliance.

---

- 3 Register the appliance using the same SSO and vCenter Server as described in [Register the Carbon Black Cloud Workload Appliance with On-Premises vCenter Server](#).
- 4 Generate the API ID and key.

For details, see [Generate an API ID and API Secret Key](#).

---

**Important** The appliance name must be unique for your Carbon Black Cloud organization. You cannot use the original appliance name or API ID and API secret key of the previously registered appliance.

---

- 5 Register the appliance using the API ID and API secret key. See [Connect the Carbon Black Cloud Workload Appliance with Carbon Black Cloud](#).

## Appliance Logs

The appliance log bundle is a collection of diagnostic information that the VMware support and engineering teams require to troubleshoot any problem that you encounter. The support team can collect the appliance log bundle from the cloud for further analysis and troubleshooting.

You can set the logging level for each service from the appliance. The VMware support team can ask you to change the appliance log level or export the logs while troubleshooting any problem. For the VMware support team, the logs upload to the *prod.cwp.carbonblack.io* domain.

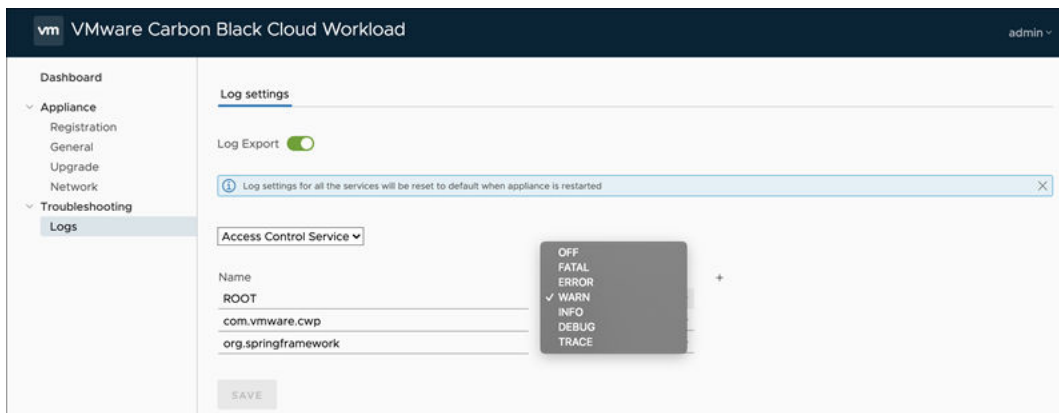
You can configure the log export and log level options. The log level can be configured in a built-in package file such as *Root* and *com.vmware.cwp*. By default, *Root* has **Warning** and *com.vmware.cwp* has **Info** as the assigned log levels.

### Prerequisites

- You must open firewall for the *prod.cwp.carbonblack.io* domain with TCP port 443.
- The VMware support team can change the appliance log level and export logs for troubleshooting. If you do not want to share any logs with VMware for troubleshooting purposes, toggle to turn **Off** the **Log Export**.

### Procedure

- 1 Log in to the vCenter Server at **https://vCenter IP/Domain address** using admin credentials.
- 2 Open the **Troubleshooting > Logs** page.



- 3 By default, the **Log Export** toggle is **On**. Toggle to turn **Off** the log export. The logs get deleted on a rolling two-month retention schedule.
- 4 Select the required service from the list. To change the log level settings, select the required log level as follows:

Log Level	Description
<b>Off</b>	Logging is turned off. Use this option to turn off logging for a specific service.
<b>Error</b>	Logs only the error events that might still allow the application to continue running.
<b>Warning</b>	Logs the potentially harmful situations.
<b>Info</b>	Logs the informational messages that highlight the progress of the application at a coarse-grained level.

Log Level	Description
Debug	Logs the fine-grained informational events that are the most useful to debug an application.
Trace	Logs finer-grained informational events than the Debug level.

5 To save your changes, click **Save**.

# Updating Carbon Black in your vSphere Environment



You can update the Carbon Black sensors when an updated sensor version is available from the Carbon Black Cloud Workload Plug-in. You can upgrade the appliance and plug-in together by scheduling upgrade frequency in the appliance.

Read the following topics next:

- [Update Carbon Black Sensors on Virtual Machines](#)
- [Upgrade the Carbon Black Cloud Workload Appliance](#)

## Update Carbon Black Sensors on Virtual Machines

You can update Carbon Black sensors on the virtual machines (VM) where your workloads are running.

To update Carbon Black on all enabled VMs:

### Procedure

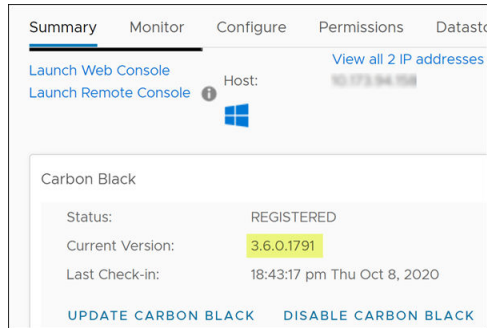
- 1 Log in to the vSphere Client using admin credentials.
- 2 In the left navigation pane, click **Carbon Black**.
- 3 Open the **Inventory > Enabled** tab.
- 4 Select VMs to update Carbon Black sensors and then click **Update**.
- 5 Click **OK**.

### Results

Carbon Black is updated to the latest available sensor version.

You can also update Carbon Black for individual VMs. Go to the VM to update. On the **Summary** tab, scroll down to the Carbon Black panel. Alternatively, you can use the **Configure > Carbon Black > Security** tab.

You can view the sensor version on the Carbon Black panel.



## Upgrade the Carbon Black Cloud Workload Appliance

You can perform either an instant appliance upgrade or a scheduled one.

You can automatically upgrade the Carbon Black Cloud Workload Appliance by scheduling the upgrade frequency. When a new upgrade bundle becomes available, your appliance upgrades based on the selected day and time.

You can use the **Upgrade Now** button to bypass the scheduler. This can be necessary when you have to respond to a critical issue in your environment.

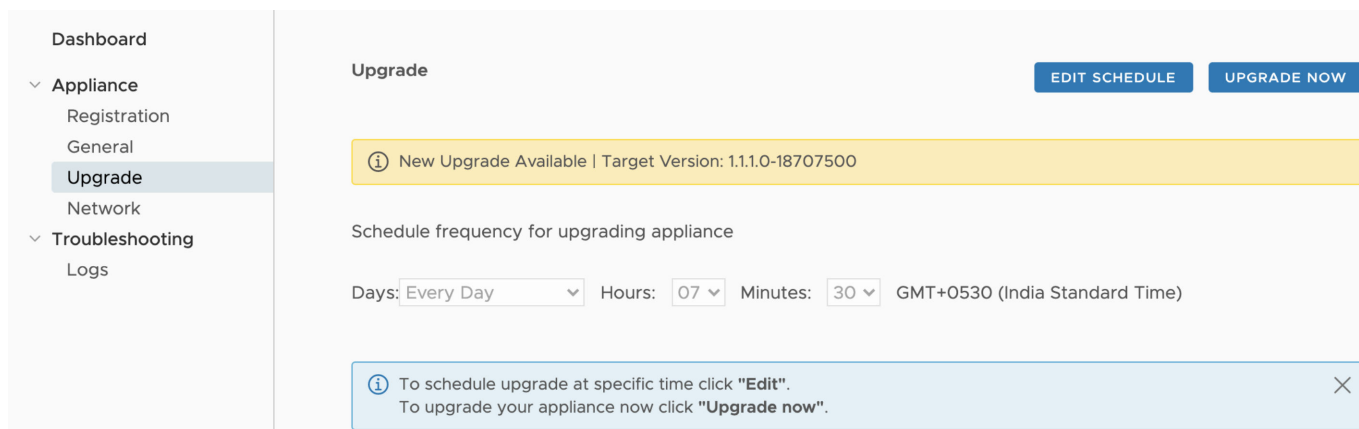
### Prerequisites

Open the firewall for the *prod.cwp.carbonblack.io* domain with TCP port 443.

### Procedure

- 1 Log in to the vCenter Server at **https://vCenter IP/Domain address** using admin credentials.
- 2 Go to the **Appliance > Upgrade** page.
- 3 Click **Edit** and select the required day, hour, and minutes for the upgrade.
- 4 Click **Save** to schedule the upgrade of the appliance.

Set the date and time for the upgrade in your local time zone. The appliance converts your local time in UTC time. Upgrade occurs in the appliance UTC time zone.

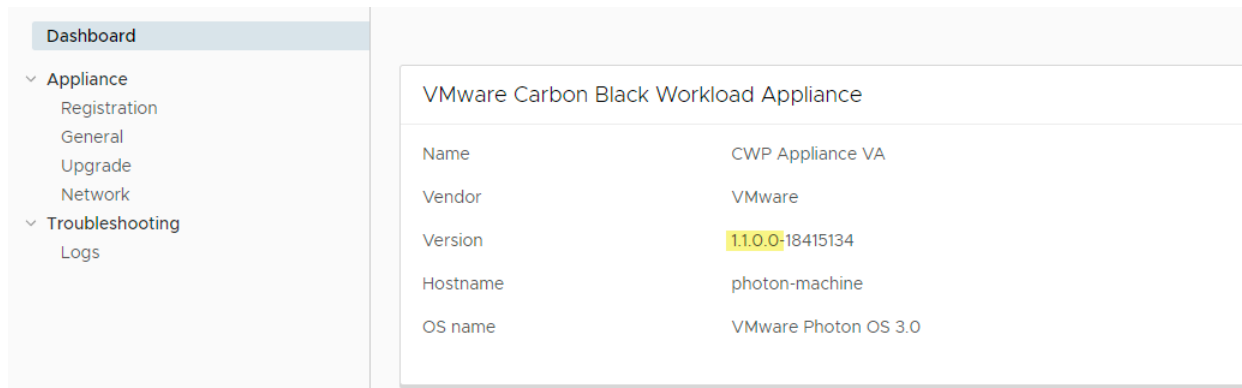


- 5 Optional. Click the **Upgrade Now** button to immediately upgrade the Carbon Black Cloud Workload Appliance.

