Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Carbon Black Protection with EventTracker

EventTracker v9.2 and later

Publication Date:

April 5, 2021

Abstract

This guide helps you in configuring Carbon Black Protection with EventTracker to receive Carbon Black Protection events. In this guide, you will find the detailed procedures required for monitoring Carbon Black Protection.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 and later, Carbon Black Protection Application Control for Servers & Critical Systems .

Audience

Administrators who are assigned the task to monitor and manage Carbon Black Protection events using EventTracker.

Table of Contents

1. Overview

Carbon Black Protection (Carbon Black Protection), formerly Bit9, is an application control product that allows departments to monitor and control application execution on systems. The best aspect of Carbon Black Protection is its ability to hash out and quickly locate executables on all workstations and servers.

EventTracker integrates to Carbon Black Protection by logging through REST API and provides reports, knowledge objects and dashboards for all generated events. This helps largely in searching for and weeding out known-bad files and suspected-bad files from the network.

2. Prerequisites

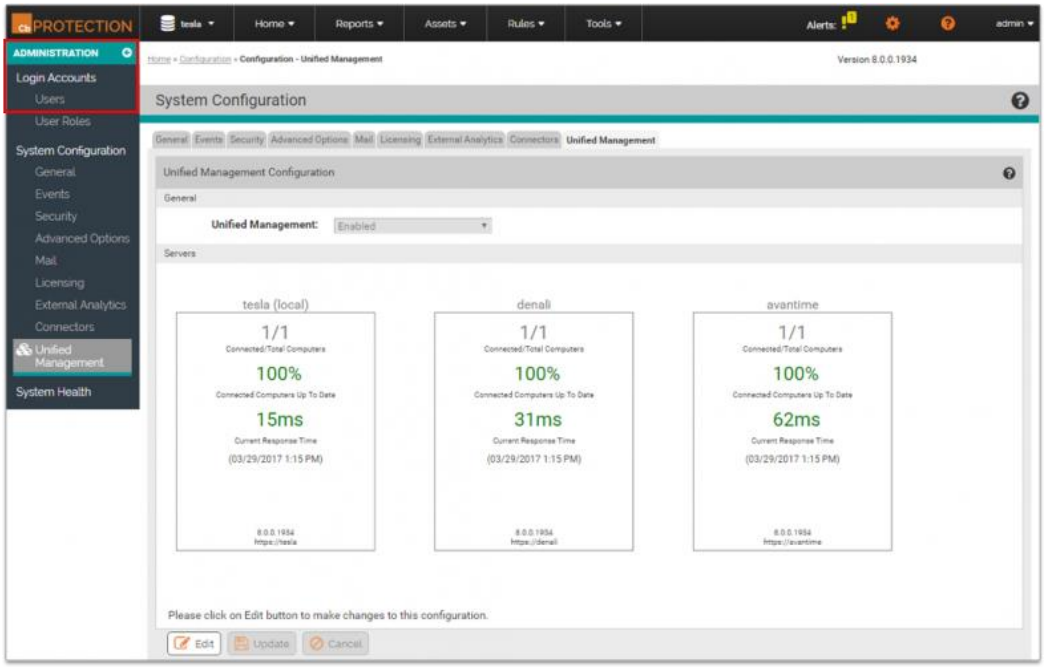
- Carbon Black Protection must be deployed.
- Contact support to get the Hostname associated with your Carbon Black Protection API backend.

3. Integrating Carbon Black Protection events to EventTracker server

EventTracker utilizes Carbon Black Protection API to fetch events from Carbon Black Protection console in CSV format. The Carbon Black Protection API is accessible through a special hostname assigned to your organization. Authentication is handled by an API token, which is generated from the administration section of the Carbon Black Protection console.

API configuration for Carbon Black Protection API is explained below:

1. Log into the console as an administrator.

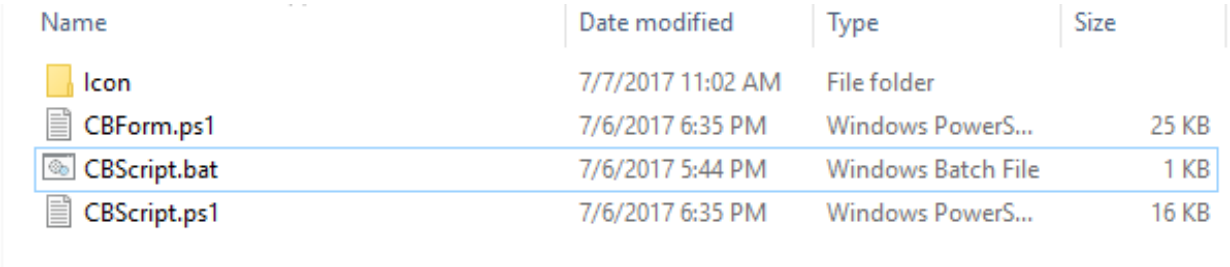


2. Select **Administration -> Login Accounts**.
3. Find the user in the list then click the **Edit** button on the left-hand side of the row containing their username.

4. This will show the details for the selected user. At the bottom of the details page, click the checkbox next to **Show API Token** in the API section. This will reveal the API token associated with the given user. If no API token is revealed, click the **Generate** button. If a new API token was created, it must be saved with the **Save** button before it becomes active.
5. Note down the API Token generated.

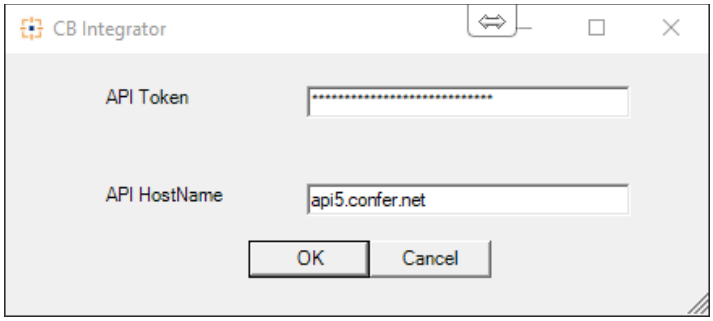
Following are the steps to integrate Carbon Black Protection to EventTracker:

- Contact the EventTracker support team for obtaining Carbon Black Protection Integrator pack.
- The Integrator package will be obtained in a Zip file format, extract the files to get the below file contents as shown in the image.



1. Double-click on the CARBON BLACKScript.bat to initialize configuration.

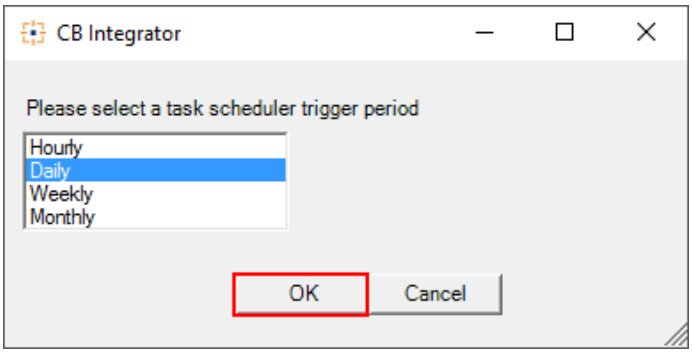
   Carbon Black Integrator configuration window will pop-up.



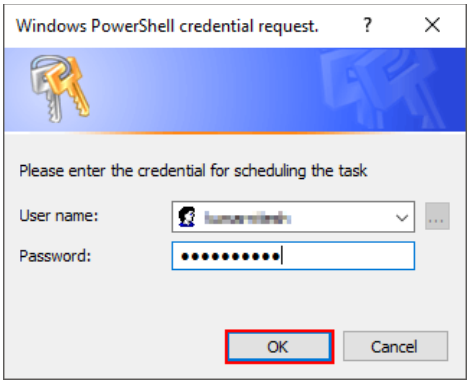
2. In the Carbon Black Integrator configuration window, enter the following details:

- API Token – Enter the API key of the configured user.
- API HostName – Enter the API backend hostname.

