VMware Carbon Black Cloud Workload Guide

Modified on 26 October 2023

VMware Carbon Black Cloud Workload 1.2

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

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware Carbon Black Cloud Workload Guide

The *VMware Carbon Black Cloud Workload Guide* provides information about how to install, configure, and use the VMware 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

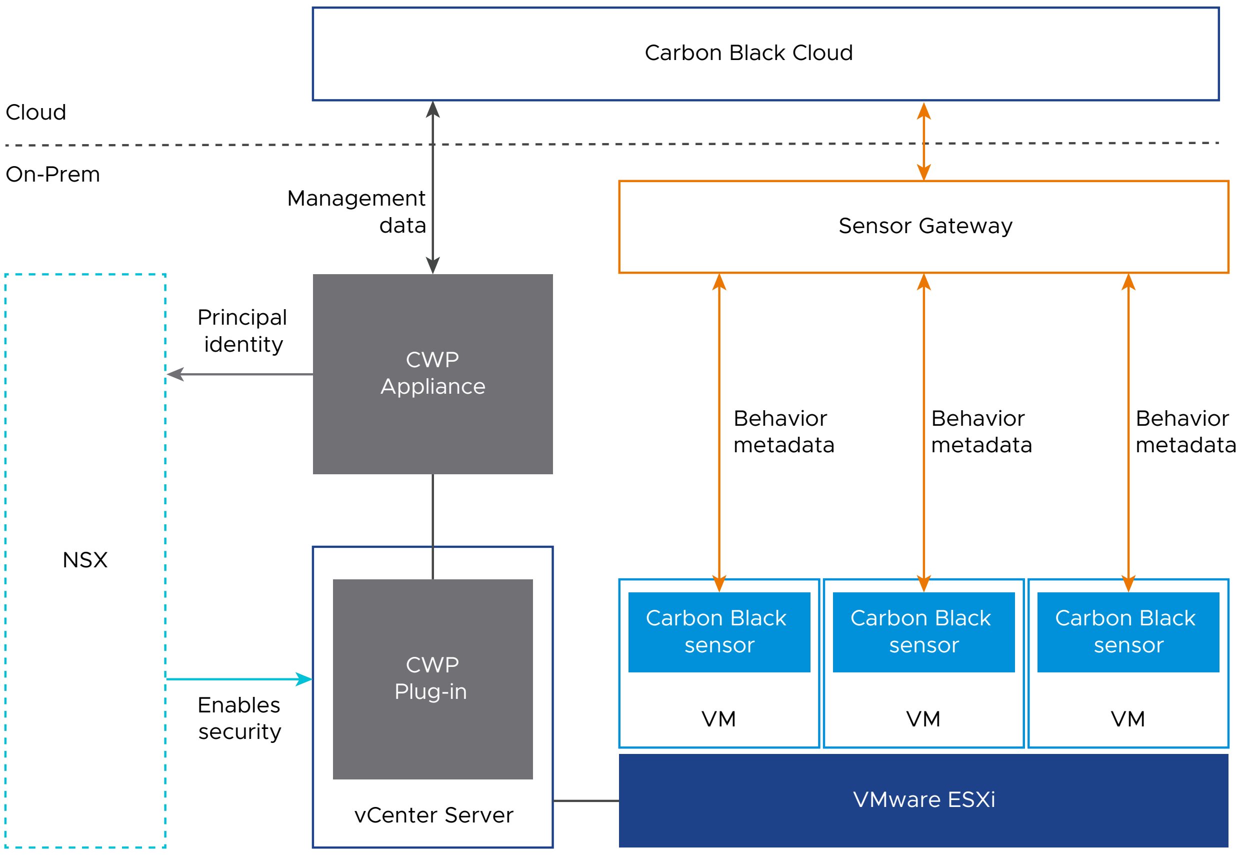
1

VMware 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 a 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 provided by Carbon Black Cloud Workload Plug-in.

You can easily monitor and protect the data center workloads from the Carbon Black Cloud console. The Carbon Black Cloud Workload Plug-in provides deep visibility into your data center inventory and end-to-end life-cycle 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 do remediations using NSX-T Distributed Firewall (DFW) policies.

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



You must first 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.

You can then enable Carbon Black on the virtual machines where your application workloads are running with the one-click install process.

After you enable Carbon Black successfully, you can view and monitor your inventory data and processes from the Carbon Black Cloud Workload Plug-in and also from the **VMs > Monitor** tab.

You can navigate to 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. For more information on Carbon Black Cloud, refer to the **User Guide** in the **Help** menu on the upper-right side of the Carbon Black Cloud console.

Carbon Black Cloud Workload Appliance

The Carbon Black Cloud Workload appliance is an on-premises based 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 also provides the channel for communication between Carbon Black Cloud and NSX Manager - the strong data analysis capabilities of Carbon Black Cloud pairs with the firewall protection capabilities of NSX. You use the appliance to register an NSX integration with your Carbon Black Cloud organization. The appliance registers to the NSX via Principal Identity. It provides a certificate-based authentication, and 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 directly 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 a concert with the Carbon Black Cloud to provide visibility and control for the entire security team.

vCenter Server

vCenter Server is used to gather 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 a direct visibility.

Carbon Black Cloud

Carbon Black Cloud is a cloud-native service that consolidates multiple workload security capabilities, using a single easy-to-use console. Different teams like Infrastructure and InfoSec can have a single, shared source of truth to improve the security together.

The Carbon Black Cloud console shows alerts based on our Next Generation Anti-Virus (NGAV) detections and behavioral analytics. You use the console to view any Carbon Black Cloud alerts that trigger remediation 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 made available with VMware Tools. When you enable Carbon Black in your data center, the silent installation is triggered where 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 with VMware Tools. To receive the launcher for your workloads, you must install or upgrade VMware Tools to version 11.2 or later.

- **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 for your guest operating system from the package repository at http://packages.vmware.com/.

NSX Manager

The NSX Manager application provides a web-based user interface for administering your NSX environment. For information on installing, administering with, and security 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 your vSphere workloads and the Carbon Black Cloud. For more information, see Installing and Using Carbon Black Sensor Gateway.

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 the following VMware Carbon Black Cloud Operating Environment Requirements:

- VMware Carbon Black Cloud™ Workloads Operating Environment Requirements
- VMware Carbon Black Cloud™ Vulnerability Management Operating Environment Requirements

Read the following topics next:

- Download the Installer
- Accessing Carbon Black Cloud

Download the Installer

The Carbon Black Cloud Workload appliance with the software for Carbon Black Cloud Workload Plug-in is all 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` for installation.

You can download the Carbon Black Cloud Workload appliance `OVA` from the VMware **Downloads** page.

Procedure

1. Log in to the VMware Customer Connect portal.

   For information about creating a Customer Connect profile, see KB 2007005. For information about inviting a user to an account in Customer Connect, see KB 2070555.

2. Go to the VMware downloads page at https://customerconnect.vmware.com/downloads.

3. Select **Endpoint & Workload Security** from the **All Products** drop-down menu.

4. Download the `OVA` to a local datastore or a local web server.

   The `OVA` filename has the following format `cwp-va-`*`<release-number>`*`-`*`<build-number>`*`_OVF10.ova`. For example, `cwp-va-1.0.0.0-17066560_OVF10.ova`.

5 Copy the file path of the Carbon Black Cloud Workload appliance `OVA` file.

For example, `http://<local-web-server>/cwp-va-1.0.0.0-17066560_OVF10.ova`, if you downloaded the `OVA` file to a local web server. You provide this path while deploying the appliance.

Results

The Carbon Black Cloud Workload appliance `OVA` file is available.

What to do next

Deploy and configure the 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 that you can use 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 need any help with the Carbon Black Cloud service, you can contact the VMware Carbon Black support team at https://www.carbonblack.com/support/. If you need any help related to vSphere, you can contact the VMware support team at https://www.vmware.com/support/contacts.html.

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 any ESXi host in your vCenter Server environment. After the appliance is deployed, you must register the appliance with the vCenter Server. You must then configure the appliance to establish a connection between the Carbon Black Cloud console and the on-premises appliance deployed in the vCenter Server. After the connection is established, the appliance imports the virtual machine inventory data to the Carbon Black Cloud console. You can then enable Carbon Black on Windows and Linux VMs.

Read the following topics next:

- Step 1: Deploy and Configure Carbon Black Cloud Workload appliance
- Preparing VMs with Carbon Black Launcher
- Step 2: Enable Carbon Black on Virtual Machines

Step 1: 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.

You must first deploy the Carbon Black Cloud Workload appliance and register the appliance with the vCenter Server. After the appliance is deployed, you must generate the API ID and key from the Carbon Black Cloud.

Now, configure the Carbon Black Cloud Workload appliance and establish a connection between the Carbon Black Cloud Workload appliance and Carbon Black Cloud.

Step 1A: Deploy Carbon Black Cloud Workload appliance in the vCenter Server

You must 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 the appliance interface access only to the authorized administrators. Unrestricted network access to the appliance interface is not required.

Prerequisites

- Verify the system requirements.
- Verify you have the Carbon Black Cloud Workload appliance `OVA` file available. For details, see Download the Installer.

Procedure

1. Log in to the vSphere Client.
2. Right-click the host where you want to install the Carbon Black Cloud Workload appliance, and then click **Deploy OVF Template**.
3. On the **Deploy OVF Template** page, configure the following values, and click **Next**.

Option	Description
Select an OVF Template	- **URL**: Enter the Carbon Black Cloud Workload appliance **URL** to a remote Web server. Supported URL sources are HTTP and HTTPS. Example: `http://<local-web-server>/cwp-va-1.0.0.0-17066560_OVF10.ova`. - **Local file**: Click **Choose Files** and select the downloaded OVA file.
Select a name and folder	(Optional) Change the name of the OVA file to **Workload Appliance**.
Select a compute resource	(Optional) Verify if the selected host is the correct resource where you want to deploy the Carbon Black Cloud Workload appliance.
Review details	Review the details. The Product must be **CBC Workload Appliance VA**.
License agreements	To accept the VMware license agreements, click **I accept all license agreements**.
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. **IP Allocation Settings**: Select **IP protocol** as **IPv4** or **IPv6**.

Option	Description
Customize template	a **Application**: - Type passwords for the *admin* and *root* user account and make sure that the password length meets the character requirements. You need these passwords later while registering with vCenter Server. The password must meet the following requirements: - At least eight characters - At least one lowercase character - At least one numeric character - At least one special character - Not more than 20 characters long b **Networking Properties**: - If you want DHCP to be available while configuring the appliance, leave the configuration values empty. - If you want to configure the static IP address: - Domain Name and Domain Search Path: Host name of the virtual machine. For example `host.example.local`, enter `host` in the domain name field and enter `example.local` in the domain search path field. - Ask your network administrator and add the following mandatory values: Default Gateway, Domain Name Servers, Network 1 IP Address, Network 1 Netmask.
Ready to complete	Verify the details and click **Finish**.

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.

   By default, the Carbon Black Cloud Workload appliance time zone is UTC and cannot be changed.

5 Note down the Carbon Black Cloud Workload appliance IP address.

Results

The Carbon Black Cloud Workload appliance is deployed.

What to do next

Register appliance with vCenter Server.

Step 1B: Options to 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 or with the one in your VMware Cloud on AWS software-defined data center (SDDC).

Register Appliance with On-Premises vCenter Server

After the Carbon Black Cloud Workload appliance is deployed, you can 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 must have HTTPS (443) connectivity to communicate with the vCenter Server.

Procedure

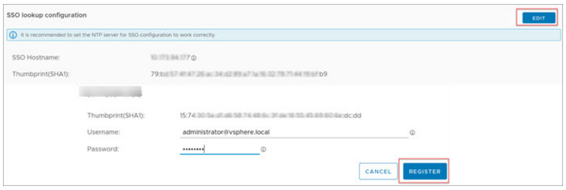
1 From your browser, log in to the Carbon Black Cloud Workload appliance at `https://<appliance IP address>` using the **`admin`** credentials.

The appliance dashboard appears as a default home page.

2 Go to the **Appliance > Registration** page.

3 In the **SSO lookup configuration** section, click **Edit** and configure the following values.

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. For details, refer to Configure NTP Server Settings.



SSO lookup configuration

It is recommended to set the NTP server for SSO configuration to work correctly.

SSO Hostname: [redacted]

Thumbprint(SHA1): 79:b[redacted]b9

[redacted]

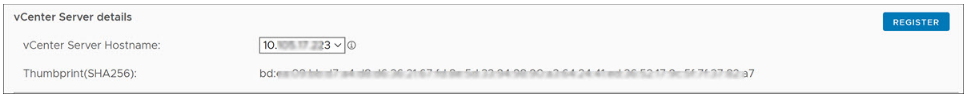
Thumbprint(SHA1): 15:74[redacted]:dc:dd

Username: administrator@vsphere.local

Password: ••••••••

SSO lookup configuration	Description
SSO Hostname	Enter the IP address or FQDN of the vCenter Single Sign-On (SSO) and click **Register**. You must have time synchronization between the SSO server and the Carbon Black Cloud Workload appliance. **Note** Carbon Black Cloud Workload appliance uses a service account to interact with vCenter. This service account is created in your SSO server for an improved security and manageability. You need SSO administrator credentials for creating this service account. The SSO administrator credentials are only used for this session and are not persisted 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, refer to vSphere documentation.

SSO lookup configuration	Description
VMware Cloud on AWS	By default, the toggle is off. Do not change the settings.
Thumbprint (SHA1)	Verify the SHA1 thumbprint of the SSO server.



vCenter Server details

vCenter Server Hostname: 10.[redacted]3

Thumbprint(SHA256): bd:[redacted]a7

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 again with the same *Administrator* role 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 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. For details, see Required Firewall Rules in SDDC.
- Configure NAT rule for the appliance IP. For details, see Create NAT Rule For Appliance IP.

Procedure

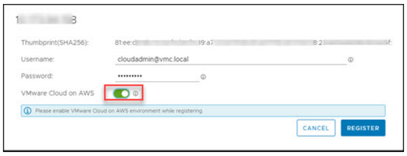
1 From your browser, log in to the Carbon Black Cloud Workload appliance at `https://<appliance IP address>` using the **`admin`** credentials.

   The appliance dashboard appears as a default home page.

2 Go to the **Appliance > Registration** page.

3 In the **SSO lookup configuration** section, click **Edit** and configure the following values.

   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. For details, refer to Configure NTP Server Settings.

SSO lookup configuration	Description
SSO Hostname	Enter the IP address or FQDN of the vCenter Single Sign-On (SSO) instance and click **Register**. The VMC URLs are listed in vmc.vmware.com, under **SDDCs > Settings**. For example, **`vcenter.sddc-x-x-x-x.vmwarevmc.com`**. Do not enter *https://* header. You must have time synchronization between the SSO server and the Carbon Black Cloud Workload appliance.
VMware Cloud on AWS	Toggle to turn on the VMware Cloud on AWS environment.  1[redacted]3 Thumbprint(SHA256): 81:ee:[redacted]39:a7[redacted]8:2[redacted]f: Username: cloudadmin@vmc.local Password: •••••••••• VMware Cloud on AWS Please enable VMware Cloud on AWS environment while registering CANCEL REGISTER
User name and Password	Enter the user name and password for the vSphere Administration in VMware Cloud on AWS. For example, **`cloudadmin@vmc.local`**.
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 🛡 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.