The **Upgrade Now** button is present only if an upgrade is available.

## Results

After the appliance upgrades, the Carbon Black Cloud Workload Plug-in upgrades as well. You can view the new version and the build number on the appliance dashboard.



## Upgrade an Appliance To 1.0.2

You must upgrade your appliance to the 1.0.2 version using the instructions provided in this topic because the automatic appliance upgrade to the version 1.0.2 does not work. The system fails to extract the downloaded upgrade bundle due to a ZIP extraction error.

- 1 Verify the appliance upgrade status:
  - a Log in to the Carbon Black Cloud Workload Appliance at **https://<appliance IP address>** using admin credentials.
  - b Open the **Appliance > Upgrade** page.
  - c The automatic upgrade starts based on your configured day and time. If the automatic upgrade has failed, you can see the `upgrade failed` error.



- 2 Verify the reason for the upgrade failure:
  - a SSH to the appliance CLI using the admin credentials. For example, `ssh admin@<appliance IP address>`.
  - b Run the following command.

```
cat /var/log/cwp/apw_upgrade_status.json
```



- c Review the value of the status field in the output. Sample output:

```
{ "status": "EXTRACTING_WRAPPER_BUNDLE_FAILED", "reboot_pending": null, "message": "Zip
entry breaches extract location, entry resolved path: /var/
vmware/bundle/bundles/staging/wrapper-1.0.2.0-xxxxxxx/cwp-appliance-bundle- 1.0.2.0-
xxxxxxx.zip, extract location/opt/vmware/cwp/etc/bundles/staging/wrapper- 1.0.2.0-
xxxxxxx", "source_version": null, "target_version": "1.0.2.0-xxxxxxx" }
```

- If status is *EXTRACTING\_WRAPPER\_BUNDLE\_FAILED*, the system fails to download the upgrade bundle due to a ZIP extraction error. This error occurs on all 1.0.1 appliances. Proceed to Step 3.
  - If status is *TIMEDOUT\_WAIT\_FOR\_TERMINAL\_STATUS*, then the root and admin passwords of your appliance are expired and you must first reset the passwords before proceeding with the upgrade. Change the passwords as explained in the [Reset Appliance Password](#) topic and then proceed to Step 3.
- 3 Download and run the shell (.sh) script file as follows.

- a Click the following link to download the script file. Extract the file to your local machine.

[https://community.carbonblack.com/gbouw27325/attachments/gbouw27325/cloud\\_workload\\_documents/7/1/update-config.zip](https://community.carbonblack.com/gbouw27325/attachments/gbouw27325/cloud_workload_documents/7/1/update-config.zip).

-OR-

Copy the following code as the `update-config` shell script file.

```
CONFIG_FILE="/opt/vmware/cwp/appliance-worker/config/application.yml"

if grep -q "upgrade.staging.location" "${CONFIG_FILE}"
then
    # Already exists, nothing to do
    echo "Settings already up-to-date. Nothing to do!"
else
    # Add config and restart service
    echo "Updating config..."
    sed "-i.$(date +%s)" 'li upgrade.staging.location: /var/vmware/bundle/bundles/
staging' "${CONFIG_FILE}"

    echo "Restarting appliance worker service..."
    systemctl restart cwp-appliance-worker.service
    sleep 10

    echo "Settings updated successfully!"
fi
```

- b Copy the script file to the appliance VM using the following command:

## Linux:

```
scp <Location_Of_update-config.sh_File> admin@<Appliance_VM_IP>:
admin@<Appliance_VM_IP>'s password:
```

## Windows:

```
pscp -scp -P 22 <Location_Of_update-config.sh_File> admin@<Appliance_VM_IP>:
admin@<Appliance_VM_IP>'s password:
```

- c SSH to the appliance VM using admin credentials and switch to the root user.

```
ssh admin@<Appliance_VM_IP>
Warning: Permanently added '<Appliance_VM_IP>' (RSA) to the list of known hosts.
admin@<Appliance_VM_IP>'s password:
admin@<Appliance_VM_IP> [ ~ ]$ su -
Password:
root@<Appliance_VM_IP> [ ~ ]#
```

- d Change the permissions of the file to make the file executable:

```
# chmod +x /home/admin/update-config.sh
```

- e Execute the script using the following command.

```
# ./update-config.sh
```

- f The sample output appears as follows.

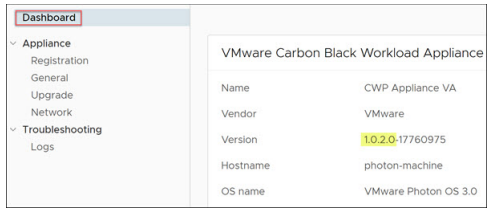
```
Updating config...
Restarting appliance worker service...
Settings updated successfully!
```

- 4 Schedule your appliance upgrade. For upgrade information, see [Upgrade the Carbon Black Cloud Workload Appliance](#) .

When the upgrade is initiated as per the schedule, monitor the upgrade page in the appliance console for the result. The upgrade process generally finishes in 10 to 15 minutes.

- 5 To verify your upgrade:

- Go to the appliance dashboard to view the updated version and build number.



The screenshot shows a web interface for the VMware Carbon Black Workload Appliance. On the left is a navigation menu with 'Dashboard' selected. The main content area displays system information for 'VMware Carbon Black Workload Appliance'.

VMware Carbon Black Workload Appliance	
Name	CWP Appliance VA
Vendor	VMware
Version	1.0.2.0-17760975
Hostname	photon-machine
OS name	VMware Photon OS 3.0

- Go to the **Upgrade** page. Make sure there is no upgrade-related error message.

# Disable Carbon Black from your vSphere Environment

# 9

You can manually disable the Carbon Black sensors or from the Carbon Black Cloud console. Disabled sensors are displayed as **Deregistered**.

You can uninstall an appliance that is no longer required.

Read the following topics next:

- [Uninstall and Delete Carbon Black Sensors](#)
- [Delete Appliance from vCenter Server](#)

## Uninstall and Delete Carbon Black Sensors

Uninstalled Carbon Black sensors persist in the Carbon Black Cloud Workload Plug-in as **Deregistered** until you remove them.

### Manually Uninstall Sensors on Windows VMs

To manually uninstall sensors on Windows VMs, follow the steps in [Uninstall a Windows Sensor from an Endpoint](#) in the *Carbon Black Cloud Sensor Installation Guide*.

### Manually Uninstall Sensors on Linux VMs

To manually uninstall sensors on Linux VMs, follow the steps in [Uninstall a Linux Sensor from an Endpoint](#) in the *Carbon Black Cloud Sensor Installation Guide*.

### Uninstall Sensors using the Carbon Black Cloud Console

To uninstall sensors by using the Carbon Black Cloud console, see [Uninstall Sensors from the Endpoint by using the Carbon Black Cloud Console](#) in the *Carbon Black Cloud Sensor Installation Guide*.

### Delete Deregistered Sensors

To delete deregistered sensors, see [Delete Deregistered Sensors from Endpoints](#) in the *Carbon Black Cloud Sensor Installation Guide*.

## Delete Appliance from vCenter Server

You can remove a Carbon Black Cloud Workload Appliance virtual machine (VM) from a vCenter Server.

### Procedure

- 1 Log in to the vCenter Server at **https://<vCenter IP/Domain address>** using admin credentials.
- 2 Open the **Appliance > Registration** tab.
- 3 In the SSO lookup configuration section, click **Edit** and then click **Unregister**.
- 4 In the vCenter Server Details section, click **Unregister**.
- 5 Click **OK**.
- 6 Log in to the vSphere Client using admin credentials.
- 7 Power off the Carbon Black Cloud Workload Appliance VM.
- 8 To delete the Carbon Black Cloud Workload Appliance VM from the datastore, right-click the appliance VM.
- 9 Select **Delete from Disk** and click **OK**. For details, refer to the *vSphere Documentation*.  
The appliance is deleted from the vCenter Server and the Carbon Black Cloud Workload Plug-in is uninstalled. To verify, log out and log in to the vCenter Server.
- 10 The Carbon Black Cloud console displays the appliance health status as **Disconnected**. You can verify appliance status in the Carbon Black Cloud console as follows.:
  - a Log in to the Carbon Black Cloud console.
  - b On the left navigation pane, click **Settings > API Access > API Keys**.
  - c Go to the appliance API. You can see the appliance name with a link next to the appliance API name.
  - d Click the appliance name with a link. The appliance health status shows as **Disconnected**.

### Results

Carbon Black Cloud Workload Appliance VM is permanently deleted.

# VM Clones and Carbon Black Workloads

# 10

When you manually clone a virtual machine on which the Carbon Black Cloud Workload is enabled, you might see some inconsistent behavior. The parent and the clone VM might present under both **Enabled** and **Not Enabled** tabs.

You might observe a similar behavior in the Carbon Black Cloud console. The problem occurs when the Carbon Black sensors use the same ID to identify both the VMs to the back end. To resolve the problem, you must perform manual steps and reregister the cloned VM with the Carbon Black Cloud.