3. Click **OK** to proceed.
4. Enter an appropriate schedule period. It is prescribed to keep it Daily.

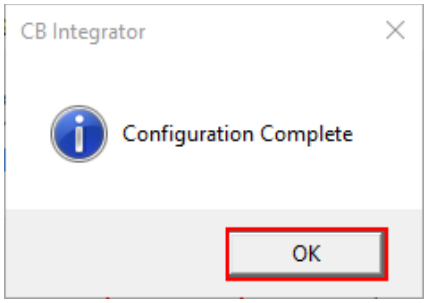


5. Click **OK** to proceed.
6. Enter admin credentials for scheduling the task.



7. Click OK to proceed.

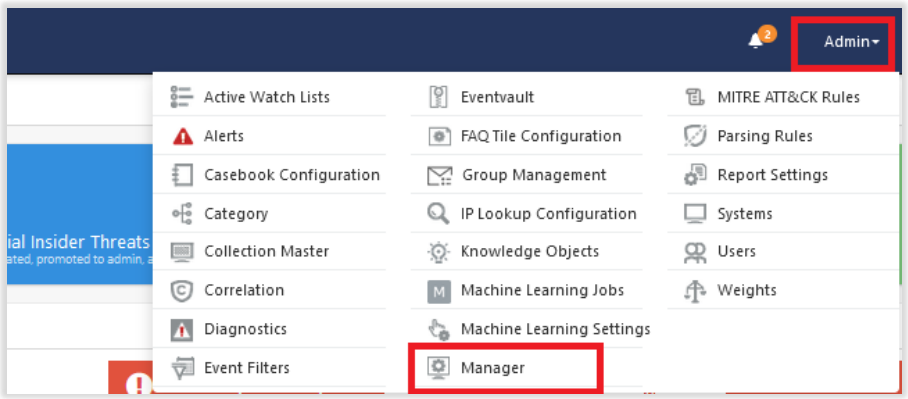
   Successful configuration pop-up message is shown.



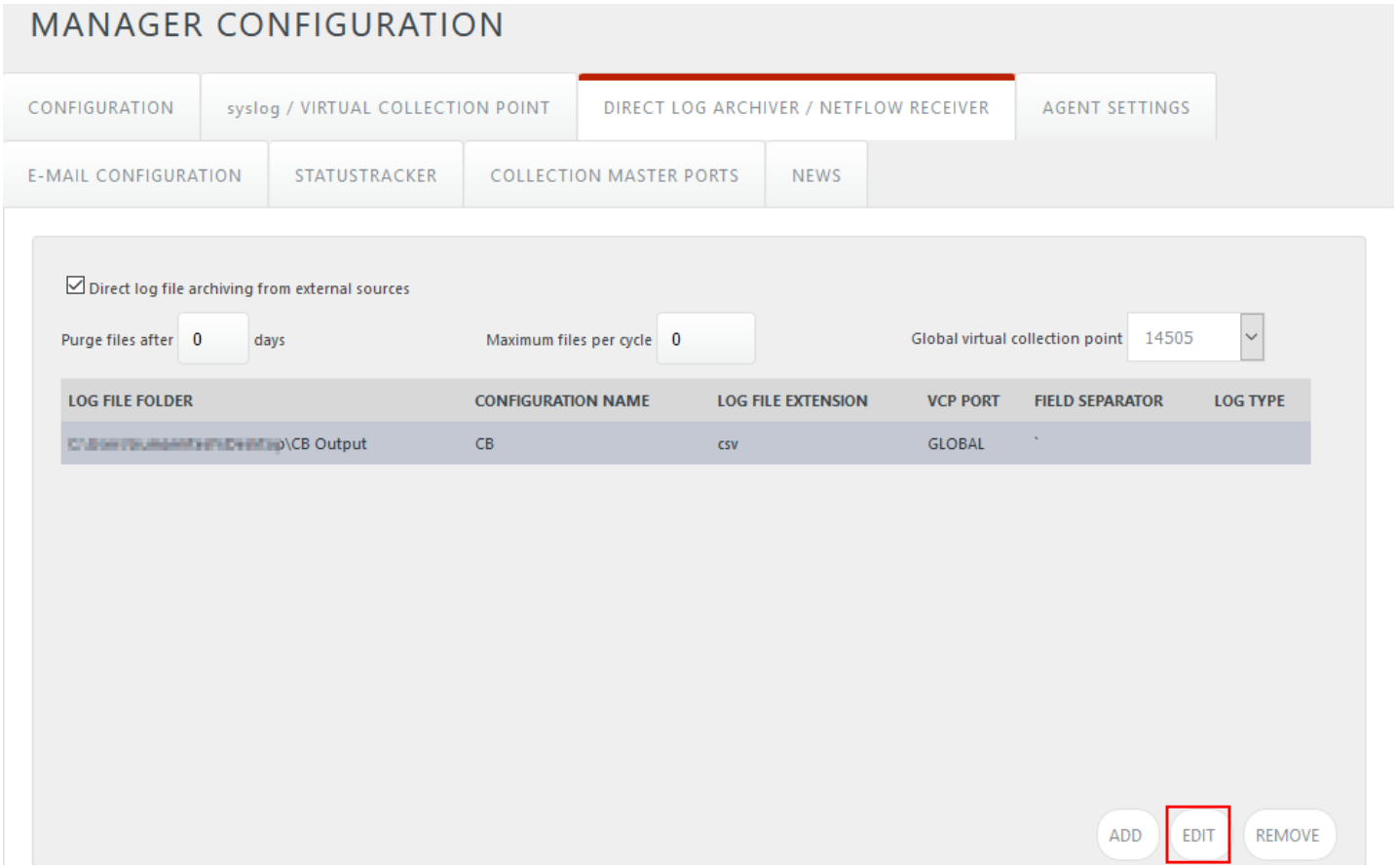
8. Click **OK** to exit Carbon Black Integrator configuration.

4. Verifying Carbon Black Protection Integration in EventTracker

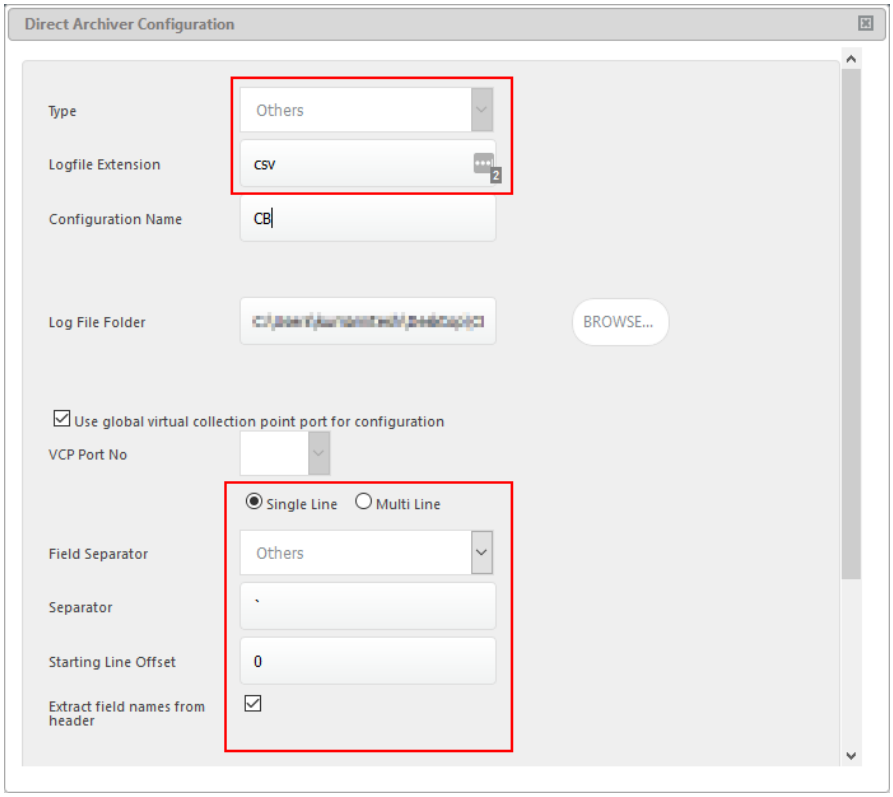
1. Launch the EventTracker Manger.
2. Select Manager under Admin drop-down.



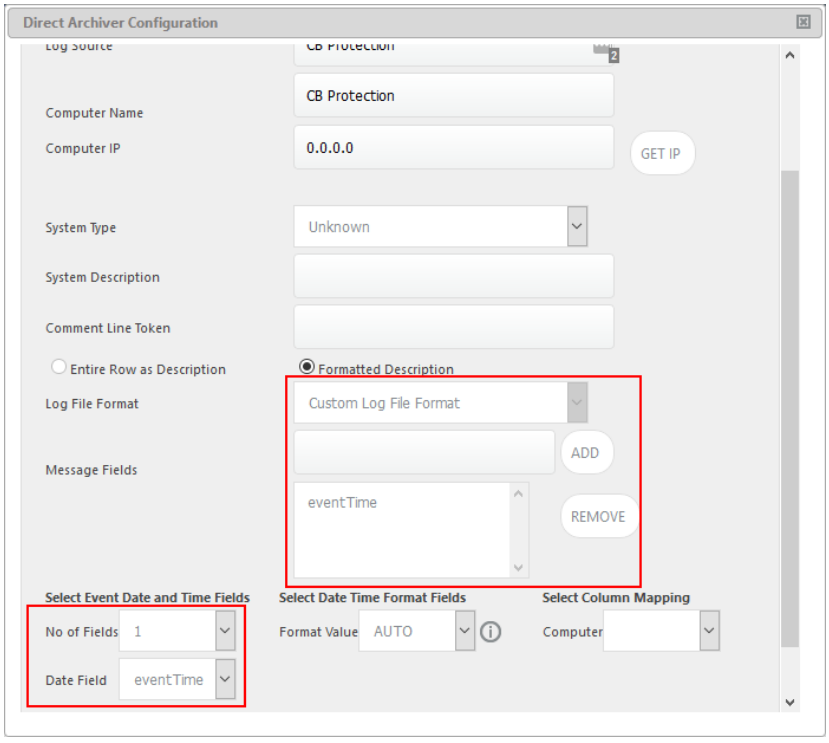
3. Go to the **Direct Log Archiver** tab and check if the configurations are replicated as shown below:



