Carbon Black.

CB Protection
Server Installation Guide

Product Version: 8.1.10

Document Date: June 2020

Copyrights and Notices

Carbon Black, Inc. acknowledges the use of the following third-party software in the CB Protection product:

Portions of this software created by gSOAP are Copyright © 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved. See **Note 1** below for additional details.

This product includes PHP, freely available from http://www.php.net. Copyright © 1999 - 2015 The PHP Group, All rights reserved. See **Note 1** below for additional details.

Portions of this software use Info-ZIP, copyright (c) 1990-2007 Info-ZIP. All rights reserved. For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals: Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White. This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions: 1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions. 2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled. 3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions. 4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

About This Book

This preface describes the contents of this publication, *CB Protection Server Installation Guide*.

Sections

Intended Audience

This manual provides information for system or network administrators who will install the CB Protection Server software and other components of CB Protection. Staff who install the software should be familiar with networking concepts and have experience with the Windows operating system and SQL Server management. In addition, if your site will use features that integrate the CB Protection Server and Active Directory, administrators and installers should be familiar with Active Directory concepts and use.

The CB Protection Agent can be installed on Windows, Mac/OS X, and Linux operating systems, so the installer or administrator responsible for installing and managing agents should be familiar with installing software on the supported client systems at your site.

Chapter Overview

CB Protection Server Installation Guide is your guide to the installation and initial configuration of the server. It is organized as follows:

	Chapter	Description
1	Preparing for Server Installation	Provides an installation overview and background information helpful to know before you begin installing the CB Protection Server.
2	Installing the CB Protection Server	Explains how to install (or upgrade) and start the CB Protection Server software.
3	The CB Protection Console	Explains how to log in to the CB Protection Console.

Notes

- This guide, which focuses on CB Protection Server installation, does not include full instructions for installing third-party products, such as Windows Server, SQL Server, or products and services integrated through the CB Protection Connector. For any third-party product that you install separately for use with CB Protection, see the documentation that came with the product.

- Instructions for uploading agent installers to the server and installing the CB Protection Agent on computers to be managed by the CB Protection Server are in the "Managing Computers" chapter in the *CB Protection User Guide* guide. This is available as both online help from the console and as a PDF file.

Other CB Protection Documentation

You will need some or all of the following documents to accomplish CB Protection tasks not covered in this document. They are available on the Carbon Black User Exchange.

Some of these documents are updated with every new released build while others are updated only for minor or major version changes:

- **Operating Environment Requirements** – Describes the hardware and software platform requirements for CB Protection Server, the SQL Server database that stores CB Protection data, and the CB Protection Agent.

- **SQL Server Configuration** – Describes some of SQL best practices as well as pre- and post-installation tasks that are necessary to ensure proper database operation.

- **CB Response sensors & CB Protection agents** – Describes the currently supported agents and the operating systems on which they are supported.

- **CB Protection User Guide** – Provides full information about configuring and operating the CB Protection Server and instructions for deploying and managing agents.

- **CB Protection Release Notes** – Provide information about new features, corrective content, and known issues with that release. These documents are specific to the version and build of CB Protection Server or agent. See:
  - CB Protection Server Release Notes
  - CB Protection Windows Agent Release Notes
  - CB Protection Linux Agent Release Notes
  - CB Protection Mac Agent Release Notes

- **CB Protection Events Guide** – Provides a detailed inventory of events recorded by the CB Protection Server and includes instructions for integrating event data with third-party SIEM systems via Syslog.

- **CB Protection API documentation** – Documentation for the CB Protection REST API can be found at https://developer.carbonblack.com/reference/enterprise-protection. See Appendix B, "CB Protection API," in *Using CB Protection* for more information about Carbon Black API documentation.

In addition to the documents listed above, the User Exchange includes other, more specialized documentation that may be of use in planning or maintaining your CB Protection Server installation. Use the "Documentation and Downloads" button on the CB Protection page in the User Exchange to search for these documents.

Community Resources

In addition to being a source for user documentation, the Carbon Black User Exchange website at https://community.carbonblack.com provides access to information shared by Carbon Black customers, employees and partners. It includes information and community participation for users of all Carbon Black products.

When you login to this resource, you can:

- ask questions and provide answers to other users' questions
- "vote" to bump up the status of product ideas
- download the latest user documentation

- participate in the Carbon Black developer community by posting ideas and solutions or discussing those posted by others
- view the training resources available for Carbon Black products

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

Contacting Support

Please view our Customer Support Guide on the User Exchange for more information about Technical Support:

https://community.carbonblack.com/t5/Support-Zone/Guide-to-Carbon-Black-Customer-Support/ta-p/34324

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

- **Carbon Black 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 call or e-mail technical support, please 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.
Problem	Action causing the problem, error message returned, and any other appropriate output
Problem severity	Critical, serious, minor, or enhancement

Contents

Chapter 1

Preparing for Server Installation

This chapter provides an installation overview for CB Protection, including preparation requirements. This document also includes instructions for upgrading CB Protection from a previous version. You may receive additional upgrade documentation from your Carbon Black Support representative, and, if so, you should have it available for the upgrade process.

The separate *Operating Environment Requirements* document for this release provides guidelines for hardware and software required for CB Protection. Your environment must meet these requirements before you begin the procedures described in this document.

The CB Protection Console includes a System Health Page that provides reports on the state of your system. A prime purpose of these indicators is to monitor compliance with the Operating Environment Requirements and report any non-compliance so that you can remedy it. See "Monitoring System Health" in *CB Protection User Guide* for more information.

Sections

About the CB Protection Distribution

Carbon Black supplies the CB Protection installation program as a download. New sites will also receive a license key to be used during installation.

Table 1: CB Protection Distribution Contents

Contents	Description
CB Protection Software	The CB Protection server installation files. **Note:** You upload CB Protection Agent installers packages from the Carbon Black User Exchange after the server is installed.
Documentation	The CB Protection Console includes online Help describing product features and procedures, including how to install the agent on endpoints. You can view the Help contents page by clicking the question mark button in the top right in the main console menu. *Context-sensitive help* can be launched by clicking the question mark button lower on the page in the panel for a particular console page. PDF versions of this and other user documentation can be downloaded by logging to the Carbon Black User Exchange.

License Keys

CB Protection can be licensed at two primary feature levels:

• **CB Protection Visibility:** This level provides all of the CB Protection file and event tracking and reporting capabilities, but does not include support for control features such as file bans and device blocking.

• **CB Protection Suite:** This provides both Visibility and Control capabilities.

Licenses are based on the number of agents running at each level. You can mix licenses on the same server, having, for example, 20 Visibility licenses and 50 Suite licenses. In addition, you can purchase upgrades to bring Visibility licenses up to full Suite level.

> **Important**
>
> During a new server installation, you will be prompted for a license key. Have this key available before you begin installation. A new installation completed without a license key is a full-featured, 7-day evaluation version (without special options). You can add or upgrade a license key after installation, on the System Configuration page of the CB Protection Console.

Upgrade installations and reconnections to existing CB Protection databases do not require a new license key for completion, but if one is provided by Carbon Black, apply it during the installation process. For instructions on adding licenses after installation, see the "System Configuration" chapter in the *CB Protection User Guide* guide or online Help.

Licenses for Optional Features

In addition to determining the number of licensed agents and their mode, the license key can add optional features to your CB Protection installation, including the CB Protection Connector for Network Security Devices and the File Upload feature. To use these features, be sure to obtain the correct license.

Installation Overview

CB Protection includes server and agent components. You install the server software on standard Windows-Server-based computers, and it can be run on a virtual machine. The server installation procedure handles all operating system configuration except for IIS, for which you must follow the configuration in the *Operating Environment Requirements* for this release.

You can install agent software on server, desktop, and laptop computers, and on POS (point-of-sale) systems; it may be installed on Windows, Mac, and Linux systems that meet the requirements in the *Operating Environment Requirements* document for this release and the relevant listings in *CB Response sensors & CB Protection agents* on the User Exchange. The agent provides security rules to endpoint computers and enables connected systems to interact with the CB Protection Server for ongoing management.

> **Note**
>
> Agent installers are created through a two-step process:
>
> - Agent installer and rule packages are available on the Carbon Black User Exchange and must be uploaded to the CB Protection Server.
> - Once the installer package is on your server, separate downloadable agent installers are created dynamically for each security policy configured on your server.
>
> Instructions for uploading agent packages and installing agents appear both in the "Managing Computers" chapter of the *CB Protection User Guide* guide (online help and PDF versions).

A CB Protection Server installation follows these summary steps:

Step 1: Determine your appropriate hardware and database configuration.

The CB Protection Server and its database may be set up on a single system. Depending upon your own preferences and the number of clients you will manage with CB Protection, you may require a dedicated system for a database server and/or for a Syslog server. You also may install the server and agents in a virtualized environment. See the *Operating Environment Requirements* document to determine the right choices for your environment.

Step 2: Procure the required hardware for the CB Protection Server.

Step 3: Install Windows Server, IIS, and .NET on the CB Protection Server hardware.

Use a clean, US English Windows Server installation with all the latest patches from Microsoft. Then install the Internet Information Services (IIS) version supplied with your Windows Server, using the configuration described in the *Operating Environment Requirements* for this release. Also, make sure that Microsoft .NET Framework 4.5.2 (or later) is installed with the default settings and the latest patches.

Important: The Carbon Black Collective Defense Cloud (CDC), which provides file trust and threat information and allows automatic updates of certain rules, requires a TLS 1.2 connection from the CB Protection Server. If you intend to connect to the CDC, use of .NET 4.6 (or later) is recommended. Earlier versions of .NET will default to pre-TLS-1.2 protocols, and this will prevent a CDC connection unless you disable those older protocols. Disabling older TLS/SSL protocols may be a security issue for connections to other services from your CB Protection Server.

Step 4 - option 1: Install your own licensed copy of SQL Server (US English) on the same system *before* you install CB Protection.

Follow the SQL Server configuration instructions in the *Operating Environment Requirements* and *CB Protection SQL Server Configuration* documents. In particular, note whether the number of endpoints you plan to manage requires the use of option 2. The SQL Server must be a US English version.
- or -

Step 4 - option 2: To use a remote database server, procure the hardware, operating system, and your own licensed copy of SQL Server, then prepare the system.

Connect the SQL Server hardware to the CB Protection Server hardware by a minimum latency, gigabit backbone. The SQL Server must be a US English version.

Step 5: Install and configure the CB Protection Server software.

The installation procedure is described in this document. Configuration is described in *Using CB Protection* (in console help and PDF versions).

Step 6: Upload the CB Protection rule and agent installer packages to the server and install agents on endpoints.

See *CB Protection User Guide* (in console help and PDF versions) for these procedures.

SQL Server Account Configuration

The user account that will access a remote CB Protection database should have the following permissions:

Permission	Required	Reason
Create Any Database	Yes, during installation.	This permission is required during product installation, and can be revoked after installer finishes.
View Server State	Yes	Allows collection of CB Protection Server performance statistics
View Any Definition	Yes	Allows collection of CB Protection Server performance statistics
Alter Trace	Yes	Allows collection of on-demand SQL trace for performance diagnostics
Alter Server State	No (Recommended)	Allows server to reset performance counters on daily basis, and provides better performance diagnostics

Note that many of these permissions allow server metrics to be collected by Carbon Black for monitoring of the internal health of the server and to provide diagnostics in case of SQL database issues. This information is very important in helping Carbon Black support your server installation, and also provides server performance data that may contribute to future product improvements. Contact your Carbon Black representative if you would like more information about data collection from your server.

In addition to the permissions shown in the table, the CB Protection service account must remain **db_owner** after the server is installed.

SQL Server Memory Configuration

If you are using a single-tier configuration (CB Protection Server and SQL Server on the same system), you should configure the SQL Server to use shared memory for the connection to gain the maximum performance benefit of the single-tier archictecture. Use of TCP introduces unnecessary latency into the system.

Follow these configuration guidelines to make the SQL Server use shared memory for its connection to the CB Protection Server when they are on the same machine:

- Do not use a FQDN to specify the SQL Server name – it causes the server to use TCP for the connection. To make the SQL Server connection use shared memory instead, use a local server name.

- Make sure that Shared Memory protocols are enabled for both network and client configuration in the SQL Configuration Manager.

Installing the Platform Software

Follow these guidelines for installing or upgrading platform software for the CB Protection Server:

1. Ensure that the server is a dedicated, trusted computer that uses the NTFS file system, not FAT or FAT32.

2. If you are repurposing another computer to use as the CB Protection Server, reformat the disk. During reformatting, select NTFS (the default file system).

