# VMware Carbon Black EDR Unified View User Guide

**Product Version: 7.3**

**Document Date: September 2020**

# Copyrights and Notices

We acknowledge the use of the following third-party software in our software products:

- Antlr python runtime - Copyright (c) 2010 Terence Parr
- Backbone - (c) 2010–2012 Jeremy Ashkenas, DocumentCloud Inc. Beautifulsoup - Copyright (c) 2004–2015 Leonard Richardson
- D3 - Copyright (c) 2010–2015, Michael Bostock FileSaver - Copyright (c) 2015 Eli Grey.
- Heredis - Copyright (c) 2009–2011, Salvatore Sanfilippo and Copyright (c) 2010–2011, Pieter Noordhuis
- Java memcached client - Copyright (c) 2006–2009 Dustin Sallings and Copyright (c) 2009–2011 Couchbase, Inc.
- Jedis - Copyright (c) 2010 Jonathan Leibiusky
- jQuery - Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors
- Libcurl - Copyright (c) 1996 - 2015, Daniel Stenberg, daniel@haxx.se. libfreeimage.a - FreeImage open source image library.
- Meld3 - Supervisor is Copyright (c) 2006–2015 Agendaless Consulting and Contributors. moment.js - Copyright (c) 2011–2014 Tim Wood, Iskren Chernev, Moment.js contributors MonthDelta - Copyright (c) 2009–2012 Jess Austin
- nginx - Copyright (c) 2002–2014 Igor Sysoev and Copyright (c) 2011–2014 Nginx, Inc. OpenSSL - Copyright (c) 1998–2011 The OpenSSL Project. All rights reserved.
- OpenSSL - Copyright (c) 1998–2016 The OpenSSL Project, Copyright (c) 1995–1998 Eric Young, Tim Hudson. All rights reserved.
- PolarSSL - Copyright (C) 1989, 1991 Free Software Foundation, Inc.
- PostgreSQL - Portions Copyright (c) 1996–2014, The PostgreSQL Global Development Group and Portions Copyright (c) 1994, The Regents of the University of California
- PostgreSQL JDBC drivers - Copyright (c) 1997–2011 PostgreSQL Global Development Group Protocol Buffers - Copyright (c) 2008, Google Inc.
- Pyrabbit - Copyright (c) 2011 Brian K. Jones
- Python decorator - Copyright (c) 2008, Michele  Simionato
- Python flask - Copyright (c) 2014 by Armin Ronacher and contributors
- Python gevent - Copyright Denis Bilenko and the contributors, http://www.gevent.org
- Python gunicorn - Copyright 2009–2013 (c) Benoit Chesneau benoitc@e-engura.org and Copyright 2009–2013 (c) Paul J. Davis paul.joseph.davis@gmail.com
- Python haigha - Copyright (c) 2011–2014, Agora Games, LLC All rights reserved. Python hiredis - Copyright (c) 2011, Pieter Noordhuis
- Python html5 library - Copyright (c) 2006–2013 James Graham and other contributors Python Jinja - Copyright (c) 2009 by the Jinja Team
- Python Markdown - Copyright 2007, 2008 The Python Markdown Project Python ordereddict - Copyright (c) Raymond Hettinger on Wed, 18 Mar 2009
- Python psutil - Copyright (c) 2009, Jay Loden, Dave Daeschler, Giampaolo Rodola'
- Python psycogreen - Copyright (c) 2010–2012, Daniele Varrazzo daniele.varrazzo@gmail.com Python redis - Copyright (c) 2012 Andy McCurdy
- Python Seasurf - Copyright (c) 2011 by Max Countryman. Python simplejson - Copyright (c) 2006 Bob  Ippolito

# Contents

List of Tasks

# How to . . .

# About this Document

This document describes how to use Carbon Black EDR Unified View. It assumes that you are familiar with Carbon Black EDR server and its features.

**Sections**

| Topic | Page |
|---|---|
| What this Document Covers | 8 |
| Other Documentation | 8 |
| Community Resources | 9 |
| Contacting Support | 9 |

# What this Document Covers

This document includes the following chapters:

| Chapter | Description |
| --- | --- |
| Chapter 1, Introduction | Introduces Carbon Black EDR Unified View concepts, architecture, and terminology. |
| Chapter 2, Installing a Server | Provides Carbon Black EDR Unified View server requirements, and describes how to install and configure Carbon Black EDR Unified View. |
| Chapter 3, Managing Clusters | Describes cluster management tasks in Carbon Black EDR Unified View. |
| Chapter 4, Operating Contexts | Explains the concept of "operating context" in Carbon Black EDR Unified View and its significance in using the product. |
| Chapter 5, Managing Users | Describes user management tasks for the user store in Carbon Black EDR Unified View. |
| Chapter 6, Server Configuration Settings | Describes configuration settings for Carbon Black EDR Unified View server. |
| Chapter 7, Command Line Tools | Describes the Carbon Black EDR Unified View actions you can perform on the command line as an alternative to within the user interface. |

# Other Documentation

Visit the Carbon Black User eXchange to locate documentation for tasks that are not covered in this guide, as well as other documents that are maintained as a knowledge base for technical support solutions. Some of these documents are updated with every new release, while others are updated only for minor or major version changes. Documents include:

- *VMware Carbon Black EDR Unified View User Guide* (this document) – Describes how to install and manage a Carbon Black EDR Unified View server.

- *VMware Carbon Black EDR Unified View Release Notes* – Includes information about new and modified features, issues resolved, general improvements in this release, and known issues and limitations. It also includes required or suggested preparatory steps before installing the server.

- *VMware Carbon Black EDR Operating Environment Requirements (OER)* – Describes performance and scalability considerations in deploying a particular version of Carbon Black EDR. Note that in earlier releases, this was called the *Server Sizing Guide.*

- *VMware Carbon Black EDR Server/Cluster Management Guide* – Describes how to install and manage a Carbon Black EDR server/cluster.

- *VMware Carbon Black EDR User Guide* – Describes the Carbon Black EDR product and explains how to use all of its features and perform administration tasks.

- *VMware Carbon Black EDR Release Notes* – Provides information about new and modified features, issues resolved and general improvements in the release, and known issues and limitations. It also includes required or suggested preparatory steps before installing the server.

- *VMware Carbon Black EDR Server Configuration (cb.conf) Guide* – Provides all of the `cb.conf` configuration file functions, descriptions, and parameters for the Carbon Black EDR server (not the Carbon Black EDR Unified View server).

- *VMware Carbon Black EDR Integration Guide* – Provides information for administrators who are responsible for integrating Carbon Black EDR with various tools.

# Community Resources

The VMware Carbon Black User Exchange website at https://community.carbonblack.com provides access to information shared by VMware Carbon Black customers, employees and partners. It includes information and community participation for users of all VMware Carbon Black products.

When you log into this resource, you can:

- Ask questions and provide answers to other users' questions.

- Enter a "vote" to bump up the status of product ideas.

- Download the latest user documentation.

- Participate in the VMware Carbon Black developer community by posting ideas and solutions or discussing those posted by others.

- View the training resources available for VMware Carbon Black products.

You must have a login account to access the User Exchange. Contact your Technical Support representative to get an account.

# Contacting Support

For your convenience, VMware Carbon Black Technical Support offers several channels for resolving support questions:

- **User Exchange:**  https://community.carbonblack.com

- **Support Home Page:**  https://www.carbonblack.com/resources/support/

- **Email:**  support@carbonblack.com

- **Phone:**  877.248.9098

- **Fax:**  617.393.7499

# Reporting Problems

When you contact technical support, provide the following information to the support representative:

| Required Information | Description |
| --- | --- |
| **Contact** | Your name, company name, telephone number, and email address |
| **Product version** | Product name and version number |
| **Hardware configuration** | Hardware configuration of the server or computer the product is running on (processor, memory, and RAM) |
| **Document version** | For documentation issues, specify the version of the manual you are using. The date and version of the document appear on the cover page, or for longer manuals, after the Copyrights and Notices section of the manual. The month of release also appears in the footers on each page. |
| **Problem** | Action causing the problem, error message returned, and any other appropriate output |
| **Problem severity** | Critical, serious, minor, or enhancement |

Chapter 1

# Introduction

This chapter introduces you to Carbon Black EDR Unified View and explains basic concepts.