4. Select Carbon Black Protection integrator DLA configuration and click **Edit** to verify DLA configuration further.

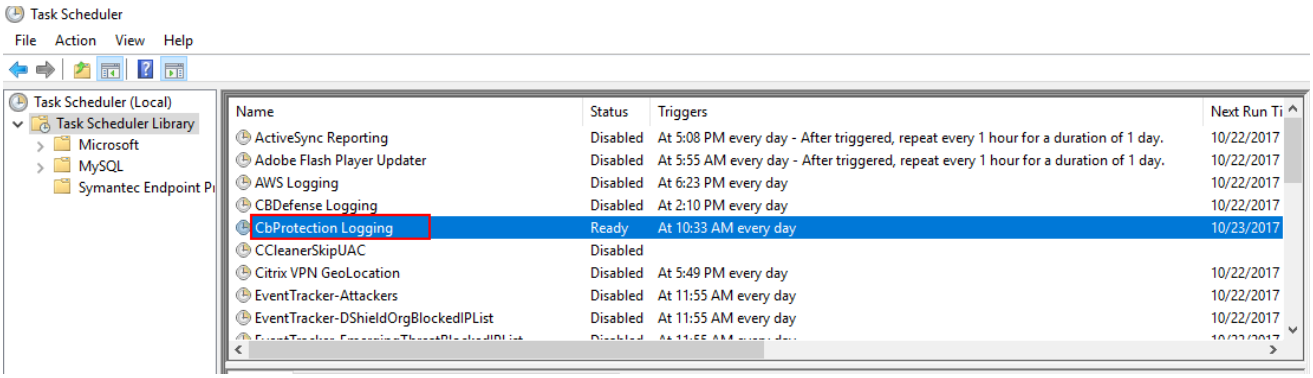


5. Verify configured settings and click **Configure** to proceed.



6. Verify configured settings and click Cancel if settings are correct.

7. Go to Start and open **Task Scheduler** to verify **Carbon BlackProtection Logging** scheduled task.



- Adjust task trigger schedule for the task as per your requirement.
- If task is altered, save it with admin credentials.

5. EventTracker Knowledge Pack

Once logs are received into EventTracker; alerts, reports can be configured into EventTracker.

The following knowledge packs are available in EventTracker to support Windows.

5.1 Flex Reports

- **Carbon Black Protection - Approval request details:** This report provides details regarding file approval requests received on Carbon Black Protection.

LogTime	Workstation	Creation Date	Modification Date	Modified By	Created By	Requestor Comments	Requestor Email	File Path	Application Platform	Rule Type
09/18/2017 02:45:28 PM	JLAULA101393	5/24/2017 12:20:04 PM	5/24/2017 12:20:04 PM		JLA\DenaM	need to email a slideshow of pictures for a ECSC HR Managers group to a large group of people.	denam@contoso.com	c:\users\denam\downloads	Windows	Unapproved executable
09/18/2017 02:45:28 PM	JLAULA101222	5/15/2017 11:55:41 AM	5/15/2017 11:55:41 AM		JLA\donr	to program meters	donr@contoso.com	c:\users\donr\appdata\local\microsoft\windows\temporary internet files\content.ie5\a6zfxc86	Windows	Unapproved executable
09/18/2017 02:45:28 PM	JLAULA101222	5/12/2017 12:42:31 PM	5/12/2017 12:42:31 PM		JLA\donr	hey guys this is for meter programing software Jeff K will be downloading it soon as well thanks don	donr@contoso.com	c:\users\donr\appdata\local\temp\install	Windows	Unapproved executable
09/18/2017 02:45:28 PM	JLAULA101459	4/25/2017 8:18:59 AM	4/25/2017 8:18:59 AM	michaelt@JLA.com	NT AUTHORITY\SYSTEM	Is this OK to approve? It is the news app in windows.	matts@contoso.com	c:\program files\windowsapps\microsoft.bingnews_4.20.1102.0_x64__8wekyb3d8bbwe	Windows	Unapproved executable
09/18/2017 02:45:28 PM	JLAULA101459	4/10/2017 12:42:59 PM	4/10/2017 12:42:59 PM		JLA\matts	This keeps popping every 15-20 min.	matts@contoso.com	c:\program files\windowsapps\c27eb4ba.dropbox_4.6.5.0_x64__xbfy0k16fey96	Windows	Unapproved executable
09/18/2017 02:45:28 PM	JLAULA101473	7/20/2017 9:58:23 AM	7/20/2017 9:58:23 AM		JLA\ChrisM	David Wasson	chrism@contoso.com	c:\users\chrism\appdata\local\temp\{f8222330-0742-4c4e-93d7-bbd3a29457b3}\.cr	Windows	Unapproved executable

Log Considered

id : 1

fileCatalogId : 118540

processFileCatalogId : 96411

installerFileCatalogId : 0

computerId : 31

computerName : CONTOSO\WKSTS101383

dateCreated : 9/27/2016 11:01:46 AM

dateModified : 9/27/2016 11:01:46 AM

modifiedBy :

enforcementLevel : 20

resolution : 0

requestType : 1

createdBy : Contoso\maya

requestorComments : this is my trouble entry

requestorEmail : maxx@rctpten.com

priority : 0

resolutionComments :

status : 1

policyId : 47

multipleBlocks : True

fileName : dbx.jar

pathName : \\svr-db-prod.apps.Contoso.com\programs\sienatech\trouble

process : c:\siena\java\jre7\bin\javaw.exe

createdByUserId : 81

modifiedByUserId : 81

customRuleId : 31

duplicates : 1

related : 0

platform : Windows

publisherReputation :

customRuleType : Unapproved script

installer :

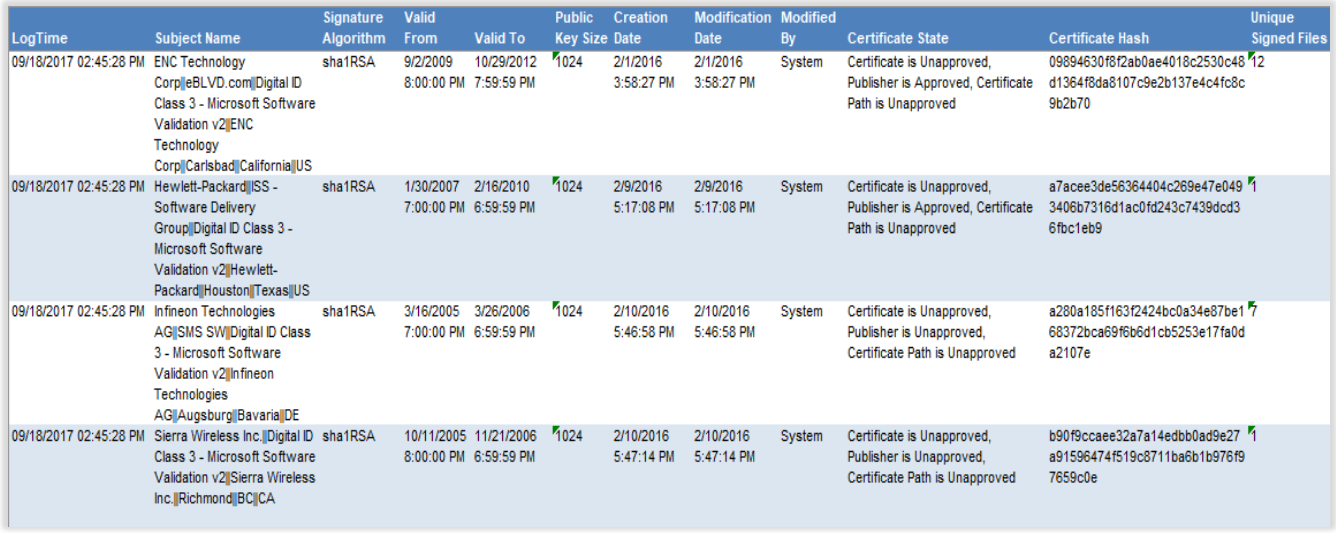
processName : javaw.exe

processPath : c:\siena\java\jre7\bin

responseMailSent :

file : \\svr-db-prod.apps.Contoso.com\programs\sienatech\trouble\dbx.jar

- **Carbon Black Protection - Certificate details:** This report provides details regarding various certificates being used in the network.