> **Important**
>
> - Commercial servers commonly bundle vendor-specific server-management utilities with Windows Server. If you install the CB Protection Server on a server platform that is bundled with such utilities, there might be unexpected interactions between them.
>
> - If you intend to use any server-hardening procedures on this server, contact Carbon Black Support to confirm that the CB Protection Server will run in the environment you create.
>
> - Apply server-hardening procedures *before* installing the CB Protection Server.

3. If the operating system is not preinstalled, follow the standard Microsoft instructions for installing it. Be sure you are using the US English version. Carbon Black recommends that you select the default installation options.

4. If you have a network domain and you want to use the CB Protection Server's Active Directory integration, add the server to the domain.

5. Install Internet Information Services (IIS) — you may need the Windows Server media. See "Web Server Configuration" on page 15 for the required IIS configuration.

> **Important**
>
> Once IIS is installed, you cannot change the server name and still have IIS function correctly. If you need to change the server name for any reason, contact Carbon Black Support.

6. If you currently have an earlier version of Windows than those listed in the CB Protection *Operating Environment Requirements* document for this release, upgrade to the required version and service pack.

7. Install Microsoft .NET Framework 4.5.2 (or later) on the CB Protection Server. If necessary, go to http://www.microsoft.com/downloads and choose the latest version for download. To avoid TLS mismatch issues, version 4.6 or later is recommended if you intend to connect to the Carbon Black Collective Defense Cloud (CDC).

8. Download and install any current patches for each element of the platform software.

9. If you are running AppLocker on the system where the CB Protection Server will be installed, either temporarily disable AppLocker or be sure it uses only default rules. If AppLocker is configured with customer-specific rules, the server installation could fail. An AppLocker-related installation failure is reported as an "unknown error," and install logs (or debug view) show that installer was not able to expand its own installer files in the temp folder and wasn't able to execute the "unzip.exe" utility.

Network Requirements

See the *Operating Environment Requirements* document for full network details. In addition to the requirements described there:

*   If you intend to use the Active Directory integration features of the CB Protection Server, the server must be a member of a domain. See the *CB Protection User Guide* guide for more information on Active Directory integration features.

*   Carbon Black recommends that your server have access to a remote network share for backup purposes, or that you make other reliable backup arrangements.

Web Server Configuration

The CB Protection Server works with the following configurations:

*   IIS 7.5 on Windows Server 2008 R2
*   IIS 8.0 on Windows Server 2012 R2
*   IIS 10 on Windows Server 2016
*   IIS 10 on Windows Server 2019

Do a clean IIS installation before you install the CB Protection Server. In normal use, the web server starts at boot time. The CB Protection Server does not support substitution or co-installation of any other web servers.

Configure the IIS Roles Manager according to the instructions in the *Operating Environment Requirements* for this release.

> **Notes**
>
> Once IIS is installed, you cannot change the server name and still have IIS function correctly. If you need to change the server name for any reason, contact Carbon Black Support.

Supported Web Browsers

You access CB Protection features through a Web-based user interface called the console. Although other browsers with HTML frame support should work, these CB Protection-certified browsers are recommended:

- Microsoft Internet Explorer Version 11.0 or higher
- Mozilla Firefox latest version
- Chrome latest version
- Safari version 13 (on macOS or OS X only)

Browser Configuration

All browsers must be enabled for JavaScript to access to the console and online Help.

In Internet Explorer, you may need to adjust your overall security settings or set the CB Protection Console address to be part of your Local Intranet or Trusted Sites zone in order to access the console. The security settings are accessed by choosing **Tools > Internet Options** in Internet Explorer and clicking on the **Security** tab.

Data Export Options

CB Protection provides data export options including:

- downloadable reports in CSV format, read-only views into certain elements of the database
- Syslog messaging that exposes relevant event data and statistics for programmatic analysis
- logging of CB Protection events to an external SQL Server
- external views into the database (Live Inventory SDK)
- export of events and other data to third-party analytics platforms, such as Splunk

See the separate manual, *CB Protection User Guide,* for more information on these topics (also available as online console help). See the *CB Protection Events Guide* for more on exports of event data to syslog.

Chapter 2

Installing the CB Protection Server

This chapter explains how to install or upgrade the CB Protection Server. When you have successfully completed the server installation procedures, see "Managing Computers" in the *CB Protection User Guide* guide (or online help from the CB Protection Console) for agent installation and upgrade instructions.

Sections

Pre-installation Check

Before installing the CB Protection Server, ensure that:

- the server on which you will install it meets the requirements in the *Operating Environment Requirements* for this CB Protection release.

- IIS is installed and configured as described in the *Operating Environment Requirements* for this release.

- SQL Server is installed according to the requirements in the *Operating Environment Requirements* for this CB Protection release.

- If you are running AppLocker on the system where the CB Protection Server will be installed, you have either temporarily disabled it or made sure it uses only default rules.

Important

- **Install SQL First** -- SQL Server must be installed *before* you install the CB Protection Server. See the separate *Operating Environment Requirements* document for information about supported versions and configuration of SQL Server. Have the SQL Server location, instance (if any), and login information available during CB Protection Server installation.

- **Authentication** -- During installation, you will have a choice to use Windows authentication or SQL authentication to configure access to the SQL Server by the CB Protection Server. Carbon Black strongly encourages using a specific Windows Domain account for installing and logging in to the CB Protection Server, and using Windows authentication for database access. For either authentication method, the account you use to access the database must be added to SQL Server with "sysadmin" checked in the Server Roles.

If you use dedicated SQL Server hardware, the CB Protection Server installer also installs the required SQL Server drivers locally on the CB Protection Server machine. The drivers installed are from SQL Server 2008 R2 and should be able to communicate with the any of the supported SQL Server versions listed in the *Operating Environment Requirements*.

Installing the Cb Protection Server Software

The server installer uses standard installation dialogs. During installation, you specify system configuration information for the server and optionally provide your own web-server certificate. You must log in as a Windows administrator to install the CB Protection Server.

The system on which you install the server must have an IP address that is visible to all computers running the CB Protection Agent, with a fully qualified DNS domain name or alias. In addition, to use Active Directory integration features without special configuration, the CB Protection Server must be installed in the same AD forest as:

- users you plan to allow CB Protection Console access via their AD login

- computers and users whose AD information you plan to use for automatic security policy assignment

> **Important**
>
> If you need to have the CB Protection Server in a different AD forest than computers and users you want to use in CB Protection integrations, contact Carbon Black Support for special instructions.

If you are installing a completely new CB Protection Server, follow the steps in "Installing a New Cb Protection Server" on page 20.

If you are installing new CB Protection Server software with a backup database from a previous version, skip to "Installing the Server with a Restored or Reconnected Database" on page 33.

If you are upgrading from a previous version of the CB Protection Server (including Bit Platform and Parity Servers), skip to "Upgrading from a Previous CB Protection Version" on page 45. You also might receive a supplemental document with newer instructions for an upgrade from your Carbon Black Support representative.

> **Important**
>
> Several CB Protection Server administrative features are disabled by a reinstallation or upgrade of the server. When an upgrade installation is complete, log in to the console and re-enable the ones you use:
>
> - System backup is disabled. To re-enable, go to the Advanced Options tab on the System Configuration page.
>
> - Automatic upgrades of agents are disabled. To re-enable, go to the Advanced Options tab of the System Configuration page. This should be done only after determining and configuring an upgrade plan that avoids excess load on the server and network. You should also check the Carbon Black User Exchange for new agent and rule versions to upload to your server.
>
> - See "Review Post-Upgrade Server Configuration" on page 50 for more details about re-enabling features after an upgrade.

Installing a New Cb Protection Server

These instructions are for a completely new installation of CB Protection, with a new database (no restorations of or reconnections to an existing database).

To install a new CB Protection Server:

1. Log in using an account with local Windows administrator credentials. If you plan to use Windows Authentication to login to a remote CB Protection database, install the CB Protection Server using an account that has been added to SQL Server with "sysadmin" checked in the Server Roles. Carbon Black strongly encourages using a specific Domain account for installing and logging in to the CB Protection Server, and for database access, to simplify control of both database and Active Directory permissions.

> **Important**
>
> Do not change the privileges of the account used to install the server after installation. This account must continue to have local administrator privileges for the server to function properly, and will also be used for server upgrades.

2. Make the server installation file available to the installation computer (either by download or inserting media in an accessible location).

3. Run the installer in either of the following ways:

    a. To install on a local server, double-click the `ParityServerSetup.exe` file to start the installation program. Continue to the next step.

    b. To install from a remote desktop, copy the `ParityServerSetup.exe` file to the installation computer and execute the file.

4. If the installer detects that required Microsoft redistributable packages are not present, a dialog box listing those packages appears. Click Install on the dialog to install the packages and continue with the CB Protection installation.
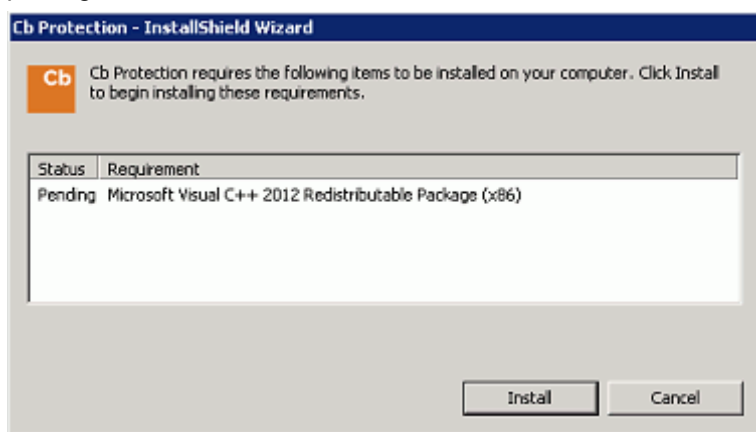
If no missing packages were detected, or when the installation is completed, the Welcome dialog appears.
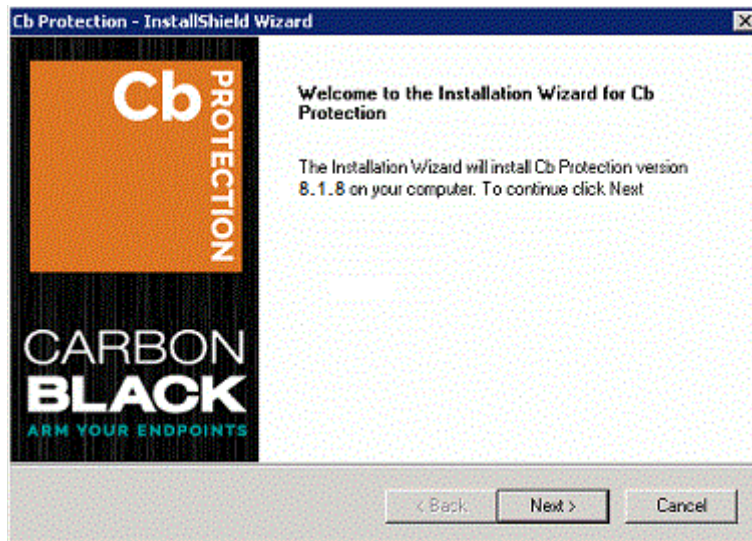
5.   On the Welcome page, click **Next**. The License Agreement screen appears.
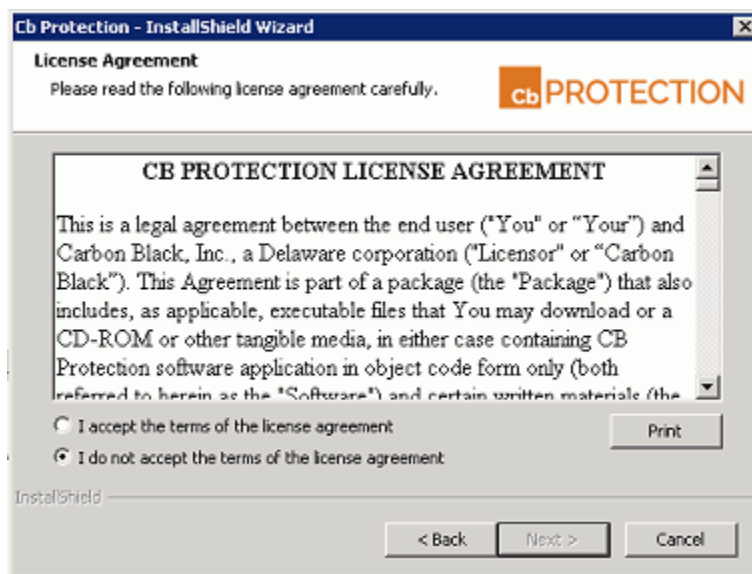
6.   Review the software license agreement. You must agree to the license terms to install the CB Protection Server. When you click **I accept** and continue, you agree to all terms of use. To continue, click the **Next** button. The Select Features dialog appears.
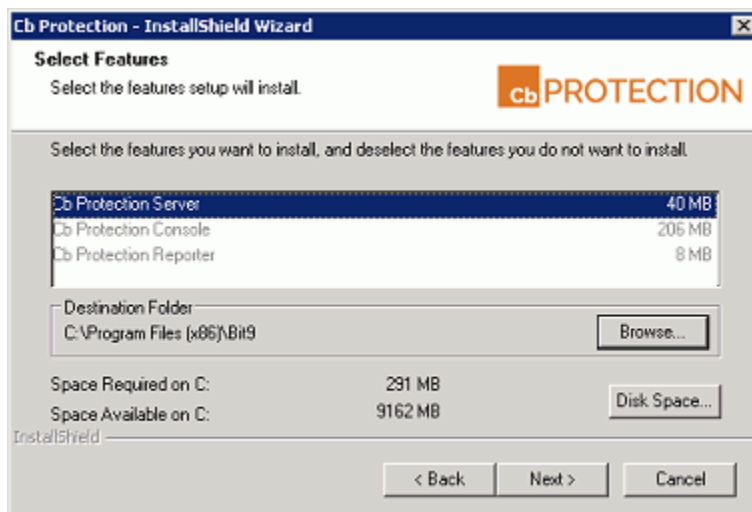
7. The Select Features screen provides information about the CB Protection features being installed, the installation folder, and the space required and available for installation:

   a. CB Protection Server, CB Protection Console, and CB Protection Reporter are always installed — they cannot be deselected. The console is the web interface to the server. The reporter is the service that connects the server to CB Collective Defense Cloud, which provides access to a database of information about files and threats. Reporter, which runs as a Windows service, also provides other essential reporting capabilities, including collection of support information for the server.

   b. Either keep the default installation folder (which differs from 32-bit to 64-bit systems) or click **Browse** and navigate to the folder in which you want to install the server. If you don't choose the default, use a path that has only valid ASCII characters, not Unicode. When you have chosen the folder, click **Next**.