**Sections**

| Topic | Page |
|-------|------|
| Overview | 12 |
| Architecture | 12 |
| Terminology | 13 |
| Logging | 13 |
| Setup Summary | 14 |

# Overview

Carbon Black EDR Unified View provides a single interface for process and binary searches across multiple Carbon Black EDR clusters, returning a unified set of results. From the search results, you can drill down to process analysis and binary details pages. You also can open a connection to a single Carbon Black EDR instance, which might be a single server or a cluster of servers.

> **Note**
>
> To simplify presentation in this document, all Carbon Black EDR instances that Carbon Black EDR Unified View accesses are described as "clusters," but the information provided is valid for single-server instances as well.

The Carbon Black EDR Unified View server has its own user store, and a configuration store for the servers it queries. However, it does not store any of the queried data on the server.

There are two types of user in Carbon Black EDR Unified View: administrators and non-administrators. A Carbon Black EDR Unified View administrator can determine which of the available Carbon Black EDR clusters to include in the Carbon Black EDR Unified View deployment and also create and manage user accounts on the Carbon Black EDR Unified View server.

Connections between Carbon Black EDR Unified View and the clusters it draws data from are accomplished using API keys for user accounts on each cluster.

# Architecture

Carbon Black EDR Unified View runs on a separate server from the Carbon Black EDR clusters it manages. It provides a graphical front end that does the following:

- Manages queries to the Carbon Black EDR Unified View server
- Runs those queries against each configured Carbon Black EDR cluster
- Merges the results into a unified set

The following figure illustrates the architecture of a Carbon Black EDR Unified View deployment, which uses a modified version of the Carbon Black EDR user interface.
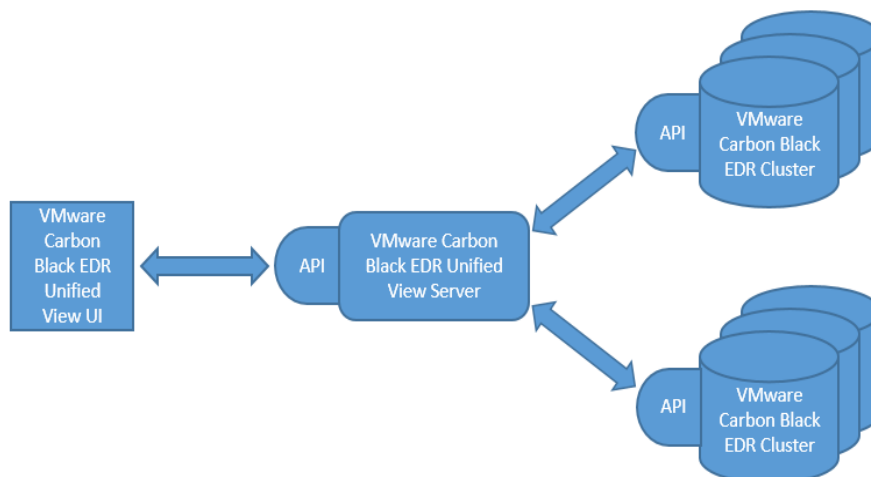
# Terminology

This document uses the following terms:

- An *instance* refers to either a single Carbon Black EDR server (and the sensors it monitors), or multiple Carbon Black EDR servers in one clustered configuration.

- A *cluster* refers to a single- or multi-server instance of Carbon Black EDR.

- A *standalone instance* refers to Carbon Black EDR that is not connected to Carbon Black EDR Unified View.

# Logging

Carbon Black EDR Unified View rotates log files on a daily basis and stores them for 7 days. The server generates logs from two sources:

- **nginx** – Logs basic access and error logs that are stored in `/var/log/cb/nginx/` `access.log` and `error.log`, respectively. The logs contain the basic HTTP requests made to the Carbon Black EDR Unified View server for the API.

- **uvservices** (the Carbon Black EDR Unified View service) – Generates and stores in `/var/log/cb/uvservices` the following log files:

| Log file | Description |
|---|---|
| `startup.log` | Captures output that is generated before the logging framework starts up. |
| `access.log` | Not currently used. |
| `debug.log` | General log file that includes status of pool workers and end-user activity. |

# Setup Summary

The following steps are needed to setup and use Carbon Black EDR Unified View – they are described in detail elsewhere in this document:

- **Install Carbon Black EDR Unified View** – See Chapter 2, "Installing a Server," for full installation and upgrade instructions.

- **Choose clusters** – Decide which Carbon Black EDR clusters to connect to your Carbon Black EDR Unified View.

- **Collect cluster API keys for authentication** – For each Carbon Black EDR cluster you plan to include, collect an API token from a user account *on that cluster*. This is necessary to authenticate the connection to Carbon Black EDR Unified View and have the cluster appear as available. See "Add or Remove Clusters" on page 21 for details.

- **Choose shared or per-user authentication** – For each Carbon Black EDR cluster, decide whether you want all users authenticated using a shared API token or each user authenticated using their own token. The privileges of the *cluster user* whose token is used determine what information is displayed from that cluster in Carbon Black EDR Unified View as well as what features are available when a Carbon Black EDR Unified View user browses to the cluster. See "Authentication Method (API Token)" on page 23 for details.

- **Create Carbon Black EDR Unified View users** – As an administrator, create any additional Carbon Black EDR Unified View accounts needed at your site. You can designate any account as an administrator if you choose, in which case the user will be able to create and modify user accounts and add and delete clusters from Carbon Black EDR Unified View. If you choose authentication via individual API token for any cluster, inform new users that they will have to provide an API token from their own account on that cluster to enable access to the cluster and its information. See "Overview of User Accounts" on page 34 for details.

# Chapter 2

# Installing a Server

This chapter describes preparations and procedures for Carbon Black EDR Unified View server installation and upgrades, and describes how to log in to a Carbon Black EDR Unified View server.

**Sections**

# Server Requirements

The Carbon Black EDR Unified View server can be installed on a physical or virtualized server that meets the following requirements:

**Server OS** – A base install of one of the following:

- 64-bit CentOS OS 6, 7, or 8
- Red Hat Enterprise 6, 7, or 8

Carbon Black EDR Unified View 7.0 has the same server OS requirements as Carbon Black EDR Server 7.0. See the latest *VMware Carbon Black EDR Operating Environment Requirements*.

**Memory and CPU** – Depends on the size of your Carbon Black EDR deployment:

- For ten or fewer Carbon Black EDR servers and up to 100 concurrent end users:
  - 8 GB of RAM
  - 4 CPU cores
- For more than ten Carbon Black EDR servers:
  - Minimum 16 GB of RAM
  - Minimum 8 CPU cores.

**Storage** – Because the Carbon Black EDR Unified View server does not store search data and does not have substantial disk I/O requirements, a typical enterprise-level hard drive or equivalent is sufficient.

> **Note**
>
> Carbon Black recommends configuring at least 40 GB of log space in `/var/log/cb`.

**Carbon Black EDR servers** – The Carbon Black EDR Unified View server aggregates search results from at least one Carbon Black EDR server (the minimum for a cluster). Carbon Black EDR servers that provide results to this release of Carbon Black EDR Unified View must meet the following requirements:

- Carbon Black EDR server version 7.0 or newer.
- HTTPS query access to each underlying Carbon Black EDR server.

> **Note**
>
> The Carbon Black EDR Unified View server does not support HTTP proxies and must have direct HTTPS access to the servers.

- The ability to make HTTPS API queries to the RESTful API using the configured Carbon Black EDR port, usually 443.

# Installing Carbon Black EDR Unified View

This section describes how to perform a clean installation of Carbon Black EDR Unified View (that is, on a system that has no previous version installed).

> **Note**
>
> This release of Carbon Black EDR Unified View supports only 6-series Carbon Black EDR servers and above. To manage 5-series Carbon Black EDR servers and earlier with Carbon Black EDR Unified View, you must use a separate Carbon Black EDR Unified View (CB-Fed) version 1.1.0, which is available from the Carbon Black yum repository. You cannot manage Carbon Black EDR 5- and 6-series servers from a single Carbon Black EDR Unified View server.

This release of Carbon Black EDR Unified View does not support in-place upgrades from the earliest Carbon Black EDR Unified View versions, named CB-Fed v.1.x.x, but does allow you to upgrade from Carbon Black EDR Unified View 6.1.3. See

**To install Carbon Black EDR Unified View on a new system:**

1. Obtain the RPM installation package for Carbon Black EDR.

   If you are a Carbon Black EDR on-premises customer, you received this RPM package when you installed the Carbon Black EDR server.

