VMware Carbon Black Cloud Workload Guide

29 Oct 2020

VMware Carbon Black Cloud Workload 1.0

vmware®

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

Copyright © 2020 VMware, Inc. All rights reserved. Copyright and trademark information.

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

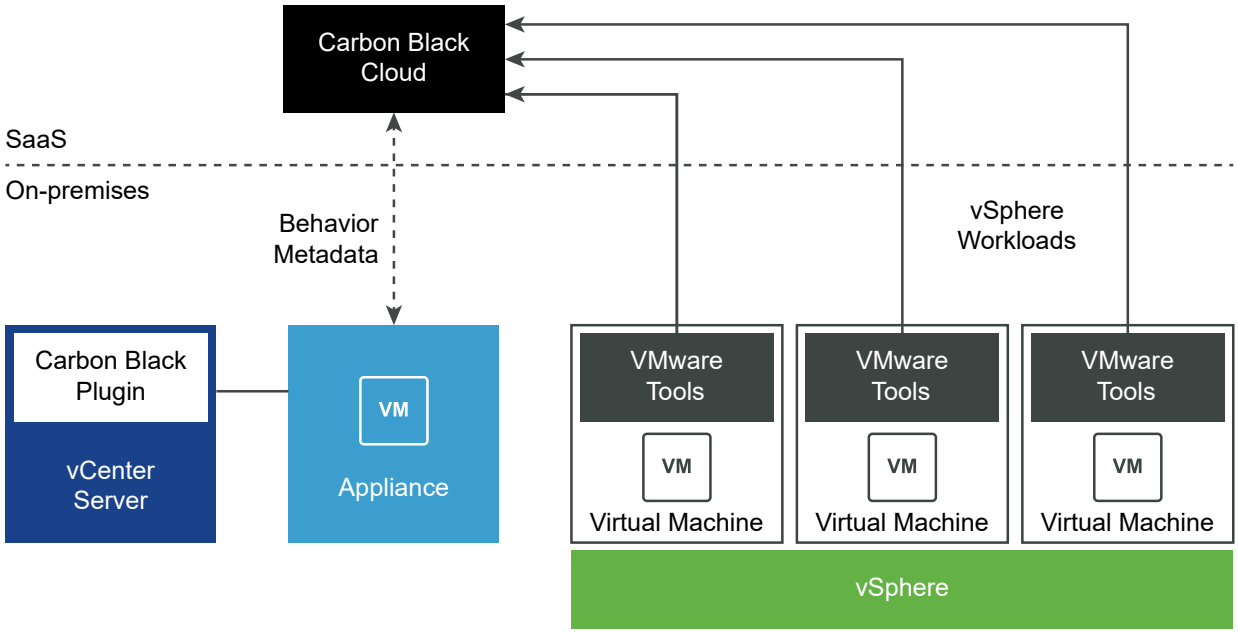
The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. This manual assumes familiarity with VMware vSphere®, including VMware ESXi™, VMware vCenter Server®, and VMware Tools™.

Carbon Black Cloud Workload Overview

1

Carbon Black Cloud Workload is a data center security product that protects your workloads running in a virtualized environment. Carbon Black Cloud Workload ensures that security is intrinsic to the virtualization environment by providing 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 now 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.

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



You must first deploy an on-premises OVF/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

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.

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.

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/.

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.

This chapter includes the following topics:

System Requirements

Before you install or upgrade Carbon Black Cloud Workload Plug-in, consider your network configuration and resources. You can install one Carbon Black Cloud Workload appliance per vCenter Server.