Read the following topics next:

- [Reregister Windows VM Clone and Golden Image](#)
- [Reregister Linux VM Clone](#)

## Reregister Windows VM Clone and Golden Image

To reregister a Windows VM clone and adjust the golden image for future clones, perform the following procedure.

See also [Manage Windows Sensors by using RepCLI](#).

### Procedure

- 1 Log in to the clone VM. For example, *WIN10\_X64\_VDI*.
- 2 Run the `repcli reregister` command:

```
repcli reregister now
```

The clone VM is reregistered and the problem is remediated.

- 3 Log in to the parent VM where the Carbon Black sensors are installed. For example, *WIN10\_X64\_GOLDEN*.
- 4 Complete the background scan and verify that the policy is updated by using the `RepCLI Status` command:

```
repcli status
```

- Schedule the reregistration for the clone VM. Use the following `repcli reregister` command, and replace *GOLDEN* with the computer name of the parent VM.

```
if /i %computername% == GOLDEN (echo Skipping reregistration) ELSE ("C:\Program
Files\Confer\RepCLI.exe" reregister now) > C:\Temp\CB_reregister.txt
```

For example:

```
if /i %computername% == WIN10_X64_GOLDEN (echo Skipping reregistration) ELSE ("C:\Program
Files\Confer\RepCLI.exe" reregister now)
```

- Create clones from the golden image.

The next time you log in to the clone VM, the scheduled command runs and registers the cloned VM.

- Log in to the new clone VM. The clone VM is registered as separate device and is assigned a new device ID.

## Reregister Linux VM Clone

To reregister a Linux VM clone, perform the following procedure.

### Procedure

- Log in to the clone VM. For example, *LIN\_CENTOS\_VDI*.
- Stop the `cbagentd` by issuing the following command with the root privilege based on the Linux distribution:

- For CentOS/RHEL/Oracle 6, use the following command:

```
$ sudo service cbagentd stop
```

- For all other distributions, use the following command:

```
$ sudo systemctl stop cbagentd
```

- Register the clone VM using the following command:

```
$ sudo /opt/carbonblack/psc/bin/cbagentd -R
```

The clone VM is registered as separate device and is assigned a new device ID and registration ID.

- Start the `cbagentd` by issuing the following command with the root privilege based on the Linux distribution:

- For CentOS/RHEL/Oracle 6, use the following command.

```
$ sudo service cbagentd start
```

- For all other distributions, use the following command.

```
$ sudo systemctl start cbagentd
```



# Carbon Black Sensor Gateway User Guide

11

The Carbon Black® Sensor Gateway™ User Guide provides information about how to install, configure, and use Sensor Gateway to secure your Cloud connection.

Sensor Gateway is an on-prem component that acts as a bridge for all inbound and outbound communications between the Carbon Black sensors that are deployed on your workloads and the Carbon Black Cloud.

## Intended Audience

This guide is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. It assumes familiarity with VMware vSphere®, including VMware ESXi™, VMware vCenter Server®, and VMware Tools™.

Read the following topics next:

- [Sensor Gateway Overview](#)
- [Set up your OVA Environment for Sensor Gateway](#)
- [Provision Sensor Gateway API Key](#)
- [Carbon Black Cloud API Access](#)
- [Sensor Gateway Certificates](#)
- [Create a Certificate Chain File](#)
- [Install Sensor Gateway as an Appliance](#)
- [Installing Carbon Black Cloud Sensors for Sensor Gateway](#)
- [Manage Connectivity to Carbon Black Cloud](#)
- [Sensor Gateway Notifications](#)
- [Upgrade a Sensor Gateway Appliance](#)
- [Troubleshooting Sensor Gateway](#)
- [Installing Sensor Gateway on a Linux Server](#)

## Sensor Gateway Overview

You can control the communication between the sensors installed on your assets and Carbon Black Cloud. The sensors can connect either directly to the Cloud or through a Sensor Gateway.

Consider using the Sensor Gateway in the following cases:

- You operate a tightly controlled environment and want to ensure that your workloads are secure and not directly exposed to Internet traffic.
- To remove the burden of owning, managing, and budgeting for additional proxy servers.
- When you have network environments where sensor communication with the Carbon Black Cloud is not possible due to corporate policy or compliance requirements.

The Sensor Gateway has a registration mechanism that allows for communication only when registered with Carbon Black Cloud. It uses the API key mechanism to make sure that no rogue Sensor Gateway servers can initiate communication with the Cloud.

Carbon Black Cloud supports Sensor Gateway deployment as an OVA. When deploying the OVA, you can use either the vSphere Client or the ESXi Web Client. For details, see [Install Sensor Gateway as an Appliance](#).

The Carbon Black Cloud console triggers notifications for Sensor Gateway server failure conditions, such as reaching maximum connections or resource capacity, or if the Sensor Gateway is down.

## Set up your OVA Environment for Sensor Gateway

To ensure a successful installation of the Sensor Gateway appliance, perform required tasks and pre-checks before running the installer.

- 1 Provision an SSL signed certificate. See [Sensor Gateway Certificates](#). Choose between:
  - Certificate authority (CA) signed certificate. This certificate is the preferred choice.
  - Self-signed certificate. This certificate requires pushing these certificates into the trust store of each sensor workload.

---

**Note** You need the private key for the certificate.

---

- 2 If you have a CA-signed certificate or an internal certificate that has an Online Certificate Status Protocol (OCSP) responder, you might have to provision the entire certificate chain. The Sensor Gateway uses the certificate and its chain to get the OCSP response and staple it with every request. This ensures that the sensors do not reach out to the OCSP responders directly.

Generate the Certificate Chain file by using any online service that offers a certificate chain composition. See [Create a Certificate Chain File](#).

- 3 Acquire a Static IP for each Sensor Gateway server.

- 4 Reserve a DNS entry. For example, `sensorgateway.company.com`

To install the Sensor Gateway in your environment, map its DNS to the IP address that you allocated to the server.

Use the DNS mapping to IP address if you plan to configure your Sensor Gateway with its FQDN.

---

**Note** You can use an IP address and create the certificates with the IP address being the same as the CN.

---

- 5 If you use the proxy feature of the Sensor Gateway and there is a proxy server between the Sensor Gateway and Carbon Black Cloud, you must make sure that the Carbon Black Cloud URLs are accessible through the proxy.

---

**Note** A proxy between the sensor and the Sensor Gateway is not supported.

---

## Provision Sensor Gateway API Key

You must generate an API key from the Carbon Black Cloud console and then use the generated API key to establish a connection between the Carbon Black Cloud console and the Sensor Gateway deployed in the vCenter Server. If you are configuring multiple Sensor Gateways, generate a separate API key for each instance.

Use the pre-defined custom access level and generate an API key for the Sensor Gateway. You can use the same custom access level to configure multiple Sensor Gateway instances for your organization.

### Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 On the left navigation pane, click **Settings > API Access > API Keys**.
- 3 Click **Add API Key**.
- 4 Enter a unique name for your Sensor Gateway API key.
- 5 From the **Access Level type** dropdown menu, select **Custom**.

- From the **Custom Access Level** dropdown menu, select **Sensor Gateway**.

### Add API Key ✕

---

**\* Name**

**Description**

**\* Access Level type** **\* Custom Access Level**

Custom Sensor Gateway

**Authorized IP addresses**

*Specify a comma separated list of single IP address, or an IP address range in CIDR notation (for example, 203.0.113.5/32).*

---

Save Cancel

- To generate the API key, click **Save**.

The Carbon Black Cloud console generates the API ID and API secret key.

- Copy the credentials.

You will use these keys to establish a connection between the Sensor Gateway and Carbon Black Cloud.

---

**Note** You can use only one set of API ID and secret key per Sensor Gateway. After you use the generated credentials for your Sensor Gateway, you cannot use the same API ID and secret key for any other instance.

---

- 9 To view and copy the API keys at a later time, or to generate a new API secret key, perform the following steps:
  - a On the left navigation pane, click **Settings > API Access > API Keys**.
  - b Go to the Sensor Gateway API name click the down-arrow in the **Actions** column.
  - c Select **API Credentials**.

The **API Credentials** dialog box displays. You can copy the API ID and API secret key.

## Carbon Black Cloud API Access

You must configure your firewall-protected network to allow connection to environment-specific URLs.

To configure a firewall and grant access to additional URLs, see [Configure a Firewall](#) in the *Carbon Black Cloud Sensor Installation Guide*.