   If you do not have access to this file, or if you are a Carbon Black Hosted EDR customer, contact Carbon Black Technical support to obtain the file.

2. Install the RPM package using the following command:

   ```
   sudo rpm -ivh carbon-black-release-<license
   version>.<customername>.x86_64.rpm
   ```

   This file adds Carbon Black EDR SSL certificates and keys in the following directory:

   ```
   /etc/cb/certs/
   ```

3. Remove the file `CarbonBlack.repo` from the `/etc/yum.repos.d` directory, or edit the file and set `enabled=0`.

4. Create the following **new** repo file specific to Carbon Black EDR Unified View:

   ```
   /etc/yum.repos.d/CarbonBlackUnifiedView.repo
   ```

5. Edit the `CarbonBlackUnifiedView.repo` file to have the following contents:

   ```
   [CbUnifiedView]
   name=CbUnifiedView
   baseurl=https://yum.distro.carbonblack.io/unifiedview/stable/
   $releasever/$basearch/
   gpgcheck=0
   enabled=1
   metadata_expire=60
   sslverify=1
   sslclientcert=/etc/cb/certs/carbonblack-alliance-client.crt
   ```

```
sslclientkey=/etc/cb/certs/carbonblack-alliance-client.key
```

6. For EL6 and EL7 servers, run the following command:

```
$ sudo yum install cb-unifiedview
```

For EL8 servers, run the following commands:
```
$ sudo yum module disable postgresql redis
$ sudo yum install cb-unifiedview
```

7. Type **y** to confirm that you want to install the available packages comprising the Carbon Black EDR Unified View installation.

8. Initialize the Carbon Black EDR Unified View server using the following script:

```
/usr/share/cb/cbinituv
```

This script does the following:

- Presents the End User License Agreement (type **yes** to accept).

- Sets up the initial administrator account with the username and other values that you specify.

- Completes the operating environment for Carbon Black EDR Unified View server (firewall, database, encryption key).

9. Start services by typing **y** at the prompt. Or, you can start services later by using the following command:

```
service cb-unifiedview start
```

Carbon Black EDR Unified View server installation is now complete.

You can log into the Carbon Black EDR Unified View server (through `https://localhost` or `https://<serveraddress>`) using credentials for the initial administrator account you created when you ran `/usr/share/cb/cbinituv` in the preceding procedure. See "Logging In to Carbon Black EDR Unified View" on page 19 for additional details and Next Steps.

# Upgrading from an Earlier Release

If you have Carbon Black EDR Unified View 6.1.3 or later currently installed, you can upgrade to a newer version without uninstalling the previous version:

**To upgrade Carbon Black EDR Unified View from a 6.1.3 or later version:**

1. On the server, stop the Carbon Black EDR Unified View services:

```
sudo service cb-unifiedview stop
```

2. (Optional) Clean the yum cache of metadata and packages:

```
yum clean all
```

3. Update the Carbon Black EDR Unified View services:

```
sudo yum upgrade cb-unifiedview
```

4. Restart the Carbon Black EDR services:

```
sudo service cb-unifiedview  start
```

# Logging In to Carbon Black EDR Unified View

When you log into Carbon Black EDR Unified View, Cluster Management appears as the landing page. The left-hand Clusters panel lists all clusters in your deployment – it will be blank the first time you log in. Once you have added clusters, you can select a cluster to view or edit its settings in the panel to the right.
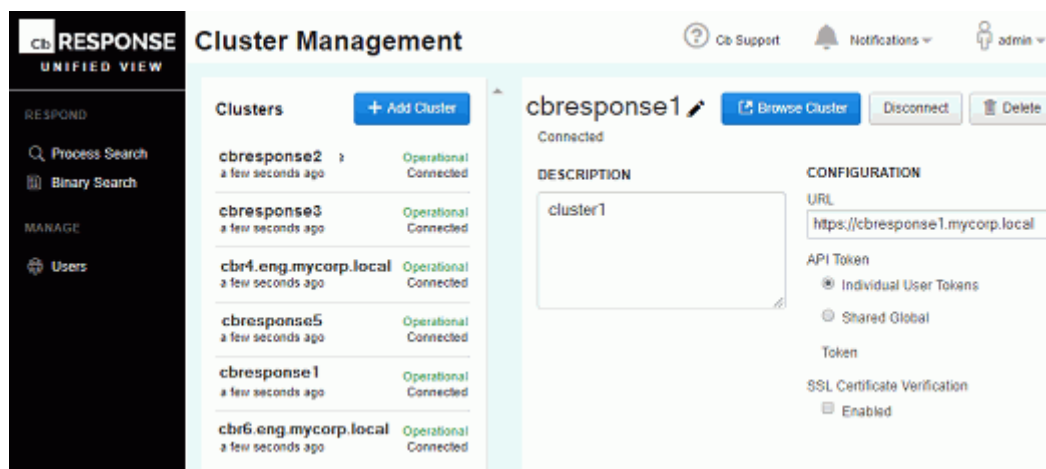


To return to the Cluster Management page from anywhere in the multi-cluster context of Carbon Black EDR Unified View, click the logo at the top of the navigation bar.

## Next Steps

- See Chapter 3, "Managing Clusters," on page 20 for instructions on setting up clusters in your Carbon Black EDR Unified View environment.

- See Chapter 4, "Operating Contexts," on page 27 for details about multi-cluster vs. single-cluster operating contexts in Carbon Black EDR Unified View.

- See Chapter 5, "Managing Users," on page 33 for details about setting up user accounts in your Carbon Black EDR Unified View environment.

- See Chapter 6, "Server Configuration Settings," on page 42 for instructions on customizing the configuration of your Carbon Black EDR Unified View server.

- See Chapter 7, "Command Line Tools," on page 48 for instructions on using command-line options to manage users and clusters in Carbon Black EDR Unified View.

# Chapter 3

# Managing Clusters

This chapter describes how to manage clusters in Carbon Black EDR Unified View.

**Sections**

# Overview of Cluster Management

Carbon Black EDR Unified View administrators can perform the following cluster management tasks:

- Add and remove clusters from Carbon Black EDR Unified View, specify their authentication parameters, and configure SSL certificate settings. See "Add or Remove Clusters" below.

- Specify the type of API token for authenticating users to a cluster — either shared or individual. See "Authentication Method (API Token)" on page 23.

- Specify the clusters that are available for searching in Carbon Black EDR Unified View. See "Cluster Connection Status" on page 24.

- Monitor the operating (health) status of clusters. See "Cluster Health Status" on page 25.

> **Note**
>
> Administrators also manage Carbon Black EDR Unified View users, as described in Chapter 5, 'Managing Users' on page 33.

Individual Carbon Black EDR Unified View users, whether administrators or not, can specify how they manage clusters on the My Profile page, as follows:

- Set their own authentication credentials for clusters that require user authentication via individual API tokens.

- Specify which of the available clusters to enable (include) or disable (exclude) for personal searches. For details, see "Choose Clusters for Personal Global Searches" on page 41.

# Add or Remove Clusters

Use the Cluster Management page in Carbon Black EDR Unified View to add, modify, or remove clusters.

**To add a cluster to Carbon Black EDR Unified View:**

1. Log in to Carbon Black EDR Unified View using an administrator account.

2. If you are viewing a single cluster through Carbon Black EDR Unified View, click the browser tab for the multi-cluster view.

3. If the Cluster Management page is not already showing, click the Carbon Black EDR logo at the top left of the navigation bar.

   If clicking this logo brings you to a HUD page, you are still in single-cluster view and should click on a different browser tab. There is no HUD page in Carbon Black EDR Unified View.

4. In the list of clusters in the left pane, click **Add Cluster**.

5. Complete settings in the Add Cluster dialog box as described in "Cluster Configuration Settings" on page 22.

**To remove a cluster from Carbon Black EDR Unified View:**

1. If the Cluster Management page is not already showing, in multi-cluster mode, click the Carbon Black EDR logo at the top left of the navigation bar.