Product/Component	Supported Version
VMware vCenter Server	6.7 U1, 6.7 U2, 6.7 U3, 7.0, 7.0 U1
VMware ESXi	6.5 U3, 6.7 U1, 6.7 U2, 6.7 U3, 7.0, 7.0 U1
VMware Tools for Windows Operating System (OS)	11.2 or later **Important** Virtual machines in your vCenter Server inventory must have VMware Tools version 11.2 or later.
Open VM Tools (*open-vm-tools*) for Linux OS	10.3.2 or later
Windows Guest OS	Only 64-bit architecture is supported. ■ Windows Server 2008 R2 Service Pack 1 (SP1) x64 ■ Windows Server 2012 x64 ■ Windows Server 2012 R2 x64 ■ Windows Server 2016 x64 ■ Windows Server 2019 x64 ■ Windows 7 SP1 x64 ■ Windows 8 x64 ■ Windows 8.1 x64 ■ Windows 10 x64

Product/Component	Supported Version
Linux Guest OS	■ RHEL 6: 6.1–6.10 ■ RHEL 7: 7.0–7.8 ■ RHEL 8: 8.0–8.2 ■ CentOS 6: 6.1–6.10 ■ CentOS 7: 7.0–7.8 ■ CentOS 8: 8.0–8.1 ■ Oracle 6: 6.1–6.10 ■ Oracle 7: 7.0–7.8 ■ Oracle 8: 8.0–8.2 ■ SUSE 12: 12.2–12.5 ■ SUSE 15: 15.0–15.1 ■ OpenSUSE 15: 15.0–15.2 ■ OpenSUSE 42: 42.2–42.3 ■ Ubuntu 16: 16.04 LTS ■ Ubuntu 18: 18.04 LTS, 18.10 ■ Ubuntu 19: 19.04 LTS, 19.10 ■ Ubuntu 20: 20.04 LTS ■ Amazon Linux 2
Vulnerability Assessment support for Windows OS	■ Windows Server 2008 R2 Service Pack 1 (SP1) x64 ■ Windows Server 2012 x64 ■ Windows Server 2012 R2 x64 ■ Windows Server 2016 x64 ■ Windows Server 2019 x64
Vulnerability Assessment support for Linux OS	■ RHEL 6: 6.1–6.10 ■ RHEL 7: 7.0–7.8 ■ CentOS 6: 6.1–6.10 ■ CentOS 7: 7.0–7.8 ■ SUSE 12: 12.2–12.5 ■ SUSE 15: 15.0–15.1 ■ Ubuntu 16: 16.04 LTS ■ Ubuntu 18: 18.04 LTS, 18.10 ■ Ubuntu 19: 19.04 LTS, 19.10 ■ Ubuntu 20: 20.04 LTS
Supported Browsers	vSphere Client supported web browsers
Carbon Black Sensor	■ Windows 3.6 or later ■ Linux 2.9 or later

For information about interoperability with VMware products, see VMware Product Interoperability Matrices.

For the Carbon Black version compatibility matrix, refer Carbon Black Cloud support matrix. You must first log in to the Carbon Black User Exchange page.

Hardware Requirements

Before you install or upgrade Carbon Black Cloud Workload, your system hardware must meet the following requirements. You can install one Carbon Black Cloud Workload appliance per vCenter Server.

Carbon Black Cloud Workload appliance	Requirements
Memory	4 GB
Storage	41 GB (thick provisioned)
vCPU	4 vCPU

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 My VMware portal.

   For information about creating a My VMware profile, see KB 2007005. For information about inviting a user to a My VMware account, see KB 2070555.

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

   Carbon Black Cloud Workload is listed under **Endpoint & Workload Security**.

3. 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`.

4. 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.

Connectivity with 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.

This chapter includes the following topics:

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.

Prerequisites

- You have verified the System Requirements.

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

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`. See Download the Installer for more information. ■ **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, 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: Register Carbon Black Cloud Workload Appliance With vCenter Server

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

Prerequisites

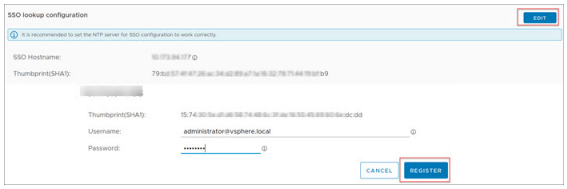
- You have deployed the Carbon Black Cloud Workload appliance.
- The Carbon Black Cloud Workload appliance VM is powered-on.