   Note

   At this point in the installation, the installer program checks to be certain that it can write to the folders and registry locations needed. If any issues are found, they (and their paths) are listed in a dialog, and you must resolve them before continuing the CB Protection installation.

8. The Database Server screen appears next. It includes two configuration choices:
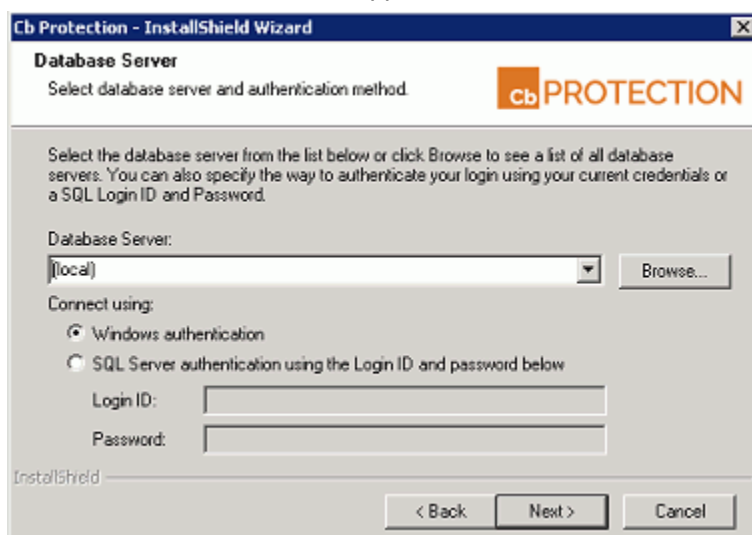
    a. In the Database Server field, enter the name of the SQL server, and (if any), its instance name, you are using for CB Protection data. If the SQL Server and CB Protection Server are on the same system, use a local name (not an FQDN) to allow use of shared memory for the connection between the two. See "SQL Server Memory Configuration" on page 14 for more details.

    b. With the Connect Using radio buttons, choose Windows Authentication (i.e. with the user doing the CB Protection installation) or SQL Server Authentication. If you choose SQL Server Authentication, provide the Login ID and Password. Your choice here determines how access to the SQL Server by CB Protection will be authenticated, both during and after the installation.

    c. When you have entered all database information, click **Next**.

    Note: For either authentication method, the user must have been given the "sysadmin" Server Role in SQL Server.

**9.** The CB Protection Database Configuration Options screen appears next.
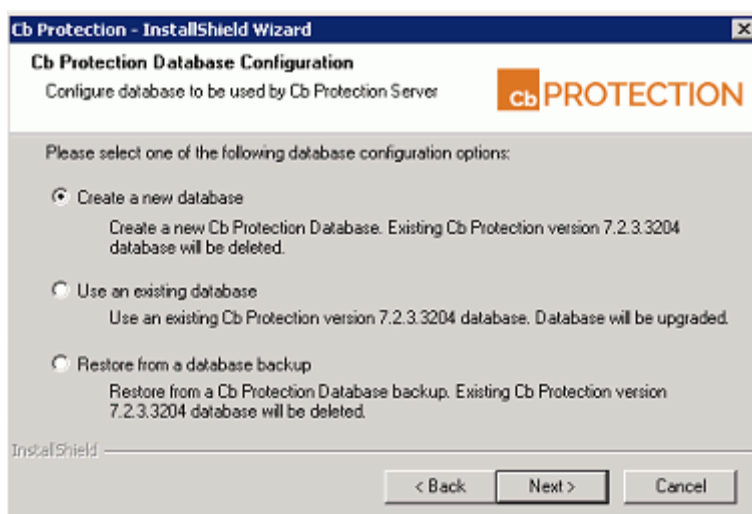
On this dialog, choose **Create a new database** if you are installing the CB Protection Server for the first time, then click **Next**.

> **Note**
>
> The other database configuration options, *Use an existing database* and *Restore from a database backup*, are described in "Installing the Server with a Restored or Reconnected Database" on page 33.

10. On the Logon CB Protection Server As screen, choose the logon account to be used by the CB Protection Console. This will also be the account used to install future patches and upgrades. You can choose one of two modes of logging in:
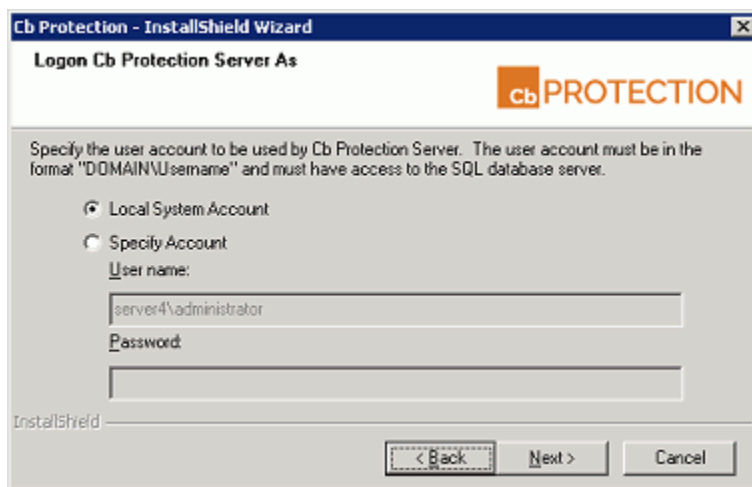
a. The Local System Account radio button instructs the installer to configure CB Protection to use the built-in Windows System account.

b. The Specify Account radio button activates the Username and Password fields so that you can provide account information. As the screen notes, the account you provide must be in the format DOMAIN\Username and have full access to the SQL database server. The default for this choice is the currently logged in user. You cannot use "\Username" without a domain or a dot before the backslash.

> **Notes**
>
> • Carbon Black strongly encourages using the Specific Account option to simplify control of database and Active Directory permissions. In general, the installer should be run by this same Domain account.
>
> • For local SQL Server Express databases, the currently logged in user *must* be the same as the user specified in the Logon Information installation dialog, and the user must have the "sysadmin" Server Role. If you enter a different user, an error message appears and you must re-enter the current user.
>
> • To use a Domain account to access a *remote* SQL database, you must use that account to run the installer and enter it as a Specific Account in the dialog above. The account must have the "sysadmin" Server Role in SQL Server. Use of an invalid login account causes server installation to fail later in the process; you will need to reinstall.

c. When you have provided logon information, click **Next**.

11. The Server Configuration Options screen appears next.

From the Server Configuration Options screen, review the configuration settings. In the Server Address field, the preferred address for the server is a fully qualified DNS name or alias that is resolvable by all computers running CB Protection Agent. Although not recommended, if the server is assigned a static IP address that will not change at reboot time, you can keep the default IP address selected for the server. The installation program automatically supplies the correct information for the installation computer. The Console Port, which is used for communications between the server and its browser console, is 41001. The Agent Port, which is used for SSL communication with CB Protection Agents, is 41002.

Notes

- Carbon Black strongly recommends the use of a fully qualified DNS name or alias for Server Address whenever possible. Use of a CNAME (alias) may provide more flexibility and reliability.

- If you use multiple NICs, make sure the FQDN you use in the Server Configuration screen refers to the address of the card(s) you want the agents to connect to.

- An SSL certificate is automatically generated to protect communications between the server and its agents. If the Common name of the server does not match the server name configured here, server and agents will be unable to communicate correctly. After installation is complete, you can replace this certificate with an existing certificate on the **Security** tab of the **System Configuration** page in the console.

After reviewing the server configuration and made any necessary changes, click **Next**.

12. If you chose Specify Account in the (CB Protection Server) Logon Information screen (step 10), another Logon Information screen appears next, for *Login for Console Application*. This screen allows you to specify different user credentials to start the IIS process for CB Protection Console, the web-based user interface for the server.

a. Choose **Local System Account** to configure the server to use the built-in Windows system account to start the IIS process for the console.

b. Choose **Specify Account** to activate the Username and Password fields so that you can provide account information. As the screen notes, the account you provide must be in the format DOMAIN\Username. You cannot use "\Username" without a domain or a dot before the backslash.

> **Note**
>
> If you use an account other than the current user, a warning dialog will be shown: "The CB Protection Server installer is unable to validate whether the specified account is able to access the SQL database server. Are you sure you want to continue?" If you are certain the account you provided is valid, choose **Yes**.

c. Click **Next**.

13. The CB Protection Console (IIS) Certificate screen appears next. Choose the digital certificate that will appear to CB Protection Console users. You either create a certificate using a template provided by Carbon Black or substitute your company's certificate.
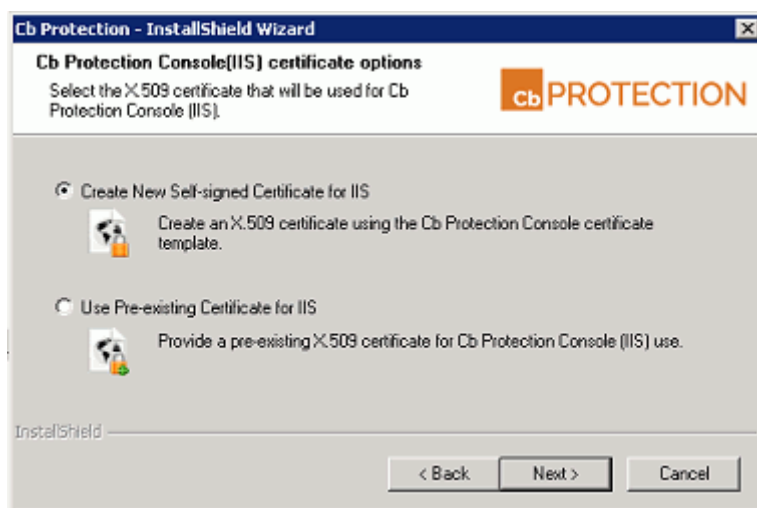
a. If you do not have your own certificate, choose **Create Certificate**. This allows you to create a Carbon Black self-signed certificate. You can either leave Carbon Black's default information or supply certificate information that identifies your own organization instead. Self-signed certificates will generate warning boxes when you log in to the CB Protection Console using Internet Explorer or Firefox, although Firefox will allow you to permanently accept the certificate to eliminate future warnings. To create a certificate, choose **Create Certificate**, click the **Next** button, and skip to Step 14.

b. To substitute your own certificate, choose **Use Pre-existing Certificate**, click the **Next** button, and skip to Step 15.

Notes

- The Carbon Black self-signed certificate cannot be universally trusted because it is not created through a trusted provider such as Verisign or Thawte. This is why it generates a warning on login. While this doesn't interfere with CB Protection operation, you may want to acquire your own, trusted certificate to avoid the warning.

- Self-signed certificates with a validity period greater than 20 years are not usable. If necessary, create and use a new certificate with a shorter validity.