2. Click to select the cluster to delete.

3. At the top of cluster details in the right pane, click **Delete**.
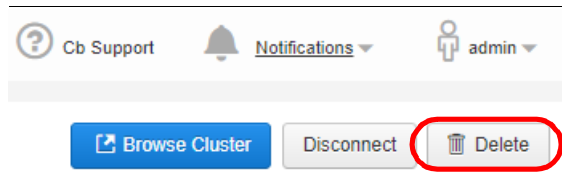


4. Confirm the deletion by clicking **Delete Cluster** in response to the Confirmation prompt.

# Cluster Configuration Settings

Cluster settings include basic details, authentication method, connection status, and SSL certificate verification.
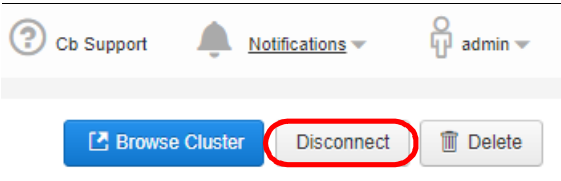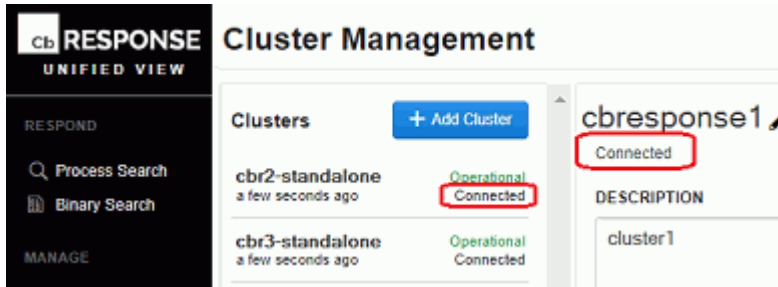
## Basic Settings

| Setting | Description |
|---|---|
| **Name** | Enter the name of the cluster. |
| **Description** | Optionally, enter a description of the cluster. |
| **URL** | Enter the URL for the cluster. |

## Authentication Method (API Token)

| Setting | Description |
|---------|-------------|
| **API Token** | In Carbon Black EDR Unified View, users authenticate to clusters through API tokens instead of usernames and passwords. Select one of the following authentication methods for users to access the cluster through Carbon Black EDR Unified View:<br><br>• **Individual User Tokens** – Each user must obtain an API token from a user account on the cluster (such as their own account), and then add it to settings for that cluster on their My Profile page in Carbon Black EDR Unified View. This option is useful if you want to limit users to no more access via Carbon Black EDR Unified View than they would have by directly logging in to the cluster.<br><br>• **Shared Global Token** – All users can access the cluster using an API token entered at creation time (in the Add Cluster dialog box), or later, in cluster settings on the Cluster Management page. With this option, users can access the cluster without having to configure their own tokens. A shared token is convenient, for example, when all Carbon Black EDR Unified View users require the same access to this cluster. It is not appropriate if you require different privileges on a cluster for different Carbon Black EDR Unified View users. |

## Cluster Connection Status

| Setting | Description |
| --- | --- |
| **Disconnect/ Connect** | Click to specify the cluster's connection status, which determines whether the cluster is available for global searches in Carbon Black EDR Unified View.<br><br>Settings are as follows:<br><br>• **Connect** (the default) – The cluster is connected and available for all users to include in global process or binary searches. When the cluster is *connected*, the middle button at the top of the settings panel reads **Disconnect**:<br><br><br><br>The word "Connected" also appears in the following locations:<br><br><br><br>When the cluster is connected through the Cluster Management page, individual users can use My Profile to enable or disable the cluster for personal searches, without affecting access for other users.<br><br>• **Disconnect** – The cluster is disconnected and temporarily unavailable for global process or binary searches, but its configuration information is saved. When the cluster is *disconnected*, the middle button at the top of the settings panel reads **Connect**. Also, the word "Disconnected" appears in place of "Connected."<br><br>When the cluster is disconnected, users cannot enable or disable it in My Profile.<br><br>You can browse a cluster from Carbon Black EDR Unified View whether it is connected or disconnected for searching.<br><br>See "Scope for Multi-cluster Searches" on page 30. |

### SSL Certificate Verification

| Setting | Description |
|---------|-------------|
| **SSL Certificate Verification** | Specify whether the Carbon Black EDR Unified View server verifies that the cluster certificate has a valid and trusted CA-signed SSL certificate. |
| | • Do not select this option (leave it blank) if the cluster uses a self-signed certificate, such as a certificate that the Carbon Black EDR server initialization script generates, and the SSL certificate used within the SSL handshake is not validated. |
| | • Select **Enabled** to specify that the Carbon Black EDR Unified View server verifies that the Carbon Black EDR cluster certificate has a valid SSL certificate that is signed by a trusted CA. |

# Cluster Health Status

Every 30 seconds, Carbon Black EDR Unified View gathers key health metrics from the managed clusters and aggregates the collected statistics into reports every five minutes. A five-day history of these reports is stored, beginning with the current time. The following statistics are stored in each interval:

- **Average heartbeat time** – The average time value it takes for the Carbon Black EDR Unified View server to query the info API endpoint on the cluster.
- **Average query time** – The average time value for all non-heartbeat queries made to the cluster. This value can be zero if no queries are made against the server.

The Cluster Management page provides a high-level overview of all the clusters within Carbon Black EDR Unified View. The overall health status of each cluster is determined by a combination of the average query time, heartbeat round-trip time, and number of errors. Health status is indicated by colored text as follows:

- Green – **Operational**. Network communications to the Carbon Black EDR server are working properly and API calls can go through.
- Yellow/Orange – **Unstable**. Can connect to the Carbon Black EDR server, but issues affecting network communication are detected. Possible cause might be failing SSL verification or query time delays.
- Red – **Unavailable**. Cannot connect to the Carbon Black EDR server. Possible cause might be wrong IP or blocked port, for example.

In the cluster settings panel of the Cluster Management page, the five most recent errors that occurred when communicating with the server appear, as well as the error count and time of the last query timeout.

The Carbon Black EDR Unified View server stores the last 50 errors (the default) that occurred when the Carbon Black EDR Unified View server queried the cluster. You can change the default number of stored errors with the server configuration setting `UnifiedViewMaxNumberOfDbErrorLogs` in `cb.conf` (see ).

To export these errors to a CSV file, click the icon next to the Recent Errors section heading:

# Chapter 4

# Operating Contexts

This chapter describes the global and single-cluster operating contexts in Carbon Black EDR Unified View.

**Sections**

| Topic | Page |
|-------|------|
| Context Overview | 28 |
| Multi-Cluster Context | 29 |
| Single-Cluster Context | 31 |

# Context Overview

Carbon Black EDR Unified View operates in either multi-cluster (global) context or single-cluster context. The operating context determines the information displayed, the operations available, and the scope to which the operations apply.

Cues in the user interface identify and help track the current context and, in the case of single-cluster view, the current cluster. For example:

- When an operation switches context, a new browser window opens to display the new view.

- In a given context, only the actions relevant to that context are available.

  For example, the navigation bar includes only the actions that are available in the current context, as follows:

| Multi-cluster context | | Single-cluster context | |
|---|---|---|---|
| *Collapsed* | *Expanded* | *Collapsed* | *Expanded* |
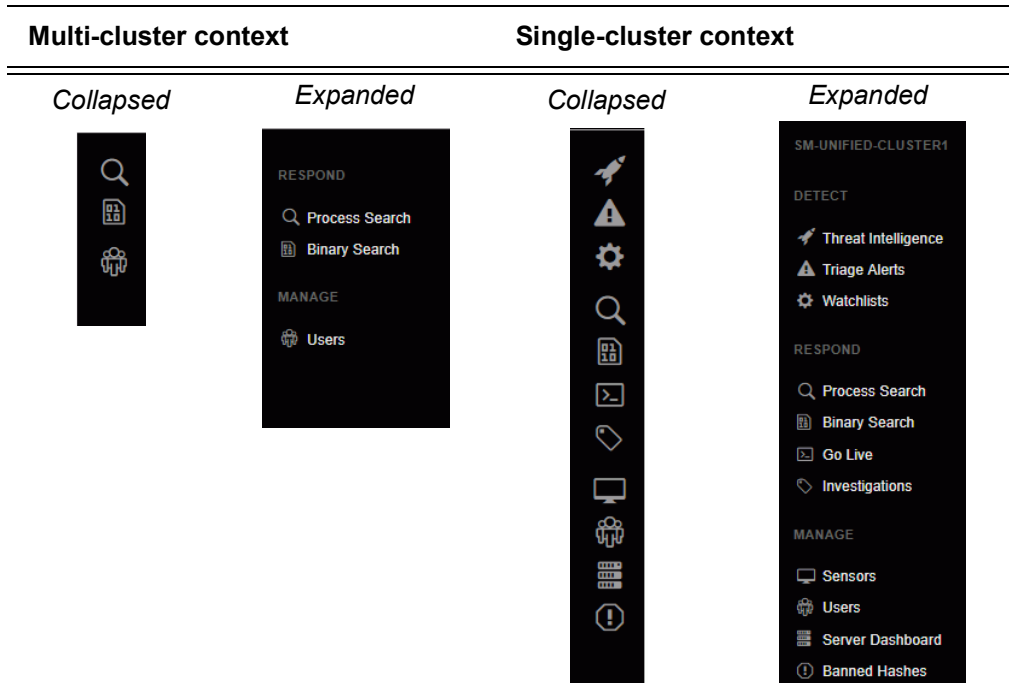


In single-cluster context, the name of the current cluster appears in these locations:

- In the title of the page.