## Carbon Black Cloud API URLs

Environment	AWS Region	Carbon Black Cloud URL	Device Services URL
Prod05	US-East-1	https://defense-prod05.conferdeploy.net	https://dev-prod05.conferdeploy.net
Prod06	EU-Central-1	https://defense-eu.conferdeploy.net	https://dev-prod06.conferdeploy.net
ProdNRT	AP-Northeast-1	https://defense-prodnrt.conferdeploy.net	https://dev-prodnrt.conferdeploy.net
ProdSYD	AP-Southeast-2	https://defense-prodsyd.conferdeploy.net	https://dev-prodsyd.conferdeploy.net
UK Point of Presence	EU-West-2	https://ew2.carbonblackcloud.vmware.com	https://ew2-device.carbonblackcloud.vmware.com

## Sensor Gateway Related URLs

Environment	Carbon Black Cloud URL	AWS URL	IP Address	Protocol/Port
Prod05	https://defense-prod05.conferdeploy.net	psc-cwp-prod-applianceservice-content-us.s3.us-east-1.amazonaws.com	Dynamic	TCP/443
Prod06	https://defense-eu.conferdeploy.net	psc-cwp-prod-applianceservice-content-eu.s3.us-east-1.amazonaws.com	Dynamic	TCP/443

Environment	Carbon Black Cloud URL	AWS URL	IP Address	Protocol/Port
ProdNRT	https://defense-prodnrt.conferdeploy.net	psc-cwp-prod-applianceservice-content-au.s3.us-east-1.amazonaws.com	Dynamic	TCP/443
ProdSYD	https://defense-prodsyd.conferdeploy.net	psc-cwp-prod-applianceservice-content-ap.s3.us-east-1.amazonaws.com	Dynamic	TCP/443
UK Point of Presence	https://ew2.carbonblackcloud.vmware.com	prdlew2-applianceservice-infra-content.s3.eu-west-2.amazonaws.com	Dynamic	TCP/443

## Sensor Gateway Certificates

A Carbon Black sensor talks to the Sensor Gateway through a certificate. The Sensor Gateway can run on both CA-signed certificate and self-signed certificate. Carbon Black recommends using the CA-signed certificates so you can install all needed certificates on all Sensor Gateway servers at once instead of installing the trusted certificate on each machine individually.

### CA-Signed Certificates

When the certificate authority (CA) issues a certificate, the certificate has a fully qualified domain name (FQDN) associated with it and every browser or device that trusts the CA can talk to this certificate.

For example, if you have a CA-signed certificate called `sensorgateway.example.com`, when you open it up in a browser or when the Carbon Black sensor tries to communicate with the Sensor Gateway, you do not get a certificate validation error if the fully qualified domain name (FQDN) of the machine matches the certificate.

In the process of generating a CA certificate, you can assign it an IP address. When a browser or a Carbon Black sensor communicates with the Sensor Gateway at the `https://sensorgateway.example.com` or the IP address (available in the subject alternative names or common names), neither the browser, nor the sensor generate an error.

If you have a certificate with an IP address in the subject alternate name (SAN) and an FQDN in the common name (CN), and some sensors access the Sensor Gateway using FQDN and others through an IP address, you must register the Sensor Gateway entry point with an IP address. Therefore, when the Carbon Black Cloud sends an URL to the sensor, it modifies the URL to point to the Sensor Gateway.

## Self-Signed Certificates

Similar to the CA-signed certificates, in self-signed certificates the CN that is provided at the time of generating a certificate must match the FQDN or IP address of the machine. When generating a self-signed certificate, you can provide an IP address or FQDN when prompted for a CN. For example, if you use the IP address 192.168.10.100 for the CN of a self-signed certificate, you must install this certificate on the Sensor Gateway machine that has the same IP address. Thus, when the sensors access the Sensor Gateway, the certificate is valid.

## Create a Certificate Chain File

Carbon Black uses a certificate chain file to perform a proper OCSP stapling.

You can generate a certificate chain by using any online Certificate Chain Composer. The following procedure is an example of creating the certificate chain by using the Certificate Chain Composer.

### Procedure

- 1 Edit the certificate `sgw_certificate.pem` in a plain text editor and copy all the content together with `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.

If your certificate already has the chain, copy only the first occurrence of `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.

- 2 Paste the content in the text box on the Certificate Chain Composer site and click **Compose**.

The tool generates the entire chain of certificates – your own certificate and all the certificates that are used to sign your certificate. You can view the certificate chain in the lower half of the page.

- 3 Copy the content and paste it in a plain text editor.

---

**Note** Delete the section that corresponds to the section in your certificate from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----`.

---

- 4 Save the file as `sgw_chain.pem`.
- 5 Copy the `sgw_chain.pem` file in the `/data/certs` directory on the server hosting the Sensor Gateway.

- 6 To ensure that the OCSP Stapling works correctly for the Sensor Gateway, run the following commands:

a `openssl x509 -noout -ocsp_uri -in sgw_certificate.pem`

Outputs the OCSP responder URL for your certificate.

b `openssl ocsp -issuer sgw_chain.pem -cert sgw_certificate.pem -verify_other sgw_chain.pem -CAfile sgw_chain.pem -no_nonce -url <OCSP Responder URL from Previous Command>`

Outputs the response from the OCSP Responder. For example,

```
sgw_certificate.pem: good
This Update: Jul 18 15:35:01 2023 GMT
Next Update: Jul 25 15:35:00 2023 GMT
```

If there is no response, check the network connectivity and firewall configuration to confirm that the OCSP response is received from the OCSP responder.

## Install Sensor Gateway as an Appliance

Install a Sensor Gateway on a Windows virtual machine either from a vSphere Client or directly on an ESXi host by using its Web client interface. You can install an OVA file or an OVF file.

As an alternative to the following procedure, you can deploy the Sensor Gateway appliance directly on the ESXi host. To do so, log in to the ESXi Web Client interface (`https://ESXi_host_IP_address_or_hostname`), right-click **Virtual Machines**, and click **Create/Register VM**. Select **Deploy a virtual machine from an OVF or OVA file** and then proceed with the installation wizard starting with Step 4.

### Prerequisites

- Verify that you have API access credentials available. See [Provision Sensor Gateway API Key](#).
- Verify that your environment is configured using the required network settings. See [Configure a Firewall](#).
- Verify that the firewall setup on your virtual machine does not block `projects.registry.vmware.com` on port 443.

### Procedure

- 1 Log in to your vCenter Server by using the vSphere Client.
  - a Open a Web browser and enter the URL for the vCenter Server instance: `https://vcenter_server_ip_address_or_fqdn`.
  - b If a warning message displays regarding a potential security risk, select the option to continue to the website.



- c On the vSphere Welcome page, select **Launch vSphere Client (HTML5)**.
  - d Enter the credentials of a user who has permissions on vCenter Server and click **Login**.  
The vSphere Client connects to all the vCenter Server systems on which the specified user has permissions. You can view and manage the vSphere inventory.
- 2 To retrieve the Sensor Gateway appliance installer, go to the [Broadcom Support Portal](#) page. Select the latest version and download the installer.
  - 3 Navigate to a cluster in your data center, right-click an ESXi host, and click **Deploy OVF Template**.

The **Deploy OVF Template** wizard opens.

- 4 Select a template and click **Next**.
  - To use the copied OVA link address, select **URL** and paste the address.
  - To use a locally saved OVA file, select **Local file** and upload the OVA. If you upload an OVF file, you must also upload all VMDK files that relate to the OVF.
- 5 Enter a unique name identifier and select the location for your deployed Sensor Gateway virtual machine.
- 6 Select the compute resource to use for your deployed Sensor Gateway and click **Next**.  
Verify that the appliance is compatible with the selected resource.
- 7 Review and verify the details for the virtual appliance and click **Next**.
- 8 Read and accept the end-user license agreement and click **Next**.

## 9 Select a virtual disk format and storage location:

Virtual Disk Format	Advantages	Disadvantages
Thin Provisioned	<ul style="list-style-type: none"> <li>Fastest to provision</li> <li>Allows disk space to be over-committed to VMs</li> </ul>	<ul style="list-style-type: none"> <li>Slowest performance due to metadata allocation overhead and additional overhead during initial write operations</li> <li>Over-commitment of storage can lead to application disruption or downtime if resources are actually used</li> <li>Does not support clustering features</li> </ul>
Thick Provisioned Lazy Zeroed	<ul style="list-style-type: none"> <li>Faster to provision than Thick Provisioned Eager Zeroed</li> <li>Better performance than Thin Provisioned</li> </ul>	<ul style="list-style-type: none"> <li>Slightly slower to provision than Thin Provisioned</li> <li>Slower performance than Thick Provisioned Eager Zero</li> <li>Does not support clustering features</li> </ul>
Thick Provisioned Eager Zeroed	<ul style="list-style-type: none"> <li>Best performance</li> <li>Overwriting allocated disk space with zeros reduces possible security risks</li> <li>Supports clustering features such as Microsoft Cluster Server (MSCS) and VMware Fault Tolerance</li> </ul>	Longest time to provision

## 10 Select a destination network for each source network and click **Next**.

## 11 Configure the deployment settings for the Sensor Gateway virtual machine:

Option	Action	Example
Initial root password	Enter a password for the root user account.	
Initial admin password	Enter a password for the admin user account.	
CBC URL	Enter the Carbon Black Cloud URL that represents the environment where your services are hosted. Carbon Black Cloud is hosted in several regions. For a list of Carbon Black Cloud environments, see <a href="#">Carbon Black Cloud API Access</a> .	<p><code>https://defense-prod05.confirdeploy.net</code></p> <p><b>Note</b> The value must begin with <code>https://</code></p>
API ID	To allow authenticated communication between a Sensor Gateway and the	9Z5QY2ZDAN