Required Firewall Rules in SDDC

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

1 Log in to the VMC Console.

2 On the **Networking & Security** tab, click **Gateway Firewall**.

3 Go to the required tab and ensure that the following firewall rules are configured.

Firewall Rule	Source	Destination	Service/Applied To
Go to the **Management Gateway** 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 **Management Gateway** 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 **Compute Gateway** 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 down rule for specific URL based on network settings of your organization. Make sure appliance has external connectivity with the Carbon Black Cloud.

Create NAT Rule For Appliance IP

After you deploy Carbon Black Cloud Workload appliance, the IP address of the appliance is a private IP accessible only from inside the SDDC network. To make the IP address securely accessible, you must generate publicly accessible IP address for the appliance and map the public IP address with the private IP address of the appliance using Network Address Translation (NAT).

1 Log in to the VMC Console.

2 On the **Networking & Security** tab, click **Public IPs**.

3 Generate 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
Give any name to your NAT rule	Add Public IP address generated earlier	All Traffic	Any	Add IP address of the Carbon Black Cloud Workload appliance	Match Internal Address

To create or modify NAT rules, see *VMware Cloud on AWS Networking and Security*.

Step 1C: Generate API ID and API Secret Key

You must 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 Carbon Black Cloud Workload appliance 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, generate a separate API key for each appliance.

After you deploy the 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

- Verify you have deployed the Carbon Black Cloud Workload appliance in the vCenter Server. For details, see Step 1A: Deploy 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 the necessary permissions.

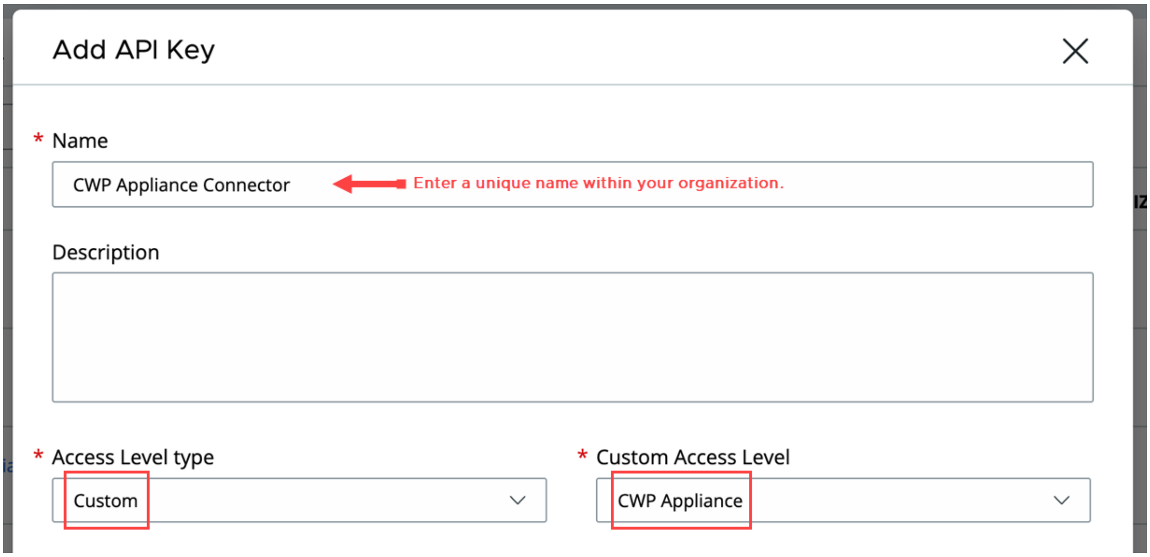
Procedure

1 Log in to the Carbon Black Cloud console.

2 From the left navigation pane, go to the **Settings > API Access** page.

3 Select the **API Keys** tab and click **Add API Key**.

The **Add API Key** window displays.



Add API Key

* Name

CWP Appliance Connector

Description

* Access Level type

Custom

* Custom Access Level

CWP Appliance

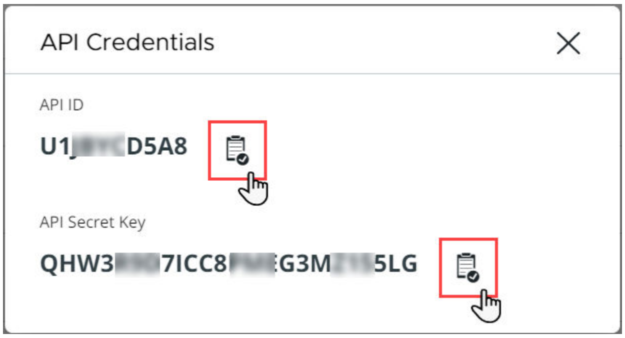
4 Enter a name for your appliance API key. The name must be UNIQUE for your Carbon Black Cloud organization.

5 Select **Custom** from the **Access Level type** drop-down menu.

6 From the **Custom Access Level** drop-down menu, find and select the `CWP Appliance` custom access level for your appliance.

7 Click **Save**.

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



API Credentials

API ID

U1[redacted]D5A8

API Secret Key

QHW3[redacted]7ICC8[redacted]G3M[redacted]5LG

8 Copy both of the keys.

You use these keys later to establish a connection between the appliance and the Carbon Black Cloud console.

Note You can use only one API ID and secret key per appliance. Once you use the generated API ID and secret key for your appliance, you cannot use the same API ID and secret key for any other appliance.

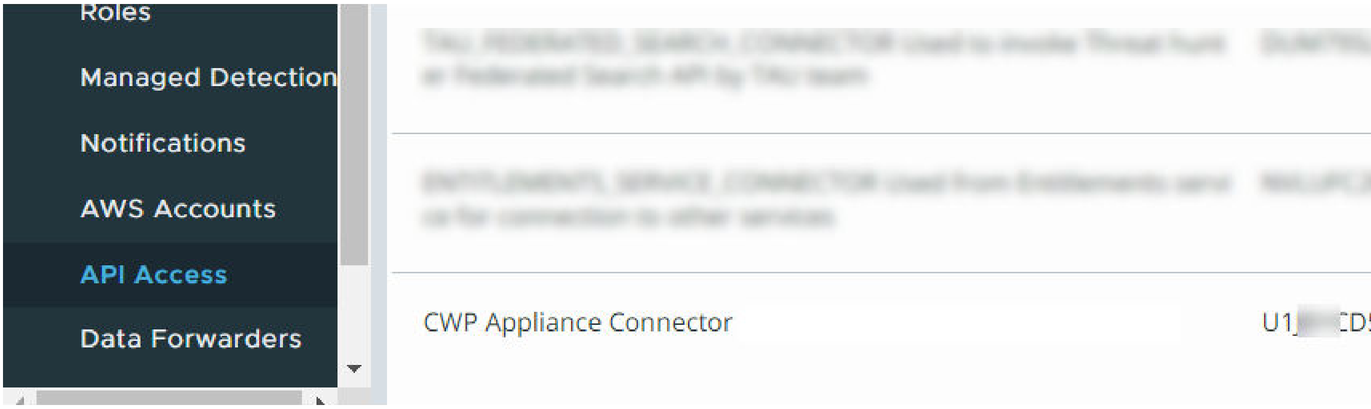
What to do next

Use the keys to Connect Carbon Black Cloud Workload Appliance with Carbon Black Cloud between Carbon Black Cloud Workload appliance and the Carbon Black Cloud console.

If you want to view and copy the keys later, perform the following steps.

1 Go to the **Settings** > **API Access** > **API Keys** tab.

2 Go to the appliance API name created earlier and click the down arrow next to the edit icon.



3 Click **API Credentials**.

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

Step 1D: Register 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 can register the appliance with Carbon Black Cloud.

Connect 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. For more information, refer to Step 1C: Generate API ID and API Secret Key.

- 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.

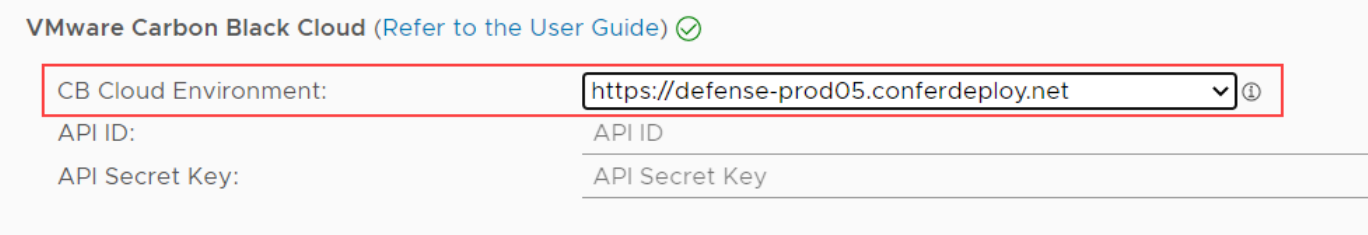
2 To verify that the Carbon Black Cloud Workload appliance VM is powered on, open the VM console and note down the IP address of the appliance.

3 From your browser, log in to the Carbon Black Cloud Workload appliance at **`https://<appliance IP address>`** using the **`admin`** credentials.

4 Go to the **Appliance > Registration** page.

5 In the Carbon Black Cloud section, click **Edit**.

6 Select a Carbon Black Cloudenvironment from the **CB Cloud Environment** drop-down menu.



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

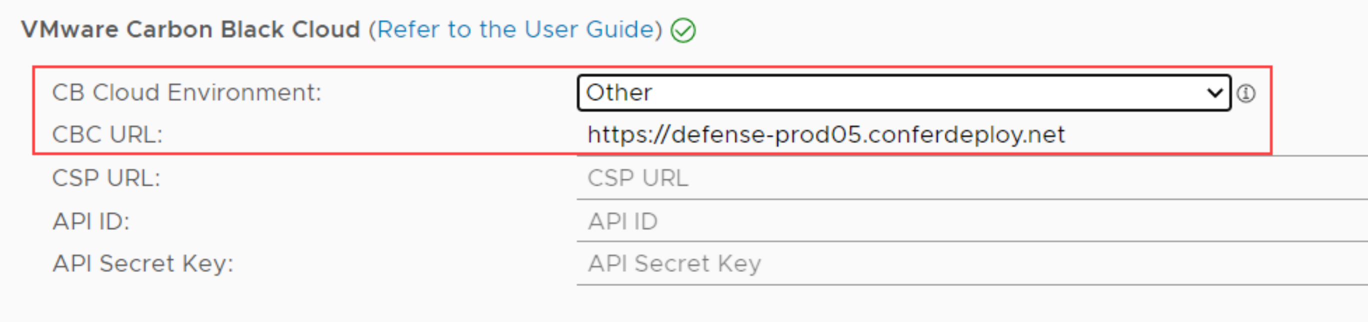
CB Cloud Environment: https://defense-prod05.conferdeploy.net

API ID: API ID

API Secret Key: API Secret Key

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

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

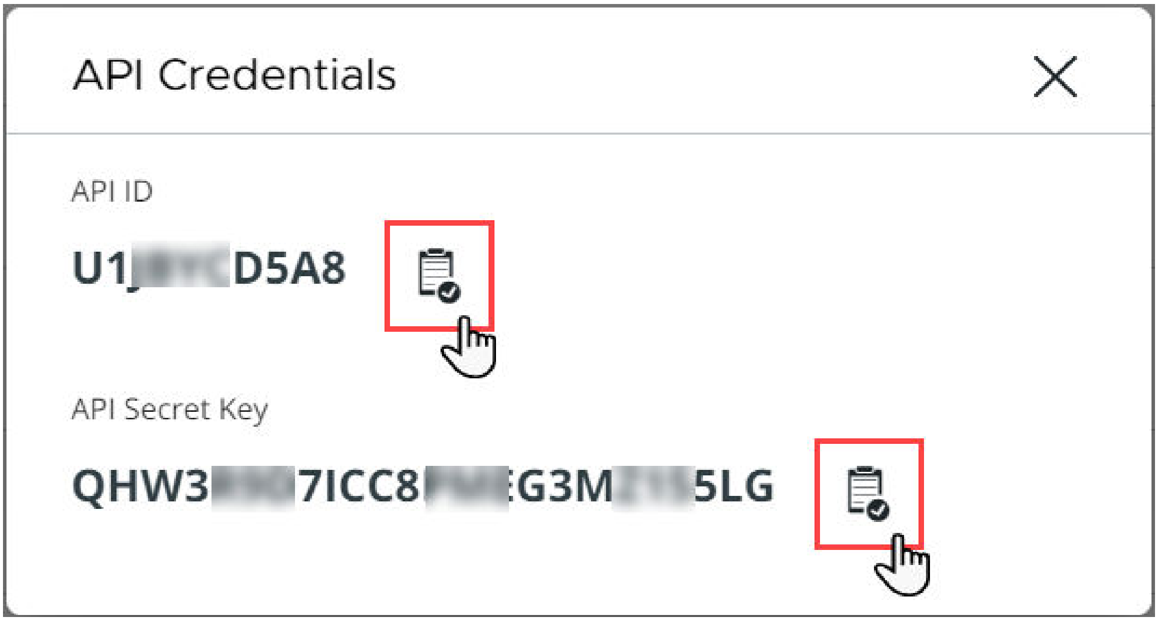
API Secret Key: API Secret Key

8 Configure the following mandatory values.

   a **CB Cloud Environment**: Enter the Carbon Black Cloud console URL as per your hosted Carbon Black Cloud location.

   b API ID: Paste the 10 digit *API ID* copied from the Carbon Black Cloud console.

   c API secret key: Paste the *API secret key* copied from the Carbon Black Cloud console.



API Credentials

API ID

U1[redacted]D5A8

API Secret Key

QHW3[redacted]7ICC8[redacted]G3M[redacted]5LG

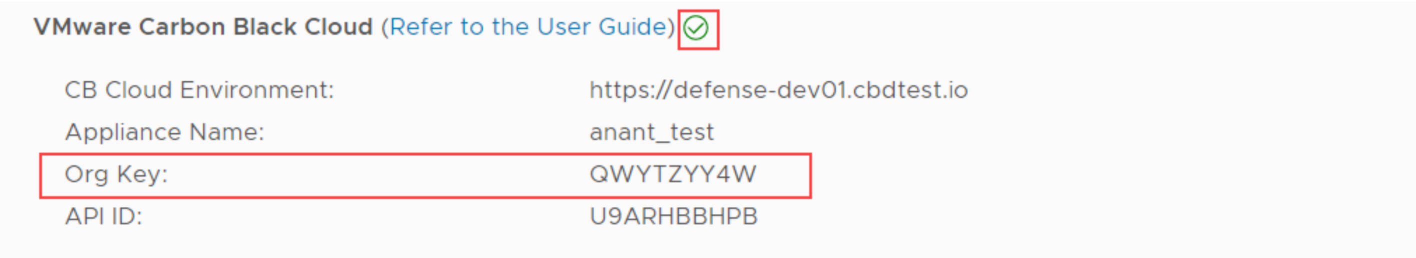
9 Click **Save**.