LogTime	Subject Name	Signature Algorithm	Valid From	Valid To	Public Key Size	Creation Date	Modification Date	Modified By	Certificate State	Certificate Hash	Unique Signed Files
09/18/2017 02:45:28 PM	ENC Technology Corp|eBLVD.com|Digital ID Class 3 - Microsoft Software Validation v2|ENC Technology Corp|Carlsbad|California|US	sha1RSA	9/2/2009 8:00:00 PM	10/29/2012 7:59:59 PM	1024	2/1/2016 3:58:27 PM	2/1/2016 3:58:27 PM	System	Certificate is Unapproved, Publisher is Approved, Certificate Path is Unapproved	09894630f8f2ab0ae4018c2530c48d1364f8da8107c9e2b137e4c4fc8c9b2b70	12
09/18/2017 02:45:28 PM	Hewlett-Packard|ISS - Software Delivery Group|Digital ID Class 3 - Microsoft Software Validation v2|Hewlett-Packard|Houston|Texas|US	sha1RSA	1/30/2007 7:00:00 PM	2/16/2010 6:59:59 PM	1024	2/9/2016 5:17:08 PM	2/9/2016 5:17:08 PM	System	Certificate is Unapproved, Publisher is Approved, Certificate Path is Unapproved	a7acee3de56364404c269e47e0493406b7316d1ac0fd243c7439dcd36fbc1eb9	1
09/18/2017 02:45:28 PM	Infineon Technologies AG|SMS SW|Digital ID Class 3 - Microsoft Software Validation v2|Infineon Technologies AG|Augsburg|Bavaria|DE	sha1RSA	3/16/2005 7:00:00 PM	3/26/2006 6:59:59 PM	1024	2/10/2016 5:46:58 PM	2/10/2016 5:46:58 PM	System	Certificate is Unapproved, Publisher is Unapproved, Certificate Path is Unapproved	a280a185f163f2424bc0a34e87be168372bca69f6b6d1cb5253e17fa0da2107e	7
09/18/2017 02:45:28 PM	Sierra Wireless Inc.|Digital ID Class 3 - Microsoft Software Validation v2|Sierra Wireless Inc.|Richmond|BC|CA	sha1RSA	10/11/2005 8:00:00 PM	11/21/2006 6:59:59 PM	1024	2/10/2016 5:47:14 PM	2/10/2016 5:47:14 PM	System	Certificate is Unapproved, Publisher is Unapproved, Certificate Path is Unapproved	b90f9ccaee32a7a14edbb0ad9e27a91596474f519c8711ba6b1b976f97659c0e	1

Log Considered

id : 1

parentCertificateId : 0

publisherId : 46

thumbprint : be36a4562fb2ee05dbb3d32323adf445084ed656

thumbprintAlgorithm : SHA1

subjectName : Thawte Timestamping CA||Thawte Certification||Thawte||Durbanville||Western Cape||ZA

signatureAlgorithm : md5RSA

serialNumber : 00

validFrom : 12/31/1996 7:00:00 PM

validTo : 12/31/2020 6:59:59 PM

publicKeyAlgorithm : RSA

publicKeySize : 1024

firstSeenComputerId : 1

description :

sourceType :

dateCreated : 2/1/2016 3:31:46 PM

dateModified : 2/1/2016 3:31:46 PM

modifiedByUser : System

certificateState : 1

certificateEffectiveState : 1

certificateGlobalState : Unapproved

certificateGlobalStateDetails : Certificate is Unapproved, Publisher is Unapproved, Certificate Path is Unapproved

intermediary : True

valid : True

embedded : False

detached : False

signer : False

cosigner : False

clVersion : 0

modifiedByUserId : 32768

certificateHash : 6b6c1e01f590f5afc5fcf85cd0b9396765048659fc2c6d1170d68b045216c3fd

uniqueSignedFiles : 0

pathPositionId : 3

lastValidation : 2017-09-15T22:15:48.11Z

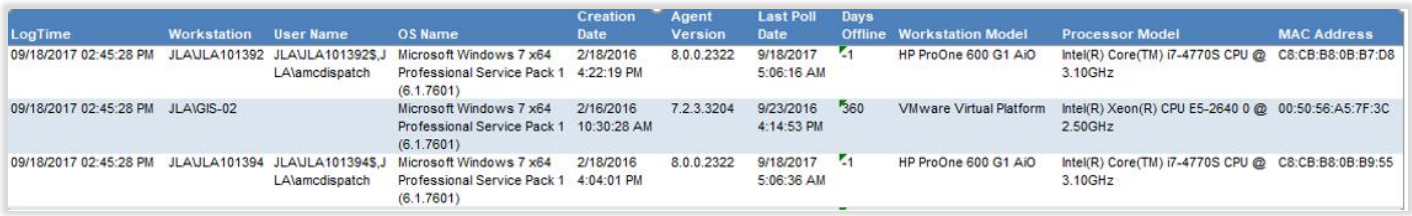
validationError :

validationErrorCode : 0

certificateStateSource :

stateReadOnly : False

- **Carbon Black Protection - Device sensor details:** This report provides details regarding sensor status of all devices in the network.



LogTime	Workstation	User Name	OS Name	Creation Date	Agent Version	Last Poll Date	Days Offline	Workstation Model	Processor Model	MAC Address
09/18/2017 02:45:28 PM	JLA\JLA101392	JLA\JLA101392$,JLA\amcdispatch	Microsoft Windows 7 x64 Professional Service Pack 1 (6.1.7601)	2/18/2016 4:22:19 PM	8.0.0.2322	9/18/2017 5:06:16 AM	-1	HP ProOne 600 G1 AiO	Intel(R) Core(TM) i7-4770S CPU @ 3.10GHz	C8:CB:B8:0B:B7:D8
09/18/2017 02:45:28 PM	JLA\GIS-02		Microsoft Windows 7 x64 Professional Service Pack 1 (6.1.7601)	2/16/2016 10:30:28 AM	7.2.3.3204	9/23/2016 4:14:53 PM	360	VMware Virtual Platform	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz	00:50:56:A5:7F:3C
09/18/2017 02:45:28 PM	JLA\JLA101394	JLA\JLA101394$,JLA\amcdispatch	Microsoft Windows 7 x64 Professional Service Pack 1 (6.1.7601)	2/18/2016 4:04:01 PM	8.0.0.2322	9/18/2017 5:06:36 AM	-1	HP ProOne 600 G1 AiO	Intel(R) Core(TM) i7-4770S CPU @ 3.10GHz	C8:CB:B8:0B:B9:55

Log Considered

id : 1

name : CONTOSO\WKSTS101142

policyId : 47

previousPolicyId : 4

users : CONTOSO\WKSTS101142$,CONTOSO\usr.it,CONTOSO\usr.it,CONTOSO\usr.it,CONTOSO\user.user

ipAddress : 10.1.1.20

connected : True

enforcementLevel : 20

```
disconnectedEnforcementLevel : 20
computerTag                  :
osShortName                  : Windows 7
osName                       : Microsoft Windows 7 x86 Professional Service Pack 1 (6.1.7601)
dateCreated                  : 2/1/2016 3:49:54 PM
agentVersion                 : 8.0.0.2322
lastPollDate                 : 9/18/2017 5:03:13 AM
policyName                   : CONTOSO-Default-WS-WIN-HE
description                  : IT Server Room - HP Compaq 8200 - kenneth
automaticPolicy              : False
localApproval                : False
prioritized                  : False
daysOffline                  : -1
uninstalled                  : False
syncPercent                  : 100
initPercent                  : 100
hasDuplicates                : False
isActive                     : True
deleted                      : False
processorCount               : 4
CLIPassword                  : AENN-SEYB-FERV-EHKK
machineModel                 : HP Compaq 8200 Elite AiO Business PC
processorSpeed               : 3292.0
processorModel               : Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz
memorySize                   : 3328
upgradeError                 :
upgradeStatus                : Up to date
syncFlags                    : 0
```

```
refreshFlags              : 0
platformId                : 1
template                  : False
templateComputerId        : 0
virtualized               : No
virtualPlatform           :
macAddress                : D0:E3:55:00:50:0C
debugLevel                : -1
kernelDebugLevel          : 0
debugFlags                : 0
activeDebugLevel          : 0
activeKernelDebugLevel    : 2
activeDebugFlags          : 16
debugDuration             : 0
ccLevel                   : 0
ccFlags                   : 0
supportedKernel           : True
hasHealthCheckErrors      : False
clVersion                 : 25283
lastRegisterDate          : 9/15/2017 12:13:45 PM
policyStatus              : Up to date
policyStatusDetails       : Up to date
upgradeErrorCount         : 0
upgradeErrorTime          :
agentMemoryDumps          : 0
systemMemoryDumps         : 0
initializing              : False
tamperProtectionActive    : True
```

agentCacheSize : 43590

agentQueueSize : 0

forceUpgrade : False

tdCount : 0

templateDate :

templateCloneCleanupMode :

templateCloneCleanupTime :

templateCloneCleanupTimeScale :

templateTrackModsOnly : False

Carbon BlackSensorVersion : 6.0.2.70329

Carbon BlackSensorFlags : 3

Carbon BlackSensorId : 2

SCEPStatus : 0

- **Carbon Black Protection - Event details:** This report provides details regarding all system events generated by Carbon Black Protection.