Option	Action	Example
API Secret Key	<p>Carbon Black Cloud, enter the Carbon Black Cloud API ID and API Secret Key. You generate them in pairs in the Carbon Black Cloud console. If there is a mismatch, Carbon Black Cloud rejects any communication coming from the Sensor Gateway.</p> <hr/> <p><b>Note</b> Due to the sensitivity of the data, the vSphere Client prompts for a confirmation twice and hides the value.</p>	<p>8UE3SHE470T2LZLJZJ2M98TY</p> <hr/> <p><b>Important</b> You must generate a new API ID and API Secret Key for every Sensor Gateway instance.</p>
Sensor Gateway Entry Point (https://<sensor-gateway-node-fqdn>)	<p>To define how the sensors address the Sensor Gateway, enter a Sensor Gateway entry point. The entry point must match the following:</p> <ul style="list-style-type: none"> <li>■ If you use a CA-signed or self-signed certificate, the value must be the same as the common name (CN) given to the certificate.</li> <li>■ The IP address or the FQDN of the machine must be the same as the CN of the certificate.</li> </ul>	<p>https:// sensorgateway.example.com</p> <p>This example assumes that the CN of the certificate is sensorgateway.example.com</p> <hr/> <p><b>Note</b> Because the Sensor Gateway hosts its services by using SSL, the value must begin with https://.</p>
Sensor Gateway Certificate	<p>Paste the content, including BEGIN and END lines, of the Sensor Gateway certificate file. It allows the Carbon Black sensor to talk to the Sensor Gateway.</p>	
Sensor Gateway Certificate Private Key	<p>Paste the content, including BEGIN and END lines, of the Sensor Gateway certificate private key file in the <b>Password</b> field.</p> <hr/> <p><b>Note</b> Due to the sensitivity of the data, the vSphere Client prompts for a confirmation twice and hides the value.</p>	
Sensor Gateway Certificate Chain	<p>Paste the content, including BEGIN and END lines, of the Sensor Gateway certificate chain file.</p>	

Option	Action	Example
Sensor Gateway Certificate Passphrase	<p>Use the same password you created at the time of certificate generation to protect the private key. The Sensor Gateway uses this password to encrypt its communication with the Carbon Black sensor.</p> <hr/> <p><b>Note</b> Due to the sensitivity of the data, the vSphere Client prompts for a confirmation twice and hides the value.</p>	
Proxy Type	<p>To enable the Sensor Gateway to communicate over a proxy, select the proxy type.</p> <ul style="list-style-type: none"> <li>■ By default, <code>None</code></li> <li>■ <code>HTTP</code> or <code>HTTPS</code>. For each, choose one of the following options: <ul style="list-style-type: none"> <li>■ Proxy Host: Provide the FQDN or IP address of the Proxy Host</li> <li>■ Proxy Port: Provide the port where the Proxy server receives requests</li> </ul> </li> </ul> <p>If you select <code>HTTPS</code> as your proxy type, you must include HTTPS Proxy Certificate.</p>	
Proxy Host	Enter the FQDN or IP address of the Proxy Host.	
Proxy Port	By default, the Sensor Gateway hosts its services over SSL on port 443. If this port is in use on the virtual machine where you are installing the Sensor Gateway, you can enter a different port.	
HTTPS Proxy Certificate	<p>If you selected <code>HTTPS</code> as the proxy type, paste the entire content of the HTTPS proxy certificate file.</p> <p>To avoid updating the HTTPS proxy certificate, Carbon Black recommends that you include the issuer of the certificate.</p>	

Option	Action	Example
Default Gateway	Optional. Set the default gateway for this virtual machine.	Although input is optional, you must populate these fields to use a static DNS and static IP address allocated to the Sensor Gateway. If you leave the fields blank, the Sensor Gateway acquires its IP address from the DHCP server.
Domain Name	Optional. Enter the domain name for the virtual machine.	
Domain Search Path	Optional. Enter the domain names for this virtual machine.	
Domain Name Servers	Optional. Enter the IP addresses for this virtual machine that are mapped to the domain names.	
Network 1 IP Address	Optional. Set the IP address for the network interface.	
Network 1 Netmask	Optional. Set the netmask or prefix for the network interface.	

**12** Review your configuration setup and click **Finish**.

### Results

It takes some time for the deployment to complete. You can monitor the deployment progress under the **Recent Tasks** tab or by opening the **Monitor > Tasks** page.



Sensor Gateway Setting	Dependent Sensor Gateway Settings	Notes
CBC URL	API ID, API Secret Key	If you change the Carbon Black Cloud URL, update the API ID and API secret key only if the Sensor Gateway is already registered with Carbon Black Cloud; that is, there is an existing Carbon Black Cloud URL and generated API ID.
API ID	API Secret Key	If you generated the API secret key from a different environment, update the Carbon Black Cloud URL to point to that environment.
API Secret Key	None	-
Entry Point URL	API ID, API Secret Key, and certificates	If you change the Sensor Gateway entry point, re-enter the entire content of the certificate.
Proxy Type	None	-
Proxy Host	Proxy Certificate Required when proxy type is set to HTTPS.	-
Proxy Port	None	-

## Procedure

- 1 Log in to the Sensor Gateway appliance using admin credentials.
- 2 Run the configurator command:

```
$ configure-sgw
```

The SGW Configurator terminal opens.

- 3 Update the settings under **General Settings** or **TLS settings**.

For example, if you must update the connection to the Carbon Black Cloud, enter the new Carbon Black Cloud URL in the related field.

If you enter an invalid value, an error message displays and provides a suggestion for a valid input. If you enter a valid URL, a success message displays.

- 4 To return to the main menu, click **Back**.
- 5 Optional. Repeat Step 3 to update required values.
- 6 Click **Save and Quit**.
- 7 Review the updated values and confirm your changes.
- 8 Optional. Repeat step 3 to update any of the required values.

## Results

The SGW Configurator tool restarts the Sensor Gateway service with the updated configuration.

## What to do next

To access the log file and view summary of all your configuration changes, run the following command:

```
$ vim /opt/vmware/sgw/data/logs/configure-sgw.log
```

---

**Note** The log file hides sensitive data such as the private key.

---

## Update Sensor Gateway Appliance Certificate

You can update the TLS certificate of a Sensor Gateway OVA when the certificate is about to expire or has been compromised.

### Prerequisites

Verify that all sensors are connected to the Sensor Gateway appliance to access and download the new certificate. When you upload a new certificate, Carbon Black Cloud sends it to each sensor individually.

---

**Important** Virtual machines that are shut down might not receive the new certificate. The sensors cannot connect to the Carbon Black Cloud when the new certificate is replaced on the Sensor Gateway. Therefore, to receive the new certificate and avoid connectivity issues, make sure that all sensors connected through the Sensor Gateway are in an active state.

---

### Procedure

- 1 Obtain a new certificate.

The new certificate must have the same common name (CN) as the current certificate.

- 2 Open the **Settings > API Access > Sensor Gateways** tab and double-click the Sensor Gateway OVA for which you must renew the certificate.
- 3 In the **Sensor Gateway Details** section, select the **Options** dropdown menu and click **Update certificate**.
- 4 Click **Upload File**, select the newly obtained certificate, upload it, and click **Close**.

It takes up to eighty minutes for the process to complete depending on the number of sensors connected to the Sensor Gateway. The Carbon Black Cloud sends the newly uploaded certificate to all sensors connected to the Cloud through the Sensor Gateway. Each sensor sends a status back to the Cloud confirming whether it has successfully accepted the new certificate. The Carbon Black Cloud console only displays any errors received by the sensors.



- 5 To see reported errors, click **Inventory > VM Workloads > Enabled**.
  - a Select the Sensor Gateway from the **Sensor Gateway** filter facet.
  - b Select **Errors** from the **Status** filter facet.
  - c To see the details for the sensor reporting the error, double-click the relevant row.
  - d You can try to fix existing errors by uploading the new certificate again.  
If errors persist, contact Broadcom Carbon Black Support.

---

**Important** Continue updating the certificate on the Sensor Gateway only if there are no errors reported by the sensors.

---

- 6 Replace the TLS certificate of the Sensor Gateway that is deployed as an OVA.
  - a Log in to the Sensor Gateway using admin credentials.
  - b Run the configurator command:

```
$ configure-sgw
```

The SGW Configurator terminal opens.

- c Select **TLS Settings > Sensor Gateway > Sensor Gateway Certificate**.
- d When prompted, paste the content of the new certificate including the **BEGIN CERTIFICATE** and **END CERTIFICATE** lines, and press **Ctrl+D** two times.

The configuration tool validates the content in the background. If the new certificate is invalid, an error displays.

- e Click **Save and Quit**.

The SGW Configurator tool restarts the Sensor GatewaySensor Gateway service with the updated configuration.

### Results

It takes up to five minutes for the Sensor Gateway to re-register with the Carbon Black Cloud.

## Update HTTPS Proxy Certificate

If during the Sensor Gateway appliance installation you specified the proxy type as an **HTTPS**, you also included an HTTPS proxy certificate. Perform the following procedure to update the proxy certificate when it is about to expire or if it has been compromised.

Use the SGW Configurator tool to update the proxy certificate. See [Reconfigure the Sensor Gateway Appliance](#).

## Prerequisites

Make sure that you can provide one of the following:

- Recommended. The issuer of the HTTPS proxy certificate. If you provide the Certificate Authority, you do not have to update the Sensor Gateway proxy certificate when it is about to expire.
- The certificate chain of the Proxy server. If you use the certificate chain, you must update the Sensor Gateway proxy certificate.

## Procedure

- 1 Obtain the new HTTPS proxy certificate.
- 2 Log in to the Sensor Gateway using admin credentials.
- 3 Run the configurator command:

```
$ configure-sgw
```

The Sensor Gateway Configurator terminal opens.

- 4 Select **TLS settings > Proxy > Proxy Certificate**.
- 5 Paste the entire content of the new proxy certificate, including the **BEGIN CERTIFICATE** and **End CERTIFICATE** lines, and press **Ctrl+D**.

If you entered incorrect content, an error message displays, such as `ERROR: You've entered invalid value. Please enter a valid X509 certificate.`

- 6 Click **Save and Quit**.
- 7 Review the updated values and confirm your changes.