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 see the Org Key.
- If the registered Carbon Black Cloud Workload appliance is with version 1.1, you see the Org Name.
- If the registered Carbon Black Cloud Workload appliance is with version earlier then 1.1, you 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:	QWYTZYY4W
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

Verify if the connection between the Carbon Black Cloud Workload appliance and the Carbon Black Cloud is established successfully

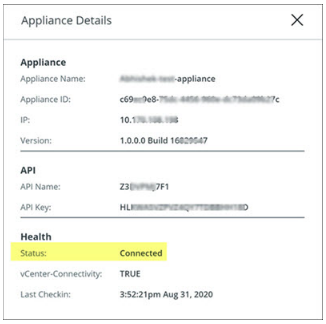
Procedure

1 Log in to the Carbon Black Cloud console.

2 From the left navigation pane, click the **Settings > API Access > API Keys** page.

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 with a link. You can view appliance health and connection status.



Appliance Details

Appliance

Appliance Name: [redacted]-appliance

Appliance ID: c69[redacted]9e8-[redacted]7c

IP: 10.1[redacted]

Version: 1.0.0.0 Build 16829547

API

API Name: Z3[redacted]7F1

API Key: HL[redacted]D

Health

Status: Connected

vCenter-Connectivity: TRUE

Last Checkin: 3:52:21pm Aug 31, 2020

5 Go to the **Inventory > Workloads > Not Enabled** page. You can view the virtual machine (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. For more details, see Appliance Logs.

View Inventory

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

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, Step 2: Enable Carbon Black on Virtual Machines .
2. View your inventory in the Carbon Black Cloud console.
   a. From the left navigation pane, go to the **Inventory > Workloads > Not Enabled** tab.
   b. Refresh the **Not Enabled** tab.

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

Step 1E: Register 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` – With this policy 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` – With this policy 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 within the Carbon Black Cloud console or remove already applied NSX policies from certain 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 and later.

Procedure

1. 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 **NSX details** section, select the NSX Manager IP address from the **NSX hostname** drop-down menu.

   The **Register** button becomes active.
4. To trigger the NSX on-boarding, click **Register**.
5. Enter the NSX administrator user and password, and click **Register**.

   Once NSX on-boards, a green check mark confirms the successful registration. It can take up to 15 seconds for the process to complete.

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

You can trigger the off-boarding process for NSX by selecting and confirm the off-boarding.

Preparing VMs with Carbon Black Launcher

You can enable Carbon Black in your data center with an easy one-click deployment. To minimize your deployment efforts, a lightweight Carbon Black launcher is made available with VMware Tools. Carbon Black launcher must be available on the Windows and Linux VMs.

When you enable Carbon Black from the Carbon Black Cloud Workload Plug-in, the silent installation is triggered where the launcher downloads and installs the Carbon Black sensor on the virtual machine. The install process takes care of installing the right components which are supported on a particular platform.

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 or later.

- **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 for your guest operating system from the package repository at http://packages.vmware.com/. For details, refer to Carbon Black Launcher for Linux VMs.

After the launcher is available, you can proceed to enable Carbon Black from the Carbon Black Cloud Workload Plug-in.

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 or later.

For more information, refer to VMware Tools documentation.

Important 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 or later.
- 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 Carbon Black on the guest Linux virtual machines (VM) where your workloads are running, you must first install the Carbon Black launcher using the VMware package repository. The Linux VM (or server that is used to supply binaries to VMs) must be able to access the *https://packages.vmware.com* site.

This method is the preferred method for installation. Perform the steps as applicable for your Linux distribution. You must have the *root* privilege on the Linux VM.

Prerequisites

- The Linux VM (or server that is used to supply binaries to VMs) must have access to https://packages.vmware.com. To verify accessibility to *packages.vmware.com*, use the `ping packages.vmware.com` command. Then run the `curl -Is https://packages.vmware.com/cb/cblauncher` command. The curl request returns the `HTTP/1.1 200 OK` status code.
- The following dependencies must be installed on the Linux VM.
  - *libglib-2.0*
  - *libgthread*
  - *gnupg2*

- Use Carbon Black launcher 1.3 or later for Linux VMs to install Carbon Black sensor kit version 2.13 or later with an optional sensor configuration file that you can upload if you have custom configurations. The Carbon Black launcher 1.3 introduces support for custom configuration with Linux sensor kit version 2.13 and later.
- Use Carbon Black launcher 1.1 or later for Linux VMs to install Carbon Black sensor kit with version 2.11.2 or later. The Carbon Black launcher 1.1 enforces full digital-signature verification for all files contained in a sensor kit 2.11.2 or later.
  - Starting with Carbon Black sensor version 2.11.2, the tar-balls are enabled with full signature verification. If you use Carbon Black launcher 1.1 or later to download and install a Carbon Black sensor kit with version earlier than 2.11.2, the signature verification capability is not enabled on the sensor kit and the sensor installation cannot complete due to signature verification failure.
  - If you use a Carbon Black launcher 1.0 or earlier to install a Carbon Black sensor kit 2.11.2 or later, the launcher installs the sensor without full verification.

Procedure

1 **For Ubuntu systems**:

a Obtain and import the VMware packaging public keys using the following commands.

```
curl -L https://packages.vmware.com/cb/cblauncher/key/VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub --output VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub
```

```
apt-key add VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *cblauncher.list* under `/etc/apt/sources.list.d`.

c Create or edit `/etc/apt/sources.list.d/cblauncher.list` with the following content:

```

deb [arch=amd64] https://packages.vmware.com/cb/cblauncher/latest/ubuntu xenial main
```

d Install the package using the following commands:

```

apt-get update
apt-get install cblauncher
```

2 **For RHEL/CentOS/Oracle/Amazon Linux systems**:

a Obtain and import the VMware packaging public keys using the following commands:

```
wget https://packages.vmware.com/cb/cblauncher/key/VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-
KEY.pub

rpm --import VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *cblauncher.repo* under `/etc/yum.repos.d`.

c Edit the `/etc/yum.repos.d/cblauncher.repo` file with the following content:

```

[repo-cblauncher]
name=cblauncher repo
baseurl=https://packages.vmware.com/cb/cblauncher/latest/
enabled=1
gpgcheck=1
```

d Install the Carbon Black launcher package using the following command:

```
yum install cblauncher
```

3 **For SLES systems**:

a Obtain and import the VMware packaging public keys using the following commands:

```
wget https://packages.vmware.com/cb/cblauncher/key/VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-
KEY.pub

rpm --import VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub
```

b Add the following repository:

```
zypper ar "https://packages.vmware.com/cb/cblauncher/latest/" cblauncher
```

c Install the Carbon Black launcher package using the following command:

```
zypper install cblauncher
```

4 To verify if the Carbon Black launcher is installed, run the following command with the root privilege based on the Linux distribution:

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

```
service cblauncher status
```

- For all other distributions like SUSE/Ubuntu/Amazon, use the following command.

```
systemctl status cblauncher
```

The status must be running.

Results

After the launcher is installed, you can enable Carbon Black on the Linux VMs similar to the Windows VMs from the Carbon Black Cloud Workload Plug-in.

Alternate Method to Install Launcher on Linux VMs

To enable Carbon Black launcher on Linux virtual machines (VM) where your workloads are running, you must first install the launcher. This method for installation is an alternate method. If you do not want to configure the repository, you can use this alternate method.

Perform the steps as applicable for your Linux distribution.

1 Go to the Linux VM.

2 Download the package and run the command for the appropriate Linux distribution.

Note The actual build number might change. You must replace the build number with the correct available one. For example, replace 16928845 in the cblauncher-1.0.0-*16928845*.x86_64 with the available build number.

Table 3-1. Linux Package and Command to Use for Installation

Linux Distribution	Link to Download Package	Command to Use for Installation
Ubuntu	1 Navigate to `https://packages.vmware.com/cb/cblauncher` 2 Select a specific version or click the **latest** one. 3 Click **ubuntu/** and navigate to the `cblauncher_[version]-[build-number]_amd64.deb` package.	■ `dpkg -i cblauncher_[version]-[build number]_amd64.deb` For example: `dpkg -i cblauncher_1.0.0-16928845_amd64.deb`
RHEL/SUSE/CentOS/Oracle/ Amazon Linux	1 Navigate to `https://packages.vmware.com/cb/cblauncher` 2 Select a specific version or click the **latest** one. 3 Locate the `cblauncher-[version]-[build-number].x86_64.rpm` package.	■ `rpm -Uvh cblauncher-[version]-[build number].x86_64.rpm` For example: `rpm -Uvh cblauncher-1.0.0-16928845.x86_64.rpm`

3 To start the Carbon Black launcher daemon, run the following command with the root privilege based on the Linux distribution.

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

```
service cblauncher start
```

- For all other distributions like SUSE/Ubuntu/Amazon, use the following command.

```
systemctl start cblauncher
```

4 To stop the Carbon Black launcher daemon, run the following command with the root privilege based on the Linux distribution.

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

```
service cblauncher stop
```

- For all other distributions like SUSE/Ubuntu/Amazon, use the following command.

```
systemctl stop cblauncher
```

5 To verify the Carbon Black launcher status, run the following command with the root privilege based on the Linux distribution.

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

```
service cblauncher status
```

- For all other distributions like SUSE/Ubuntu/Amazon, use the following command.

```
systemctl status cblauncher
```

The status must be running.

After the launcher is installed, you can enable Carbon Black on the Linux VMs similar to the Windows VMs from the Carbon Black Cloud Workload Plug-in.

Install Sectigo Certificates

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.

You use 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 the 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 of the 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.

Step 2: Enable Carbon Black 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 are not using 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.
- 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 Go to the **Inventory > Not Enabled** tab.

4 Verify the VM eligibility in the Status column. You can enable Carbon Black only 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	Due to few reasons, your VMs might not be eligible to enable Carbon Black. For example, - VM is powered off. - The required version of the VMware Tools or Carbon Black launcher is not available. - If the *isolation.tools.setinfo.disable* parameter for the VM is set to *true*. To make your VM eligible, you can perform any of the following actions based on the non-eligibility criteria. - Power on the VM. - For Windows VMs: Install or upgrade VMware Tools to 11.2 or later. - For Linux VMs: Install the launcher manually. For details, refer to Carbon Black Launcher for Linux VMs. - Set the *isolation.tools.setinfo.disable* parameter to *false*. For details, refer vSphere documentation.
Not Supported	Carbon Black Cloud Workload does not support the Operating System (OS) or the OS version. Upgrade to the supported OS and version. For details, see Chapter 2 Preparing to Enable Carbon Black in Your vSphere Environment.

5 Select one or more eligible VMs for which you want to enable Carbon Black, and then 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.	1 Click **Advanced**. A list of available version appears for each Operating System (OS). 2 Only the supported sensor versions are listed. Select the required version from the drop-down menu. 3 (Optional) You can preconfigure Carbon Black Cloud settings using the *configuration* file. You can upload the configuration file in a *.ini* file format. Click **Upload File**. Browse and select the *configuration* file. To view the sample configuration file and the parameter details, refer Configuration File Details.

6 A confirmation dialog box appears. 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. You can view VM status is *Active*.

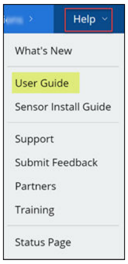
What to do next

After enabling Carbon Black on VMs where your 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 navigate to your 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.

For more information on Carbon Black Cloud, refer to the **User Guide** in the **Help** menu on the top-right hand of the Carbon Black Cloud console.



Configuration File Details

When you want to enable Carbon Black with a specific sensor version, you can upload a *configuration* file. You can preconfigure the Carbon Black Cloud settings using 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.

Sample Configuration File

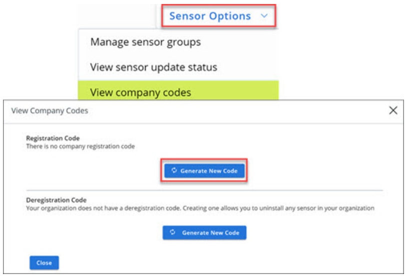
```
[customer]
EncodedCompanyCode = 7X2KTWJQHO@RUO@R5I1LNO3@E319A
CompanyCode = NBEA3DLZ
BackendServer = prod01.xyz.io
```

Mandatory Configuration File Parameters

EncodedCompanyCode, *CompanyCode*, and *BackendServer* are the mandatory parameters required in the configuration file. You can obtain values for the mandatory parameters as follows.

EncodedCompanyCode and **CompanyCode**: To obtain the company registration codes.

1. Sign in to the Carbon Black Cloud console and from the left navigation pane, click **Workloads**.
2. Click **Sensor Options**, and click **View company codes**.

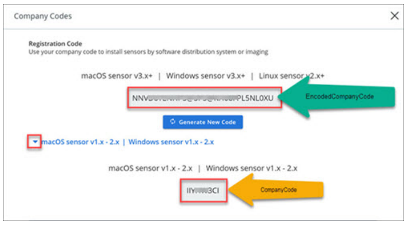


Registration Code
There is no company registration code

Deregistration Code
Your organization does not have a deregistration code. Creating one allows you to uninstall any sensor in your organization

3 Under **Registration Code**, click the **Generate New Code** button.

4 Take note of the generated code. The long string code is the **EncodedCompanyCode**. Copy and paste the code into a plain text editor.


Company Codes
macOS sensor v3.x+ | Windows sensor v3.x+ | Linux sensor v2.x+
EncodedCompanyCode
Generate New Code
macOS sensor v1.x - 2.x | Windows sensor v1.x - 2.x
macOS sensor v1.x - 2.x | Windows sensor v1.x - 2.x
CompanyCode

Registration Code
Use your company code to install sensors by software distribution system or imaging

NNV[redacted]PL5NL0XU

IIY[redacted]3CI

5 Expand the section and view the short string code. The short string code is the **CompanyCode**. Copy and paste the code into a plain text editor.

6 Paste both the codes in your configuration file.

BackendServer: Enter the device services URL for the Carbon Black Cloud based on your region. For example, **`https://devices.confer.net`**. To view the complete list of device services URL for each region, refer to Carbon Black Cloud: What URLs are used to access the APIs.

Additional Configuration File Parameters

You can add additional parameters in the configuration file as the described in the Install Sensors on VM Workloads.

Using the Carbon Black Cloud Workload Plug-in

4

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

To view the Carbon Black Cloud Workload Plug-in:

- Log in to the vSphere Client using your administrator credentials.
- 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. You can also view vulnerabilities affecting your assets and critical product vulnerabilities.

- Go to the **Inventory > Not Enabled** tab to enable Carbon Black for your data center inventory.
- 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.

  The Carbon Black Cloud Workload Plug-in detects and segregates the protected inventory into Workloads and VDI in the **Inventory > Enabled > Deployment Type** column.
- Go to the **Vulnerabilities** tab to view vulnerabilities affecting your assets.

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.

Read the following topics next:

- Sensor Statuses and Details
- Install Host User World Automatically
- Install Host User World Manually
- Vulnerability Management

Sensor Statuses 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.

Table 4-1.