14. If you chose Create Certificate, the Create X.509 Certificate screen appears.

a. By default, all certificate details correspond to Carbon Black name and address data. Please replace them with details of your company. The default password is 'password'. Carbon Black recommends that you change it, and keep a record of your new password so it can be retrieved for later use. The Common Name field defaults to the IP Address or DNS Name of the server; it cannot be changed. If the server is reachable by multiple DNS names, you can use the Subject Alternate Name field to specify the alternate names.

When the certificate is validated against a computer, it is validated against a Common Name or one of the Subject Alternative Name entries (if they exist). If both are present, names in the Subject Alternative Name field have priority.

b. When all fields are filled in as you want, click **Next** to create the certificate and move to the License Key screen (step 16).

15. If you chose Use Pre-existing Certificate, the Use Pre-existing X.509 Certificate screen appears. Enter the required information:

a. Click the **Browse** button next to the *Enter Certificate File* field, navigate to the PFX (PKCS.12) certificate file you want to use, and click **Open** when you have located the file. The filename appears in the certificate file box.

b. Enter the password for the certificate, and re-enter it in the confirmation field.

c. When you have entered the certificate file and the passwords, click **Next** to validate the certificate file with the password.
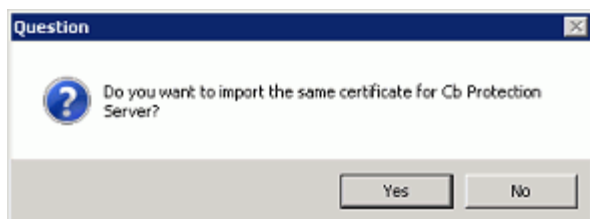
d. A dialog box appears allowing you to use the same certificate for Agent-Server communications. Choose **Yes** to use the same certificate or **No** if you want the CB Protection installer to generate a different, self-signed certificate for Agent-Server communications (you can modify this certificate or choose a new one through the CB Protection Console later). After you make your choice, the License Key screen appears.

16. On the License Key screen, you enter the license key provided by Carbon Black. This key determines how many agents you can run at each of the two fundamental feature levels: Visibility-Only or Visibility-and-Control. It may also include permission for optional features.
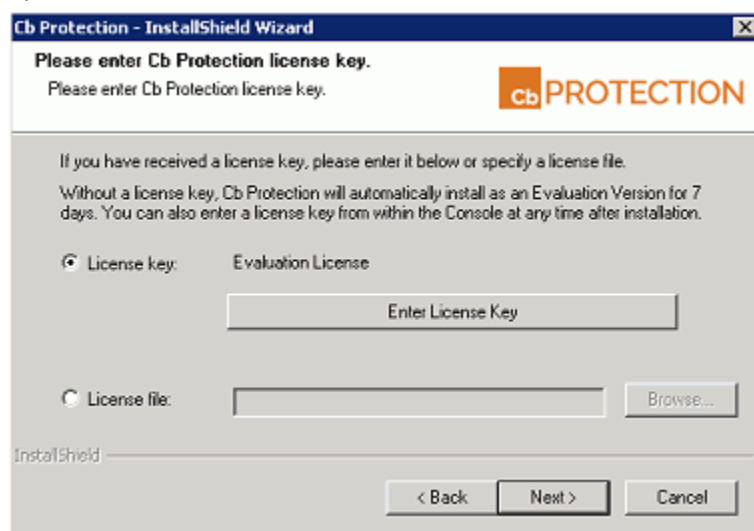
You have two options for entering the key:

a. Click the *License key* radio button to cut and paste the license key into a window (for example, from an email message or other communication).
   -or-
   Click the *License file* radio button to provide the name and path to a license file containing the key. License key files have the file extension **.lic**. When you click this radio button, the Browse button is activated so that you can locate and select the license file using the standard Windows Choose File dialog.

> **Note**
>
> If no license key is entered here, the server is installed with a 7-day evaluation license. After installation, you can update the license at any time from the System Configuration page of the console.

b. When you have provided either the license key text or a license file, or have chosen not to enter a key, click **Next**. The CB Protection Agent Management screen appears.

17. On the CB Protection Agent Management screen, you can enable global access to agent management commands used for diagnostics, recovery, and other special situations. Although you can configure this after installing the server, it is highly recommended that you configure this feature before installing agents since your choice (or lack of one) is built into the agents when you install them. It is especially important to set up a global access method if you will have agents that are offline frequently or at all times. The choices are:

a. Specify a global password for managing agents: Check this box, then enter and confirm a password, if you want to enable access to agent management commands on all agents via a single password. Password must be between 1 and 64 characters long, be in the ASCII character set, and must not contain the following DOS special characters: | > < & % ( ) @ . [ ] { } : ; ^ = ! ' " ` ~ ,

b. Specify a user or group allowed to manage agents for each platform (Windows and Mac are supported at this time): Check this box if you want to enable access to agent management commands by choosing a pre-defined group from a menu (for Windows) or by entering a user or group name used at your site. Provide a user or group for each agent platform you have in your environment.

> **Notes**
>
> - If you define both a user/group and a password, *either* access method is sufficient on its own.
>
> - If you plan to manage clients from computers running Vista or Windows 7, use of pre-defined Windows groups for access privileges is not recommended because Windows UAC may not provide the expected membership in a group.
>
> - See "Configuring Agent Management Privileges" in the *CB Protection User Guide* guide for more information about configuring agent management access.

    c. Click **Next**. The Ready to Install screen appears.

18. If you are satisfied with your installation choices, click the **Install** button on the Ready to Install screen:
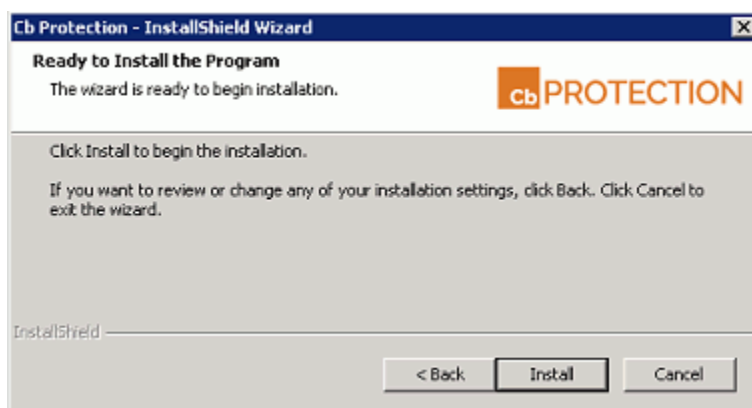
19. CB Protection Server installation begins. There is a status box overlaying the main dialog to show the progress of SQL script execution. The main dialog also has a status indicator for the overall installation.
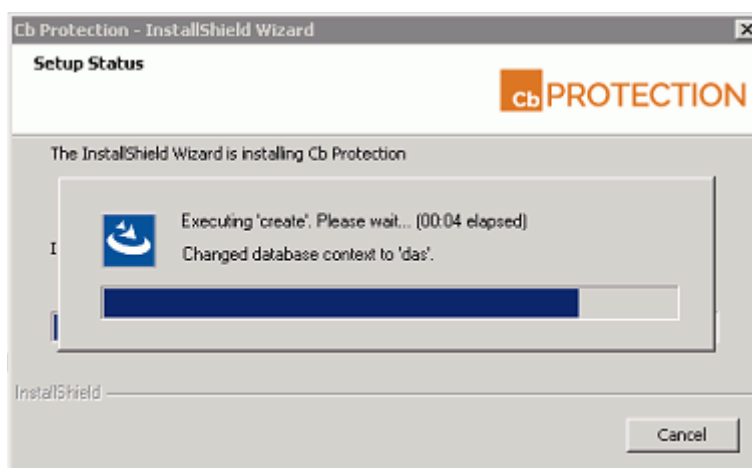
20. When the InstallShield Wizard Complete screen appears, the installation is complete.

    a. In some cases, you will need to restart the server computer after installation is completed, and the dialog will include an option to restart now. Choose to restart now unless you need to complete some other activity on this computer.

    b. Click the **Finish** button. CB Protection Server, which runs as a service, begins to operate after you click this button. Installation logs are placed in the CB Protection installation folder (for example, *C:\Program Files (x86)\Bit9*).
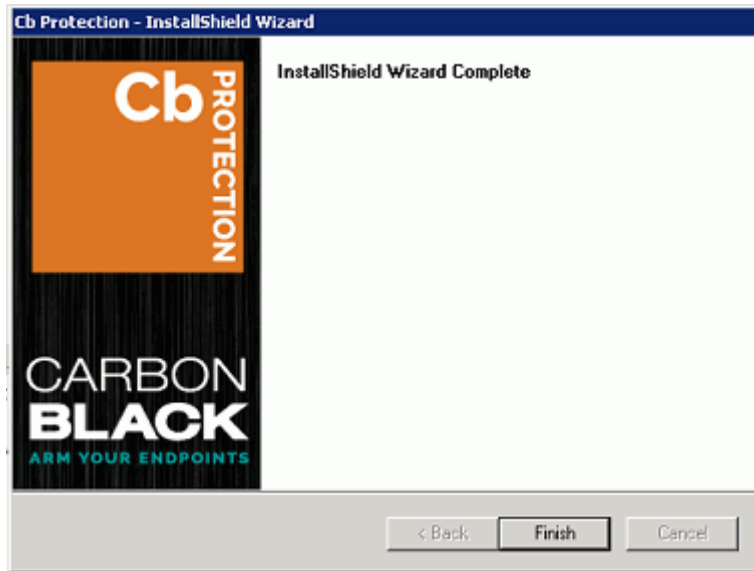
Once you have finished installing the server, you can log in via the console, upload rules and agent installers from the User Exchange, configure security policies and rules, and install agents on your endpoints. Login basics are described in this document in Chapter 3, "The CB Protection Console." Other topics are covered in *Using CB Protection*, which is available as a PDF download or through the console as context-sensitive help.

Installing the Server with a Restored or Reconnected Database

The CB Protection Server installation program provides the option of reconnecting to an existing database. In addition, you can restore a database from backup, if necessary, and then reconnect to that.

- If your database server and the CB Protection Server are on the same machine, you can *reconnect* to an existing database or *restore* the database from backup using the procedure below. The installation program prompts you for all necessary information.

- If you have a remote CB Protection database and that database is operational, you can *reconnect* to it using the procedure below. The installation program prompts you for all necessary information.

- To restore your database from a local backup created using the native CB Protection backup feature, you can choose the Restore option in the installation dialogs. If you used any other backup mechanism, use that mechanism to restore the database first and then use the Reconnect option in the CB Protection installation dialogs.

- *Restore* is not an option for remote databases. If you want to *restore* a CB Protection database on a remote system, contact Carbon Black Support.

- To upgrade from a previous version of the CB Protection Server, see "Upgrading from a Previous CB Protection Version" on page 45 instead of this section. You may also receive supplemental field upgrade instructions from Carbon Black Support.

> **Important**
>
> - When you reinstall or upgrade the CB Protection Server, system backup and automatic agent uprades are disabled. External event logging may also be disabled. You can re-enable them on the console System Configuration page Advanced Options and Events tabs.
>
> - If the database you want to restore or reconnect to is a SQL Server 2005 Express database, contact Carbon Black Support before continuing.
>
> - When restoring from or reconnecting to a database, if you imported any certificates as part of your original installation, those certificates are in the database, and can be used when you restore or reconnect. You will need the password for each certificate to reuse them.
>
> - You will have a choice during installation to use Windows authentication or SQL authentication for access to the SQL Server by the CB Protection Server. For either choice, the account used to access the database must be added to SQL Server with "sysadmin" checked in the Server Roles.
>
> - If you left a CB Protection Agent on the system where you are installing the CB Protection Server, the agent could block installation of the new server or cause faulty installation. Disable tamper protection on this agent, which will require you to have the access password or user account you provided for client management during the previous server installation or configuration. Although the installation program warns you if an agent is present in some cases, the agent is not always detected. Check the Windows Control Panel to see if a CB Protection (or Bit9) agent is present.
>
> - If you are running AppLocker on the system where the CB Protection Server will be installed, either temporarily disable AppLocker or be sure it uses only default rules.

To install the CB Protection Server and reconnect to (or restore a backup of) a database:

1. Log in using an account with local Windows administrator credentials. If you plan to use Windows Authentication to login to a remote CB Protection database, install the CB Protection Server logged in with an account that has been added to SQL Server with "sysadmin" checked in the Server Roles. Carbon Black strongly encourages using a specific Domain account for installing and logging in to the CB Protection Server, and for database access, to simplify control of both database and Active Directory permissions.

> **Important**
>
> Do not change the privileges of the account used to install the CB Protection Server after installation. This account must continue to have local administrator privileges for the server to function properly, and will also be used for server upgrades.

2. Make the server installation file available to the installation computer (either by download or inserting media in an accessible location).