## Results

The Sensor Gateway Configurator tool restarts the Sensor Gateway service with the updated configuration.

# Installing Carbon Black Cloud Sensors for Sensor Gateway

After you install the Sensor Gateway and register it with Carbon Black Cloud, you can perform a fresh Carbon Black sensor installation.

The following Carbon Black Cloud sensor versions are supported with the Sensor Gateway:

- Carbon Black Cloud Windows sensor 3.8.0.684+

- Carbon Black Cloud Linux sensor 2.13.2.997598+

---

**Note** You can install a Windows sensor using a COMPANY CODE that contains a Sensor Gateway URL with any Windows sensor 3.8.0.684+. However, to switch an existing Windows sensor that is currently communicating with the Carbon Black Cloud to a Sensor Gateway, you must be using Windows sensor 3.9 MR2+.

---

## Locate a Sensor Gateway Instance

You can use the Carbon Black Cloud console to locate the Sensor Gateway instance.

### Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 On the left navigation bar, click **Settings > API Access > Sensor Gateways**.
- 3 Find the name of the Sensor Gateway that corresponds to the IP address or the API ID.
- 4 Make a note of this name — you will need it when you generate the company code.

## Generate a Company Code

You must generate a company code prior to sensor installation. You can obtain the company code in the Carbon Black Cloud console.

### Procedure

- 1 On the left navigation bar, click **Inventory > VM Workloads**.
- 2 From the **Sensor Options** dropdown menu, select **View company codes**.

- 3 Click the **Connect to Carbon Black Cloud through Sensor Gateway** option.

### View Company Codes

Registration | Deregistration Regenerate registration code

Use your registration code to install sensors by distribution system or imaging

**Sensor connection**

Connect to Carbon Black Cloud directly
   
 Connect to Carbon Black Cloud through Sensor Gateway
 Select ▼

**Registration code**

XFKEDSWXHSNEBSNEF8#M1SGNWXG#JV

Copy

Windows v1.x - 2.x | macOS v1.x - 2.x Show

Close

The Sensor Gateway dropdown menu becomes available.

- 4 Select the Sensor Gateway entry point URL for the sensor installation.  
The dropdown menu displays the URLs for the connected Sensor Gateways.
- 5 If necessary, click **Regenerate registration codes**.

If you generate a new company code, it invalidates the previous one and cannot be undone.

If you change the company code and install sensors using the new code, the old sensors continue to operate. Installed sensors are unaffected. Only new installation packages must use the new code.

- 6 Copy the Registration code.

This is the company code you will use when you install the sensors.

## Install Carbon Black Cloud Linux Sensor for Sensor Gateway

To enable the Carbon Black Cloud sensor on your Linux VM workload to communicate with the Carbon Black Cloud through a Sensor Gateway, you must install and configure the sensor to work with the Sensor Gateway.

### Prerequisites

- Verify that you have access to the latest Carbon Black Cloud sensor for Linux version (2.15+).
- If you install the sensor through the console, include the `UseSystemCerts=true` property in the `/var/opt/carbonblack/psc/cfg.ini` file. See [About the Linux Sensor cfg.ini File](#) in the *Carbon Black Cloud Sensor Installation Guide*.

- The company code must be available. See [Generate a Company Code](#).

#### Procedure

- 1 Download the latest version of the Carbon Black Cloud Linux sensor. See [Download Sensor Kits](#) in the *Carbon Black Cloud Sensor Installation Guide*.
- 2 Omit this step if the Sensor Gateway is already configured with a CA-signed certificate. To use a self-signed certificate in the Sensor Gateway, you must add the certificate chain to the trust store.
  - a Copy the certificate `sgw_certificate.pem` file to use for communication with the Sensor Gateway to your Linux VM workload.
  - b Add the content of the self-signed certificate `sgw_certificate.pem` into the CA signed certificate `ca-certificates.crt` file on your VM workload.

```
cat sgw_certificate.pem >> CERTFILE_PATH
```

The `CERTFILE_PATH` points to `/etc/ssl/certs/ca-certificates.crt` on most Linux systems. However, we recommend you confirm in the documentation of your distro how to locate the Trusted CA certs file.

- 3 Retrieve the sensor installation file by running the following command:

```
wget <location of the sensor installation file>
```

- 4 Unzip the sensor installation file:

```
tar -xvf <tgz installation file>
```

- 5 Use the company code to complete the sensor installation:

```
./install.sh "<company_code>" --sensor-gateway-cert CERTFILE_PATH
```

The `CERTFILE_PATH` points to `/etc/ssl/certs/ca-certificates.crt` on most Linux systems. However, we recommend you confirm in the documentation of your distro how to locate the Trusted CA certs file.

#### Results

After the sensor is installed, you can view the running Sensor Gateway in the Carbon Black Cloud console.

## Install Carbon Black Cloud Windows Sensor for Sensor Gateway

After your Sensor Gateway is up and running, you must perform a fresh sensor install. You install a Carbon Black sensor on your Windows VM workload and configure it to communicate with the Carbon Black Cloud through the Sensor Gateway.

For more information about installing Carbon Black Cloud Windows sensors, see the *Carbon Black Cloud Sensor Installation Guide*.

### Prerequisites

- Ensure you have access to the latest Carbon Black sensor for Windows version (3.8.0.684+).
- For information on using the Carbon Black Cloud console to install sensors on VM workloads, see [Installing Windows Sensors on Endpoints](#) in the *Carbon Black Cloud Sensor Installation Guide*.
- The company code must be available. See [Generate a Company Code](#).
- If you install the Carbon Black sensor in a Sensor Gateway environment configured with a proxy, you might see the local scanner setting `UpdateServers` set to `None` after the sensor installation completes. By default, the sensor uses a random timeout (up to 2 hours) to download the signature packs in case a large number of sensors are being deployed. To avoid the random delay in the signatures download, set the `DELAY_SIG_DOWNLOAD` command line parameter to `0` during the sensor installation. For information on Windows sensor supported commands, see [Windows Sensor Supported Commands](#) in the *Carbon Black Cloud Sensor Installation Guide*.

### Procedure

- 1 Omit this step if the Sensor Gateway uses a CA-signed certificate. Add a self-signed certificate in the Trusted Root Certificates folder on the Windows VM workload.  
The sensor uses this certificate to communicate with the Sensor Gateway
- 2 Download the sensor installer. See [Download Sensor Kits](#) in the *Carbon Black Cloud Sensor Installation Guide*.
- 3 Install the sensor by using the Carbon Black Cloud console or by existing scripts.
- 4 Use the company code you generated to complete the sensor installation.  
After your sensor is successfully installed, you can view the running Sensor Gateway in the Carbon Black Cloud console.

## Manage Connectivity to Carbon Black Cloud

Use the Carbon Black Cloud console to manage the connection between your sensor and Carbon Black Cloud. Your workloads can communicate with Carbon Black Cloud directly or through a Sensor Gateway.

---

**Note** This functionality is not supported on Windows 7 using a self-signed certificate.

---

### Prerequisites

Verify that you have installed the Carbon Black Cloud Windows sensor 3.9 MR2+.

**Procedure**

- 1 Log in to the Carbon Black Cloud console.
- 2 On the left navigation pane, click **Inventory > VM Workloads** or **Inventory > Endpoints > Enabled**.
- 3 In the **Status** column, select the check box for the VM workloads or Endpoints upon which to take action.
- 4 In the **Actions** dropdown menu, select **Manage Sensor Gateway Connection**.

- 5 Perform one of the following.
  - To assign a Sensor Gateway, click the **Connect through Sensor Gateway** dropdown menu and select an entry point.  
  
If this connection exceeds the number of supported sensors, you are notified immediately upon your Sensor Gateway selection.  
  
If you performed a bulk selection of assets in the **Enabled** tab and the total number of the assets exceeds a single page size, a check box appears for applying this setting to all assets.
  - If there is an issue with your Sensor Gateway, configure the sensor to communicate directly with Carbon Black Cloud by selecting **Connect directly**.
- 6 To change the connection type between the sensor and Carbon Black Cloud, click **Apply**.

**Results**

It takes up to ten minutes for the console to reflect the changes.

## Sensor Gateway Notifications

After you install and start running one or more Sensor Gateway servers, you can subscribe to Sensor Gateway notifications.

After you are subscribed, you get in-product notifications and notifications through email in the following cases:

- When one or more Sensor Gateway instances in your organization have not responded in the last five minutes or less and are currently disconnected from the Carbon Black Cloud .
- When one or more Sensor Gateway instances in your organization exceed the number of configured sensors. .

---

**Note** Each Sensor Gateway supports up to ten thousand Carbon Black Cloud sensors

---

## Subscribe to Receive Sensor Gateway Notifications

To receive in-product and email notifications of the state of your registered Sensor Gateway instances, perform the following procedure.

### Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 In the left navigation pane, click **Settings > Notifications > Integrations**.
- 3 Click **Add Notification**.

**Add Notification** ✕

---

\* Name

\* Component type

\* **When do you want to be notified?**

Sensor Gateway is disconnected

Sensor limit is exceeded (10,000)

Certificate will expire in 30 days

**How do you want to be notified?**

\* Email

Send 1 reminder email at the end of the day

---

**Save** **Cancel**

- 4 Provide a name for the notification
- 5 From the **Component type** dropdown menu, select Sensor Gateway.