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 host name or IP address 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.
User name and Password	Enter the user name and password for the vCenter SSO administrator. To add a member to the vCenter SSO administrator group, refer to vSphere documentation.
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 vCenter Server is registered.

Results

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 to reflect the changes.

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.

Step 1C: Create the Carbon Black Cloud Workload Appliance Custom API Access Level

Create a custom API access level for the appliances in your organization. Creating an access level for your organization is a one-time task and is available only for the Carbon Black Cloud *Super Admin* role. Using the created custom access level, generate an API key for the appliance.

Creating a custom API access level for your appliance is a one time task for your organization. You can use the same custom access level to configure multiple appliances for your organization.

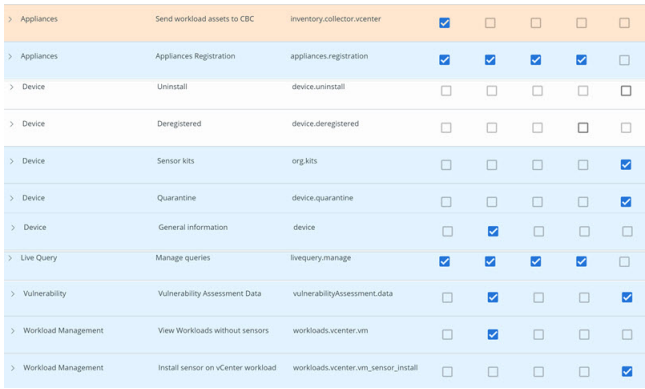
Procedure

1 Log in to the Carbon Black Cloud console. Make sure you have *Super Admin* permissions.

2 From the left navigation pane, click the **Settings > API Access > Access Levels** tab.

3 On the **Access Levels** tab, click **Add Access Level**.

4 Enter a name and description for the custom API access level for your appliance. Enter a name that users in your organization can identify easily. For example, you can add *Appliance* in the name.



5 Select the boxes of the permission functions (CRUDE) and include the following access level.

- Go to **Appliances** with the permission name as *Send workload assets to CBC* and select **Create**.
- Go to **Appliances** with the permission name as *appliance registration* and select **Create**, **Read**, **Update**, **Delete**.
- Go to **Device** with the permission name as *sensor kits* and select **Execute**.
- Go to **Device** with the permission name as *general information* and select **Read**.
- Go to **Live Query** with the permission name as *manage queries* and select **Create**, **Read**, **Update**, **Delete**.
- Go to **Vulnerability** with the permission name as *vulnerability assessment data* and select **Read** and **Execute**.
- Go to **Workload Management** with the permission name as *view workloads without sensors* and select **Read**.
- Go to **Workload Management** with the permission name as *install sensor on vCenter workload* and select **Execute**.

6 Click **Save**.

Results

Using the same custom API access level for the appliance, you can generate the API key for multiple appliances in your organization.

What to do next

Generate API keys for your appliance.

Step 1D: Connect to Carbon Black Cloud and 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.

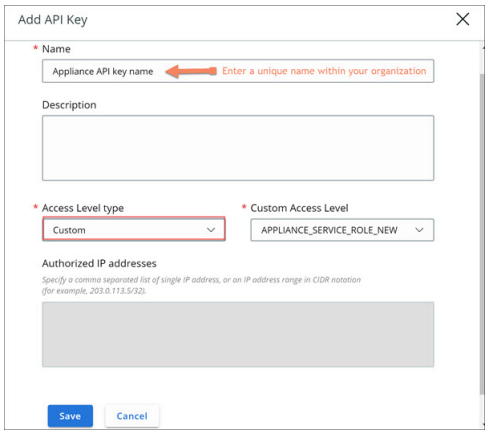
After the appliance is deployed, using the created custom access level, generate an API key for the appliance. You can use the same custom access level to configure multiple appliances for your organization.