3. Run the installer in either of the following ways:

   a. To install on a local server, double-click the `ParityServerSetup.exe` file to start the installation program. Continue to the next step.

   b. To install from a remote desktop, copy the `ParityServerSetup.exe` file to the installation computer and execute the file. Continue to the next step.
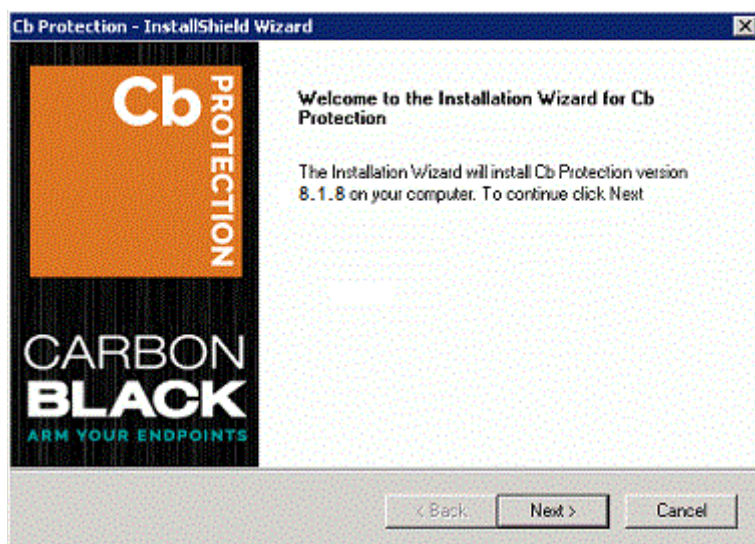
4. From the Welcome page, click **Next**. The License Agreement screen appears.

5. Review the software license agreement. You must agree to the license terms to install the server. When you click the **I accept** button and continue, you agree to all terms of use. To continue, click the **Next** button. The Select Features dialog appears.
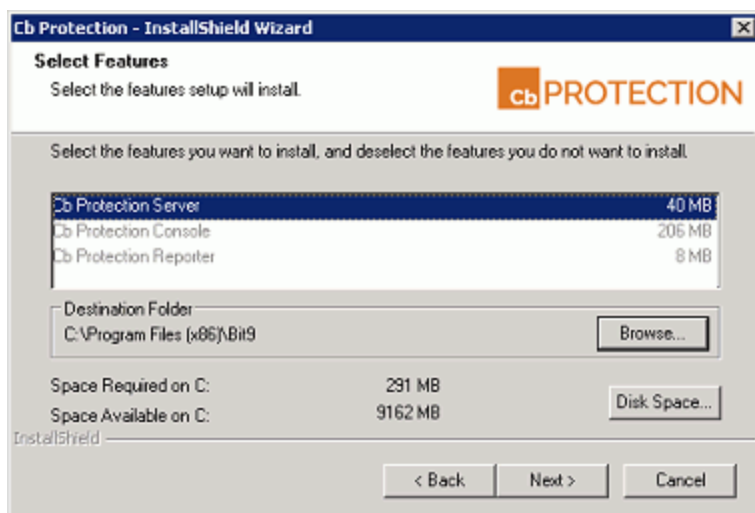
a. Although they have checkboxes, CB Protection Server, CB Protection Console, and CB Protection Reporter are always installed — they cannot be deselected. The console is the web interface to the server. The reporter is the service that connects the server to CB Collective Defense Cloud, which provides access to a database of information about files and threats. Reporter, which runs as a Windows service, also provides other essential reporting capabilities, including collection of support information for the server.

b. Either keep the default installation folder (which differs from 32-bit to 64-bit systems) or click **Browse** and navigate to the folder in which you want to install the server. If you don't choose the default, use a path that has only valid ASCII characters, not Unicode. When you have chosen the folder, click **Next**.

6. At this point, the installation program checks that the server environment meets the requirement for CB Protection Server installation. If no issues are found, you will not see any additional dialogs, and the Database Server screen will appear (step 8). Warning dialogs appear under the following conditions:

   a. If files are detected in the installation directory, you will see a warning dialog. You can continue the installation without removing the files, but should examine the files to see whether you want to copy and/or remove them. In most cases, these will be log files from CB Protection Connector appliances or services.

   b. If a CB Protection Agent is detected on the CB Protection Server computer, you will see the following dialog
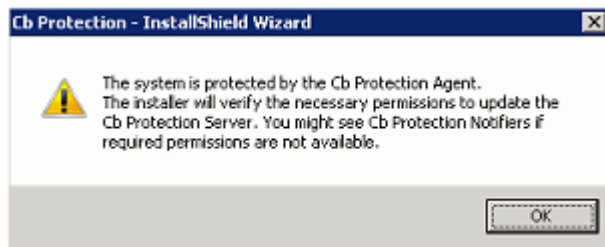
   If this dialog appears, click **OK** to dismiss it and initiate the system check that determines whether the agent and/or other factors would prevent successful installation of the server.

   c. If the system check finds any issues that would prevent successful server installation, a dialog box appears describing those issues. If this happens, correct the issues and then click **Next** (you do not need to exit the installation while you remediate the problems). When you click Next, the system check runs again, and if all issues are remedied, the installation moves to the next step. If there are still outstanding issues, they will be listed again and you will have another opportunity to correct them. If necessary, click **Cancel** to exit the installation dialogs.

   Note: If you did not disable tamper protection in advance and are prompted to do so here, you must have a client management access password or user account from the previous server installation or configuration. In the reconnect/restore case, you cannot disable tamper protection through the console.

7. The Database Server screen appears next. It includes two configuration choices:

    a. Database Server is the name of the SQL server, and optionally, its instance. Enter the server name and instance name (if any) you use to connect to the server. If the database server is local, you will be able to reconnect, and if necessary, restore from backup files you have on the server. If the database server is remote, you will be able to reconnect only.

    b. With the Connect Using radio buttons, choose Windows Authentication (i.e. authenticate with the user doing the CB Protection Server installation) or SQL Server Authentication. If you choose SQL Server Authentication, provide the Login ID and Password. Your choice here determines how access to the SQL Server by the CB Protection Server will be authenticated, both during and after the installation.

    c. When you are finished entering database information, click **Next**.

    For either authentication method, the user must have been given the "sysadmin" Server Role in SQL Server.

8. The CB Protection Database Configuration Options screen appears. The options on the screen depend upon whether a CB Protection database was detected at the location you provided on the previous screen:
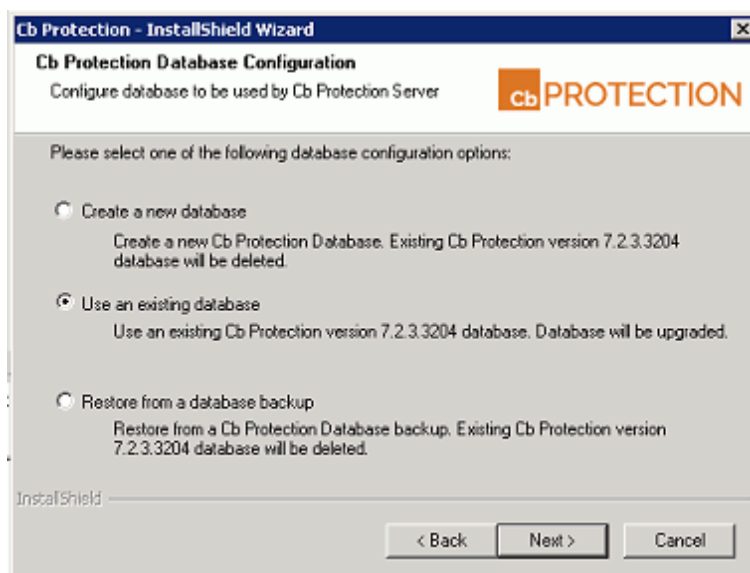
    a. If the installation program detects a usable CB Protection database, your choices are to create a new database (and delete the existing database) or use an existing database and upgrade it to this release. Choose **Use an existing database** to preserve your CB Protection (including previous Bit9 Platform and Parity) data and upgrade the database, and then click **Next**. If you choose this option, a warning appears reminding you to backup your CB Protection database before proceeding. If you have recent backups, click **Yes** to continue, and skip to step 12.

    b. If the database location you provided is local, the **Restore from a database backup** option is enabled. Choose this option to restore your previous database from a backup file, and click **Next** to continue. This option can be used only to restore backup files created by CB Protection.

9. If you chose **Restore from a database backup**, the CB Protection Backup Restoration screen appears.
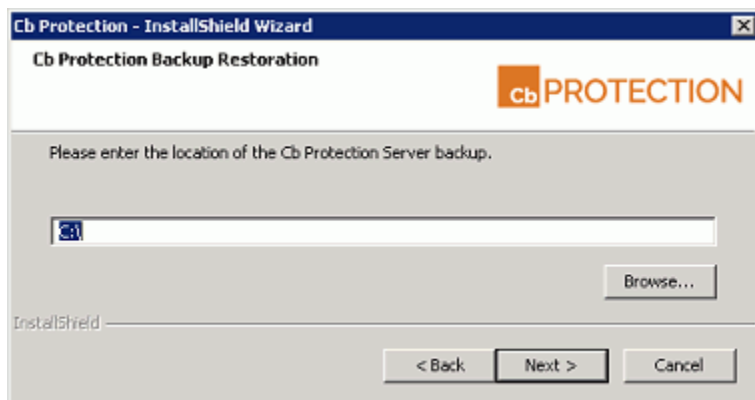
10. On the Backup Restoration screen, enter the path to the folder containing the backup database, or use the **Browse** button to locate it. Click **Next**. If the backup is from a previous version, a message box appears explaining that the database will be upgraded. When you click **OK** on this box (or if it doesn't appear), another message box appears telling you that backups will be disabled after the database restoration. When you have clicked **OK** on each of the message boxes, the CB Protection Server Backup Information screen appears.

11. Examine the information on the Server Backup Information screen. Note that if you are restoring from a backup from a previous version of CB Protection (including Bit9 Platform or Parity), that database will be updated to the version matching your installer if you proceed. Use the **Back** button if you want to use a backup other than the one described on this screen.

12. When the information on the Server Backup Information screen is correct, click **Next** to proceed. If there are certificates stored in the database, you are prompted to decide whether to re-use any stored certificates. The dialog will specify whether there is a console certificate only or certificates for both the console and the server.

13. If you want to re-use the certificate(s), click **Yes** in the dialog.
    - If you are restoring a database from backup, you will be prompted for the certificate passwords *after* the database is restored.
    - If you are reconnecting to a database, the Restore Pre-Existing X.509 Certificate for the CB Protection Console screen appears.

14. The database can contain either one or two certificate files, and there will be a dialog for each one found. Enter a password and click **Next** in each dialog.
    By default, the verified password from the first dialog is pre-populated in the second dialog (if there is one). If there is a password problem, an error message will indicate that immediately and give you the chance to re-enter the password. If a valid password is provided but another certificate restoration problem occurs during the installation, an error message appears and a self-signed certificate is generated instead so that installation may continue.

15. After you complete the certificate dialogs, the Logon Information screen appears. On this screen, choose the logon account to be used by the CB Protection Server. You can choose one of two modes of logging in:
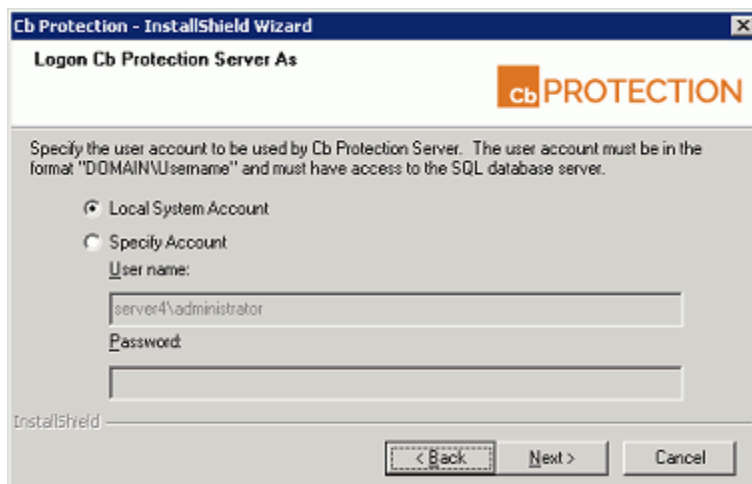
a. The Local System Account radio button instructs the installation to configure the server to use the built-in Windows system account.

b. The Specify Account radio button activates the Username and Password fields so that you can provide account information. As the screen notes, the account you provide must be in the format DOMAIN\Username and have full access to the SQL database server. The default for this choice is the currently logged in user. You must include a a domain name or a dot before "\Username".