- 6 Select the checkboxes for notification preferences:
  - When the Sensor Gateway is disconnected.
  - When the maximum number of 10,000 Carbon Black sensors is exceeded.
  - When the Sensor Gateway certificate is about to expire.
- 7 Add the email addresses of users to receive the notifications.
- 8 Optional. To receive a notification at the end of the day with a summary of all Sensor Gateways that are unresolved in your environment, select the checkbox for **Send 1 reminder email at the end of the day**.

Sensor Gateway instances that already have restored connections are excluded.
- 9 To complete the notification subscription setup, click **Save**.

## Upgrade a Sensor Gateway Appliance

To upgrade a Sensor Gateway appliance with the latest available version, perform the following procedure.

---

### Note

- Do not power down the Sensor Gateway appliance while the upgrade is in progress. Otherwise, you might have to reinstall the Sensor Gateway.
  - Sensors that are connected to the Sensor Gateway might lose connectivity to the Carbon Black Cloud during the upgrade.
  - Carbon Black Cloud provides a fallback mechanism in case of a system error or if you revert to a previous version of the Sensor Gateway.
- 

### Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 In the left navigation pane, click **Settings > API Access > Sensor Gateways**.
- 3 Double-click the Sensor Gateway to upgrade.

The **Sensor Gateway Details** pane displays the current version of the Sensor Gateway together with the newly available version in parentheses.
- 4 From the **Options** dropdown menu, select **Upgrade version**.

The **Upgrade Sensor Gateway** window opens.
- 5 To confirm the upgrade, click **Upgrade**.

### Results

The Sensor Gateway upgrades successfully and the sensors resume their connectivity to the Carbon Black Cloud.

## What to do next

In the left navigation pane, click **Settings > Audit Log** to view the status of the upgrade.

# Troubleshooting Sensor Gateway

This topic describes solutions for situations when installing, using, or upgrading the Sensor Gateway is not successful.

## Sensor Gateway Appliance is Unreachable

**Cause:** The virtual machine is powered off.

**Solution:** Power on the virtual machine and wait for it to enter a healthy state. If the operational state is not healthy after few restarts, initiate a new installation of the Sensor Gateway appliance. See [Install Sensor Gateway as an Appliance](#).

When you install the Sensor Gateway appliance, make sure that you provide the Sensor Gateway entry point URL. The entry point URL must match the common name (CN) you provided when generating the Sensor Gateway certificate. See [Sensor Gateway Certificates](#).

## Installing Sensor Gateway on a Linux Server

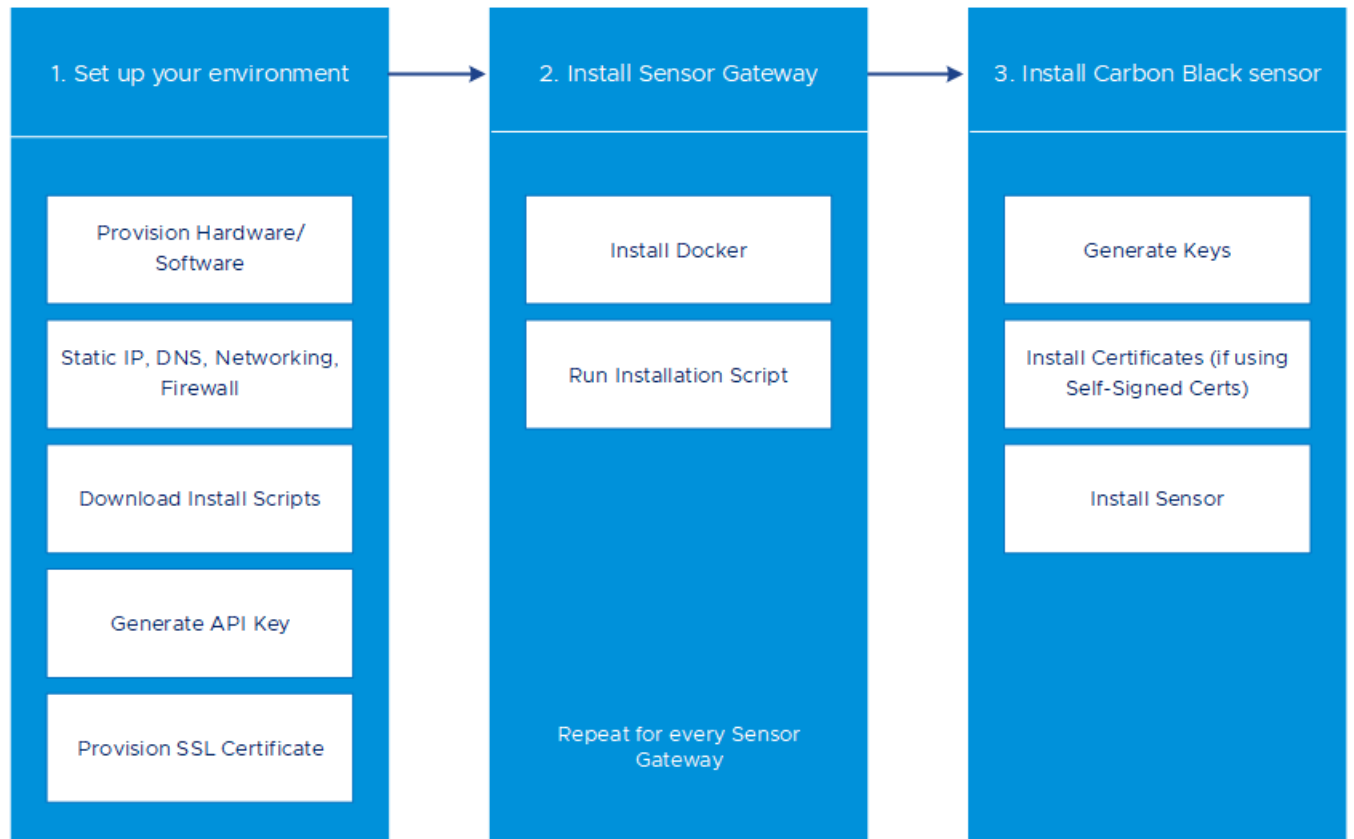
This section describes how to set up a Linux server and install the Sensor Gateway on the configured Linux machine.

---

**Important** Carbon Black recommends that you set up your system with the Sensor Gateway appliance. For details, see [Install Sensor Gateway as an Appliance](#). Sensor Gateway for Linux and the related highly available (HA) capabilities will be deprecated.

---

The following high level installation workflow depicts the steps for installing and configuring components in your system so that sensors can communicate with Carbon Black Cloud through the Sensor Gateway.



The Sensor Gateway is reliable and highly available. You can deploy multiple Sensor Gateway servers and manually configure them in a highly available mode to handle the traffic at an acceptable latency. If a Sensor Gateway server fails due to a connection or resource threshold, you can spin up another Sensor Gateway instance to take over managing the connections.

## Configure Your Linux Server for Sensor Gateway Installation

To set up a Linux server for the Sensor Gateway installation, follow this procedure.

### Prerequisites

- Provision an SSL signed certificate. Choose between:
  - Certificate authority (CA) signed certificate. This certificate is the preferred choice.
  - Self-signed certificate. This certificate requires pushing these certificates into the trust store of each sensor workload.
  - See [Sensor Gateway Certificates](#).

---

**Note** You need the private key for the certificate.

---

- If you have a CA-signed certificate or an internal certificate that has an Online Certificate Status Protocol (OCSP) responder, you might have to provision the entire certificate chain. The Sensor Gateway uses the certificate and its chain to get the OCSP response and staple it with every request. This ensures that the sensors do not reach out to the OCSP responders directly.

Generate the Certificate Chain file by using any online service that offers a certificate chain composition. See [Create a Certificate Chain File](#).

- Acquire a Static IP for each Sensor Gateway server.
- Reserve a DNS entry. For example, `sensorgateway.example.com`

To install the Sensor Gateway in your environment, map its DNS to the IP address that you allocated to the server.

Use the DNS mapping to IP address to configure the Sensor Gateway with its FQDN.

---

**Note** You can use an IP address and create the certificates with the IP address being the same as the CN.

---

- Verify that sensors can reach the Sensor Gateway.
- Verify that the Sensor Gateway has connectivity to the Internet. The Sensor Gateway must have connectivity to Carbon Black Cloud. However, the Sensor Gateway might need to reach out to CA providers to get Online Certificate Status Protocol (OCSP) responses for the validity of its digital certificate.
- To run the Sensor Gateway behind a proxy, configure the Docker client to use the proxy. See [Configure Docker to use a proxy server](#).
- If you use the proxy feature of the Sensor Gateway and there is a proxy server that sits between the Sensor Gateway and Carbon Black Cloud, make sure that the Carbon Black Cloud URLs are accessible through the proxy.
- Verify that your environment is configured with the necessary network settings. See [Configure a Firewall](#).
- Verify that your firewall setup does not block `projects.registry.vmware.com` on port 443.

## Procedure

- 1 Log in to your Linux server as root and confirm that OpenSSL is installed.

If OpenSSL is not already installed, use a system package manager to install OpenSSL.

- 2 Prepare the certificates:

- a Name the SSL Certificate file to be `sgw_certificate.pem`.
- b Name the SSL Certificate Private Key file to be `sgw_key.pem`.
- c (Omit this step if you are using a self-signed certificate.) Name the SSL Certificate Chain file to be `sgw_chain.pem`.

- d (Omit this step if you are using a self-signed certificate.) To verify the certificate validity, run the following command:

```
openssl verify -CAfile sgw_chain.pem sgw_certificate.pem
```

If the certificate is valid, the returned response is: `sgw_certificate.pem: OK`

- e Create a `/data` folder at the root level and make the following subfolders on the server.
- `/data/certs` - Stores certificates, keys, and optionally, certificate chain file.
  - `/data/logs` - Stores the logs generated at runtime.
- f Copy the certificate, the private key, and the chain file to the `/data/certs` directory.