Prerequisites

- You have deployed the Carbon Black Cloud Workload appliance in the vCenter Server. To know more about how to deploy the appliance in the vCenter Server, refer Step 1A: Deploy Carbon Black Cloud Workload appliance in the vCenter Server.
- The Step 1C: Create the Carbon Black Cloud Workload Appliance Custom API Access Level is available for appliances in your organization. Creating a custom access level for your appliance is a one-time task and is available only for the Carbon Black Cloud *Super Admin* role.

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. On the **API Keys** tab, click **Add API Keys**.



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 custom access level created by the *Super Admin* for your appliance. For details, refer to Step 1C: Create the Carbon Black Cloud Workload Appliance Custom API Access Level.

Tip: Look for **Appliance** in the name.

7 Click **Save**.

The API ID and API secret key are generated.

8 Copy both 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 Step 1E: Establish Connection Between Appliance and 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** page.

2 Go to the appliance API name created earlier and click the down arrow next to the **Edit** button.

3 Click **API Credentials**.

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

Step 1E: Establish Connection Between Appliance and Carbon Black Cloud

After generating the API keys from the Carbon Black Cloud console, configure the Carbon Black Cloud Workload appliance to establish connection between Carbon Black Cloud Workload appliance and Carbon Black Cloud.

Prerequisites

- Verify the Carbon Black Cloud Workload appliance VM is powered-on.

- API keys are generated and copied from the Carbon Black Cloud console. For more information, refer to Step 1D: Connect to Carbon Black Cloud and Generate API ID and API Secret Key.

Procedure

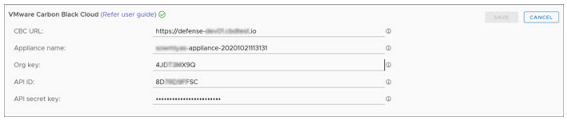
1 Log in to the vSphere Client.

2 Verify 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**.



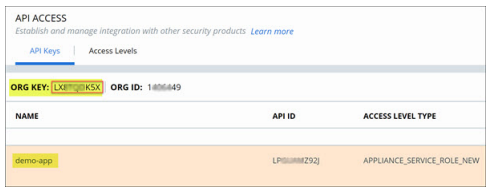
6 Configure the following values.

a **CBC URL**: Enter URL of the Carbon Black Cloud console as per your hosted Carbon Black Cloud location. For example, https://dashboard.confer.net/.

b **Appliance name**: Enter a unique name for the appliance in your Carbon Black Cloud organization.

Important The appliance name must be UNIQUE for your Carbon Black Cloud organization. One **Appliance name** is associated with one Carbon Black Cloud organization. You cannot use the same appliance name with a different set of API keys or use a different appliance name for the same set of API keys.

c **Org key**: Enter the organization key for your Carbon Black Cloud organization.



To find the org key, log in to the Carbon Black Cloud console and navigate to the **Settings > API Access > API Keys** page. You can find your **Org Key** value in the upper left.

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

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

For more information, refer to Step 1D: Connect to Carbon Black Cloud and Generate API ID and API Secret Key.

7 Click **Save**.

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

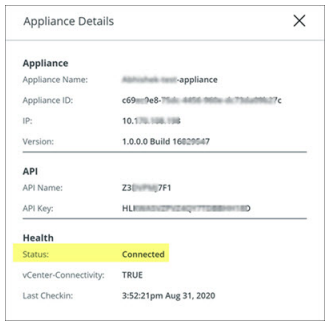
8 Verify if the connection between the Carbon Black Cloud Workload appliance and the Carbon Black Cloud is established successfully.