> **Note**
>
> • Carbon Black strongly encourages using a specific Domain account and the Specific Account option to simplify control of both database and Active Directory permissions. In general, the installer should be run by this same Domain account.
>
> • In this release, an SSL certificate is automatically generated to protect communications between the server and its agents. If the Common name of the server does not match the configured server name (or one of the names if the certificate used SAN), then server and agents will be unable to communicate correctly.
>
> • For local SQL Server Express databases, the currently logged in user must be the same as the user specified in the Login Account installation dialog. If you attempt to enter a different user, an error message appears and you must re-enter the current user. The logged in user must have been given the "sysadmin" Server Role in SQL Server.
>
> • In the case of remote databases, the installation program cannot confirm the validity of the account you provide. Note that if you provide an invalid login account, server installation will be unsuccessful and you will need to reinstall.

16. When you have provided logon information, click **Next**. The Server Configuration Options screen appears.
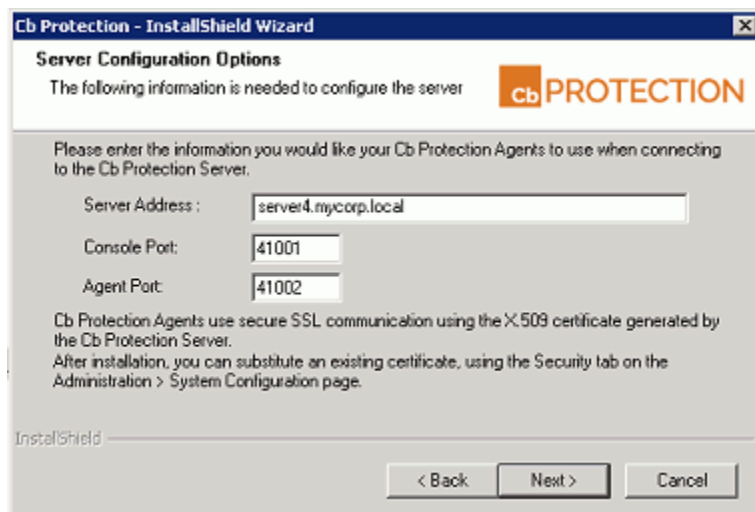
17. From the Server Configuration Options screen, review the configuration settings. In the Server Address field, the preferred address is a fully qualified DNS name (or alias) that is resolvable by all computers running the CB Protection Agent. Although not recommended, if the server is assigned a static IP address that will not change at reboot time, you can keep the default IP address selected for the CB Protection Server. The installation program automatically supplies the correct information for the installation machine. Console Port, which is used for communications between the server and its user interface, is **41001**. Agent Port, which is used for communication with agents, is **41002**.

> **Notes**
>
> • Carbon Black strongly recommends the use of a fully qualified DNS name for Server Address whenever possible. Use of a CNAME (alias) may provide even more flexibility and reliability.
>
> • If you use multiple NICs, make sure the FQDN you use in the Server Configuration screen refers to the address of the card(s) you want the agents to connect to.
>
> • If you are reconnecting to an existing CB Protection database,and you enter a Server Address other than the one you used previously, a dialog appears asking you to choose one of the two. If the new address is actually a different server, click **Yes** to modify the database with the new name. If the new address is an *alias* for the address currently in the database, click **No** to use the existing address. If you use the new address (i.e. click **Yes**), existing agents will not be able to reconnect to the server unless you create a DNS alias between the new and old names. If you are unsure of your choice or you made an error entering the name, click **Cancel** to return to the configuration screen.

18. If you are reconnecting to an existing CB Protection database and you enter a Server Address other than the one you used previously, a dialog appears asking you to choose one of the two:

- If the new address is a different server, click **Yes** to modify the database with the new name. Note, however, that if you use the new address (i.e. click **Yes**), existing agents will not be able to reconnect to the server unless you create a DNS alias between the new and old names.

- If the new address is an *alias* for the address currently in the database, click **No** to use the existing address.

19. If you are reconnecting to an existing database and you had CB Collective Defense Cloud (formerly Bit9 SRS) activated, another dialog appears if you are not using the same CB Protection Server name as previously used with this database. You will be asked, "Do you want to generate a new key for CB Threat Intel?"

- If you are cloning this database as a new instance for a new server, click **Yes**. This might be the case if you have been using an early version of a release and want to use the same database for a newer version.

- If you are reinstalling the same server as previously connected to the database, and if no other server is using the same database server name, choose **No**.

20. If you chose Specify an Account in the (CB Protection Server) Logon Information screen (step 12), another Logon Information screen appears next, for the CB Protection Console under IIS. Otherwise, go to step 21.


This screen allows you to specify a different logon for the CB Protection Console, the web-based user interface for the server.

a. Choose **Local System Account** to configure the server to use the built-in Windows system account for console logons.

b. Choose **Specify Account** to activate the Username and Password fields so that you can provide account information. As the screen notes, the account you provide must be in the format DOMAIN\Username. You cannot use "\Username" without a domain or a dot before the backslash.

> **Note**
>
> If you use a logon other than the current user, a warning dialog will be shown: "The CB Protection Server installer is unable to validate whether the specified account is able to access the SQL database server. Are you sure you want to continue?" If you are certain the account you provided is valid, choose **Yes**.

   c. When you have provided console logon information, click **Next**. If you restored certificates in a previous step, skip to step 24.

21. If there were no certificates stored in the database, or if you chose not to restore them in a previous step, the Certificate Options screen appears. From the Certificate Options screen, choose the digital certificate that will appear to console users. You either create a certificate using a template provided by Carbon Black or substitute your company's certificate.
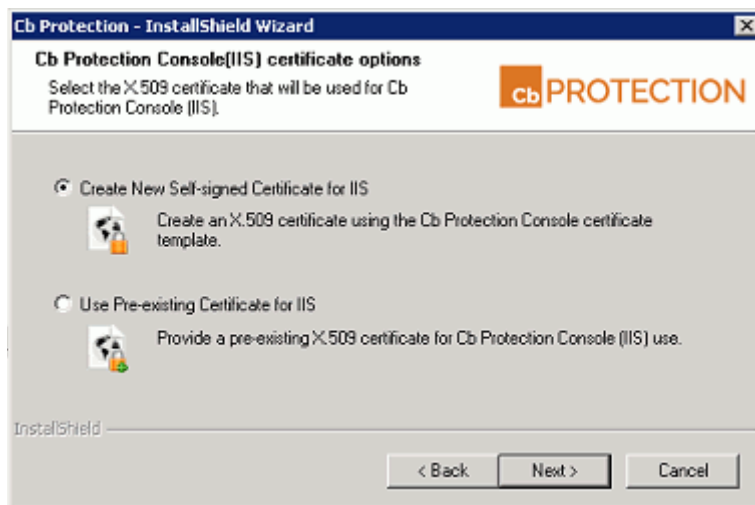

   a. If you do not have your own certificate, choose **Create Certificate**. This allows you to create a Carbon Black self-signed certificate. Self-signed certificates will generate warning boxes when you log in to CB Protection Console using Internet Explorer or Firefox, although Firefox will allow you to permanently accept the certificate to eliminate future warnings. To create a certificate, choose **Create Certificate**, click the **Next** button, and skip to Step 22.

   b. To substitute your own certificate, choose **Use Pre-existing Certificate**, click the **Next** button, and skip to Step 23.
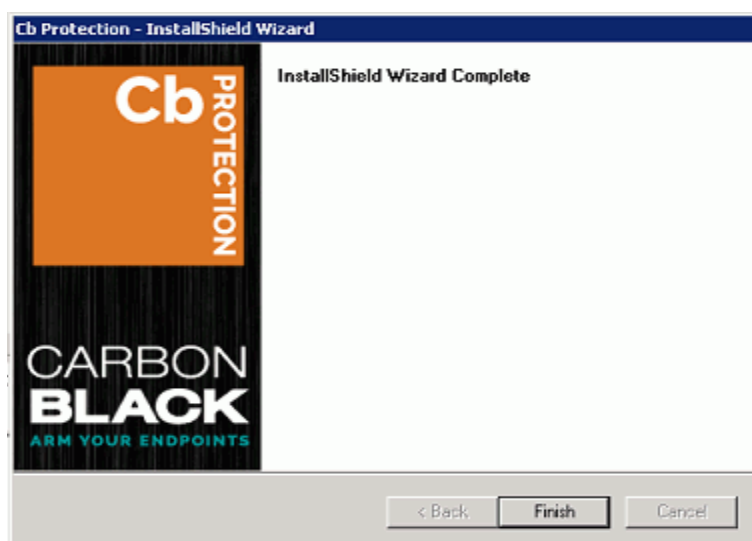
22. If you chose Create Certificate, the Create X.509 Certificate screen appears.

    a. By default, all certificate details correspond to Carbon Black name and address data. Please replace them with details of your company. The default password is 'password'. Carbon Black recommends that you change it, and keep a record of your new password so it can be retrieved for later use. The Common Name field defaults to the IP Address or DNS Name of the CB Protection Server; it cannot be changed. If the CB Protection Server is reachable by multiple DNS names, you can use the Subject Alternate Name field to specify the alternate names.
When the certificate is validated against a computer, it is validated against the Common Name or one of the Subject Alternative Name entries (if they exist). If both are present, names in the Subject Alternative Name field have priority.

    b. When the information you want is in all fields, click **Next** to create the certificate and skip to step 24.

23. If you chose Use Pre-existing Certificate, the Use Pre-existing X.509 Certificate screen appears. Enter the required information.

    a. Click the **Browse** button next to the Enter certificate file field, navigate to the PFX (PKCS.12) certificate file you want to use, and click **Open** when you have located the file. The filename appears in the certificate file box.

    b. Enter the password for the certificate, and re-enter it in the confirmation field.

    c. When you have entered the certificate file and the password, click **Next**. The Ready to Install screen appears.

24. If you are satisfied with your installation choices, click the **Install** button.
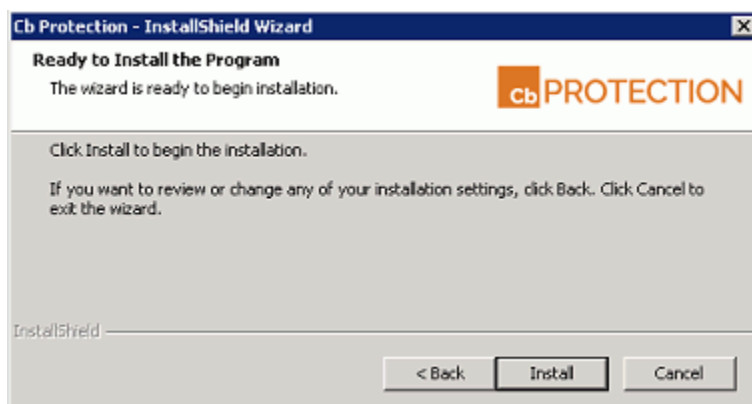
25. CB Protection Server installation commences, and an installation status bar shows progress. When the InstallShield Wizard Complete screen appears, the installation is complete.

    a. In some cases, you will need to restart the server computer after installation is completed, and the dialog will include an option to restart now. Choose to restart now unless you need to complete some other activity on this computer.

    b. Click the **Finish** button. CB Protection Server, which runs as a service, begins to operate after you click this button. Installation logs are placed in the CB Protection installation folder (for example, *C:\Program Files (x86)\Bit9*).

Beginning with CB Protection Server v8.1.4, agent installers and rules are distributed separately from the CB Protection Server. Check the Carbon Black User Exchange to get the latest packages and upload them to your server once it is installed.

Upgrading from a Previous CB Protection Version

Upgrading to CB Protection 8.1.10 requires that your existing server be at a supported 8.x patch level. Additional information about supported upgrade paths may be available in the *Release Notes* for this release.

> **Important**
>
> You must backup the CB Protection database before running an upgrade. Some database upgrade failures are non-recoverable. Be sure you have a backup no more than one day old.
>
> Dialogs during the upgrade process will warn you if your database backup is not recent (or its status cannot be determined). Proceeding in these cases is not recommended.

In addition to backing up your server, you should consider the following requirements and recommendations before performing an upgrade:

- Changing the CB Protection Server name at upgrade is not recommended, especially if you use your own distribution methods to upgrade CB Protection Agents. Consider using a CNAME for the server to avoid having to change the name.

- CB Protection Server upgrades must be run as the CB Protection Server service *user account* that was configured during server installation. You can determine the name of this account by opening the Windows Task Manager and clicking the Services button in the bottom right corner. The name in the Log On As field next to the server must be used (either by *login* or *runas*) to install the upgrade.

- If you are upgrading the server on a system that is protected by a CB Protection Agent, disable tamper protection on that agent prior to installing the upgrade. The upgrade installation program normally warns you if a CB Protection rule or third-party software is blocking access to a folder or registry location that the server installer must access to complete the upgrade. However, the best practice is to disable tamper protection in advance in case the blocking condition is not identified. In this case, be certain to re-enable tamper protection as soon as the server upgrade is completed.