---

**Note** You do not need the chain file if you are using a self-signed certificate.

---

- 3 Download the script that installs and sets up Sensor Gateway on the Linux server.

```
wget https://prod.cwp.carbonblack.io/sgw/installer/linux/1.2.0/sensor_gw_install.zip
```

- 4 Unzip the Sensor Gateway installation zip file. Locate the shell script `sensor_gw_install.sh`.
- 5 By default, the shell script is not executable. Run the following command to make the script executable:

```
chmod +x sensor_gw_install.sh
```

- 6 Acquire the Sensor Gateway registration API key.

See [Provision Sensor Gateway API Key](#).

#### What to do next

Install the Sensor Gateway.

## Install Sensor Gateway on a Linux Server

You can host the Sensor Gateway on a Linux server as a container image. The Linux server must have a container running capability. To install more than one Sensor Gateway server, you must repeat the following steps for every Sensor Gateway server.

#### Prerequisites

- Verify that port 443 is open on the Sensor Gateway.
- To have the Sensor Gateway running behind a proxy, configure the Docker client to use proxy. See [Configure Docker to use a proxy server](#).

## Procedure

### 1 Install Docker.

For information about installing a Docker engine on a Sensor Gateway-supported the Linux distribution, see [Install Docker Engine on CentOS](#), [Install Docker Engine on RHEL](#), or [Install Docker Engine on Ubuntu](#).

### 2 To make the installation script executable, run the following command:

```
chmod +x sensor_gw_install.sh
```

### 3 Run the installation script.

```
./sensor_gw_install.sh
```

### 4 Provide the following input:

Option	Description	Example
API ID	The API ID and API Secret Key generated in the Carbon Black Cloud console allow an authenticated communication between the Sensor Gateway and the Carbon Black Cloud.	9Z5QY2ZDAN
API Secret Key	Both the API ID and API Secret Key are generated in a pair. If there is a mismatch, the Carbon Black Cloud will reject any communication from the Sensor Gateway.  <b>Note</b> You must generate new API ID and API Secret Key for every Sensor Gateway.	8UE3SHE475T2LZLJNJ2M98TK
Carbon Black Cloud URL	This URL represents the environment where your services are hosted. Carbon Black Cloud is hosted in several regions. For a list of Carbon Black Cloud environments, see <a href="#">Carbon Black Cloud API Access</a> .	https://defense-prod05.conferdeploy.net  <b>Note</b> The value must begin with https://.
Sensor Gateway entry point URL (https://<sensor-gateway-node-fqdn>)	An entry point defines how the sensors address the Sensor Gateway. The entry point must match the following: <ul style="list-style-type: none"> <li>■ If you use a CA-signed or self-signed certificate, this value should be the same as the CN given to the certificate.</li> <li>■ The IP address or the FQDN of the machine must be the same as the CN of the certificate.</li> </ul>	https:// sensorgateway.example.com This example assumes that the CN of the certificate is sensorgateway.example.com.  <b>Note</b> Because the Sensor Gateway services are hosted using SSL, the value must begin with https://.
Proxy type	<ul style="list-style-type: none"> <li>■ None: This is the default option.</li> <li>■ HTTPS or HTTP: Choose one of the following options: <ul style="list-style-type: none"> <li>■ Proxy Host: Provide the FQDN or IP address of the Proxy Host.</li> <li>■ Proxy Port: Provide the port where the Proxy server receives requests.</li> </ul> </li> </ul>	HTTP

Option	Description	Example
<b>Optional:</b> Volume mount directory	<p>The Sensor Gateway uses a fixed directory to look for certificates and to store logs.</p> <p>If you do not provide a value, the default location is a <code>/data</code> directory. To store your certificates or logs in a different directory, provide an absolute path.</p> <p>If you have a different folder, create <code>certs</code> and <code>logs</code> folders in this path. Make sure that the certificate, private key, and optional certificate chain are stored in the <code>certs</code> folder before you proceed.</p> <p>Because the install script executes with root permissions, by default these directories have root permissions as owner and group.</p>	<code>/data</code>
<b>Optional:</b> Port where Sensor Gateway runs	By default the Sensor Gateway services are hosted over SSL on port 443. You can specify a different port.	By default, Sensor Gateway runs on port 443.
<b>Optional:</b> Certificate private key passphrase	<p>We recommend that you provide a password when you generate a certificate to protect the private key. When prompted during the Sensor Gateway installation, provide this password.</p> <p>The Sensor Gateway uses the same password to use the certificate and encrypt the communication between the sensor and itself.</p>	Provide a password if your <code>sgw_key.pem</code> is password-protected.

## Results

After the registration completes, the Sensor Gateway displays as connected in the **Settings > API Access > Sensor Gateways** page of the Carbon Black Cloud console.

The Sensor Gateway name comes from the API key.

## Update a Linux Server Sensor Gateway SSL Certificate

You can update the SSL certificate on a Linux Sensor Gateway when the certificate is about to expire, or has been compromised, and thereby avoid the sensors being permanently disconnected from the Carbon Black Cloud.

### Prerequisites

Verify that all sensors are connected to the Sensor Gateway to access and download the new certificate. When you upload a new certificate, Carbon Black Cloud sends it to each sensor.

---

**Important** Virtual machines that are shut down might not receive the new certificate. The sensors cannot connect to the Carbon Black Cloud when the new certificate is replaced on the Sensor Gateway. Therefore, to receive the new certificate and avoid connectivity issues, make sure that all sensors connected through the Sensor Gateway are in an active state.

---

## Procedure

- 1 Obtain a new certificate.

The new certificate must have the same common name (CN) as the current certificate.

- 2 Log in to the Carbon Black Cloud console.
- 3 In the left navigation pane, click **Settings > API Access > Sensor Gateways** tab and double-click the Sensor Gateway.
- 4 In the **Sensor Gateway Details** section, from the **Options** dropdown menu, click **Update certificate**.
- 5 Click **Upload File**, select the newly obtained certificate, upload it, and click **Close**.

It takes up to eighty minutes for the process to complete depending on the number of sensors connected to the Sensor Gateway. The Carbon Black Cloud sends the newly uploaded certificate to all sensors connected to the Cloud through this Sensor Gateway. Then, each sensor sends a status back to the Carbon Black Cloud confirming that it has successfully accepted the new certificate. The Carbon Black Cloud console only displays the errors received by the sensors.

- 6 To see errors reported by the sensors, in the left navigation pane click **Inventory > VM Workloads > Enabled**.
  - a Select Sensor Gateway from the **Sensor Gateway** filter.
  - b Select **Errors** from the **Status** filter.
  - c To see the details for the sensor reporting the error, double-click the relevant row.
  - d You can potentially fix existing errors by re-uploading the new certificate.

If the errors persist, contact Broadcom Carbon Black Support.

---

**Important** Continue with updating the certificate on the Sensor Gateway only if there are no errors reported by the sensors connected to this Sensor Gateway in the Carbon Black Cloud console.

---

- 7 Replace the SSL certificate of the Sensor Gateway.
  - a Rename the new certificate to `sgw_certificate.pem` and its private key to `sgw_key.pem`.
  - b Copy the new certificate public and private keys to the `/data/certs` folder on the Sensor Gateway device.
  - c Restart the Sensor Gateway by first retrieving its container ID `sudo docker ps -a` and then running the command `sudo docker restart <contained id>`.

## Results

It takes up to five minutes for the Sensor Gateway to re-register with the Carbon Black Cloud.



## Upgrade a Linux Server Sensor Gateway

You can upgrade a Sensor Gateway on a Linux server by running a dedicated upgrade script.

---

**Note** Upgrade of the Sensor Gateway does not enable proxy support. To configure a Sensor Gateway environment with a proxy, you must re-install the Sensor Gateway.

---

### Prerequisites

- You must have the following information available from your initial Sensor Gateway installation.
  - The Sensor Gateway Entry point. Use the same name as before. If not, existing sensors can stop communicating through the Sensor Gateway.
  - API ID
  - API Key
- Supported Carbon Black Linux sensor versions are 2.13.2.997598+.
- Confirm that the existing version of the Sensor Gateway is running and has active connectivity with Carbon Black Cloud.

### Procedure

- 1 Download and unzip the `sensor-gateway-x.x.x.zip` file on your Linux server.
- 2 Identify the current Sensor Gateway and stop it.
  - a Log in to the Linux server using root credentials.
  - b To get the running instance of the Sensor Gateway, execute the following command:

```
docker ps
```

The first column displays the `Container ID`.

- c To stop the running Sensor Gateway, execute the command:

```
docker stop <the Container ID>
```

- d To get a list of all containers, run the following command:

```
docker ps -a
```

- e Remove the Sensor Gateway instance.

```
docker rm <the Container ID>
```

- f Get a list of all containers and confirm that there is no Sensor Gateway in `Running` or `Stopped` status.

```
docker ps -a
```

If you do not see any result from executing the command, it indicates that the previous commands were unsuccessful. Do not proceed with the next step: contact Broadcom Carbon Black Support.

- 3 `cd` to the directory where you unzipped the latest version of the Sensor Gateway file.
- 4 Install the Sensor Gateway.

```
./sensor_gw_install.sh
```

You are prompted to supply the same data as you input during the initial Sensor Gateway installation. See [Install Sensor Gateway on a Linux Server](#).