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 and connection status.



e Go to the **Inventory > Workloads > Not Enabled** page. You can view the virtual machine (VM) data.

Results

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.

What to do next

To view your inventory in the Carbon Black Cloud Workload Plug-in:

1 Go to the Carbon Black Cloud Workload Plug-in in the vCenter Server.

2 Go to the **Inventory > Not Enabled** tab.

3 To secure your workloads, Step 2: Enable Carbon Black on Virtual Machines .

To view your inventory in the Carbon Black Cloud console:

1 Navigate to your Carbon Black Cloud console.

2 Go to the **Inventory > Workloads > Not Enabled** tab.

3 Refresh the **Not Enabled** tab. The virtual inventory appears within a few minutes after your appliance is connected.

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.

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*

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	https://packages.vmware.com/cb/cblauncher/latest/ubuntu/dists/trusty/main/binary-amd64/cblauncher_1.0.0-16928845_amd64.deb	■ `dpkg -i cblauncher_1.0.0-`*`16928845`*`_amd64.deb`
RHEL/SUSE/CentOS/Oracle/ Amazon Linux	https://packages.vmware.com/cb/cblauncher/latest/cblauncher-1.0.0-16928845.x86_64.rpm	■ `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.

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 System Requirements.
- 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 as per the System Requirements.

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*.