Sensor Status	Description
Active	Sensors are communicating to the Carbon Black Cloud properly.
Inactive	Sensors are not communicating to the Carbon Black Cloud for last 30 days.
Registered	Sensors are registered.
Deregistered	Sensors are deregistered or uninstalled. Sensors persist on the **Inventory > Not Enabled** tab in the *Deregistered* status until removed from the Carbon Black Cloud console. **Note** The sensor gets deleted when VM is deleted or VM is moved to another vCenter Server. The deleted sensors are displayed as *Deregistered* on the Carbon Black Cloud console. The workload sensors that are inactive for three or more days and have received a *delete* action from the vCenter Server gets **Deregistered** automatically.
Errors	Sensors are reporting errors.
Eligible for update	Sensors can be updated to the most current, available sensor version.
Bypass	Sensors have been put into the *Bypass* mode by the Carbon Black Cloud administrator. All policy enforcement on the asset is disabled and the sensor do not send data to the cloud. Sensors can momentarily enter *Bypass* mode during a sensor update.
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.

Install Host User World Automatically

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 of a host user world on every host in your vCenter Server and then configure its settings to communicate with the appliance, you can use a newly introduced automatic installation and configuration flow.

You 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.

   Once 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 being connected.
4. To upgrade the host user world to its latest version, click the **Upgrade Host Module**.

   Once 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 within 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 **VMware Carbon Black Cloud** pop-up.

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. For more information, see *VMware Carbon Black Cloud Sensor Installation Guide*.

Install Host User World Manually

You can install the 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 allows you to use a vSphere Lifecycle Manager single image as an alternative way to install and manage the lifecycle of the ESXi hosts in your environment.

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

Then, 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, is visible under the **Image Depot** tab. When vSphere Lifecycle Manager synchronizes to online depots, it downloads only the update metadata. The actual payload downloads during staging or remediation.

Finally, 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.

For details on the vSphere Lifecycle Manager user interface in the vSphere client, see *Managing Host and Cluster Lifecycle*.

Prerequisites

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

Procedure

1. Log in to the vSphere Client using your administrator credentials.
2. Select **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
https://prod.cwp.carbonblack.io/cbhost/*us*/online-depot/index.xml	Depot URL for the United States region.
https://prod.cwp.carbonblack.io/cbhost/*au*/online-depot/index.xml	Depot URL for the Africa Union region.
https://prod.cwp.carbonblack.io/cbhost/*ap*/online-depot/index.xml	Depot URL for the Asia-Pacific region.
https://prod.cwp.carbonblack.io/cbhost/*eu*/online-depot/index.xml	Depot URL for the Europe region.

   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** drop-down menu, and select **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 setup the image.

   a From the vSphere Client drop-down **Menu**, click **Hosts and Clusters**, and select the cluster you want to manage with the image.

   b On the **Updates** tab, select **Hosts > Image**, and click the **Setup Image** button.

      The **Convert to an Image** page displays.

   c To define the image in step 1, select the ESXi version from the related drop-down menu, click **Add Components**, and select the VMware Carbon Black component.

      The Carbon Black component shows in the **Additional components** table.

   d Select **Validate**, and once 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** card and **Image Compliance** card show summary of the image setup.

8 Remediate all your hosts in the cluster.

   a While in the **Image Compliance** card, select 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** card 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, select **Configuration > Security**.

   The hosts display in `Needs install` state.

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

   After the operation completes successfully, the hosts display in `Latest sensor installed` state.

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 **Check Compliance** again.

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

Vulnerability Management

As a vCenter Server administrator, you want to have 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 now monitor known vulnerabilities from the Carbon Black Cloud Workload Plug-in. You can discover vulnerabilities from the plug-in **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 looks into 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 the Windows VMs.
  - **Linux Apps**: Displays application-level vulnerabilities for the 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 go to the 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).

Depending on how you want to view the vulnerability data, 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.

Each VM can have multiple vulnerabilities and each vulnerability can have different risk scores. Based on the risk score, vulnerabilities are filtered on the level of severity such as critical, important, moderate, and low. The higher the risk score, the higher the severity. The highest risk score is considered as a critical vulnerability. To learn more, refer to Evaluating Risk.

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 based on Windows and Linux systems. To view more details about the risk score and the Common Vulnerability Scoring System (CVSS), click the **Vulnerability Count** number. Expand the row the 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 which takes you to 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. If you want to view the updated vulnerability data immediately, click **Reassess**.

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

Evaluating Risk

The Risk Score is a metric that accurately represents the risk of a given vulnerability in your data center. It does so by combining CVSS information with proprietary threat data and advanced modeling from *Kenna Security*.

Measures of Risk

Carbon Black Cloud partners with *Kenna Security* to leverage the largest database of vulnerability, exploit, and event threat data in the industry. This data is distilled into three main measures of risk:

- **Active Internet Breach**: Presence of a near-real-time exploitation.
- **Malware Exploitable**: Availability of an exploit module in a weaponized exploit kit.
- **Easily Exploitable**: Availability of a recorded exploit.

There are few metrics defined for Common Vulnerability Scoring System (CVSS). Few of the metrics are about the attack method itself, whereas the others depend on how the application assesses impact - the direct consequence of a successful exploit. To learn more about CVSS, visit Common Vulnerability Scoring System.

Risk Score

Every vulnerability is assigned a risk score of between 0.0 (no risk) and 10.0 (maximum risk). The risk score range and severity are defined as follows.

Score Range	Severity
0.0–3.9	Low
4.0–6.9	Moderate
7.0–8.9	Important
9.0–10.0	Critical

To learn more about how the risk is calculated, refer to Understanding the Kenna Security Vulnerability Risk Score.

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

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

1 Go to the **VM** > **Monitor** > **Carbon Black** > **Vulnerabilities** tab.

2 Click the **App** tab.

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

For your quick reference, 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 may be empty if there is no update available from the product to fix the vulnerability or Carbon Black does not have enough information to point to a specific resolution.

Using the Carbon Black Cloud Workload Appliance

5

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 only to the authorized administrators. Unrestricted network access to the appliance interface is not required.

You can log in to the Carbon Black Cloud Workload appliance GUI 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 Appliance
- Appliance Health Status
- Maintaining the Appliance Password
- Reboot Appliance
- Redeploy Carbon Black Cloud Workload Appliance
- Appliance Logs

Manage Appliance Users

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

Prerequisites

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

Procedure

1 Log in to the appliance with *root* credentials.

2 To create a new user with a specified home directory and a group, to which the user belongs to, use the command `useradd -m -G <group-name> <user-name>`.

For example, 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 the newly created user, use the command `passwd <user-name>`.

For example, 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 that 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 From your browser, log in to the vCenter Server at **`https://<vCenter IP/Domain address>`** using the **`admin`** credentials. The Carbon Black Cloud Workload appliance is located here.

2 To configure the time synchronization settings with the vCenter Server, go to the **Appliance > General** tab.

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

Note 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 the Knowledge Base article.

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, **`pool.ntp.org`**. 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 if the date and time are synchronized with the vCenter Server.

4 Click **Save**.

Results

The NTP server setting is configured.

View and Update Network Settings

Use the **Network** page to view network settings of the appliance VM. 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 (UI).

Procedure

1 Log in to the appliance with *root* credentials.

2 Run the virtual appliance management interface (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 the **`admin`** credentials.

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

Results

The NTP server settings are updated.

Configure Proxy Settings for Appliance

By configuring the proxy server, you can 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. You configure a proxy server of type **HTTP**, **HTTPS**, **SOCKS4**, or **SOCKS5**.

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

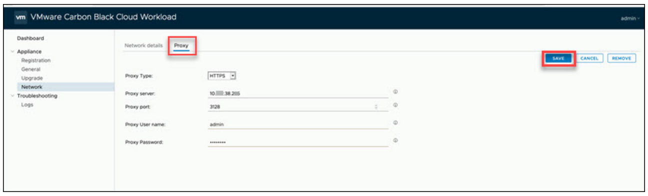
- Register the Carbon Black Cloud Workload appliance with Carbon Black Cloud, and vCenter Server.
- The proxy support for appliance is available for version 1.1 or later.

Procedure

1 From your browser, log in to the vCenter Server at **`https://<vCenter IP/Domain address>`** using the **`admin`** credentials. The Carbon Black Cloud Workload appliance is located here.

2 To configure the proxy settings, go to the **Appliance > Network** page.

3 Select the **Proxy** tab, and click **Edit**.



Proxy Type: HTTPS

Proxy server: 10.[redacted].38.2[redacted]

Proxy port: 3128

Proxy User name: admin

Proxy Password: ••••••••

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 on which 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 not being able 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 prompts an error message.

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

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

6 Select the Carbon Black Cloud environment you want the appliance to connect to 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 updates 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 on the Carbon Black Cloud Workload Plug-in. Appliance Worker, vSphere Worker, Gateway, and Access Control Service are the appliance services. You can also view the connectivity status of each appliance service on the Carbon Black Cloud Workload Plug-in. You can also view service-wise health status on the Carbon Black Cloud Workload appliance dashboard.

The appliance can have one of the following health statuses:

- **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. For details, refer to Connect Carbon Black Cloud Workload Appliance with Carbon Black Cloud .

  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 properly 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 individual service statuses. For the disconnected appliance service, you can restart the service as follows.

  a SSH to the Carbon Black Cloud Workload appliance using the *admin* credentials.

  b Switch to the *root* user using the `sudo su` command.

  c Use the appropriate command for the service that you want 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 Verify the appliance service status again.

  e If any of your appliance services is still down, you can contact the VMware Carbon Black support team at https://www.carbonblack.com/support/ or VMware support team at https://www.vmware.com/support/contacts.html.

  Log files help the support team to troubleshoot any issues for which you have opened the support ticket. For details, refer to Appliance Logs.

Maintaining the Appliance Password

Your appliance password is active for a certain amount of time. To maintain it, either 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 UI displays a notification when your password is due to expire. The message appears 15 days before the password expiry and is similar to `Password expires in X days`. The Carbon Black Cloud Workload Plug-in also shows notification on appliance's password expiry with the following message `Password for appliance expires in X days`. 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 UI shows a root password expiration notification. You can also view the appliance root password expiration notification in the Carbon Black Cloud Workload Plug-in, part of the vSphere Client UI.

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. From your browser, log in to the vCenter Server at **`https://<vCenter IP/Domain address>`** using the **`admin`** credentials. The Carbon Black Cloud Workload appliance is located here.
2. Under **Hosts & Clusters**, select the Carbon Black Cloud Workload appliance.
3. In vCenter Server, click the **Summary** tab and click **Launch Web Console**.

   Allow pop-up windows if needed.
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, then use the following command to unlock:

   ```
   pam_tally2 -r -u admin
   ```
7. To change the *admin* user password.

   a. SSH to the Carbon Black Cloud Workload appliance using the *admin* credentials.

      For example, `SSH admin@<Appliance_IP_Address>`.

   b. Use the `passwd admin` command.

   c. Enter the current password and then the password that you want, and note it for the future reference.

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

   d. Reenter the admin password.

      The Carbon Black Cloud Workload appliance *admin* user password is changed.
8. To reset the expired password. The appliance password automatically expires after 90 days.

   a. SSH to the Carbon Black Cloud Workload appliance using the *admin* credentials.

   b. When prompted for a password, enter the admin password that you want, and note it for the future reference.

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

c Reenter the admin password.

The password is changed successfully.

d SSH to the Carbon Black Cloud Workload appliance again to verify that the password change is successful.

e Now log in to the Carbon Black Cloud Workload appliance UI with the *admin* user name and the changed password.

9 To reset the *root* password.

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

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 password that you want, and note it for the future reference.

Carbon Black Cloud Workload appliance *root* user password is changed.

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. If needed, 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 the *admin* credentials.

b Run the following commands and extend the password expiration time to the number of days required, for both *root* and *admin* users. The following example shows 180 days. You can replace 180 to the number of days required.

```
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
```

The password expiration time is reset to 180 days.