- At the top of the navigation bar (expanded).
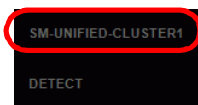
# Multi-Cluster Context

The available actions in multi-cluster context are as follows:

- Cluster management – See Chapter 3, "Managing Clusters" on page 20.
- Process search and process analysis – See "Process Search" on page 29.
- Binary search and binary details – See "Binary Search" on page 30.
- User management – See Chapter 5, "Managing Users" on page 33.

Process and binary searches in multi-cluster context apply to all data provided from all *included* clusters in Carbon Black EDR Unified View. Included clusters are those connected in Cluster Management for each Carbon Black EDR Unified View user, and included data from each cluster depends upon the permissions provided by the cluster API token for the user.

Carbon Black EDR operations in Carbon Black EDR Unified View multi-cluster context are similar to being logged directly into a single instance of Carbon Black EDR, with some exceptions. For example, the Sensor Details page is unavailable in multi-cluster context, but if you click on a sensor name in multi-cluster search results, a single-cluster view opens in a separate tab and show the Sensor Details page on the cluster that the sensor reports to.

## Process Search

To search for process activity across clusters in the Carbon Black EDR Unified View (multi-cluster context), click **Process Search** in the navigation bar. On the Process Search page, perform the search the same as you would for single-instance Carbon Black EDR. Results are from all included clusters in Carbon Black EDR Unified View, subject to any limitations imposed by the cluster user account whose API token was used for authentication. Each returned process includes the cluster name and the sensor name.

In search results on the Process Search page, the following actions are available:

- To filter results to a specific cluster, click the name of the cluster using the Cluster filter in the left.
- To see details about a specific process, click the name of the process in the Process of the search results. The Process Analysis page (described in the next section) appears and displays a global-context view of process details.
- To see details about a sensor, click the name of the Host in the Endpoint column for a returned process. This displays the single-cluster view of the cluster this host reports to and shows the Sensor Details page.
- To go to the Carbon Black EDR HUD page for one cluster (switching to single-cluster context), click the name of the cluster in the Endpoint column for a returned process.

### Process Analysis

Carbon Black EDR Unified View displays the Process Analysis page in multi-cluster context, although the process details are cluster-specific. The page is similar to the Process Analysis page in single-cluster context, with the following exceptions:

- Searches initiated by clicking a link on the page are performed across clusters in Carbon Black EDR Unified View.
- Investigations are available in single-cluster context, but do not apply in multi-cluster context.

- Carbon Black EDR Go Live is unavailable. It is, however, available in single-cluster context.

# Binary Search

To search for binaries across the Carbon Black EDR Unified View, click **Binary Search** in the navigation bar.

In the multi-cluster context for binary search, if a particular binary occurs on multiple clusters, it appears multiple times in the search results. For example, if four clusters report the same binary (based on its md5), the binary appears four times in the results.

Click on the binary in the search results to display the Binary Details page.

## Binary Details

In Carbon Black EDR Unified View, the Binary Details page displays aggregated information about the binary from across all clusters in Carbon Black EDR Unified View. Similarly, links on the Binary Details page perform Carbon Black EDR Unified View-wide searches across clusters.

> **Note**
>
> In some cases, Carbon Black EDR clusters return conflicting Digital Signature Metadata status for a particular binary. This can happen because signature status is verified on the sensor level, and different environments (clusters) can have different certificate trust settings. When such a conflict occurs, you can see which cluster reported a particular status by clicking the signature status.

# Scope for Multi-cluster Searches

All clusters added to Carbon Black EDR Unified View are potentially available (connected) for global process and binary searches. However, several factors determine which clusters are available for searches and single-cluster views. Some factors affect all Carbon Black EDR Unified View users and some are specific to individual users:

- **Was the cluster added to Carbon Black EDR Unified View?** – On the Cluster Management page, a cluster must be configured for connection to Carbon Black EDR Unified View by an administrator before it becomes available. See "Add or Remove Clusters" on page 21 for more information.

- **Is the cluster connection enabled for this Carbon Black EDR Unified View server?** – On the Cluster Management page, administrators can temporarily disconnect a particular cluster for all users without deleting it. This prevents its data from being available in searches and also presents access via single-cluster view. Removing a cluster from searches temporarily can be helpful in certain situations, such as when you need to improve performance during heavy usage periods, to perform scheduled maintenance on a cluster, or to narrow searches to a particular set of clusters. See "Cluster Connection Status" on page 24 for more information.

- **Is the cluster connection enabled for this user?** – On the My Profile/My Cluster page, individual users can enable and disable inclusion of available clusters in their own searches. See "Choose Clusters for Personal Global Searches" on page 41.

- **What permissions does the API token provide on the cluster?** – The API token specifies the *cluster user* whose permissions are used for access to that cluster. If the

cluster is set up to use a Shared Token for all users, that API token is specified on the Cluster Management page. If the cluster is set up to use Individual Tokens for each user, the token is specified on the user's My Profile/My Clusters page.

For a Carbon Black EDR Unified View user to have access to data from a cluster, the user whose API token is used for authentication must have access to that data. Cluster user accounts can be set up to give the user access to some Sensor Groups and not others. In this case, only data from the permitted Sensor Groups can be searched by the Carbon Black EDR Unified View user authenticated through that API token. See the managing users chapters in the *VMware Carbon Black EDR User Guide* for details on user permissions.

# Single-Cluster Context

On the Cluster Management page in Carbon Black EDR Unified View, clicking **Browse Cluster** to navigate to a particular cluster opens a new browser tab that displays that cluster's HUD page. In this view, no multi-context operations are available. Single-cluster context is also initiated when you click the cluster name on certain pages.

Carbon Black EDR operations in the single-cluster context of Carbon Black EDR Unified View are mostly the same as when logged directly into a standalone instance of Carbon Black EDR, with the exceptions noted in "Operating Exclusions in Single-Cluster Context."

> **Note**
>
> In the single-cluster context of Carbon Black EDR Unified View, clicking the logo at the top of the navigation bar displays the cluster's HUD (heads-up display) page instead of the Cluster Management page.

## Operating Exclusions in Single-Cluster Context

You cannot perform the following actions in the single-cluster context of Carbon Black EDR Unified View:

- Log out of Carbon Black EDR on the cluster. The **Logout** command is unavailable in the single-cluster context of Carbon Black EDR Unified View because authentication to the cluster is through a shared or individual API token, not a username and password.

- Modify your cluster user profile. The cluster user profile is unavailable in single-cluster context for the same reason that **Logout** is unavailable.

- Request email notifications for threat intelligence hits.

- Request email notifications for watchlist hits.

To perform these actions on one cluster, you must log into that instance directly.

## Features Limited by User Permissions in Single-Cluster Context

In addition to cluster console features that are never available from Carbon Black EDR Unified View, some features are limited by the permissions of the user whose API token authenticates a cluster's connection to Carbon Black EDR Unified View:

- If their token is from a global administrator for the cluster, Carbon Black EDR Unified View users have privileges for all cluster console features not excluded by Carbon Black EDR Unified View.

- If their token is from a non-administrator user for the cluster, and that user is limited to accessing only some sensor groups, the Carbon Black EDR Unified View user will be similarly limited when using Browse Cluster.

- If their token is from a non-administrator user for the cluster, and that user is only allowed to view data but not take actions that affect the cluster or its sensors, the Carbon Black EDR Unified View will be similarly limited when using Browse Cluster. See the managing users chapters in the *VMware Carbon Black EDR User Guide* for information about how permissions are controlled for cluster users.

# Chapter 5

# Managing Users

This chapter describes how to manage Carbon Black EDR Unified View users.