- If you are running AppLocker on the system where the CB Protection Server will be installed, either temporarily disable AppLocker or be sure it uses only default rules.

Upgrade Installation Overview

Upgrading to CB Protection version 8.1.10 involves the following high-level steps, most of which are described in more detail later in this section:

- Read through the separate *Operating Environment Requirements* document for the current distribution of CB Protection version 8.1.10 to be sure your server platform meets the current hardware and software requirements for this release. When you upgrade, the first dialog in the installation program is a reminder to view the new OER. It provides a link to the OER on the customer portal (you will need your customer portal login to access the OER).

- Read through this upgrade section to get a full overview of the upgrade process.

- Contact Carbon Black Support (support@carbonblack.com or 877-248-9098) for any recent changes to upgrade procedures, or for advice on special cases, including strategies for getting to this server version from out-of-support versions of Bit9 Parity

and what to do if you are currently running a version of SQL Server Express installed by a previous Bit9 or Parity release.

- Backup the CB Protection Server database. Do not proceed with the upgrade without a recent backup since database upgrade failures are non-reversible.

- Disable third-party agent deployment mechanisms (such as SCCM).

- Stop any other activity (including backup jobs) or user access on the SQL Server.

- If there is an CB Protection Agent on the system hosting the CB Protection Server, disable tamper protection on that agent. You can do this on the Computer Details page for this system in the CB Protection Console.

- Either log in as the CB Protection Server service user account that was configured during server installation or use *runas* that user to install the upgrade.

- Beginning with version 8.1.4, use the server installer program (ParityServerSetup.exe) for all upgrades unless otherwise directed by Carbon Black representatives. There is no longer a separate installer for patch releases and hotfixes. See the Release Notes for any special installation considerations for your release.

- Wait for automatic post-installation server updates to complete. After an upgrade is finished and the installation dialog is closed, upgrade-related tasks are performed in the background. Depending on your system performance and the extent of the upgrade, these tasks might take long enough that you could experience console login failures. These should be temporary.

- If you have an agent installed on the same system as the server and you disabled tamper protection, re-enable it.

- Make any needed System Configuration changes to the server.

- Check the User Exchange for new agent package and rules files and upload them to your server if available. Beginning with version 8.1.4, updates to agents and rules have been separated from server installation to allow for greater update flexibility. See "Managing Computers" in the *CB Protection User Guide* for a detailed description of uploading these files to your server.

- If you distribute agents using your own deployment mechanism, upgrade agent distribution points and re-enable deployment mechanisms.

- If you plan to upgrade agents using the CB Protection Console, re-enable the upgrade features.

> **Important**
>
> When the CB Protection Server is upgraded from one major version to another, ongoing enhancements to "interesting" file identification require rescanning the fixed drives on all agent-managed computers. These upgrades may also require a new inventory of files in any trusted directories to determine whether previously ignored files are now considered interesting. For some upgrades, this process can involve activity similar to agent initialization, and may cause considerable input/output activity. This could take less than an hour or last for many hours, depending on the number of agents and files.
>
> For both CB Protection-managed upgrades and third-party distribution methods, Carbon Black recommends a phased upgrade of agents to avoid an unacceptable impact on network and server performance.
>
> See the "Managing Computers" chapter in the *CB Protection User Guide* guide for full agent installation and upgrade procedures.

- For agent upgrades, reboot on systems that prompt you to do so. This should only be necessary for certain systems running Windows XP or Windows 2003.
- If you have used Syslog / SIEM integrations (such as QRadar and ArcSight) with previous versions of this product, consult the *CB Protection Events Guide* for this release to prepare your configuration for any required changes.

> **Note**
>
> Changing the server name at upgrade is not recommended, especially if you use your own distribution methods to upgrade CB Protection Agents. Consider using a CNAME for the server to avoid changing the configured name in CB Protection.

Preparing to Upgrade

Check Supported Upgrade Paths

Before upgrading the CB Protection Server, be sure that your existing server is at a version listed in the supported upgrade paths in the version 8.1.6 *Release Notes*.

Also, all agents on all systems you plan to use with version 8.1.6 should be at a currently supported version. See the "Managing Computers" chapter in the *CB Protection User Guide* guide (or console help) for details on agent upgrades.

Backup the CB Protection Server Database

You must backup the CB Protection Server database *before* running the server installer to do an upgrade. Some failures of the database portion of the server upgrade are non-recoverable, and if you haven't backed up recently, you will lose data.

Carbon Black recommends that you use your own backup mechanism to back up the CB Protection database. However, if you have not backed up the database and need to use the built-in mechanism, go to the Advance Options tab on the CB Protection Console System Configuration page and enable backups.

> **Important**
>
> System Backup does not backup IIS certificates. Please do a separate backup of IIS certificates. Store the backups on a system other than the CB Protection Server.
>
> If you used the CB Protection (Bit9) backup mechanism, imported server certificates signed by a certificate authority *are* included in the backup. Self-signed certificates are not, and backups of self-signed certificates are of limited value.

Disable Software Deployment Mechanisms

Please disable any software deployment mechanisms, such as SCCM, used to distribute CB Protection Agent until after the upgrade completes and you have had an opportunity to update their respective distribution points with the upgraded agent installers.

Stop SQL Background Jobs

Because the CB Protection database is updated during a server upgrade, no other database jobs should be running. This includes background jobs such as database maintenance and backup activity. Stop all of these jobs, and confirm that no one else is using the database before initiating the server upgrade.

Run the CB Protection Server Upgrade Installation

Make the server installer files available to your CB Protection Server. Launch the **ParityServerSetup.exe** application to validate and upgrade the server components.

Upgrade Installation Checks

The upgrade installation program checks that the server environment meets the requirements for installation of this server version. There are two important checks that might produce warnings after you initiate the upgrade:

- **Blocked Access Warning** – If the CB Protection Agent is installed on the system, a dialog box appears reporting that the installer will check to confirm that it has access to the necessary locations for an upgrade.
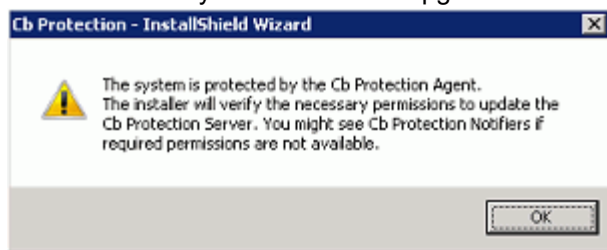
If the system check finds that the agent or any other system software is blocking access to folders or registry locations needed by the installer, the issues will be listed in a dialog, and you will have the opportunity to remedy them and continue with the upgrade. When you correct the issues listed, click the **Next** button on the dialog to run the system check again and (if all issues are corrected) proceed with the upgrade.

It is possible, although uncommon, that you will be prompted during installation to disable tamper protection on the server's agent. In this case, be certain to re-enable

tamper protection as soon as the server upgrade is completed, and do not disable tamper protection unless prompted.

- **Database Backup Warnings** – CB Protection Server upgrades include updates to your CB Protection database. Some situations can cause failure of the database update scripts, and some of these failures are unrecoverable. You must backup your database before an upgrade to make sure you can restore your most recent data. The upgrade installer checks to see whether a recent backup can be found, and displays different dialogs depending upon what is found:

  - In all cases, an informational dialog is displayed warning that a recent database backup is required.
  - If the installer determines that there is no recent backup, it will display a dialog telling you to do a backup before proceeding.
  - If the installer is unable to determine when the most recent backup was, it will display a dialog telling you to check the date of the backup before proceeding.

  You have the option of cancelling the upgrade or continuing after these warnings. Continuing without a recent backup is *not recommended*.

- **Database Size Warning** – CB Protection Server upgrades can require a considerable amount of free storage space for the database. The installer attempts to confirm that there is enough space available for a database upgrade, and displays a dialog in these cases:

  - If it cannot determine whether there is enough space (for example, because it does not have privileges to view a remote database), it will display a dialog with the current database size, the estimated amount needed for an upgrade, and a recommendation to make sure there is enough space available.
  - If the installer can determine the free space available and determines that it is insufficient, it will display a Database Upgrade Size Warning dialog with the current and required amount of free space, and a warning that there is not enough space.

  You have the option of continuing after either of these warnings, with or without remediating space issues. If the upgrade is continued and there really is not enough space, the upgrade program will exit and revert to the previously installed database and CB Protection (or Bit9 Platform or Parity) version.

- **SQL Server Express** – If you are using SQL Server Express for your existing database and your database is larger than 4Gb, the upgrade installer will detect this and a dialog will warn you that your database may become unusable upon upgrade. You will have the option of continuing the upgrade, but you should consider upgrading to a full version of SQL Server, as specified in the *Operating Environment Requirements* for this release. SQL Server Express has a firm limit on the database size, and if you see this warning, you are almost certain to exceed that limit.

- **CB Protection Connector for Check Point Password** -- If a previous installation of the server used specific credentials during server installation, you may see a message indicating that CB Protection services could not be started due to the CB Protection Connector for Check Point service. In this case, you will be prompted for the credentials needed for that service.

- **Database Update Failure** – If there is a failure in the database update portion of the server upgrade, different dialogs will be displayed depending upon the location of the failure. If the failure is potentially recoverable, you will be given the option of

continuing. If it is not recoverable, you will see a message ending the upgrade and listing recommended steps.

- **API Errors** – If there have been any errors in the CB Protection API logged in the past seven days, the installer issues a warning and aborts the upgrade. API errors are logged in **php_errors.log**, located in *<CB Protection installation folder>*\Parity Console\WebUI\Logs\. Beginnning with v8.0.0, many functions in the CB Protection console depend upon the API, and upgrading with known errors could cause various problems. If you see this error message, consult the error log, and either diagnose and fix the API problems before continuing or contact Carbon Black Support for assistance in troubleshooting.

Upgrade Completion

After the installer finishes and exits, the CB Protection Server starts running again and updates the existing agent installers for each policy and platform. This process takes a few minutes, the exact time depending upon the number of policies you have. If you are refreshing the version of the CB Protection Agent installer on distribution points for a software deployment mechanism, make sure the agent installer has completed its upgrade before deploying it.

Review Post-Upgrade Server Configuration

After you run the server upgrade installation, complete the following checklist prior to upgrading agents:

- Beginning with CB Protection Server v8.1.4, agent installers and rules are distributed separately from the CB Protection Server. Check the Carbon Black User Exchange to get the latest packages and upload them to your server once it is installed. Uploads can be performed by going to the console menu and choosing configuration (**gear icon) > Agent / Rule Version Update** page in the CB Protection Console. See *Using CB Protection* (PDF or online help) for full instructions.

- In the **Rules > Software Rules** section of the CB Protection Console, review **Updaters** as necessary (e.g. to see any new updater versions or new updaters).

- In the **Rules > Software Rules** section of the console, if you upgraded the server on a system that is protected by the agent, and you disabled certain **Custom** rules to allow the upgrade to run, re-enable those rules.

- In the **Assets > Computers** section of the console, if you disabled tamper protection on the server's agent during upgrade, open the Computer Details page for that agent and re-enable tamper protection.

- In the configuration (**gear icon) > System Configuration** section of the console, go to the **Advanced Options** tab, and modify the **Database Backup** configuration if necessary. Then re-enable backup.

- If you plan to use Reputation Approvals, it is better to enable it as soon as possible to avoid heavy network traffic later. This feature requires that you have CB Collective Defense Cloud enabled (configuration (**gear icon) > System Configuration > Licensing**). If you have it enabled, to access this feature, choose **Rules > Software Rules** on the console menu and click the **Reputation** tab. See "Reputation Approvals" in the *CB Protection User Guide* guide for more information.

- Automatic Agent Upgrade is disabled in the server upgrade process. To re-enable:

- Be sure that you have uploaded any new agent installer packages and rule files from the User Exchange and confirm that these are updating agent installers on the server.

- Be sure that you have configured the policies you want to upgrade first for automatic upgrade, and those you don't need upgraded right away not to upgrade. Upgrading large numbers of agents at once can create a large load on the server.

- In the **Administration > System Configuration** section of the console, choose the **Advanced Options** tab and re-enable automatic upgrades of agents.

- Automatic backup is disabled if a previous database was restored during the upgrade. If you use automatic backup and want to re-enable it, see "Backing Up the CB Protection Server" in the CB Protection Console help.

- If you use a third-party software distribution system to install CB Protection Agents, re-enable the distribution system and update the distribution points as the next section specifies.

- This release includes a System Health feature that monitors a variety of factors, including compliance of your system with the CB Protection *Operating Environment Requirements*. The indicators for this feature must be downloaded via CB Collective Defense Cloud. See the *CB Protection User Guide* guide or online help in the console for more information about enabling this feature.