2 To disable the password expiration permanently.

   a SSH to the appliance using the *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
   ```

   The password expiration is disabled permanently.

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 the appliance initial installation and configuration.

If your admin password expires, you are not able to 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 From your browser, log in to the vCenter Server at **`https://<vCenter IP/Domain address>`** using the **`admin`** credentials. The Carbon Black Cloud Workload appliance is located here.

2 Navigate to the **Appliance** > **General** > **Password Settings** tab.

   By default, the admin password expiry option is enabled.

3 To disable the expiration of your admin password, click the related toggle switch.

   The toggle switches its state to inactive.

Results

You are not promted for a password update.

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 Carbon Black Cloud Workload Appliance

If the Carbon Black Cloud Workload appliance is unreachable and unresponsive, you can redeploy the appliance. To redeploy the same appliance, you must register with the same 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.

You are unable to connect to the appliance or appliance is unresponsive. You are not able to log in to the appliance even after resetting the password multiple times. To resolve the appliance issue, you decided to redeploy the appliance.

Procedure

1. Delete the old Carbon Black Cloud Workload appliance from the vCenter Server. For details, refer to Delete Appliance from vCenter Server.
2. Deploy Carbon Black Cloud Workload appliance as described in Step 1A: Deploy Carbon Black Cloud Workload appliance in the vCenter Server.

   Note If you are not able to access appliance UI, clear the web browser SSL certificate cache, and then log in to the appliance.
3. Register appliance with the same SSO and vCenter Server as described in Register Appliance with On-Premises vCenter Server.
4. Generate the API ID and key. For details, refer Step 1C: Generate 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 already registered appliance.
5. Register appliance using the API ID and API secret key. For details, refer Connect 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.

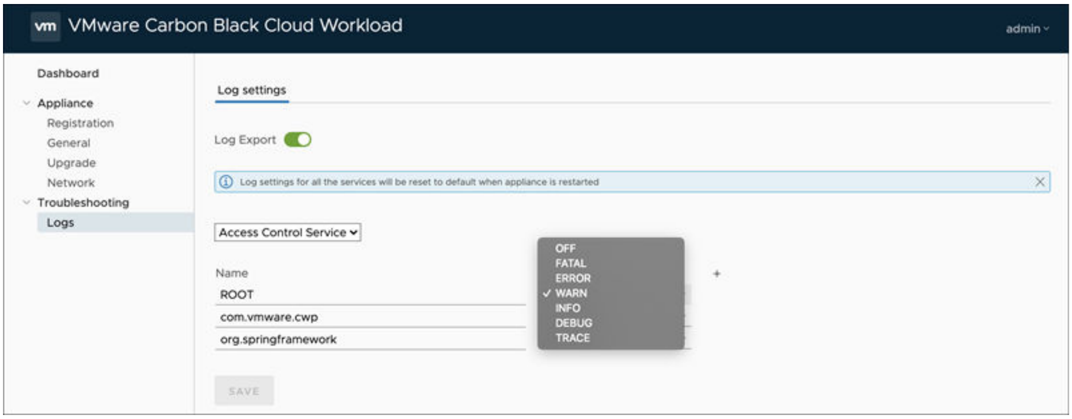
You can configure the log export and log level options. The log level can be configured in a built-in package file such as *Root* and *com.vmware.cwp*. By default, *Root* has **Warning** and *com.vmware.cwp* has **Info** as the assigned log level.

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. From your browser, log in to the vCenter Server at **`https://<vCenter IP/Domain address>`** using the **`admin`** credentials. The Carbon Black Cloud Workload appliance is located here.
2. Go to the **Troubleshooting** > **Logs** page.



Log Export ●

ⓘ Log settings for all the services will be reset to default when appliance is restarted ✕

Access Control Service

Name
ROOT
com.vmware.cwp
org.springframework

3. **Log Export**: 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 from the list as follows:

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

Results

Log export and log level settings are changed.

Updating Carbon Black in Your vSphere Environment

6

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 on Virtual Machines

You can quickly 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 your administrator credentials.
2. In the left navigation pane, click **Carbon Black**.
3. Go to the **Inventory > Enabled** tab.
4. Select one or more VMs for which you want to update Carbon Black, and then click **Update**.

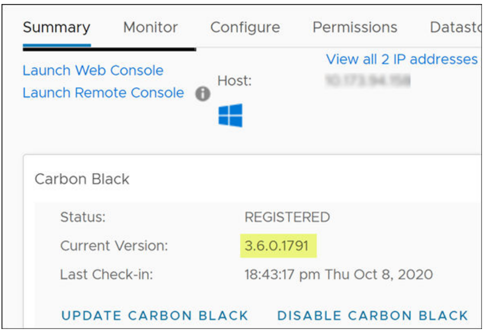
   A confirmation dialog box appears.
5. Click **OK**.

Results

Carbon Black is updated to the latest available sensor version.

You can also update Carbon Black for the individual VMs. Go to the VM (Windows or Linux) where you want to update, and on the **Summary** tab, scroll down to the Carbon Black panel. Alternatively, you can also use the **Configure > Carbon Black > Security** tab.

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



Host: [redacted]

Carbon Black

Status: REGISTERED

Current Version: 3.6.0.1791

Last Check-in: 18:43:17 pm Thu Oct 8, 2020

Upgrade Carbon Black Cloud Workload Appliance

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

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

You 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

You must open firewall for the *prod.cwp.carbonblack.io* domain with TCP port 443.

Procedure

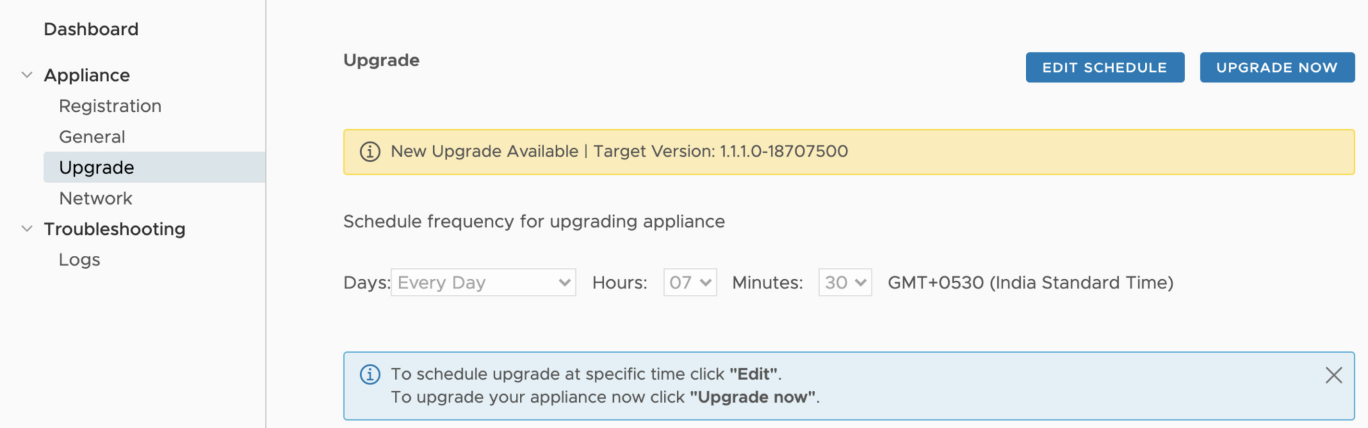
1 From your browser, log in to the vCenter Server at **`https://<vCenter IP/Domain address>`** using the **`admin`** credentials. The Carbon Black Cloud Workload appliance is located here.

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.

You 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.



New Upgrade Available | Target Version: 1.1.1.0-18707500

Schedule frequency for upgrading appliance

Days: Every Day Hours: 07 Minutes: 30 GMT+0530 (India Standard Time)

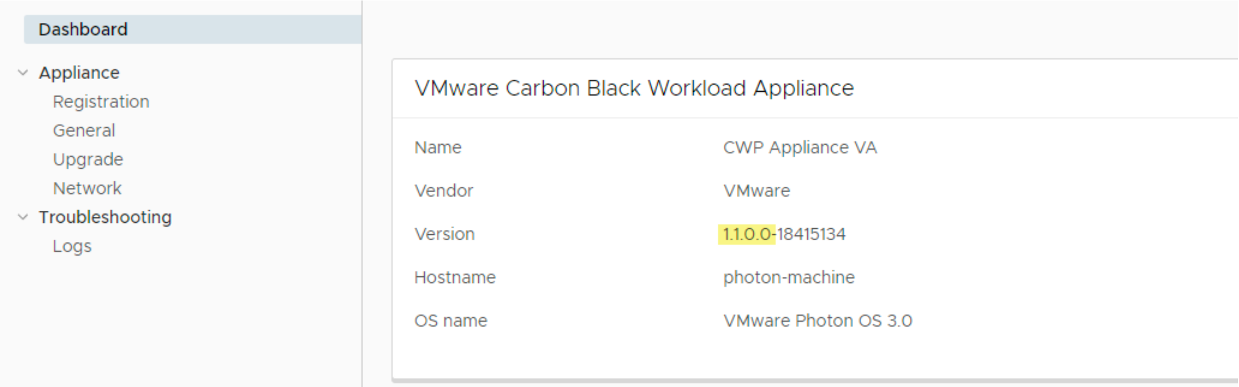
To schedule upgrade at specific time click **"Edit"**.
To upgrade your appliance now click **"Upgrade now"**.

5 Optional. Click the **Upgrade Now** button to promptly 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.



VMware Carbon Black Workload Appliance

Name	CWP Appliance VA
Vendor	VMware
Version	1.1.0.0-18415134
Hostname	photon-machine
OS name	VMware Photon OS 3.0

Upgrade Appliance To 1.0.2

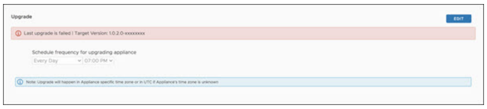
The automatic appliance upgrade to the version 1.0.2 is not working. The system fails to extract the downloaded upgrade bundle due to a ZIP extraction error. You must upgrade your appliance to the 1.0.2 version using the instructions provided in this topic.

1 Verify the appliance upgrade status.

a From your browser, log in to the Carbon Black Cloud Workload appliance at **`https://<appliance IP address>`** using the **`admin`** credentials.

b Go to 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.



Last upgrade is failed | Target Version: 1.0.2.0-xxxxxxxx

Schedule frequency for upgrading appliance
Every Day | 07:00 PM

Note: Upgrade will happen in Appliance specific time zone or in UTC if Appliance's time zone is unknown

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 See the value of the status field in the output. Here is a 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-xxxxxxxx/cwp-appliance-bundle- 1.0.2.0-
xxxxxxxx.zip, extract location/opt/vmware/cwp/etc/bundles/staging/wrapper- 1.0.2.0-
xxxxxxxx","source_version":null,"target_version":"1.0.2.0-xxxxxxxx"}
```

- 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 the 1.0.1 appliances. Proceed to the next step for your upgrade.
- 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 for the upgrade. The password for the appliance expires in 90 days. Change the passwords as explained in the Reset Appliance Password topic and then proceed to the next step.

3 Download and run the shell (.sh) script file as follows.

   a Click the following link. The script file gets downloaded. Extract the file to your local machine.

   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)" '1i 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 the *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 using the following commands 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.

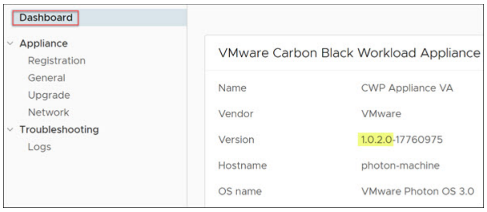
```
Updating config...
Restarting appliance worker service...
Settings updated successfully!
```

4 Schedule your appliance upgrade. For upgrade information, see Upgrade Carbon Black Cloud Workload Appliance .

Once the upgrade is triggered as per your schedule, monitor the upgrade page on the appliance UI for the result. Upgrade process generally finishes within 10 to 15 minutes.

5 To verify your upgrade.

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



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 7

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

You can uninstall the appliance that is no longer required.

Read the following topics next:

- Uninstall Carbon Black Sensors Manually
- Delete Appliance from vCenter Server

Uninstall Carbon Black Sensors Manually

You can manually deregister Carbon Black sensors. Sensors persist on the Carbon Black Cloud Workload Plug-in as *Deregistered* until removed from the Carbon Black Cloud console.

Uninstall Sensors on Windows VMs Manually

To uninstall sensors on Windows VMs manually, follow the steps mentioned in the Knowledge Base article.

Uninstall Sensors on Linux VMs Manually

To uninstall sensors on Linux VMs manually, follow the steps mentioned in the Knowledge Base article.

Uninstall Sensors from the Carbon Black Cloud Console

For instructions on how to uninstall sensors from the Carbon Black Cloud console and how to delete deregistered sensors, refer to the Carbon Black Cloud Sensor Installation Guide.

Delete Appliance from vCenter Server

You can remove the earlier deployed Carbon Black Cloud Workload appliance virtual machine (VM) from the vCenter Server.

Prerequisites

Carbon Black Cloud Workload appliance VM is deployed.

Procedure

1. From your browser, log in to the vCenter Server at **`https://<vCenter IP/Domain address>`** using the **`admin`** credentials. The Carbon Black Cloud Workload appliance is located here.
2. Go to 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**.

   A confirmation dialog box appears.
5. To unregister, click **OK**.
6. Log in to the vSphere Client using your administrator 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 *vSphere documentation*.

   The appliance is deleted from the vCenter Server. The Carbon Black Cloud Workload Plug-in is uninstalled as well. 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. From the left navigation pane, click the **Settings > API Access > API Keys** page.

    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. You can view appliance health status shows as **Disconnected**.

Results

Carbon Black Cloud Workload appliance VM is permanently deleted.

VM Clone and Carbon Black Cloud Workload 8

When you manually clone your virtual machine on which the Carbon Black Cloud Workload is enabled, you might see some inconsistent behavior. The parent and the clone VM might appear under both **Enabled** and **Not Enabled** tabs. You might observe a similar behavior in the Carbon Black Cloud console. The problem occurs as 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.

Windows VMs

Correct problem on the existing clones as follows:

1 Log in to the clone VM. For example, *WIN10_X64_VDI*.

2 Run the `repcli reregister` command as follows.

   ```
   repcli reregister now
   ```

   The clone VM is reregistered and the problem is remediated.

You must correct the problem on the golden image, so that further clones created from the golden image are reregistered correctly. Correct the problem as follows:

1 Log in to the parent VM where the Carbon Black sensors are installed. For example, *WIN10_X64_GOLDEN*.

2 Access the RepCLI Utility.

3 Complete the background scan and verify that the policy is updated with the `RepCLI Status` command.

   ```
   C:\Program Files\Confer> repcli status
   ```

4 Schedule the reregistration for the clone VM. Use the following `repcli reregister` command. Change *MASTER* with the computer name of the parent VM.

   ```
   if /i %computername% == MASTER (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)
```

5 Create clones from the golden image now.

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

6 Log in to the clone VM. For example, *WIN10_X64_VDI*. The clone VM is registered as separate device and is assigned a new device ID.

   For more details, refer Knowledge Base (KB). For more details, refer *Installing Sensors in a VDI Environment* of the Carbon Black Cloud Sensor Installation Guide.

Linux VMs

Perform the steps for registering a clone Linux VM with the Carbon Black Cloud back end:

1 Log in to the clone VM. For example, *LIN_CENTOS_VDI*.

2 Stop the *cbagentd* using the following command. Run the 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
     ```

3 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.

4 Start the *cbagentd* using the following command. Run the 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
     ```

VMware Carbon Black Sensor Gateway User Guide

9

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

The Sensor Gateway is an on-prem component that acts as a bridge for all inbound and outbound communication between the Carbon Black sensors 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. Also, it assumes familiarity with VMware vSphere®, including VMware ESXi™, VMware vCenter Server®, and VMware Tools™.

Read the following topics next:

- Sensor Gateway Overview
- Installing and Using Carbon Black Sensor Gateway
- Upgrade Your Sensor Gateway Appliance
- Troubleshooting Sensor Gateway
- Installing Sensor Gateway on Linux

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.

You might want to consider using the Sensor Gateway in the following cases.

- When you operate a tightly controlled environment and want to ensure that your workloads are secure and not directly exposed to the 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, which allows for communication only when registered with Carbon Black Cloud. It uses the API key mechanism to ensure no rogue Sensor Gateway servers can start communication with the Cloud.

With this release, 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.

Installing and Using Carbon Black Sensor Gateway

This section provides information about how to install, configure, and use the Sensor Gateway.

Preparing for Sensor Gateway Installation

Prepare your environment before installing a Sensor Gateway.

Set Up Your Environment

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

- Provision an SSL signed certificate. Choose between:
  - Certificate authority (CA) signed certificate. This certificate is the preferred choice. For more information, see Sensor Gateway Certificates.
  - Self-signed certificate. This certificate requires pushing these certificates into the trust store of each sensor workload. For more information, see Sensor Gateway Certificates.

  Note You need the private key for the certificate you are using.
- 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. For more information, see Create a Certificate Chain File.
- Acquire a Static IP for each Sensor Gateway server.
- Reserve a DNS entry. For example, `sensorgateway.`*`company`*`.com`

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

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

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

- 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, you must ensure that the Carbon Black Cloud URLs are accessible through the proxy.
- Set up a local mirror server for signature updates and configure your policy so that sensors download updates from the local server. See Signature Mirror Instructions. If you set up mirrors for the Update servers, verify that they are reachable through the proxy.

Provision Sensor Gateway API Key

You must 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 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.