LogTime	File Name	File Path	Activity	Activity Severity	Activity Type	Source IP Address	User Name	Rule Name	Source WorkStation	Application Path Name	Application File Name	Installer File Name
09/18/2017 02:45:28 PM			Cb Protection Agent detected a problem: Cb Protection Agent kernel is not attached: Drive[\Device\HarddiskVolume77] Volume[\\?\Volume{5cceaff7-853b-11e7-8e86-935d070ddb6d}\] Name[\Device\HarddiskVolume77] DriveType[Fixed] FileSystem[1] Error[80070003]. Options[00000003] TotalFailures[1] FailureId[490]	5	Agent health check	172.19.9.86			JLA\AVG-RA			
09/18/2017 02:45:28 PM	slogic.bat	\\lrns-dc2\netlogon	Computer JLA\JLA101044 discovered new file \\lrns-dc2\netlogon\slogic.bat [378fe4fe1c596c1f22ee5a3630c8fab426634fdf84a3785455c38dc9d99ba678]. DiscoveredBy[Kernel:Execute] FiJLAreated[2/17/2017 1:22:33 PM] Discovered[8/21/2017 5:28:13 AM (Hash: 8/21/2017 5:28:13 AM)]	5	New unapproved file to computer	172.19.10.160	JLA\donr		JLA\JLA101044	c:\program files (x86)\dell\desktop authority\client files\10.00.442	slagent.exe	slagent.exe

Log Considered

id : 13751700

computerId :

fileCatalogId :

installerFileCatalogId :

processFileCatalogId :

fileName :

pathName :

timestamp : 8/21/2017 12:00:54 AM

receivedTimestamp : 8/21/2017 12:00:54 AM

description : Deleting 13343 events older than Jul 24 2017 12:00AM.

severity : 5

type : 0

subtype : 107

subtypeName : Old events were deleted

ipAddress :

userName : System

ruleName :

banName :

updaterName :

indicatorName :

commandLine :

processKey :

computerName :

processPathName :

processFileName :

installerFileName :

param1 : 13343

param2 : Jul 24 2017 12:00AM

param3 :

policyId :

policyName :

stringId : 247

unifiedSource :

- **Carbon Black Protection - File catalog details:** This report provides details regarding files cataloged by Carbon Black Protection.

LogTime	File Name	File Path	File Extension	MD5 Hash	File Type	File Size	Product Name	Publisher Name	Product Version	Trust	Effective State
09/18/2017 02:45:29 PM	createrlktoastlnk.exe	c:\$windows.~bt\drivers\du\d8d65593-759d-4875-90b6-90e341ee68df	exe	0b6d39ba2f59dc5f4904c69e814152c6	Application	67600	TODO: <Product name>	Microsoft Windows Hardware Compatibility Publisher	1.0.0.1	9	Approved
09/18/2017 02:45:29 PM	migcore.dll	c:\$windows.~bt\sources	dll	a36d1404139696bbafb993638ac6c811	Supporting File	6560608	Microsoft? Windows? Operating System	Microsoft Windows	10.0.10240.16444	8	Approved
09/18/2017 02:45:29 PM	tadefxapo2.dll	c:\$windows.~bt\drivers\du\d8d65593-759d-4875-90b6-90e341ee68df	dll	46ad90381fe4865d1eb3c74bc6026d3c	Supporting File	860520	TOSHIBA Audio Enhancement APO	TOSHIBA CORPORATION	1.2.2.0	-1	Unapproved
09/18/2017 02:45:29 PM	maxxaudiometers.exe	c:\$windows.~bt\drivers\du\d8d65593-759d-4875-90b6-90e341ee68df	exe	6c54aa0f7842e690a5ad441df328d42c	Application	2876032	MaxxAudioMeters	Waves Inc	4.1.6.0	9	Approved
09/18/2017 02:45:29 PM	maxxaudiorealtek.dll	c:\$windows.~bt\drivers\du\d8d65593-759d-4875-90b6-90e341ee68df	dll	a8f1ce90e1a844cd1d56c2f5398ad094	Supporting File	13798184		Waves Inc	4.4.10.0	8	Approved
09/18/2017 02:45:29 PM	maxxaudiovienna2.dll	c:\$windows.~bt\drivers\du\d8d65593-759d-4875-90b6-90e341ee68df	dll	e339f51ecc02192bd7949e813f9cef80	Supporting File	190760	MaxxAudioVienna2	Waves Inc	1.0.7.0	8	Approved
09/18/2017 02:45:29 PM	maxxspeechapo.dll	c:\$windows.~bt\drivers\du\d8d65593-759d-4875-90b6-90e341ee68df	dll	86db94219fd6a786630da7746614324b	Supporting File	965680	Waves Audio MaxxSpeech	Waves Inc	1.1.4.0	9	Approved

Log Considered

id : 1

dateCreated : 2/1/2016 9:14:34 AM

pathName : \\?\d:\newbuild\bit9installers\hostagent\patches\parityagent7.2.1\patch

fileName : parityagent7.2.1.msp

fileExtension : msp

```
md5              : 34fde3b3916f3742ee73c79a6ac5e5ae
sha1             : 1003aedf92b4a720f3c91bbeb1eb48baad532370
sha256           : 7fe951a6ddb21c0d44b3cc57afd79e17e42c5a001d8ec1c92d7d43c26faa7980
sha256HashType   : 5
fileType         : Unknown
fileSize         :
productName      :
publisher        :
company          :
publisherOrCompany :
productVersion   :
trust            : 10
effectiveState   : Approved
publisherState   : 0
approvedByReputation : False
reputationEnabled  : True
reputationAvailable : True
trustMessages    :
threat           : -1
category         : Unknown
prevalence       : 0
dirtyPrevalence  :
fileState        : 2
fileFlags        : 4456756
installedProgramName :
verdict          :
computerId       :
publisherId      : 0
```

certificateId : 0

certificateState : 0

acknowledged : True

clVersion : 778

description :

dateModified : 2/1/2016 9:14:34 AM

stateSource : Trusted Directory

nodeType : 2

transactionId :

globalStateDetails : File is globally approved (Trusted Directory), Certificate is not present

initialized : False

unifiedSource :

- **Carbon Black Protection - File instance details:** This report provides details regarding all the files triggered in the network.

LogTime	File Name	File Path	Executed	Initialized	Creation Date
09/18/2017 02:45:29 PM	winverifysignature.compiled._verifysignature.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	appenddevicetypetofacilityidfor finditem.py	c:\lec\apps\partner\maps\electrical\config\translator-backup\transforms	True	True	9/15/2017 10:31:24 AM
09/18/2017 02:45:29 PM	win32com.shell.shell.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	win32event.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	8/23/2017 2:48:38 PM
09/18/2017 02:45:29 PM	win32evtlog.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	8/23/2017 2:48:38 PM
09/18/2017 02:45:29 PM	win32file.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	8/23/2017 2:48:38 PM
09/18/2017 02:45:29 PM	win32gui.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	8/23/2017 2:48:38 PM
09/18/2017 02:45:29 PM	win32pipe.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	8/23/2017 2:48:38 PM
09/18/2017 02:45:29 PM	win32print.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	8/23/2017 2:48:38 PM
09/18/2017 02:45:29 PM	win32process.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	8/23/2017 2:48:38 PM
09/18/2017 02:45:29 PM	win32profile.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	False	8/23/2017 2:48:38 PM

Log Considered

id : 10976

fileInstanceGroupId : 2

fileCatalogId : 656

computerId : 1

policyId : 47

dateCreated : 2/1/2016 4:49:52 PM

fileName : ntclick.dll

pathName : c:\windows\system32

executed : True

localState : 2

detailedLocalState : 4

detachedPublisherId : 4

detachedCertificateId : 13

certificateId : 0

initialized : False

topLevel : False

unifiedSource :

- **Carbon Black Protection - Deleted file instance details:** This report provides details regarding all terminated file in the network.