**Sections**

# Overview of User Accounts

Carbon Black EDR Unified View users are the administrators and security personnel who are responsible for the following activities:

- Configuring and monitoring Carbon Black EDR clusters in Carbon Black EDR Unified View.
- Creating and managing user accounts in Carbon Black EDR Unified View.
- Performing process and binary searches on clusters in Carbon Black EDR Unified View.
- Analyzing search results in Carbon Black EDR Unified View, and drilling down to individual clusters to further investigate the returned data.

You must create separate user accounts specifically for Carbon Black EDR Unified View. User accounts created on the Carbon Black EDR clusters being viewed cannot be used to log in to the Carbon Black EDR Unified View console.

There are two elements that determine what a user can do in Carbon Black EDR Unified View:

- Access to Carbon Black EDR Unified View user and cluster management features is determined by whether a Carbon Black EDR Unified View user is configured as an Administrator. Non-administrator users can use the binary and process search features of Carbon Black EDR Unified View, and browse to clusters they have been authenticated on.
- Access to each connected cluster and its information is determined on a per-user basis by the API token used to authenticate the connection to each cluster.

## Permissions for User Management Tasks

The privileges required to perform different user management tasks varies by task type and location in Carbon Black EDR Unified View or the clusters being viewed:

- **User Management Page in Carbon Black EDR Unified View** – Only a Carbon Black EDR Unified View administrator can perform the following user management tasks:
  - View all user accounts
  - Modify user accounts
  - Add users
  - Delete users
  - Grant or remove administrator permissions
- **Cluster Management Page in Carbon Black EDR Unified View** – Only a Carbon Black EDR Unified View administrator can require that users provide an individual API token to authenticate to a cluster.
- **My Profile in Carbon Black EDR Unified View** – All Unified View users can view and modify their own Carbon Black EDR Unified View user profile on the My Profiles page. This includes providing API tokens to authenticate connections to clusters, if an individual is required.
- **User Management Page on a cluster** – A Carbon Black EDR Unified View user who is also has (and is authenticated with) a global administrator account on a cluster can manage individual cluster accounts from within Carbon Black EDR Unified View.
- **My Profile on a cluster –** The My Profile on a cluster cannot be modified through Carbon Black EDR Unified View. A Unified View user with a user account on a

managed cluster must log into the cluster directly to view or modify their own profile. (See "Operating Exclusions in Single-Cluster Context" on page 31.)

# User Management Tasks

This section describes user management tasks a Carbon Black EDR Unified View administrator performs.

**To view Carbon Black EDR Unified View users:**

- In the navigation bar of Carbon Black EDR Unified View in a multi-cluster context, click **Users** (or its icon).
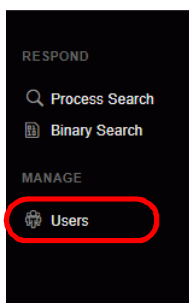


The User Management page lists all Carbon Black EDR Unified View users in the left panel. Details about the selected user appear in the right.

**To view or modify a Carbon Black EDR Unified View user:**

1. In the navigation bar, click **Users** to go to the User Management page.

2. In the list of users, search or scroll to locate the user to view or edit.

3. Click the name of the user.

   Details about the user appear in the right-hand.

4. Review or modify user settings.

5. To save your changes, click **Save Changes** at the bottom of the page.

**To add a new Carbon Black EDR Unified View user:**

1. In the navigation bar, click **Users** to go to the User Management page.

2. At the top of the page, click **Add User**.

   New User settings (blank) appear in the right.

3. Complete user settings as follows:

| Setting | Description |
| --- | --- |
| **First Name** | Enter the user's first name. |
| **Last Name** | Enter the user's last name. |
| **Username** | Enter a username for the user. |

| Setting | Description |
|---|---|
| **Administrator** | Click to specify if the user is an admin (**Yes**) or a non-admin (**No**, the default). You can change this setting later. |
| **Password**<br>**Confirm Password** | Provide the user with an initial password. Enter it twice. The new user can change the password later. |

4. Click **Save Changes**.

   The new user now appears in the list of users.

**To delete a Carbon Black EDR Unified View user:**

1. In the navigation bar, click **Users** to go to the User Management page.

2. In the list of users in the left-hand panel, search or scroll to locate the user you want to delete.

3. Click the name of the user.

4. At the bottom of the right , click **Delete User**.

5. Click **OK** in the **Delete User** dialog box to confirm the deletion.

   The user no longer appears in the list of users.

# Cluster Authentication

In addition to adding, deleting, and modifying Carbon Black EDR Unified View user accounts, Carbon Black EDR Unified View administrators determine whether each user must provide their own cluster API token to establish a connection with a cluster. Each cluster can be configured for either shared or individual user access:

- **Shared API token** – If *Shared Global Token* is chosen for a cluster, all Carbon Black EDR Unified View users access the cluster through the same, shared token that is specified in configuration settings for the cluster in Cluster Management. This is convenient, but it is not appropriate if you require different privileges on a cluster for different Carbon Black EDR Unified View users.

- **Individual API token** – If *Individual User Tokens* is chose for a cluster, each user accesses the cluster through a unique token that is obtained from a user account on the cluster and added to settings for the cluster in that users My Profile/My Clusters page.

**Notes**

- The authentication choice for each cluster affects all users. You cannot require some users to provide individual tokens with others authenticate using a shared token for the same cluster.

- There is no relationship between the API token for a Carbon Black EDR Unified View user account and the API token for a user account on a cluster, even if they are for the same person. Only *cluster* API tokens can be used for Carbon Black EDR Unified View authentication.

# Managing My Profile

All users can view their own information on the My Profile page in Carbon Black EDR Unified View, and for most fields can modify information or settings.

**To access the My Profile page:**

1. On the username menu in the upper right of the Carbon Black EDR Unified View console, choose **My Profile**.

   The My Profile page for your Carbon Black EDR Unified View user account appears.



My Profile consists of three pages that are described in the following sections.

- Profile Info
- API Token
- My Clusters

## Profile Info

On the Profile Info page in My Profile, you can view or modify your user settings, change your password, or clear user interface preferences.

**To view or change your user details:**

1. On the username menu in the upper right of the console, choose **My Profile**.
2. In the left panel, click on **Profile Info** and view or modify user settings as needed.

| Setting | Description |
|---|---|
| **First Name** | Enter your first name. |
| **Last Name** | Enter your last name. |
| **Email Address** | Enter your email address. |

Note that you cannot change your username.

3. Click **Save Changes**.

**To change your password:**

1. On the username menu in the upper right of the console, choose **My Profile**.

2. On the My Profile page, click the **Profile Info** link.

3. Click **Change Password**.

4. Complete the **Change Password** dialog.

5. Click **Save Changes** on the dialog and then again on the My Profile page.

## Preferences

Carbon Black EDR Unified View keeps track of search queries that each user saves and also tracks changes they make to the user interface, such as filter selections, sort order, and navigation bar format. These changes are saved between sessions as user preferences. Each time a user logs in, Carbon Black EDR Unified View restores saved preferences from the user's last session.

You can discard your preferences and reset the interface to the default settings.

**To clear your user preferences:**

1. On the username menu in the upper right of the console, choose **My Profile**.

2. On the My Profile page, click the **Profile Info** link.

3. On the Profile Info page, click **Clear Preferences**.

   Carbon Black EDR Unified View discards your preferences, including saved searches, and restores the default settings.

4. Click **Save Changes**.

## User API Token

The API Token page in My Profile displays your API token for Carbon Black EDR Unified View:



This token can be used in place of a user name and password in a script or custom application that integrates or interacts with the Carbon Black EDR Unified View server API. In most cases, you can disregard this token. If at some point you are required to change it, use the following procedure.

Note that this is *not* the API token used to authenticate connections to clusters.

**To reset your Carbon Black EDR Unified View API token:**

1. On the username menu in the upper right of the console, choose **My Profile**.

2. Click the **API Token** link.

3. On the API Token page, click **Reset API Token**.

4. Click **Save Changes**.

# My Clusters

The My Clusters page in My Profile displays the following:

- A list of clusters known to this Carbon Black EDR Unified View server. By default this shows all clusters, but a menu allows you to choose different subsets.

- The API Token authentication method and status for each cluster.

- Which clusters are included in or excluded from your personal global searches in Carbon Black EDR Unified View.