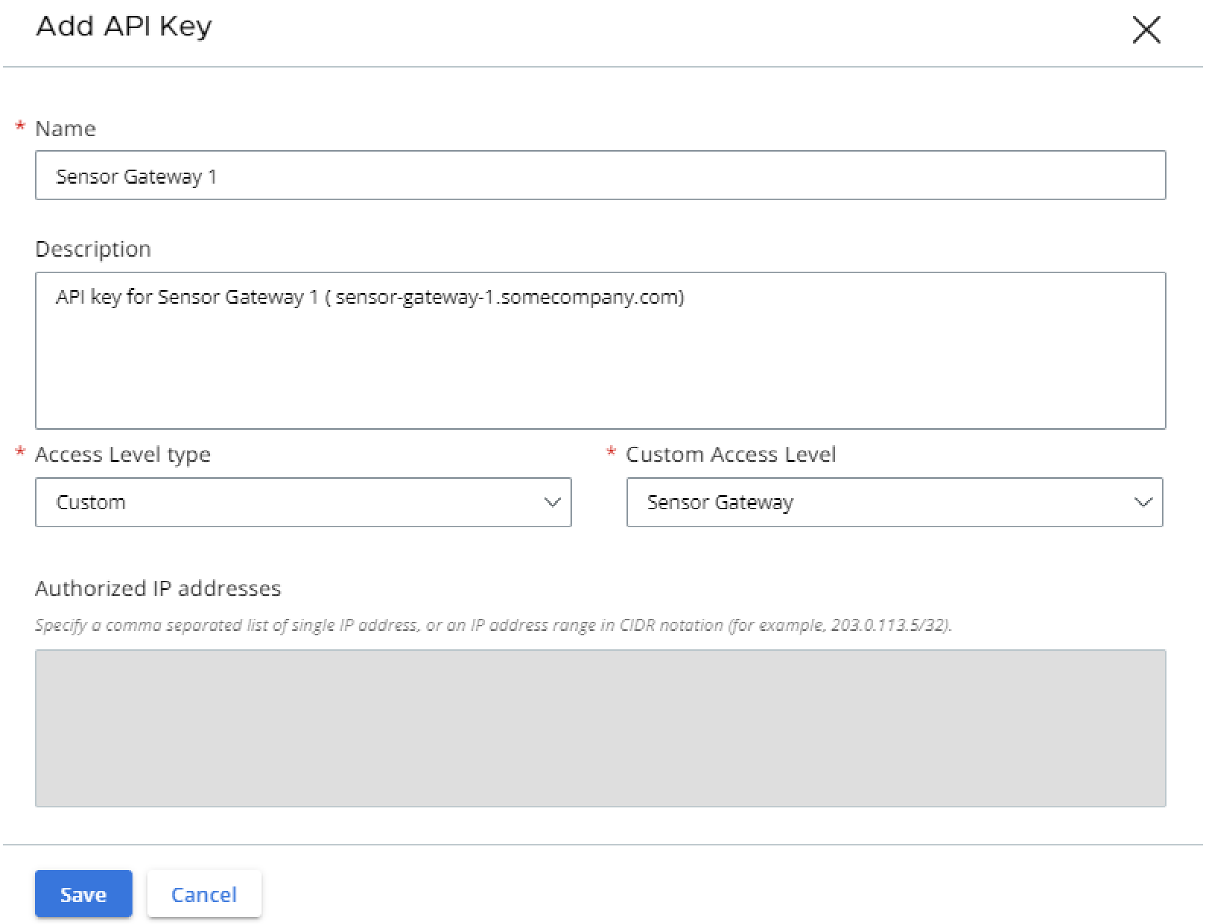
Procedure

1. Log in to the Carbon Black Cloud console.
2. Go to the **Settings** > **API Access** > **API Keys** page.
3. Click **Add API Key**.

   The **Add API Key** window displays.
4. Enter a name for your Sensor Gateway API key.

   The name must be unique for your organization.
5. Select **Custom** from the **Access Level type** drop-down menu.

6 Select **Sensor Gateway** from the **Custom Access Level** drop-down menu.



Add API Key

* Name

Sensor Gateway 1

Description

API key for Sensor Gateway 1 (sensor-gateway-1.somecompany.com)

* Access Level type

Custom

* Custom Access Level

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).

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

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

8 Copy the credentials.

You use these keys later 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. Once 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 later, or generate new API secret key, perform the following steps.

   a Go to the **Settings > API Access > API Keys** page.

   b Go to the Sensor Gateway API name created earlier and 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 Access

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

To further configure your firewall and grant access to additional URLs, see Configure a Firewall.

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`	`prd1ew2-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.company.com`, when you open it up in a browser or when the Carbon Black sensor tries to talk to 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 talks to the Sensor Gateway at the *https://sensorgateway.company.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 your Sensor Gateway entry point with an IP address. In that way, 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 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, which has this same IP address. That way, 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. For example, the KeyCDN Tools. 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 any editor of your choice and copy all the content along with `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.

  If your certificate has the chain already, you might want to 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 entire content and paste it in an editor of your choice.

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

4 Save it as the `sgw_chain.pem` file.

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`

      Prints out 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>`*

      Prints out 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, you might check the network connectivity/firewall configuration to ensure that the OCSP response is received from the OCSP responder.

Install Sensor Gateway as an Appliance

You 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 select between installing an OVA file or an OVF file.

Alternatively to the procedure below, to deploy the Sensor Gateway appliance directly on the ESXi host, log in to the ESXi Web Client interface (`https://`*`ESXi_host_IP_address_or_hostname`*), right-click **Virtual Machines**, and select **Create/Register VM**. Once you select **Deploy a virtual machine from an OVF or OVA file**, you can proceed with the installation wizard by referring to step 4 and onwards.

Prerequisites

- Verify that you have available the API access credentials. For details, see Provision Sensor Gateway API Key.
- Verify that your environment is configured with the necessary network settings. For details, 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 your vCenter Server instance: **`https://`** ***`vcenter_server_ip_address_or_fqdn`***

   b If a warning message about a potential security risk appears, select to continue to the website.

Browser	**Action**
Microsoft Edge	1 Click **Details**. 2 Under the message that appears, click **Go on to the webpage**.
Mozilla Firefox	1 Click **Advanced**. 2 Under the message that appears, click **Accept the risk and continue**.
Google Chrome	1 Click **Advanced**. 2 Under the message that appears, click **Proceed to** ***vcenter_server_ip_address_or_fqdn***.

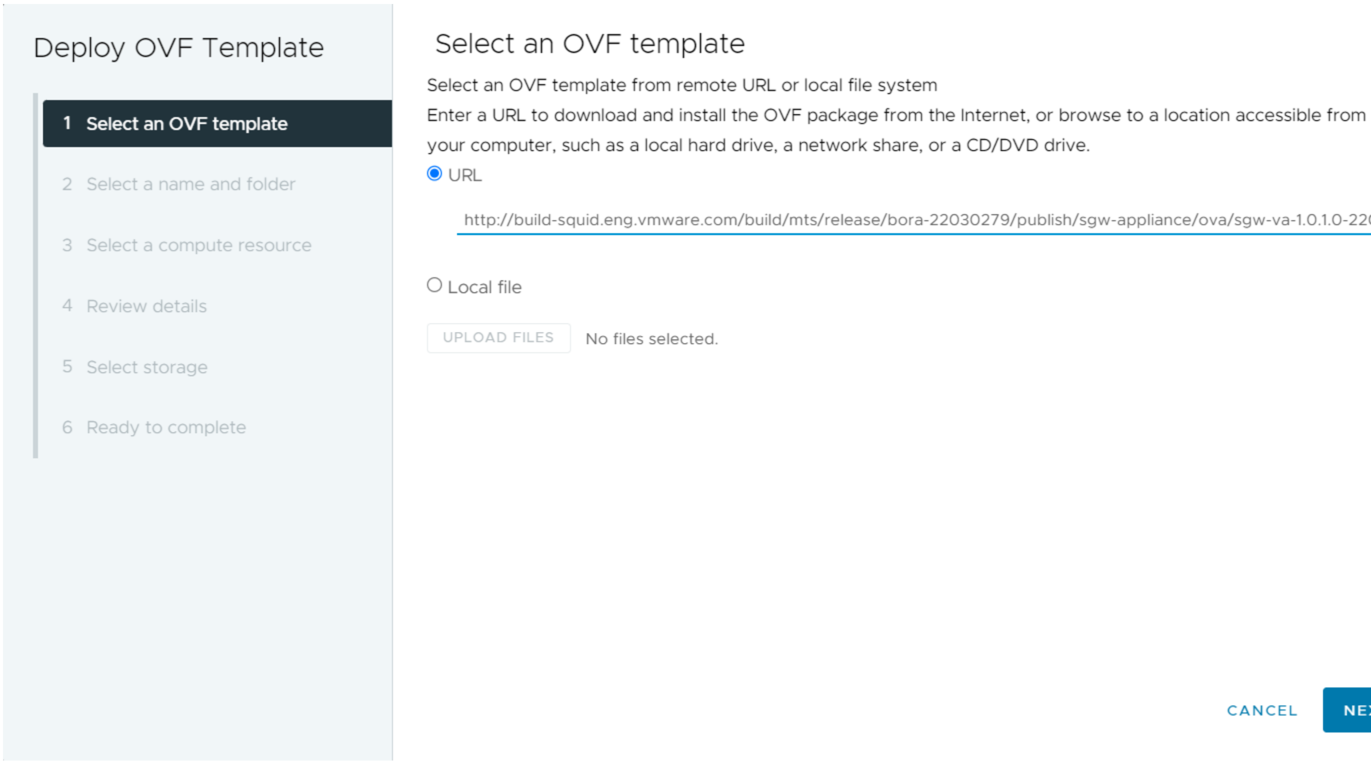
   c On the vSphere Welcome page, select **Launch vSphere Client (HTML5)**.

   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, and you can view and manage the vSphere inventory.

2 To retrieve the Sensor Gateway appliance installer `sgw-va-1.2.0.0-22635557_OVF10.ova`, go to the Customer Connect Download page and click **Download Now** under CBC-CWP-SensorGateway-OVA-122.

3 Navigate to a cluster within your data center, right-click on an ESXi host, and select **Deploy OVF Template**.



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

● URL

http://build-squid.eng.vmware.com/build/mts/release/bora-22030279/publish/sgw-appliance/ova/sgw-va-1.0.1.0-22

○ Local file

UPLOAD FILES No files selected.

The **Deploy OVF Template** wizard displays.

4 Select a template by either of the following options 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 On the next page, select the compute resource you want 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, then select **Next**.

9 Select a virtual disk format and storage location.

Virtual Disk Format	Advantages	Disadvantages
Thin Provisioned	■ Fastest to provision ■ Allows disk space to be over-committed to VMs	■ Slowest performance due to metadata allocation overhead and additional overhead during initial write operations ■ Over-commitment of storage can lead to application disruption or downtime if resources are actually used ■ Does not support clustering features
Thick Provisioned Lazy Zeroed	■ Faster to provision than Thick Provisioned Eager Zeroed ■ Better performance than Thin Provisioned	■ Slightly slower to provision than Thin Provisioned ■ Slower performance than Thick Provisioned Eager Zero ■ Does not support clustering features
Thick Provisioned Eager Zeroed	■ Best performance ■ Overwriting allocated disk space with zeros reduces possible security risks ■ Supports clustering features such as Microsoft Cluster Server (MSCS) and VMware Fault Tolerance	Longest time to provision

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

You can keep the default.

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 CBC URL that represents the environment where your services are hosted. Carbon Black Cloud is hosted in several regions and the URL might be different. For a list of Carbon Black Cloud environments, see Carbon Black Cloud Access.	`https://defense-prod05.conferdeploy.net` **Note** Ensure that the value begins with `https://`
`API ID`	To allow authenticated communication between a	`9Z5QY2ZDAN`

Option	Action	Example
`API Secret Key`	Sensor Gateway and the Carbon Black Cloud, enter the Carbon Black Cloud API ID and API Secret Key. You generate them in pairs by using the Carbon Black Cloud console. If there is a mismatch, Carbon Black Cloud rejects any communication coming from the Sensor Gateway. **Note** Due to the use of sensitive data, the vSphere Client prompts for a confirmation twice and hides the value in the UI.	`8UE3SHE470T2LZLJZJ2M98TY` **Important** You must generate a new API ID and API Secret Key for every Sensor Gateway instance.
`Sensor Gateway Entry Point (https://<sensor-gateway-node-fqdn>)`	To define how the sensors address the Sensor Gateway, enter a Sensor Gateway entry point. The entry point must match the following: ■ 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. ■ The IP address or the FQDN of the machine must be the same as the CN of the certificate.	`https://sensorgateway.company.com` This example assumes that the CN of the certificate is `sensorgateway.company.com` **Note** Since the Sensor Gateway hosts its services by using SSL, ensure the value begins with `https://`
`Sensor Gateway Certificate`	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.	
`Sensor Gateway Certificate Private Key`	Paste the content, including BEGIN and END lines, of the Sensor Gateway certificate private key file in the **Password** field. **Note** Due to the use of sensitive data, the vSphere Client prompts for a confirmation twice and hides the value in the UI.	
`Sensor Gateway Certificate Chain`	Paste the content, including BEGIN and END lines, of the Sensor Gateway certificate chain file.	

Option	Action	Example
`Sensor Gateway Certificate Passphrase`	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. **Note** Due to the use of sensitive data, the vSphere Client prompts for a confirmation twice and hides the value in the UI.	
`Proxy Type`	To have the Sensor Gateway communicate over a proxy, select the proxy type. ■ By default, None ■ HTTP or HTTPS. For each, choose one of the following options: ■ Proxy Host: Provide the FQDN or IP address of the Proxy Host ■ Proxy Port: Provide the port where the Proxy server receives requests If you select HTTPS as your proxy type, you must include HTTPS Proxy Certificate.	
`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`	If you selected HTTPS as the proxy type, paste the entire content of the HTTPS proxy certificate file. To avoid updating the HTTPS proxy certificate,Carbon Black recommends that you include the issuer of the certificate.	

Option	Action	Example
`Default Gateway`	Optional. Set the default gateway for this virtual machine.	Although input is optional, to have a static DNS and static IP allocated to the Sensor Gateway, you must populate these fields. If you leave them blank, the Sensor Gateway aquires 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.	

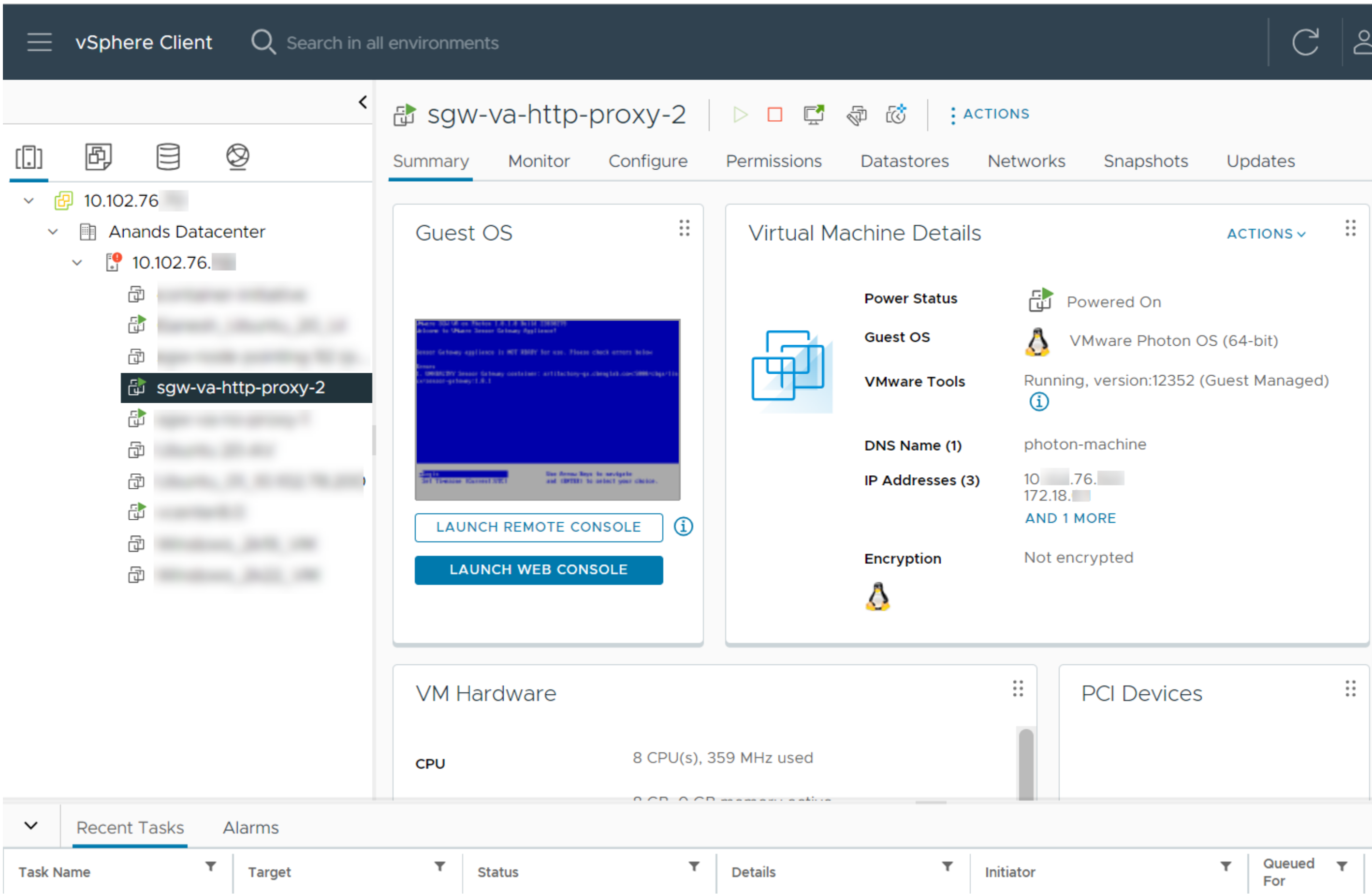
12. Review your configuration setup and click **Finish**.