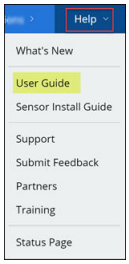
What to do next

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
```

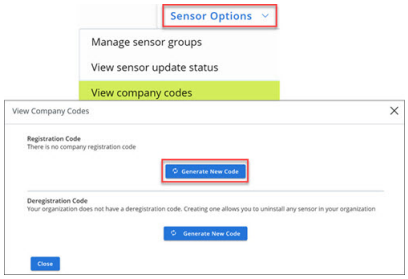
Mandatory Configuration File Parameters

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.

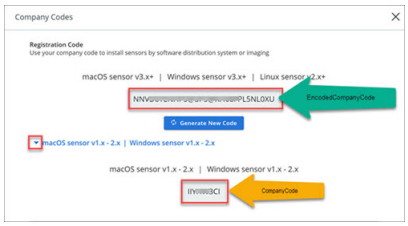
1 Sign in to the Carbon Black Cloud console and from the left navigation pane, click **Workloads**.

2 Click **Sensor Options**, and click **View company codes**.



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.



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 Carbon Black Cloud Sensor Installation Guide.

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.
- 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.

This chapter includes the following topics:

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** A *delete* action is triggered from the vCenter Server when a sensor gets deleted or moved out of the vCenter Server. 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.

Vulnerability Assessment

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 https://www.first.org/cvss/specification-document.

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 the *Kenna Security* documentation available at https://cdn.www.carbonblack.com/wp-content/uploads/VMWCB-Whitepaper-Understanding-the-Kenna-Security-Vulnerability-Risk-Score.pdf.

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.

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.

The password for the appliance expires in 90 days after you deploy the appliance for the first time. You must reset the password before getting expired. For details, refer to Reset Appliance Password. You can also extend the password expiration time manually or disable the password expiration permanently. For details, refer to Extend Password Expiration Time for Appliance.

By default, the appliance time zone is UTC.

This chapter includes the following topics:

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 Carbon Black Cloud Workload appliance at **`https://<appliance IP address>`** using the **`admin`** credentials.

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.

Appliance Health Status

You can view overall heath 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 Step 1E: Establish Connection Between Appliance and 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 .

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 Carbon Black Cloud Workload appliance at **`https://<appliance IP address>`** using the **`admin`** credentials.

2 Verify if the *admin* account is locked using the `pam_tally2 -u admin` command.

3 If the *admin* account is locked, then use the following command to unlock:

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

4 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.

5 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.

6 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 using appliance 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.

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 Step 1B: Register Carbon Black Cloud Workload Appliance With vCenter Server.

4 Generate the API ID and key. For details, refer Step 1D: Connect to Carbon Black Cloud and 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 Step 1E: Establish Connection Between Appliance and Carbon Black Cloud .

Appliance Logs

The appliance log bundle is a collection of diagnostic information that is required for the VMware support and engineering teams to troubleshoot any problem that you have encountered. 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 also change the appliance log level or export the logs while troubleshooting any problem. For the VMware support team, the logs are uploaded to the *prod.cwp.carbonblack.io* domain.

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.

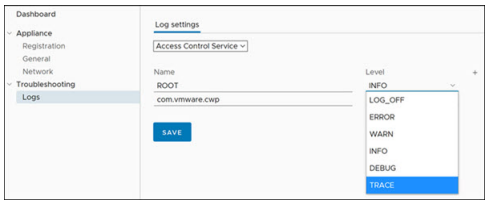
Prerequisites

You agree that the VMware support team can change the appliance log level and export logs for troubleshooting. You must open firewall for the *prod.cwp.carbonblack.io* domain.

Procedure

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

2 Go to the **Troubleshooting > Logs** page.



3 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
Log_Off	Logging is turned off.
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.

4 A logger is the entry point into the logging system to which messages can be written for processing. To add a logger and configure its log level, click the **Add new logger** (+) icon.

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

Results

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.

This chapter includes the following topics:

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**.

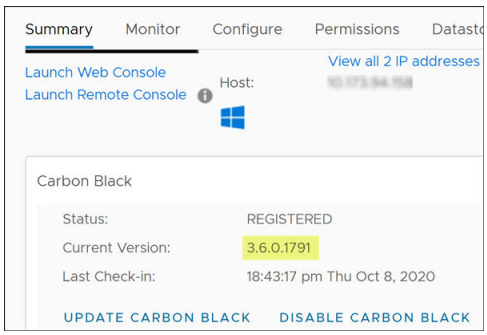
   A confirmation dialog box appears.
5. Click **OK**.

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.



Upgrade Appliance and Plug-In

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

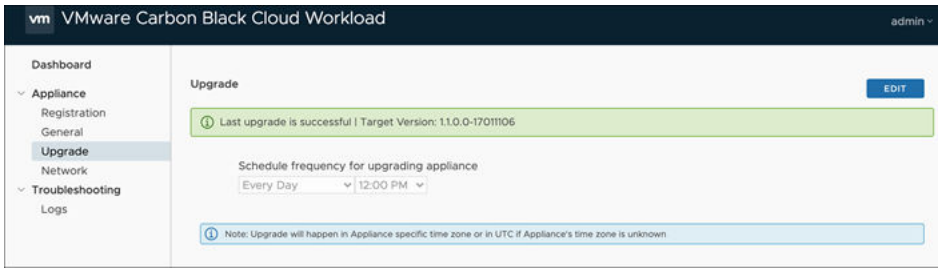
Prerequisites: You must open firewall for the *prod.cwp.carbonblack.io* domain.

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

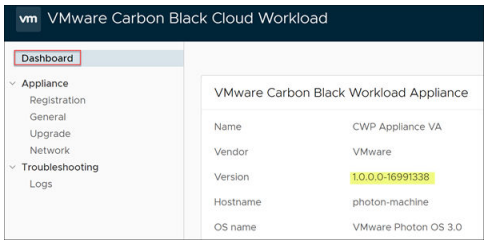
2 Go to the **Appliance > Upgrade** page.

3 Select the required day and time for the upgrade.

If not set, the default time zone for the appliance is UTC. Upgrade occurs in the appliance time zone.



After the appliance is upgraded, the Carbon Black Cloud Workload Plug-in is upgraded as well. You can view the updated version or the build number on the appliance dashboard.



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.

This chapter includes the following topics:

Disable 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 Carbon Black Cloud Workload appliance at **`https://<appliance IP address>`** using the **`admin`** credentials.
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
```