LogTime	File Name	File Path	Initialized	Creation Date	Deletion Date
09/18/2017 02:45:29 PM	winverifysignature.compiled._verifysignature.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	9/8/2017 12:50:25 PM	9/15/2017 1:52:14 PM
09/18/2017 02:45:29 PM	appenddevicetypetofacilityiddforfinditem.py	c:\lec\apps\partner\maps\electrical\config\translator-backup\transforms	True	9/15/2017 10:31:24 AM	9/15/2017 10:31:24 AM
09/18/2017 02:45:29 PM	win32com.shell.shell.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	9/8/2017 12:50:25 PM	9/15/2017 1:52:14 PM
09/18/2017 02:45:29 PM	win32event.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	8/23/2017 2:48:38 PM	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	win32evtlog.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	8/23/2017 2:48:38 PM	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	win32file.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	8/23/2017 2:48:38 PM	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	win32gui.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	8/23/2017 2:48:38 PM	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	win32pipe.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	8/23/2017 2:48:38 PM	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	win32print.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	8/23/2017 2:48:38 PM	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	win32process.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	8/23/2017 2:48:38 PM	9/8/2017 12:50:25 PM
09/18/2017 02:45:29 PM	win32profile.pyd	c:\users\drewd\appdata\roaming\dropbox\bin	False	8/23/2017 2:48:38 PM	9/8/2017 12:50:25 PM

Log Considered

id : 10976

fileInstanceGroupId : 2

fileCatalogId : 656

computerId : 1

policyId : 47

dateCreated : 2/1/2016 4:49:52 PM

fileName : ntclick.dll

pathName : c:\windows\system32

executed : True

localState : 2

detailedLocalState : 4

detachedPublisherId : 4

detachedCertificateId : 13

certificateId : 0

initialized : False

topLevel : False

unifiedSource :

- **Carbon Black Protection - File group details:** This report provides details regarding files triggered from various installed applications across the network.

LogTime	File Name	File Path	User Name	Creation Date	Installed Application Name
09/18/2017 02:45:29 PM	wmiprvse.exe	c:\windows\system32\wbem	NT AUTHORITY\NETWORK SERVICE	2/16/2016 2:01:32 PM	
09/18/2017 02:45:29 PM	2478d.msi	c:\windows\installer		2/16/2016 3:16:43 PM	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
09/18/2017 02:45:29 PM	211ff.msi	c:\windows\installer		2/16/2016 1:52:55 PM	Microsoft Office Proof (French) 2010
09/18/2017 02:45:29 PM	211c4.msi	c:\windows\installer		2/16/2016 1:52:55 PM	Google Earth
09/18/2017 02:45:29 PM	21fe2.msi	c:\windows\installer		2/16/2016 1:51:38 PM	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148
09/18/2017 02:45:29 PM	5b4f24.msi	c:\windows\installer		2/16/2016 1:51:38 PM	ABB Network Manager DMS - ORMap
09/18/2017 02:45:29 PM	21fe2.msi	c:\windows\installer		2/16/2016 1:52:56 PM	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148
09/18/2017 02:45:29 PM	5b4f24.msi	c:\windows\installer		2/16/2016 1:52:56 PM	ABB Network Manager DMS - ORMap
09/18/2017 02:45:29 PM	58fc62.msi	c:\windows\installer		2/16/2016 1:51:39 PM	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219
09/18/2017 02:45:29 PM	12aa73e.msi	c:\windows\installer		2/16/2016 1:51:39 PM	Microsoft Visual C++ 2005 Redistributable (x64)

Log Considered

id : 10

fileCatalogId : 2565

computerId : 1

policyId : 47

dateCreated : 2/1/2016 7:31:39 PM

fileName : bf42db.msi

pathName : c:\windows\installer

userName :

groupType : 3

installedProgramName : Microsoft Office OneNote MUI (English) 2010

fileGroupId : 7

unifiedSource :

- **Carbon Black Protection - File approval details:** This report provides details regarding approval status of requested files.

LogTime	File Name	File Status	File Hash	Creation Date	Modification Date	Created By	Modified By
09/18/2017 02:45:29 PM	ts_visualeffects.ps1	Unapproved	666d03fbcc7ce7e8eae11cd37930b60de05b27356d4f0b92efa5b728116be9b5	2/17/2016 3:13:35 PM	2/17/2016 3:13:35 PM	System	System
09/18/2017 02:45:29 PM	ts_forcedshutdownnocorruption.ps1	Unapproved	e8090f2529580c00f1731f7729eecdda468ab3cf74c333380664a028260cdef3	2/17/2016 3:13:35 PM	2/17/2016 3:13:35 PM	System	System
09/18/2017 02:45:29 PM	ts_displayidletimeout.ps1	Unapproved	b798aa8c6f0bad03a2d5c3b58d3d8dd3b8da877e071ebb371b7d419f3faddb3c	2/17/2016 3:13:35 PM	2/17/2016 3:13:35 PM	System	System
09/18/2017 02:45:29 PM	ts_dimdisplay.ps1	Unapproved	a822e79a8b82164b8f15274909bd08d5840f8073dbb97540305d0d0b068a2434	2/17/2016 3:13:35 PM	2/17/2016 3:13:35 PM	System	System
09/18/2017 02:45:29 PM	ts_balanced.ps1	Unapproved	3003357719cec3472db5f25f491d372c4bd39d36b644676cbc1eb570a33234f7	2/17/2016 3:13:35 PM	2/17/2016 3:13:35 PM	System	System
09/18/2017 02:45:29 PM	rs_resetidlesleepsetting.ps1	Unapproved	1a6676392da9d9e02c7967b58d9ecae69bcf9f9fdaaf4cbe5e1da1fba8127b53	2/17/2016 3:13:35 PM	2/17/2016 3:13:35 PM	System	System
09/18/2017 02:45:29 PM	rs_resetidledisktimeout.ps1	Unapproved	a4e57e8017c6ab4d03907048185306a49a78796677ab9f7af427704f9c28aeb9	2/17/2016 3:13:35 PM	2/17/2016 3:13:35 PM	System	System

Log Considered

id : 1
fileCatalogId : 0
name : b9uninstall.sh
policyIds :
description : Approval of Bit9 File[b9uninstall.sh]
fileState : 2
reputationApprovalsEnabled : True
reportOnly : False
forceInstaller : False
forceNotInstaller : False
lazyApproval : False
fileName :
sourceType : 2
sourceId : 0
hash : 6555f3edcc7b0abdb9654d094851ce56d068f3a2820392b2Carbon Black54d6b3638076ee
dateCreated : 2/1/2016 2:13:41 PM
dateModified : 2/1/2016 2:13:41 PM
createdBy : System
modifiedBy : System
clVersion : 27
platformFlags : 0
createdByUserId : 32768
modifiedByUserId : 32768
idUnique : 74c1922e-dbbc-4578-bef3-b71eabafedf1
unifiedFlag :
origIdUnique :

unifiedSource :

fileRuleType : Approval

version : 47486991

visible : True

- **Carbon Black Protection - File upload details:** This report provides details regarding files uploaded by users across the network.

LogTime	File Name	File Path	File Upload Path	File Size	Creation Date	Modification Date
09/18/2017 02:45:29 PM	ServerPatch-2016-07-28-160128.log	D:\Program Files (x86)\Bit9\Parity Server\support	D:\Program Files (x86)\Bit9\Parity Server\support\ServerPatch-2016-07-28-160128.log	264634	9/3/2017 12:01:00 AM	9/3/2017 12:01:00 AM
09/18/2017 02:45:29 PM	SQLTrace-2017-05-17-144305.csv	D:\Program Files (x86)\Bit9\Parity Server\support	D:\Program Files (x86)\Bit9\Parity Server\support\SQLTrace-2017-05-17-144305.csv	5417	9/10/2017 12:02:00 AM	9/10/2017 12:02:00 AM
09/18/2017 02:45:29 PM	ServerLog-2017-05-17-144305.bt9	D:\Program Files (x86)\Bit9\Parity Server\support	D:\Program Files (x86)\Bit9\Parity Server\support\ServerLog-2017-05-17-144305.bt9	24639718	9/10/2017 12:02:00 AM	9/10/2017 12:02:00 AM
09/18/2017 02:45:29 PM	ServerInstall-2017517-143635.log	D:\Program Files (x86)\Bit9\Parity Server\support	D:\Program Files (x86)\Bit9\Parity Server\support\ServerInstall-2017517-143635.log	793234	9/10/2017 12:02:00 AM	9/10/2017 12:02:00 AM
09/18/2017 02:45:29 PM	ReporterLog-2017-05-17-144305.log	D:\Program Files (x86)\Bit9\Parity Server\support	D:\Program Files (x86)\Bit9\Parity Server\support\ReporterLog-2017-05-17-144305.log	7560173	9/10/2017 12:02:00 AM	9/10/2017 12:02:00 AM
09/18/2017 02:45:29 PM	PHPErrors-2017-05-17-144305.log	D:\Program Files (x86)\Bit9\Parity Server\support	D:\Program Files (x86)\Bit9\Parity Server\support\PHPErrors-2017-05-17-144305.log	107843	9/10/2017 12:02:00 AM	9/10/2017 12:02:00 AM
09/18/2017 02:45:29 PM	SRSAudit-2016-12-21-111729.log	D:\Program Files (x86)\Bit9\Parity Server\support	D:\Program Files (x86)\Bit9\Parity Server\support\SRSAudit-2016-12-21-111729.log	0	9/6/2017 12:02:00 AM	9/6/2017 12:02:00 AM

Log Considered

id : 293

fileCatalogId :

computerId : 0

priority : 0

createdBy :

dateCreated : 8/28/2017 12:00:00 AM

dateModified : 8/28/2017 12:00:00 AM

fileName : ServerInstall-201621-140552.log

pathName : D:\Program Files (x86)\Bit9\Parity Server\support

uploadPath : D:\Program Files (x86)\Bit9\Parity Server\support\ServerInstall-201621-140552.log

uploadedFileSize : 711935

uploadStatus : 3

createdByUserId :

- **Carbon Black Protection - Internal event details:** This report provides details regarding all internal events generated on Carbon Black Protection.