Results

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

What to do next

Once the Sensor Gateway virtual machine is imported and deployed, you can power it on. It takes some time for the operation to complete.



Power Status: Powered On

Guest OS: VMware Photon OS (64-bit)

VMware Tools: Running, version:12352 (Guest Managed)

DNS Name (1): photon-machine

IP Addresses (3): 10.[redacted].76.[redacted]
172.18.[redacted]
AND 1 MORE

Encryption: Not encrypted

CPU: 8 CPU(s), 359 MHz used

After the appliance boots up, if you configured the Sensor Gateway virtual machine successfully, you can see it registered with the Carbon Black Cloud console under the **Settings > API Access > Sensor Gateway** tab.

If the appliance deployment ends with a failure, use the SGW configurator tool to re-enter the settings and restart the appliance. For details, see Reconfigure the Sensor Gateway Appliance.

Reconfigure the Sensor Gateway Appliance

To update the initial configuration you set during the Sensor Gateway OVA installation, use the Sensor Gateway (SGW) Configurator tool.

As a system administrator, you use the tool to update any appliance settings you previously specified and restart the Sensor Gateway to apply the new configuration. Carbon Black recommends that you use the configurator tool if the Sensor Gateway deployment fails.

There are settings in the SGW configurator tool, which have dependencies. When changing such a field, you must update its dependent fields as well. The following table lists the fields you can update with the configurator and their dependencies if any.

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 - there is an existing CBC 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` When proxy type is set to HTTPS.	-
`Proxy Port`	None	-

Procedure

1 Log in to the Sensor Gateway appliance as an admin user.

2 Run the configurator command.

```
$ configure-sgw
```

The SGW Configurator terminal UI appears. You can navigate through the configurator options by using the keyboard arrows or the letters in the square brackets.

3 Update either of 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 with suggestion for a valid input. If you enter a valid URL, a success message displays.

4 To return to the main menu, select **Back**.

5 Optional. Repeat step 3 to update any of the required values.

6 To keep your changes, select **Save and Quit**.

7 Review the updated values and confirm your changes.

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 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 it has been compromised, and avoid getting the sensors permanently disconnected from the Carbon Black Cloud.

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 inidividually.

Important Virtual machines that are shut down might not receive the new certificate. The sensors are not able to 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, ensure 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. Navigate to 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** drop-down 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 this 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 Cloud confirming if it has successfully accepted the new certificate. The Carbon Black Cloud console displays only the errors received by the sensors.

5. To see errors reported by the connected to the Sensor Gateway sensors, navigate to the **Inventory > VM Workloads > Enabled** tab.

   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 might fix existing errors by uploading the new certificate again.

      If the errors are still present, contact Carbon Black Cloud 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.

6. Replace the TLS certificate of the Sensor Gateway deployed as an OVA.

   a. Log in to the Sensor Gateway appliance as an admin user.

   b. Run the configurator command.

      ```
      $ configure-sgw
      ```

      The SGW Configurator terminal UI displays.

   c. Select **TLS Settings > Sensor Gateway > Sensor Gateway Certificate**.

   d. When promted, paste the content of the new certificate, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines, and press `Ctrl+D` twice.

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

   e. To keep your changes, select **Save and Quit**.

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

Results

It takes up to five minutes for the Sensor Gateway to register again 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. Follow this procedure to update the proxy certificate when it is about to expire or it has been compromised.

You use the SGW Configurator tool to update the proxy certificate. For details on how to use the tool, see Reconfigure the Sensor Gateway Appliance.

Prerequisites

Ensure that you can provide either 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 appliance as an admin user.
3. Run the configurator command.

   ```
   $ configure-sgw
   ```

   The SGW Configurator terminal UI appears. You can navigate through the configurator options by using the keyboard arrows or the letters in the square brackets.
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 wrong content, you get an error such as `ERROR: You've entered invalid value. Please enter a valid X509 certificate`.
6. To keep your changes, select **Save and Quit**.
7. Review the updated values and confirm your changes.

Results

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

Installing Carbon Black Cloud Sensors

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

Set Up Your Environment for Sensor Installation

Consider the following environment setup before installing a Carbon Black sensor.

- Locate a Sensor Gateway Instance

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

- Generate a Company Code

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

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 with your account credentials.

2 On the left navigation bar, select **Settings > API Access > Sensor Gateways**.

3 Find the Name of the Sensor Gateway corresponding to the IP address or the API ID.

4 Note this name as you need it when generating the company code.

Generate a Company Code

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

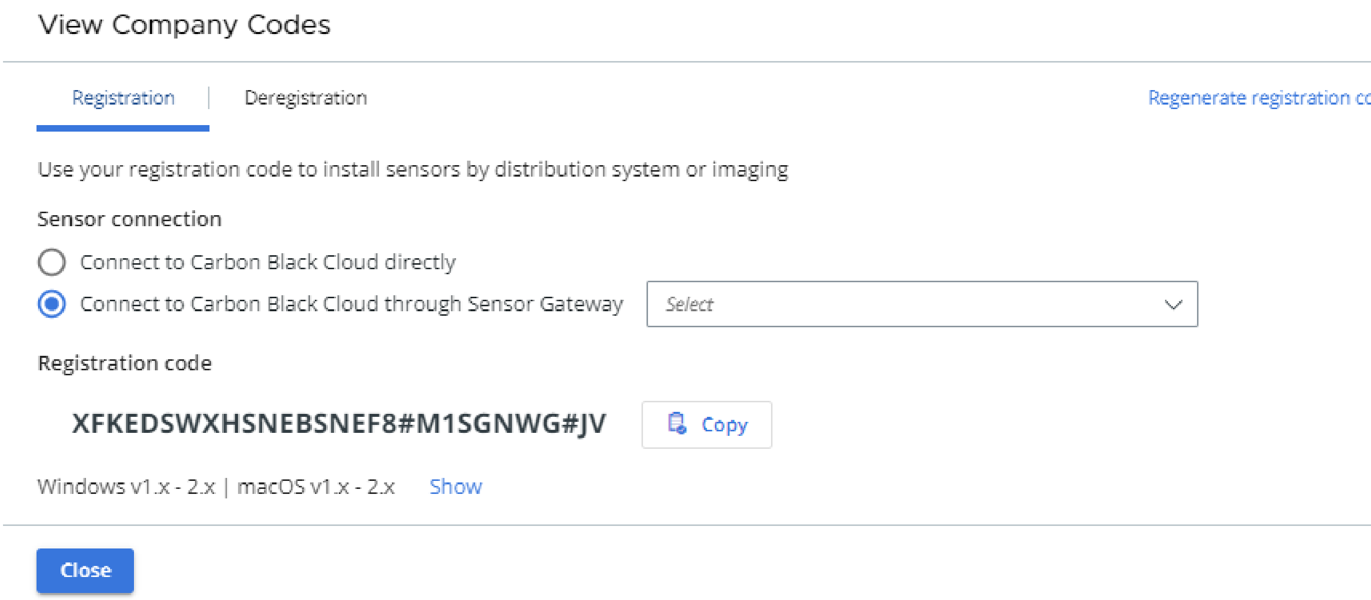
Procedure

1 On the left navigation bar, select **Inventory > VM Workloads**.

2 Select **View company codes** from the **Sensor Options** drop-down menu.

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

   The Sensor Gateway drop-down menu becomes available.



View Company Codes

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

Registration code

XFKEDSWXHSNEBSNEF8#M1SGNWG#JV

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

4 Select the Sensor Gateway entry point URL you want to use for the sensor installation.

   The drop-down menu displays only the URLs for the connected Sensor Gateways.

5. Copy the Registration code.

   This is the company code you use when installing the sensors.

Install Carbon Black Cloud Sensor for Linux

To have the Carbon Black sensor on your Linux VM workload communicating 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 sensor for Linux version (2.15+).
- For information on using the Carbon Black Cloud console to install sensors on VM workloads, see *VMware Carbon Black Cloud Sensor Installation Guide*. If you install the sensor through the console UI, include the `UseSystemCerts=true` property in the `/var/opt/carbonblack/psc/cfg.ini` file. For details, see Installing Linux Sensors on Endpoints.
- Ensure that you have the company code available. For more information, see Generate a Company Code.

Procedure

1. Download the latest version of the Carbon Black sensor for Linux.
2. Omit if the Sensor Gateway is already configured with CA-signed certificate. To use a self-signed certificate in the Sensor Gateway, you must add the certificate chain into the trust store.

   a. Copy the certificate `sgw_certificate.pem` file, which you intend to use for communication with the Sensor Gateway, into a known location on 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, you must confirm in the documentation of your distro to select the Trusted CA certs file.
3. Retrieve the sensor installation file by running the command:

   ```
   wget <location of the sensor installation file>
   ```
4. Unzip the sensor installation file:

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

5 Use the company code you previously generated 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 to select the Trusted CA certs file.

Results

Once your sensor is successfully installed, you can see the running Sensor Gateway in the Carbon Black Cloud console.

What to do next

If needed, you can uninstall the sensor from your Linux workload by running the command:

```
dpkg --purge cb-psc-sensor
```

Install Carbon Black Sensor for Windows

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.

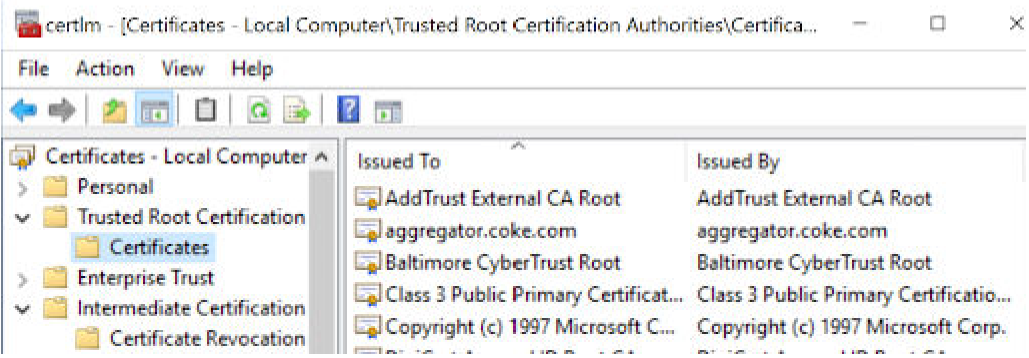
Prerequisites

- 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 *VMware Carbon Black Cloud Sensor Installation Guide*.
- Ensure that you have the company code available. For more information, see Generate a Company Code.
- If you install the Carbon Black sensor in a Sensor Gateway environment configured with 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 *VMware 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



certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certifica...
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
Certificate Revocation

Issued To	Issued By
AddTrust External CA Root	AddTrust External CA Root
aggregator.coke.com	aggregator.coke.com
Baltimore CyberTrust Root	Baltimore CyberTrust Root
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.

2 Download the sensor installer.

3 Install the sensor by using the Carbon Black Cloud console or by existing scripts.

4 Use the company code you previously generated to complete the sensor installation.

Once your sensor is successfully installed, you can see the running Sensor Gateway in the Carbon Black Cloud console.

Manage Connectivity to Carbon Black Cloud

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

Prerequisites

Verify that you have installed Carbon Black sensor for Windows 3.9+

Procedure

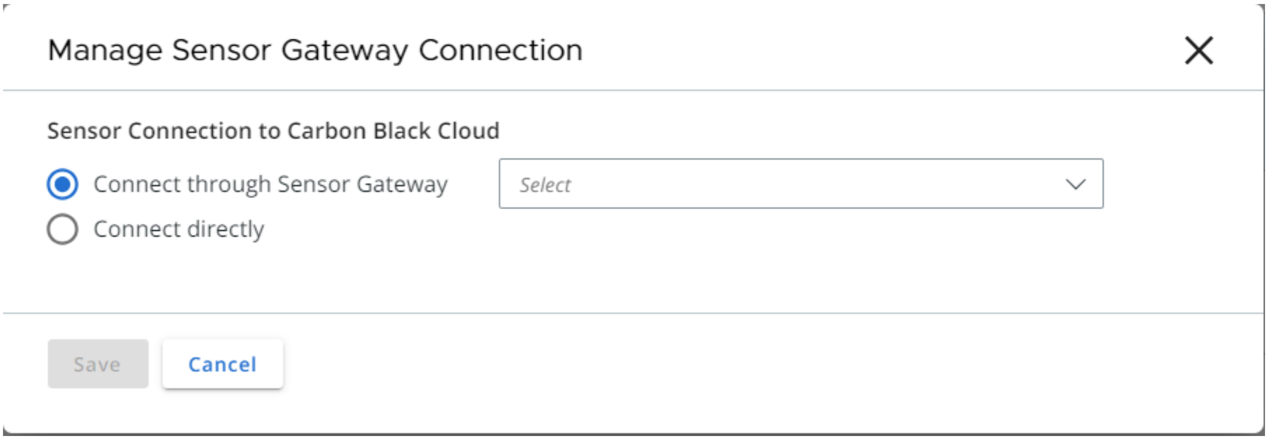
1 Log in to the Carbon Black Cloud console.

2 On the left navigation pane, click **Inventory > VM Workloads** or **Inventory > Endpoints** and select the **Enabled** tab.

3 Locate the Status column and select the check box for one or more VM workloads or Endpoints you want to take action upon.

The **Take Action** drop-down menu appears.

4 Select **Manage Sensor Gateway connection**.



Manage Sensor Gateway Connection

Sensor Connection to Carbon Black Cloud

● Connect through Sensor Gateway   Select

○ Connect directly

The **Manage Sensor Gateway Connection** window displays.

5 Perform one of the following.

- To assign a Sensor Gateway, click the **Connect through Sensor Gateway** drop-down 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, to have the sensor communicate directly to Carbon Black Cloud, select **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 use the Carbon Black Cloud console to subscribe to Sensor Gateway failure 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 for Sensor Gateway Notifications

Use the following procedure to receive in-product and email notificaitons on the state of your registered Sensor Gateway instances.