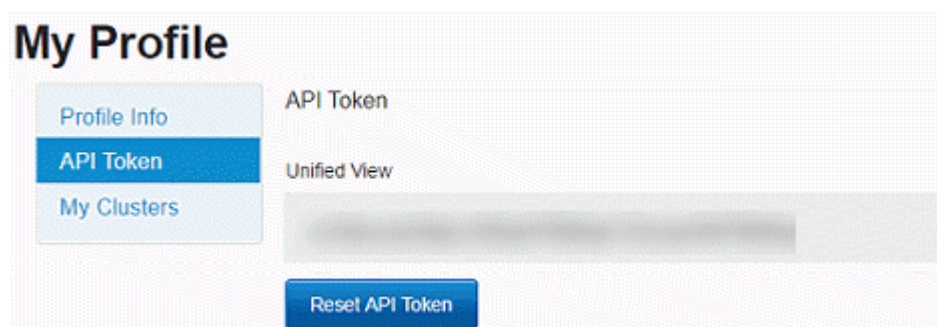**To display the clusters available to you in Carbon Black EDR Unified View:**

1. On the username menu in the upper right of the console, choose **My Profile**.

2. On the My Profile page, click the **My Clusters** link.

3. The My Clusters page appears and, by default, lists all clusters that are included in Carbon Black EDR Unified View.



# Cluster Settings

The Enabled field in the My Clusters list can have the following settings:

- **Enabled switch on (blue and white)** – These clusters are included in your global searches. You can change this setting in My Clusters.

- **Enabled switch turned off (white)** – These clusters are manually excluded from your global searches. You can click the setting to Enabled to add data from this cluster to your searches.

- **Enabled switch deactivated (gray)** – These clusters are excluded from your global searches for one of the following reasons:

  - They are missing an API token to provide cluster access but otherwise available for your global searches. Log in to the cluster itself, obtain the token from your My Profile page on that cluster, and add it to the row for that cluster on the Carbon Black EDR Unified View My Clusters page.

  - They are disconnected from Carbon Black EDR Unified View in Cluster Management and unavailable for any global searches. Connecting or disconnecting a cluster is done on the Cluster Management page and requires Carbon Black EDR Unified View administrator privileges.

The API Token column in the My Clusters list shows one of the following:

- *Shared Token* if an administrator choose this authentication method for the cluster.

- An individual API token string specific to this Carbon Black EDR Unified View user's access to the cluster

- *Enter API Token* if an individual token is required but not yet entered

Shared vs. individual token authentication is determined on the Cluster Management page and cannot be changed on My Profile.

**To enable your Carbon Black EDR Unified View access to a cluster:**

1. While logged in to the Carbon Black EDR Unified View console, choose **My Profile** on the username menu in the upper right of the console.

2. Click the **My Clusters** link.

3. If the API Token field for the cluster you want to add to your Carbon Black EDR Unified View says *Enter API Token*, get an API token from a cluster user (not Carbon Black EDR Unified View) and enter it in that field. The permissions of the user whose API token you are using will determine your access to that cluster and its data.

4. Once you have entered an API token, or if the cluster is configured for a shared token, the Enabled slider shows blue and white (i.e., the button in the slider is on the right) when access is enabled. If that is not the case, click the button to the right to enable cluster access.

After a cluster is enabled on a user's My Profile page, that user has access to the cluster's data during searches and can browse to that cluster through Carbon Black EDR Unified View. These capabilities are subject to privileges of the cluster user whose token was used for authentication. See the managing user accounts chapters in the *VMware Carbon Black EDR User Guide* for details about user permissions.

## Filtering the Cluster List

You can filter the list of clusters in My Profile using the following methods.

- From the drop-down list, select one of the following criteria:

| Setting | Description |
| --- | --- |
| **All available clusters** (the default) | Show all clusters that are available to you for global searches. |
| **Clusters missing API tokens** | Show only the clusters that need an API token to access the cluster from Carbon Black EDR Unified View. |
| **Included clusters** | Show only the clusters that are enabled and included in your global searches. |
| **Excluded clusters** | Show only the clusters that are disabled and excluded from your global searches. |

- In the search box, type the name of a cluster.

    Clusters matching the criteria in the drop-down list, and with a name starting with the characters you type appear in the list. The list of clusters narrows as you type.

# Choose Clusters for Personal Global Searches

All clusters added to Carbon Black EDR Unified View by an administrator are enabled by default for all users with a legitimate shared or individual API token for the cluster. However, each user can limit their global searches to a particular set of clusters by disabling those that they want search operations to skip.

**To customize global searches:**

1. On the username menu in the upper right of the console, choose **My Profile**.
2. Click the **My Clusters** link.
3. Click to enable (include) or disable (exclude) clusters, as appropriate.

## Chapter 6

# Server Configuration Settings

This chapter describes configuration settings for the Carbon Black EDR Unified View server.

**Sections**

# Server Configuration Overview

The Carbon Black EDR Unified View server configuration file is located in `/etc/cb/cb.conf`. The default values are appropriate for any Carbon Black EDR Unified View. You do not need to change them.

> **Note**
>
> The settings shown here are for the `cb.conf` file on the Carbon Black EDR Unified View server itself. The `cb.conf` file for the Carbon Black EDR servers that report to the Carbon Black EDR Unified View server have other settings that are not documented here.

# Global Settings

The following settings control general configuration options for Carbon Black EDR Unified View.

| Name | Description |
|------|-------------|
| `CbUser=cb`<br>`CbGroup=cb` | Service user account and group. |
| `CbFileDescriptorLimit=80000` | Sets the maximum number of file descriptors that each service process is allowed to keep open. |
| `SSLCertFile=/etc/cb/certs/cb-server.crt`<br>`SSLKeyFile=/etc/cb/certs/cb-server.key` | SSL certificate and private key files to be used for HTTPS communications from the sensor to the enterprise server. |
| `SSLUICertFile=/etc/cb/certs/cb-server.crt`<br>`SSLUIKeyFile=/etc/cb/certs/cb-server.key` | SSL certificate and private key files to be used for HTTPS communications from the user's web browser to the Carbon Black EDR Unified View server. |

| Name | Description |
| --- | --- |
| `ManageFirewall=True` | Determines whether the Carbon Black EDR Unified View configuration and setup tools will manage firewall configuration on your behalf. For manual firewall configuration, set this value to **False**.<br><br>**Note:** This was ManageIptables in pre-6.3.0 releases. |
| `ShowGdprBanner` | Determines whether the Carbon Black EDR Unified View console displays a red banner indicating that it is an EU instance and therefore data sharing should be handled with extra care. If True, the banner is displayed. Not included in the default cb.conf file.<br><br>**Note:** Clusters seen in Carbon Black EDR Unified View view Browse Cluster may also show the banner in if it is configured on the cluster itself. |

# Nginx Service Settings

These settings specify configuration options for the Nginx service.

> **Note**
>
> Settings in this section are included so that Carbon Black EDR Unified View server's internal components can read them. However, the Nginx service has a separate configuration file that has a format that prevents sourcing standard bash property files such as this one. Therefore, for any change in this section, you must make the corresponding change in the `/etc/cb/nginx/conf.d/cb.conf` file.

| Name | Description |
| --- | --- |
| `NginxWebApiHttpPort=443` | TCP port on which Web UI/API HTTP endpoint listens. |
| `FlaskSecret=[unique_string]` | Private key for encrypting cookies that the Carbon Black EDR Unified View web API uses. |
| `CSRF_DISABLE=False`<br>`CSRF_COOKIE_NAME=_xsrf_token`<br>`CSRF_HEADER_NAME=X-XSRFToken` | XSRF protection parameters. |

| Name | Description |
|------|-------------|
| `SESSION_COOKIE_SECURE=True` | Toggles the secure flag for the session cookie. If True (the default and recommended setting), requires https. If False, the session will work with either http or https. |
| `FailedLogonLockoutCount=10` | The number of times a user can fail authentication before the account is locked. |
| `AccountUnlockInterval=30` | The number of minutes before a locked account is unlocked. |
| `UserActivityQuota=10000`<br>`UserActivityQuotaDelta=.1` | The threshold at which the UserActivity table is resized, based on the value of `UserActivityQuotaDelta`.<br><br>For example, if `UserActivityQuota` is set to **10000**, and `UserActivityQuotaDelta` is set to **.1**, when the database grows to 11000 it will shrink back to 10000. This ensures that at least 10,000 of the latest records remain available. |
| `SSOConfig=/etc/cb/sso/sso.conf` | Enables a Carbon Black EDR Unified View Server integration that has an external single sign-on (SSO) provider by providing a path to an SSO configuration file. |
| `MaxSyslogSenderMessageSize=1024` | Configures the maximum syslog message size for `cb-unifiedview` syslog notifications. This setting does not automatically adjust the maximum message size setting in `rsyslog` configuration (default 1KB). |
| `MaxCbLoggingMessageSize=2048` | Configures the maximum syslog message size for `cb-unifiedview` log output under `/var/log/cb`. This configuration does not automatically adjust the maximum message size setting in `rsyslog` configuration (default 2KB). |

# PostgreSQL (cb-pgsql service) Settings

These settings specify options for the PostgreSQL data directory configuration.