LogTime	File Name	Event Details	Event Severity	Event SubType	Source IP Address	User Name	Source Workstation	Process Path Name	Process File Name
09/18/2017 02:45:28 PM	c:\windows\syswow64	File c:\windows\syswow64\cmd.exe [614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f] was executed.	5	Report execution (custom rule)	172.19.10.160	JLA\donr	JLA\JLA101044	c:\program files (x86)\dell\desktop authority\client files\10.00.442	slagent.exe
09/18/2017 02:45:28 PM	\\lrns-dc2\netlogon	Computer JLA\JLA101208 discovered new file \\lrns-dc2\netlogon\slogic.bat [378fe4fe1c596c1f22ee5a3630c8fab426634fdf84a3785455c38dc9d99ba678]. DiscoveredBy[Kernel:Execute] FiJLAreated[2/17/2017 1:22:33 PM] Discovered[8/21/2017 5:28:01 AM (Hash: 8/21/2017 5:28:01 AM)]	5	New unapproved file to computer	172.19.10.168	JLA\jeffk	JLA\JLA101208	c:\program files (x86)\dell\desktop authority\client files\10.00.442	slagent.exe
09/18/2017 02:45:28 PM		Cb Protection Agent failed a health check. Issues found Total[4] High[0] Medium[2] Low[0] TestError[2] Options[00000003]	4	Agent health check	172.19.9.86		JLA\AVG-RA		
09/18/2017 02:45:28 PM	\\lrns-dc2\netlogon	Computer JLA\JLA101471 discovered new file \\lrns-dc2\netlogon\slogic.bat [378fe4fe1c596c1f22ee5a3630c8f	5	New unapproved file to computer	172.19.10.132	JLA\jeffk	JLA\JLA101471	c:\program files (x86)\dell\desktop authority\client files\10.00.442	slagent.exe

Log Considered

id : 1065300

computerId : 218

fileCatalogId :

installerFileCatalogId :

processFileCatalogId :

fileName :

pathName :

timestamp : 8/21/2017 12:04:06 AM

receivedTimestamp : 8/21/2017 12:04:09 AM

description : Internal error reported from CONTOSO\WKSTS101095: Database errors discovered ErrorTypes[00000400:OrphanDabIEID] Number[17].

severity : 3

type : 8

subtype : 1302

subtypeName : Internal Agent error

ipAddress : 10.11.10.21

userName :

ruleName :

banName :

updaterName :

indicatorName :

commandLine :

processKey :

computerName : CONTOSO\WKSTS101095

processPathName :

processFileName :

installerFileName :

param1 : ErrorTypes[00000400:OrphanDabIEID] Number[17]

param2 :

param3 :

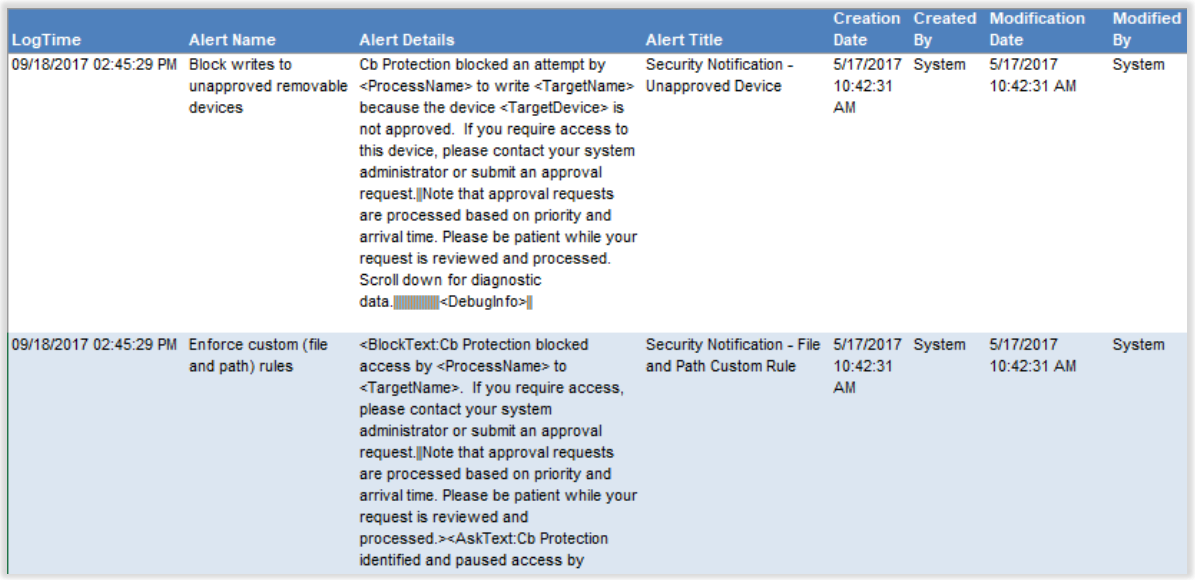
policyId : 48

policyName : CONTOSO-WS-WIN-CSR-HE

stringId : 4008

unifiedSource :

- **Carbon Black Protection - Alert details:** This report provides details regarding all alerts triggered by Carbon Black Protection.



LogTime	Alert Name	Alert Details	Alert Title	Creation Date	Created By	Modification Date	Modified By
09/18/2017 02:45:29 PM	Block writes to unapproved removable devices	Cb Protection blocked an attempt by <ProcessName> to write <TargetName> because the device <TargetDevice> is not approved. If you require access to this device, please contact your system administrator or submit an approval request.|Note that approval requests are processed based on priority and arrival time. Please be patient while your request is reviewed and processed. Scroll down for diagnostic data.|||||||||<DebugInfo>|	Security Notification - Unapproved Device	5/17/2017 10:42:31 AM	System	5/17/2017 10:42:31 AM	System
09/18/2017 02:45:29 PM	Enforce custom (file and path) rules	<BlockText:Cb Protection blocked access by <ProcessName> to <TargetName>. If you require access, please contact your system administrator or submit an approval request.|Note that approval requests are processed based on priority and arrival time. Please be patient while your request is reviewed and processed.><AskText:Cb Protection identified and paused access by	Security Notification - File and Path Custom Rule	5/17/2017 10:42:31 AM	System	5/17/2017 10:42:31 AM	System

Log Considered

id : 10001

name : Enforce tamper protection(custom 1)

messageText : Bit9 Security Platform blocked access by <ProcessName> to a protected resource <TargetName>.|||||||||||||||<DebugInfo>

eventLogText :

title : Security Notification - Tamper Protection

url :

fgImageLocation : logo.gif

bgImageLocation : bkg.gif

timeout : -1

showLogo : True

logoUrl : http://intranet.Contoso.com/images/Contoso-logo-60x60.gif

flags : 0

systemNotifier : True

defaultRuleType : 0

defaultRuleGroupId : 0

dateCreated : 2/1/2016 9:14:20 AM

createdBy : System

dateModified : 4/6/2016 12:29:15 PM

modifiedBy : it@Contoso.com

clVersion : 8584

usageCount : 30

createdByUserId : 32768

modifiedByUserId : 1

- **Carbon Black Protection - Policy details:** This report provides details regarding all policies applied across the network.