Procedure

1. While on the **Settings > Notifications** page, select the **Integrations** tab.
2. Click **Add Notification**.
3. Provide a name for the notification and select Sensor Gateway from the **Component type** drop-down menu.
4. Choose when you want to be notified - when the Sensor Gateway is disconnected, when the maximum number of 10,000 Carbon Black sensors is exceeded, or when the Sensor Gateway certificate is about to expire, or all of them.
5. Add all the users you would like to receive the notifications through an email from the related drop-down menu.

   You define these users in the **Settings > Users** page.
6. Optional. To receive a notification at the end of the day with a summary of all gateways that are still unresolved in your environment, click the **Send 1 reminder email at the end of the day** option.

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

Upgrade Your Sensor Gateway Appliance

You upgrade your Sensor Gateway appliance with the latest version available by using the Carbon Black Cloud console.

Note

- Make sure you do not power down your Sensor Gateway appliance while the upgrade is in progress. Otherwise, you might have to reinstall the Sensor Gateway.
- Sensors connected to the Sensor Gateway you are about to upgrade might loose 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 decide to revert to a previous version of the Sensor Gateway.

Procedure

1. Log in to the Carbon Black Cloud console.
2. Navigate to the **Settings > API Access > Sensor Gateways** tab.

3 Double-click the Sensor Gateway you wish to upgrade.

   The Sensor Gateway Details pane displays the current version of the Sensor Gateway and the newly available version in parentheses.

4 Click the **Options** drop-down menu and select **Upgrade version**.

   The **Upgrade Sensor Gateway** window displays.

5 To confirm the upgrade, select **Upgrade**.

Results

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

What to do next

Navigate to the **Settings > Audit Log** page where you can view the status of the upgarde. For example, when it started and if it is successful.

Troubleshooting Sensor Gateway

Use the troubleshooting topics to find solutions for situations when installing, using and upgrading the Sensor Gateway does not work as expected.

Sensor Gateway Appliance is Unreachable

Problem

You might expereince a communication issue with the Carbon Black Sensor Gateway appliance.

Cause

The virtual machine is powered off.

Solution

Power on the virtual machine and wait for it to enter in 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.

In the process of installing the Sensor Gateway appliance, ensure 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. For more information, see Sensor Gateway Certificates.

Installing Sensor Gateway on Linux

Use the following procedures to set up your 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 HA capabilities are going to be deprecated soon.

Set Up Your Environment for Sensor Gateway Installation

To set up each of your Linux servers 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. For more information, see Sensor Gateway Certificates.
  - Self-signed certificate. This certificate requires pushing these certificates into the trust store of each sensor workload. For more information, see Sensor Gateway Certificates.

  Note You need the private key for the certificate you are using.
- 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. For more information, see Create a Certificate Chain File.
- Acquire a Static IP for each Sensor Gateway server.
- Reserve a DNS entry. For example, `sensorgateway.`*`company`*`.com`

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

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

  Note You can use just an IP and create the certificates with the IP 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, it might need to reach out to CA providers to get Online Certificate Status Protocol (OCSP) responses for the validity of its digital certificate.

- To have the Sensor Gateway running behind a proxy, ensure you configure the Docker client to use proxy. For more information, 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, you must ensure that the Carbon Black Cloud URLs are accessible through the proxy. If you set up mirrors for the Update servers, verify that they are reachable through the proxy as well.
- Verify that your environment is configured with the necessary network settings. For details, 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 server as root and ensure OpenSSL is installed.

   If not already, install OpenSSL using a system package manager.

2. Prepare the certificates.

   a. Name the SSL Certificate file as `sgw_certificate.pem`.

   b. Name the SSL Certificate Private Key file as `sgw_key.pem`.

   c. (Omit this step if you are using a self-signed certificate.) Name the SSL Certificate Chain file as `sgw_chain.pem`.

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

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

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

   e. Create `/data` folder at the root level and make the following subfolders on your 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 in the `/data/certs` directory.

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

3. Download the script, which installs and sets up the Sensor Gateway on each server individually.

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

4. Unzip the Sensor Gateway installation zip file in the location where you downloaded it. 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.

For details, see Provision Sensor Gateway API Key.

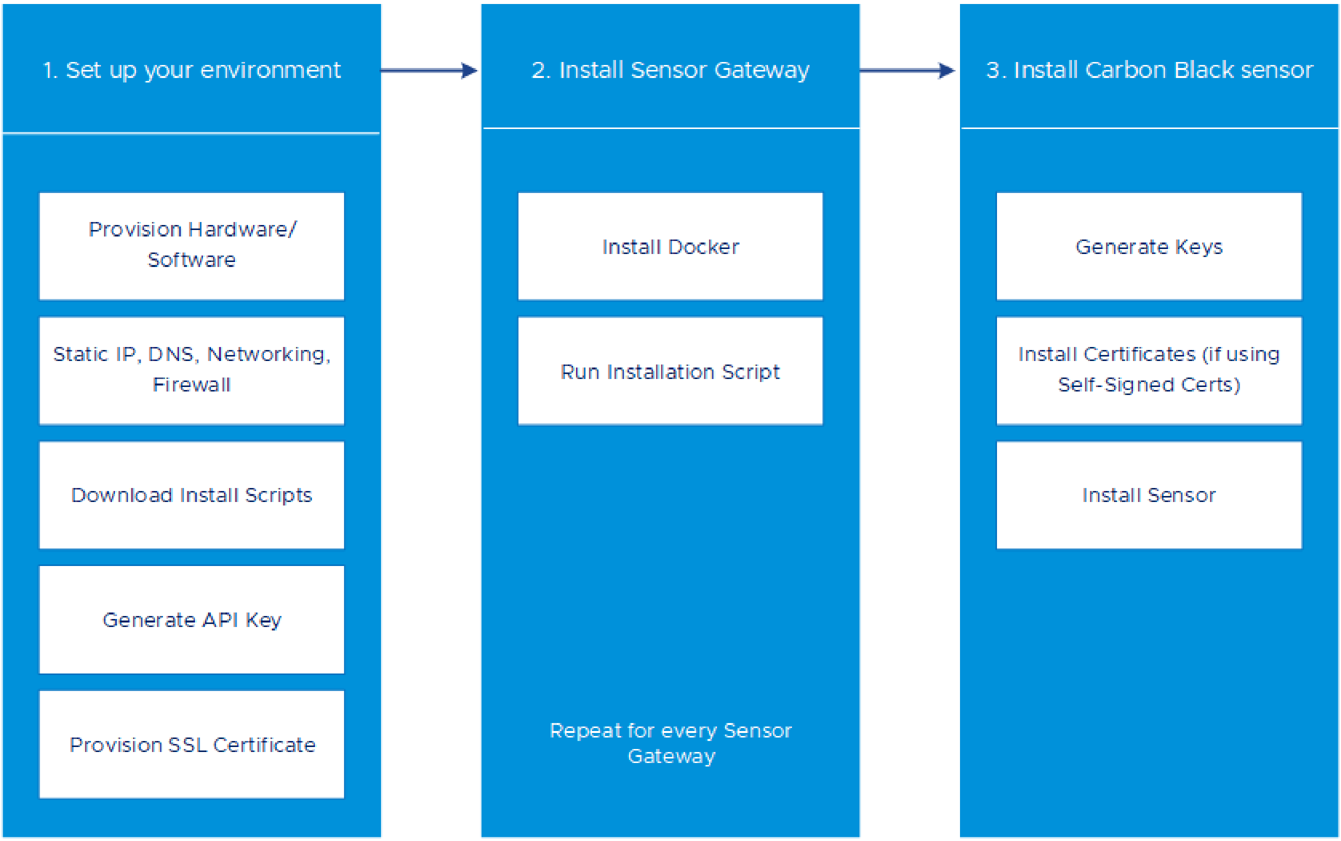
What to do next

Install the Sensor Gateway.

Install Sensor Gateway on a Linux Server

You host the Sensor Gateway on a Linux machine as a container image. Therefore, the Linux server must have a container running capability. In this type of installation, if you want to install more than one Sensor Gateway servers, you must repeat the following steps for every Sensor Gateway server.

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


1. Set up your environment
Provision Hardware/ Software
Static IP, DNS, Networking, Firewall
Download Install Scripts
Generate API Key
Provision SSL Certificate
2. Install Sensor Gateway
Install Docker
Run Installation Script
Repeat for every Sensor Gateway
3. Install Carbon Black sensor
Generate Keys
Install Certificates (if using Self-Signed Certs)
Install Sensor

Prerequisites

- Verify that port 443 is open on the Sensor Gateway.
- To have the Sensor Gateway running behind a proxy, ensure you configure the Docker client to use proxy. For more information, see Configure Docker to use a proxy server.

Procedure

1 Install Docker.

For information about installing a Docker engine on the supported by the Sensor Gateway Linux distributions, see Install Docker Engine on CentOS, Install Docker Engine on RHEL, or Install Docker Engine on Ubuntu.

2 Make the installation script executable if not so already.

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

3 Run the installation script.

```
./sensor_gw_install.sh
```

4 When prompted, provide the following input.

Option	Description	Example
API ID	The API ID and API Secret Key generated on the Carbon Black Cloud console allow an authenticated communication between the Sensor Gateway and the Carbon Black Cloud. Both the API ID and API Secret Key are generated in pair. Any mismatch and the Carbon Black Cloud rejects any communication coming from the Sensor Gateway. **Note** You must generate new API ID and API Secret Key for every Sensor Gateway.	9Z5QY2ZDAN
API Secret Key		8UE3SHE475T2LZLJNJ2M98TK
Carbon Black Cloud URL	This URL represents the environment where your services are hosted. Carbon Black Cloud is hosted in several regions and the URL might be different. For a list of Carbon Black Cloud environments, see Carbon Black Cloud Access.	`https://defense-prod05.conferdeploy.net` **Note** Ensure the value begins with a `https://`
Sensor Gateway entry point URL (https://<sensor-gateway-node-fqdn>)	An entry point means how the sensors would typically address the Sensor Gateway as. This must match the following: ■ If you use a CA-signed or self-signed certificate, this value should be the same as the CN given to the certificate. ■ The IP address or the FQDN of the machine must be the same as the CN of the certificate.	https://sensorgateway.*company*.com This example assumes that the CN of the certificate is `sensorgateway.company.com` **Note** Since the Sensor Gateway services are hosted using SSL, ensure the value begins with `https://`

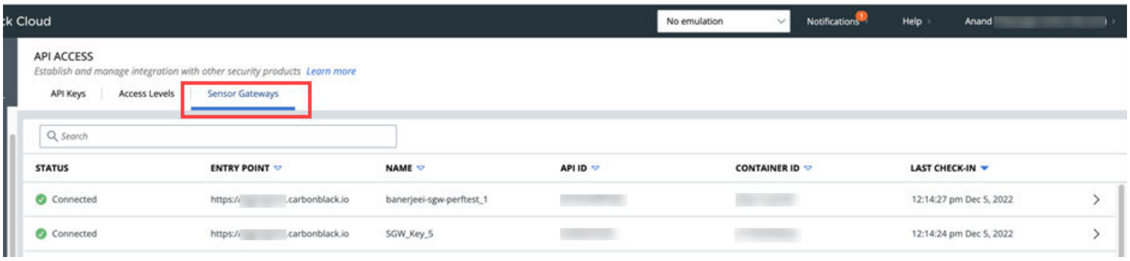
Option	Description	Example
Proxy type	- None: This is the default option. - HTTPS or HTTP: For each choose one of the following options: - Proxy Host: Provide the FQDN or IP address of the Proxy Host. - Proxy Port: Provide the port where the Proxy server receives requests.	HTTP
Optional: Volume mount directory	The Sensor Gateway uses a fixed directory to look for certificates and to store logs. If you do not provide a value, the default location is a `/data` directory. If you choose to store your certificates or logs in a different directory, you can provide an absolute path here. If you choose to have a different folder, ensure you create certs and logs folder underneath this path. At the same time you must ensure the certificate, private key, and certificate chain (optional) are stored in the certs folder before you proceed on the next parameter. Since the install script executes with root permissions, by default all these directories will have root permissions as owner and group.	`/data`
Optional: Port where Sensor Gateway runs	By default the Sensor Gateway services are hosted over SSL on port 443. If this port is in use for any reason on the machine where you are installing the Sensor Gateway, you can use a different port.	By default, Sensor Gateway runs on port 443.
Optional: Certificate private key's passphrase	As a recommendation, at the time of certificate generation provide a password to protect the private key. When prompted during the Sensor Gateway install provide the same password. The Sensor Gateway uses the same password to use the certificate and encrypt the communication between the sensor and itself.	Provide a password if your `sgw_key.pem` is password-protected.

The Sensor Gateway service starts and registers itself with the Carbon Black Cloud. It takes few minutes for the registration to complete.

Results

Once the registration completes successfully, 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.



STATUS	ENTRY POINT	NAME	API ID	CONTAINER ID	LAST CHECK-IN
Connected	https://[redacted].carbonblack.io	banerjeei-sgw-perftest_1	[redacted]	[redacted]	12:14:27 pm Dec 5, 2022
Connected	https://[redacted].carbonblack.io	SGW_Key_5	[redacted]	[redacted]	12:14:24 pm Dec 5, 2022

What to do next

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

Update Sensor Gateway Certificate

You can update the SSL certificate on a Linux Sensor Gateway when the certificate is about to expire, or it has been compromised, and avoid getting the sensors 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 inidividually.

Important Virtual machines that are shut down might not receive the new certificate. The sensors are not able to 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, ensure 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 Navigate to the **Settings > API Access > Sensor Gateways** tab and double-click the Sensor Gateway for which you must renew the certificate.

3 In the Sensor Gateway Details section, select the **Options** drop-down 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 this 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 Cloud confirming if it has successfully accepted the new certificate. The Carbon Black Cloud console displays only the errors received by the sensors.

5. To see errors reported by the connected to the Sensor Gateway sensors, navigate to the **Inventory > VM Workloads > Enabled** tab.

   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 might fix existing errors by uploading the new certificate again.

      If the errors are still present, contact Carbon Black Cloud 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.

6. 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 register again with the Carbon Black Cloud.

Upgrade Your Linux Sensor Gateway

You upgrade your Sensor Gateway by running a dedicated upgrade script.

Note Upgrade of the Sensor Gateway does not enable proxy support. To have your Sensor Gateway environment configured with proxy, you must re-install the Sensor Gateway.

Prerequisites

- Ensure you have the following information available from your initial Sensor Gateway installation.
  - The Sensor Gateway Entry point. Use the same name as before. If not, the existing sensors can stop working.
  - API ID
  - API Key
- The following Carbon Black sensor versions are supported with the Sensor Gateway.
  - Carbon Black sensor for Windows 3.8.0.684+
  - Carbon Black sensor for Linux 2.13.2.997598+
- Ensure the old version of the Sensor Gateway is running and has an 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 with root credentials.

b To get the running instance of the Sensor Gateway, excecute the 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 and thus, see the Sensor Gateway instance as exited under the `Status` column, run the 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, which is 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 might not have been successful. Please, do not proceed with the next step and contact 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
```

Prompts you for the same data as during the initial Sensor Gateway install. For more information, see Install Sensor Gateway on a Linux Server.

Results

Your Sensor Gateway upgrades successfully.