> **Note**
>
> Carbon Black EDR Unified View server runs its own instance of PostgreSQL on a non-standard port, and this instance hosts the CB database only.

| Name | Description |
|---|---|
| PgSqlDataDir=/var/cb/data/pgsql | Used for storing `pgsql` data. |
| PgSqlPidFile=/var/run/cb/cb-pgsql.pid | Path to the PID file used for `cb-pgsql` service control. |
| PgSqlLogfilePath=/var/log/cb/pgsql/ startup.log | Path to the `cb-pgsql` startup log file, which captures any output that is generated before the logging framework starts up. |
| PgSqlHost="*" | Network interfaces on which `cb-pgsql` listens. Specify **\*** to listen on all available interfaces. You can specify more than one interface by using a comma (,) separator. |
| PgSqlPort=5002 | Listening port for `cb-pgsql`. |
| DatabaseURL=postgresql+psycopg2:// cb:Uc0nllfkyLEVnRmJ@localhost:5002/cb | SQLAlchemy database URL to be used when connecting to PostgreSQL. |

# Redis (cb-redis service) Settings

These settings specify configuration options for the cb-redis service.

| Name | Description |
|---|---|
| RedisPort=6379 | Listening port for Redis (TCP). |
| RedisHost=localhost | Remote IP for creating Redis client (not the listening interface). |

# Carbon Black EDR Unified View Settings

These settings control configuration options that are specific to Carbon Black EDR Unified View.

| Name | Description |
|---|---|
| UnifiedViewEnabled=True | Enables (**True**) or disables (**False**) Carbon Black EDR Unified View. |
| UnifiedViewHost="[::]" | Host name for Carbon Black EDR Unified View server. |
| UnifiedViewPort=5003 | Listening port for Carbon Black EDR Unified View. |
| UnifiedViewHealthCheckInterval=30 | The interval (in seconds) between heartbeats to check that back-end clusters are functioning. |
| UnifiedViewMaxClustersPerMonitor=50 | Maximum number of clusters per health check query. |

| Name | Description |
| --- | --- |
| `UnifiedViewMaxNumberOfDbErrorLogs=50` | Maximum number of error logs to store in the health monitoring database. This is the number of errors displayed in the Carbon Black EDR Unified View console. All errors are logged to the error log. |
| `UnifiedViewStatsAggregationInterval=300` | The interval (in seconds) between calculations for average heartbeat and average query times. |
| `UnifiedViewStatsAggregationToKeep=1440` | The number health status intervals to store. |
| `UnifiedViewRequestTimeout=120  # seconds` | Number of seconds Carbon Black EDR Unified View waits for a response when making a request. |
| `UnifiedViewMaxClusterHealthFailures=5` | Maximum number of failed API calls before a cluster health status is marked red (poor). |
| `UnifiedViewUnstableAvgClusterHeartbeatTime = 5` | The threshold after which average heartbeat time results in a yellow (fair) cluster health status. |
| `UnifiedViewUnavailableAvgClusterHeartbeatTime = 10` | The threshold after which average heartbeat time results in a red (poor) cluster health status. |
| `UnifiedViewUnstableAvgClusterQueryTime = 60` | The threshold after which average query time results in a yellow (fair) cluster health status. |
| `UnifiedViewUnavailableAvgClusterQueryTime = 90` | The threshold after which average query time results in a red (poor) cluster health status. |

# SSL Certificates

The SSL certificates that are used for the Carbon Black EDR Unified View server are stored by default in `/etc/cb/certs`. The `cbinituv` script generates an initial set of certificates. These certificates can be changed to valid certificate authority (CA) certs.

The Carbon Black EDR Unified View configuration file contains two configuration values:

- `SSLCertFile`
- `SSLKeyFile`

## Chapter 7

# Command Line Tools

This chapter describes Carbon Black EDR Unified View command line tools.

**Sections**

# Command Line Tools

Carbon Black EDR Unified View command line tools enable console users with sudo privileges to perform user and cluster tasks on the command line instead of the Carbon Black EDR Unified View console or API.

The following tools are located in `/usr/share/cb`:

* `cbuser` – Manages users for both Carbon Black EDR Unified View server and Carbon Black EDR clusters. See "User Commands" in the following section.
* `cbuv-cluster` – Manages clusters for Carbon Black EDR Unified View. See "Cluster Commands" on page 50.

To get a screen read-out of all options for a command, type the command followed by the `commands` option. For example:

```
cbuser commands
```

# User Commands

For user-specific commands, enter `cbuser` plus one of the following options:

| Options | Description |
| --- | --- |
| get | Queries and displays information about the user who is specified by one of the following arguments:<br>• Username: `-u / --username`<br>  or<br>• User ID: `-i / --id` |
| list | Lists all users in the Carbon Black EDR Unified View server. |
| delete | Deletes the Carbon Black EDR Unified View user who is specified by one of the following arguments:<br>• Username: `-u / --username`<br>  or<br>• User ID: `-i / --id` |
| add | Adds a new user as specified by the following arguments.<br>Required:<br>• Username: `-u / --username`<br>• First name: `-f / --first_name`<br>• Last name: `-l / --last_name`<br>Optional:<br>• Set password: `-p / --password`.<br>  Otherwise, the user is prompted for a password.<br>• Create as Carbon Black EDR Unified View global administrator: `-g / --is_admin` |

| Options | Description |
|---------|-------------|
| set | Changes the specified information about the user in Carbon Black EDR Unified View.<br><br>Name options:<br>• Username: `-u / --username`<br>• First name: `-f / --first_name`<br>• Last name: `-l / --last_name`<br><br>Admin options:<br>• Set as global administrator: `-g / --set_admin`<br>  or<br>• Remove as administrator: `-r / --remove_admin`<br><br>Password options:<br>• Set new password: `-p / --password`<br>  or<br>• Prompt for password: `-P / --prompt_password` |

**Example**:

```
cbuser add -u joe_smith -f joe -l smith -p password -g
```

This adds the user Joe Smith as an administrator who has the specified password to the user store for the Carbon Black EDR Unified View server.

# Cluster Commands

To perform cluster-specific tasks from the command line, enter the command `cbuv-cluster`, followed by one of the following options:

| Options | Description |
|---------|-------------|
| get | Queries and displays configuration information about the cluster that is specified by one of the following arguments:<br>• Cluster name: `-c / --cluster_name`<br>• Cluster ID: `-i / --id` |
| list | Lists all the users from within the Carbon Black EDR Unified View server. |
| delete | Deletes the cluster specified by one of the following arguments:<br>• Cluster name: `-c / --cluster_name`<br>  or<br>• Cluster ID: `-i / --id` |

| Options | Description |
| --- | --- |
| `add` | Adds a new cluster to Carbon Black EDR Unified View using the specified parameters.<br><br>Required arguments are:<br><br>• Cluster name: `-c / --cluster_name`<br>• URL: `-u, --url`<br><br>Optional arguments are:<br><br>• Description: `-d / --cluster_desc`.<br>• Enable SSL verification: `-v / --verify_ssl`<br>• Specify shared token: `-s / --shared_token`.<br>• Otherwise, if the token type for the cluster is shared, the user is prompted for the API token. |
| `set` | Changes information about a cluster in the Carbon Black EDR Unified View according to one or more of the following arguments:<br><br>• Cluster name: `-c / --cluster_name`<br>  or<br>• Cluster ID: `-i / --id`<br>• URL: `-u, --url`<br>• Description: `-d / --cluster_desc`<br>• Token type: `-t / --token_type`, where *token_type* is either `individual` or `shared`.<br>• Enable the cluster: `-e / --enable`<br>  or<br>• Disable the cluster: `-d / --disable`<br>• Enable SSL verification: `-v / --verifiy_ssl`<br>  or<br>• Disable SSL verification: `-n / --no_verify_ssl` |

**Example**:

`cbuv-cluster get -c acme`

Retrieves and displays configuration information about the cluster named acme.