Agent Upgrade Status

To make the upgrade process easier to manage, the Computers page in the console provides an Upgrade Status column and also visually differentiates between computers running up-to-date agents and those running previous versions. On this page, computers running *previous* agent versions show an yellow dot in the "Connected" column while up-to-date agents are shown with a blue dot. Disconnected agents show a grey dot.

In addition, the Upgrade Status column in the Computers table shows a more detailed description of agent status as each agent goes through the upgrade process. Clients will transition to an Upgrade Status and Policy Status of "Up to Date" when all their upgrade processing has been completed.

See the "Managing Computers" chapter in the *CB Protection User Guide* guide (or online help) for addition information about automatic and manual agent upgrades, and about monitoring upgrade status.

Uninstalling the CB Protection Server Software

The server uninstallation program removes CB Protection files and associated third-party software installed on the system. To uninstall the server, you must log in as a user with administrative privileges, preferably as the same CB Protection Server service user that was used to install the server. The uninstall program is on the **Start > All Programs > CB Protection** menu, although you can also use the **Add or Remove Programs** interface in the Windows Control Panel. Consider the following points before you uninstall:

- If you are uninstalling and do not intend to reinstall the CB Protection Server, place all policies in Disabled mode before uninstalling. Otherwise, computer users will not be able to uninstall the agent without special assistance. If you attempted to uninstall the CB Protection Server without changing all policies to Disabled mode first, contact Carbon Black Support.

- When you start the CB Protection Server installer/uninstaller program, it verifies that you have the permissions required to uninstall the CB Protection Server. If there are any rules or permissions prevent un-installation from going forward, the installer provides a report detailing what must be done before you can proceed. This includes blocks due to an enabled CB Protection Agent on the computer running the server and other folder or registry permission issues.

- Self-signed Carbon Black certificates are removed during the uninstallation process. If you used a certificate from a certificate authority (i.e. one that is installed in the Windows Certificate Store), it is not removed.

To uninstall the CB Protection Server Server software:

1. Either go to the Control Panel and click **CB Protection** on the Remove Programs list, or on the Windows Start menu, choose **All Programs > CB Protection > Uninstall** CB Protection Server. A confirmation dialog appears.
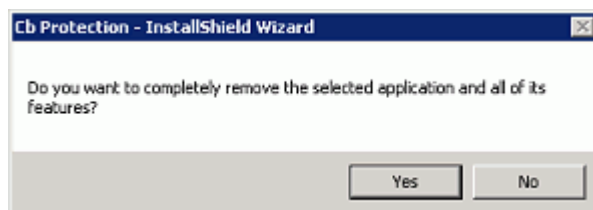
2. Click the **Yes** button to start the uninstallation process. When the uninstallation process is complete, either the dialog will close by itself or you will see the Uninstall Complete screen.

3. Generally, you do not need to reboot your system after uninstalling the server. If a reboot is necessary (which is true only if the uninstall program could not remove certain CB Protection files), the screen includes reboot options.

If the options appear, rebooting now is recommended unless you have other immediately necessary activity on the server (for example, an error in uninstalling).

a. Choose a reboot option if prompted.

b. Click **Finish**.

Notes

- For instructions on uninstalling the CB Protection Agent, refer to the *CB Protection User Guide* guide or online Help system.

- Uninstalling the server reverts the IIS configuration to its state prior to server installation. Any configuration changes applied during the time the server was installed are lost.

- The server uninstall program will *not* remove the CB Protection database. It must be deleted separately.

- If the FastCGI module was installed by the server installation program, the uninstall program presents a choice to un-install it or leave it installed once the server itself has been uninstalled.

- Visual Studio 2012 and 2015 runtimes installed during server installation are not removed when you run the uninstall program.

- If the Integrations folder in the CB Protection installation directory contains files that were not installed with the server, the folder and its contents are not removed when you uninstall the server. The Integrations folder can contain user data produced when CB Protection is integrated with third-party tools or CB Inspection.

Chapter 3

The CB Protection Console

This chapter explains how to log in to the CB Protection Console as an administrator. Logged in as an administrator, you can configure almost all aspects of the system and create hierarchical user accounts. You can also add permissions for features not accessible to the administrator by default.

Sections

Logging In to the Console

CB Protection employs a browser-based user interface called the *Console*. You can log in to the console from a supported web browser on any computer with network access to the server, including the server itself.

To use the console and online help, JavaScript must be enabled on your browser. In Internet Explorer, you may need to adjust your security settings or set the CB Protection address to be part of your Local Intranet or Trusted Sites zone in order to access the console. The security settings are accessed from the Internet Explorer **Tools > Internet Options** menu, on the **Security** tab.

For your initial login, you use the built-in administrator account, `admin`.

To log in to the CB Protection Console:

1. From a supported web browser, enter the fully qualified domain name or alias of the CB Protection (IP addresss may be used but a FQDN or alias is preferred):

   `https://server_name`

   If you installed a verifiable digital certificate from a third-party authority as part of server installation, you go directly to the login screen (step 3).
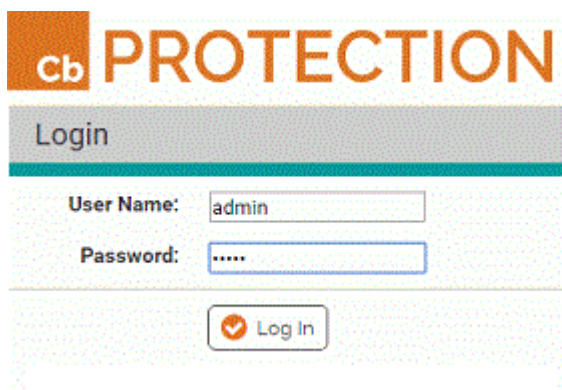
2. If you chose the Carbon Black self-signed SSL certificate during server installation, the first time you enter the server URL, a certificate error appears. You can safely ignore the warning and click through the remaining confirmation screens. The warning appears because the authority of the self-signed certificate cannot be verified.

Note

To avoid future certificate warnings:

- In Firefox, accept the certificate permanently.

- In Internet Explorer, click through the warning, click the Certificate Error button in the IE toolbar, and install the self-signed certificate.

- In Safari, click **Show Certificate** on the warning and check the *Always trust...* box for the Carbon Black certificate, and click **Continue**.

---

3. In the login screen, enter the default user name (`admin`) and password (`admin`).

4. Click the **Log In** button. The CB Protection Home page appears.

You should be able to view the entire top menu bar, from the logo on the far left to the help icon and the name of the currently logged on the far right.
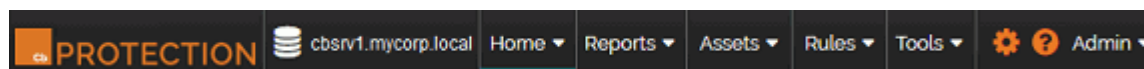
If you are not able to see all of the items on the top menu, adjust the zoom or resolution on your browser. This may be necessary on smaller laptop or tablet displays.

You should change the password for the `admin` account after logging in. See "Changing the Administrator Password" on page 57.

> **Note**
>
> For environments that require best security practices, Carbon Black recommends usng AD-based login accounts. You can also use SAML to require two-factor authorization for console logins.
>
> See the separate *CB Protection User Guide* guide for more information about AD-based and SAML logins.

The console automatically logs users out after a specified period of inactivity. This can be modified on the System Administration page Advanced Options tab. You can modify the default starting page for the console using the dialog that appears when you choose **Tools > Preferences** on the console menu. See the online help in the console for additional information.

Logging Out of the Console

On every page of the console, a log out command is available on the user name menu in the top right corner of the banner of the console web page. Logging out ends your session.

To log out of the CB Protection Console:

1. In the user name menu at the top right corner of console menu, choose **Log Out** (with the default login, this menu will show as "Admin"):
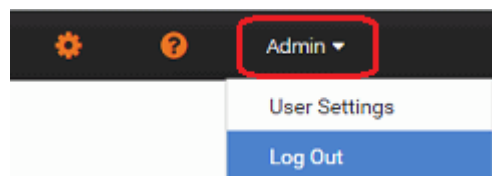
2. Respond to the confirmation prompt:
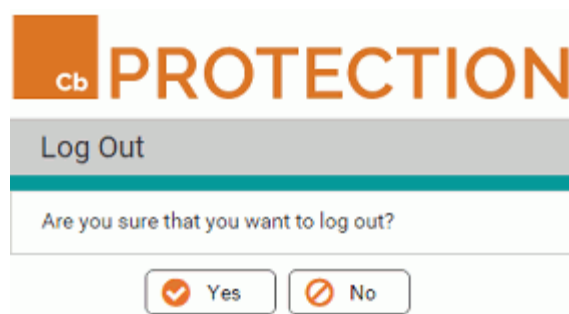
Changing the Administrator Password

For security, regularly change your administrator password. After logging in to the built-in administration account `admin` for the first time, you should immediately change the password, which initially also is `admin`.

To change the default administrator password:

1. On the configuration (gear) menu in the top right area of the console menu, choose **Login Accounts.**
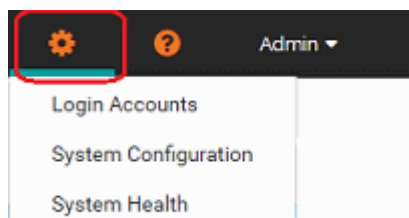
2. On the Login Accounts page, click the View Details button 🖉 next to the `admin` user.

3. On the Edit Login Account page, change the password as follows:

    a. In the Password field, enter the new password.

    b. In the Confirm Password field, enter the password again.

    c. Click the **Save** button.

> **Note**
>
> A CB Protection administrator can use this same series of steps to change the passwords of other users if their accounts were created *in* the console. If a user logged in to the console with an AD user account, that user's details, including password, cannot be individually modified in the console.

Viewing User Activities in the Events Table

You can review the combined event and exception logs in the CB Protection Events table. Messages include a record of user actions, including logins, new users created, and changes to user accounts.

To view CB Protection Server activities:

1. On the console menu, choose **Reports > Events**. The Events page appears, and by default shows All Events in the past hour in the table at the bottom of the page.

2. If you want to see a subset of the available events, you can make a choice on the Saved Views menu or create a special view using Show/Hide Filters and Show/Hide Columns.

3. If you want to use a different time range, choose a time from the Max Age menu, or click the Show/Hide Filters link to configure and **Apply** a more complex time range. The report table at the bottom of the page updates to show the new time range.

The *CB Protection User Guide* guide, available as a separate document or through online help in the console, provides more details about events:

- See the topic "Event Reports" for information other event report types and views.
- See the topic "Managing the CB Protection Event Database" for information about event log management and configuring the CB Protection Server to send events to a Syslog server .

Using Help

The console provides an online version of *CB Protection User Guide*, which is also available as a PDF file.

- When you click the question mark button in the top right of the console menu, the online help opens with an introductory screen and a table of contents.
- When you click a question mark button in one of the panels lower down on a page, the topic relevant to that page appears in addition to the table of contents.

To launch online user documentation from the console:

1. Launch help either of the following ways:

   - Click the main help button in the top right of the console menu.

   - Click the context-sensitive help button on the right opposite a page title.
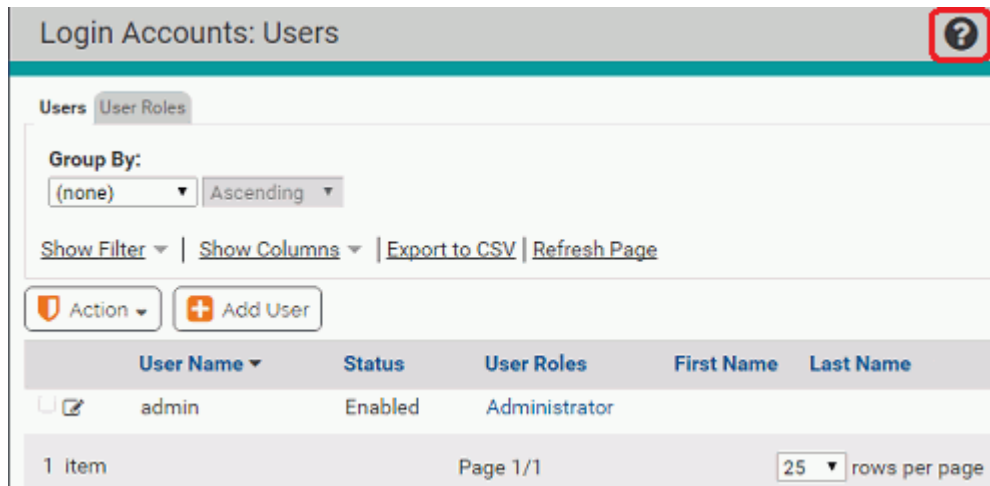
CB Protection help is displayed in a new window or tab. The controls on the help page, and their location, vary depending upon the size of the window, but all pages provide access to the index, table on contents, and search features.

Index

W