LogTime	Policy Name	Policy Description	Modification Date	Creation Date	Total Computers	Connected Computers
09/18/2017 02:45:29 PM	JLA-WS-WIN-IT-LE	JLA - Workstation - Windows - IT - Low Enforcement	9/17/2017 12:03:14 PM	2/9/2016 12:55:34 PM	4	1
09/18/2017 02:45:29 PM	JLA-WS-WIN-CSR-HE-Pilot	Candidates for High Enforcement	9/17/2017 12:03:20 PM	4/6/2016 3:20:41 PM	0	0
09/18/2017 02:45:29 PM	JLA-Default-WS-WIN-HE-Pilot	Candidates for High Enforcement	9/17/2017 12:03:19 PM	4/6/2016 3:17:11 PM	6	1
09/18/2017 02:45:29 PM	JLA-Default-SVR-WIN-HE-Pilot	Candidates for High Enforcement	9/17/2017 12:03:19 PM	4/6/2016 3:13:13 PM	1	1
09/18/2017 02:45:29 PM	JLA-WS-WIN-HR-TS	JLA - Workstation - Windows - HR - Troubleshooting	9/17/2017 12:03:18 PM	2/16/2016 12:40:11 PM	0	0
09/18/2017 02:45:29 PM	JLA-WS-WIN-HR-LE	JLA - Workstation - Windows - HR - Low Enforcement	9/17/2017 12:03:18 PM	2/16/2016 12:39:40 PM	0	0
09/18/2017 02:45:29 PM	JLA-WS-WIN-CSR-TS	JLA - Workstation - Windows - CSR - Troubleshooting	9/17/2017 12:03:18 PM	2/16/2016 12:20:49 PM	0	0
09/18/2017 02:45:29 PM	JLA-WS-WIN-CSR-LE	JLA - Workstation - Windows - CSR - Low Enforcement	9/17/2017 12:03:17 PM	2/16/2016 12:20:13 PM	2	1
09/18/2017 02:45:29 PM	JLA-SVR-DC-TS	JLA - Server - Domain Controller - Troubleshooting	9/17/2017 12:03:17 PM	2/9/2016 1:11:39 PM	0	0
09/18/2017 02:45:29 PM	JLA-Default-WS-WIN-TS	JLA - Default - Worstation - Windows - Troubleshooting	9/17/2017 12:03:16 PM	2/9/2016 1:10:57 PM	0	0
09/18/2017 02:45:29 PM	JLA-Default-SVR-WIN-TS	JLA - Default - Server - Windows - Troubleshooting	9/17/2017 12:03:16 PM	2/9/2016 1:09:36 PM	0	0

Log Considered

id : 1

name : Default Policy

description : Computers will be automatically placed into this policy if they are not assigned to a specific policy (either manually or through mapping rules)

packageName :

enforcementLevel : 60

disconnectedEnforcementLevel : 60

helpDeskUrl :

imageUrl :

dateModified : 9/17/2017 12:03:13 PM

dateCreated : 2/1/2016 1:13:31 PM

readOnly : False

hidden : False

automatic : False

loadAgentInSafeMode : False

reputationEnabled : True

fileTrackingEnabled : True

customLogo : True

automaticApprovalsOnTransition : False

allowAgentUpgrades : False

totalComputers : 1

connectedComputers : 0

atEnforcementComputers : 0

clVersionMax : 0

createdByUserId : 0

modifiedByUserId : 0

- **Carbon Black Protection - Certificate publisher details:** This report provides details about publishers whose certificates are being used in the network.

LogTime	Publisher Name	Creation Date	Signed Files Count	Signed Certificate Count
09/18/2017 02:45:29 PM	Fuji Xerox Co.,Ltd.	2/16/2016 12:44:28 PM	1	1
09/18/2017 02:45:29 PM	SkyHawke Technologies, LLC	2/16/2016 12:59:26 PM	4	2
09/18/2017 02:45:29 PM	AliphCom	2/16/2016 1:41:42 PM	3	1
09/18/2017 02:45:29 PM	SmartDraw, LLC	2/16/2016 1:41:49 PM	7	1
09/18/2017 02:45:29 PM	MarkedUp, Inc	2/16/2016 1:42:14 PM	5	1
09/18/2017 02:45:29 PM	SmartDraw Software, LLC	2/16/2016 1:42:23 PM	13	3
09/18/2017 02:45:29 PM	iZotope, Inc.	2/16/2016 1:43:36 PM	1	1
09/18/2017 02:45:29 PM	Rovi	2/16/2016 1:43:44 PM	20	1
09/18/2017 02:45:29 PM	Mindspark Interactive Network	2/16/2016 1:44:56 PM	3	2
09/18/2017 02:45:29 PM	NEXTUP TECHNOLOGIES, LLC	2/16/2016 1:45:29 PM	16	2
09/18/2017 02:45:29 PM	ThinkBuzan Ltd	2/16/2016 1:45:35 PM	6	2
09/18/2017 02:45:29 PM	ActivIdentity	2/16/2016 12:43:49 PM	3	1
09/18/2017 02:45:29 PM	Peernet Inc.	2/16/2016 12:43:51 PM	26	2
09/18/2017 02:45:29 PM	Sonic Solutions	2/16/2016 12:43:52 PM	576	3

Log Considered

```
id                  : 1
name                : Bit9, Inc
description         :
modifiedBy          : System
dateModified        : 2/1/2016 1:13:40 PM
dateCreated         : 2/1/2016 1:13:30 PM
publisherReputation : 3
publisherState      : 2
policyIds           :
reputationApprovalsEnabled : False
sourceType          : 1
```

firstSeenComputerId :

platformFlags : 0

signedFilesCount : 185

signedCertificateCount : 3

clVersion : 26

hidden : False

modifiedByUserId : 32768

acknowledgedByUserId :

dateAcknowledged :

firstSeenPlatformId : 1

acknowledged : False

stateSource : Manual

- **Carbon Black Protection - Script rule details:** This report provides details regarding script execution policies applied across the network.

LogTime	Script Type	Script Pattern	Script Process	Creation Date	Modification Date	Created By	Modified By
09/18/2017 02:45:29 PM	TCL	*.tcl	<ASSOC_EXE:.tcl>	2/1/2016 1:13:31 PM	2/1/2016 1:13:31 PM	32768	32768
09/18/2017 02:45:29 PM	Linux Perl	*.pl	/usr/bin/perl	2/1/2016 1:13:31 PM	2/1/2016 1:13:31 PM	32768	32768
09/18/2017 02:45:29 PM	Linux Shell	|*.sh|*.csh|*.zsh|*.ksh	|/bin/bash|/bin/csh|/bin/ksh|/bin/sh|/bin/tcsh|/bin/zsh|/bin/dash|/bin/static-sh|/bin/busybox|/usr/bin/bash|/usr/bin/csh|/usr/bin/ksh|/usr/bin/sh|/usr/bin/tcsh|/usr/bin/zsh|/usr/bin/dash|/usr/bin/static-sh|/usr/bin/busybox	2/1/2016 1:13:31 PM	2/1/2016 1:13:31 PM	32768	32768
09/18/2017 02:45:29 PM	Mac Python	|*.py|*.pyc|*.pyo	*/python*	2/1/2016 1:13:31 PM	2/1/2016 1:13:31 PM	32768	32768
09/18/2017 02:45:29 PM	Mac Perl	*.pl	/usr/bin/perl*	2/1/2016 1:13:31 PM	2/1/2016 1:13:31 PM	32768	32768
09/18/2017 02:45:29 PM	Mac Shell	|*.sh|*.csh|*.zsh|*.ksh	|/bin/bash|/bin/csh|/bin/ksh|/bin/sh|/bin/tcsh|/bin/zsh	2/1/2016 1:13:31 PM	2/1/2016 1:13:31 PM	32768	32768
09/18/2017 02:45:29 PM	Mozilla Extensions	*.xpi	|<ASSOC_EXE:.xpi>	2/1/2016 1:13:31 PM	2/1/2016 2:03:17 PM	32768	1
09/18/2017 02:45:29 PM	Linux Python	|*.py|*.pyc|*.pyo	|*/python|*/python?.?	2/1/2016 1:13:31 PM	2/1/2016 1:13:31 PM	32768	32768

Log Considered

id : 10

name : Batch

description :

pattern : |*.cmd|*.bat

processName : |<System>\cmd.exe|<Systemx86>\cmd.exe

dateCreated : 2/1/2016 1:13:30 PM

dateModified : 2/1/2016 1:13:30 PM

clVersion : 2

platformId : 1

createdByUserId : 32768

createdBy : System

modifiedByUserId : 32768

modifiedBy : System

hidden : False

enabled : True

rescanComputers : True

definitionType : 1

- **Carbon Black Protection - Server settings details:** This report provides details regarding settings of Carbon Black Protection.

LogTime	Setting Name	Setting Value	Modified By	Modification Date	Setting Version
09/18/2017 02:45:29 PM	ReporterLastSSTaskTimestamp	9/18/2017 3:34:36 AM	System	9/18/2017 3:34:36 AM	59118623
09/18/2017 02:45:29 PM	UpdaterLoaderRowVersion	1074203	System	9/6/2017 12:09:13 PM	1074203
09/18/2017 02:45:29 PM	UpdatersVersion	8000	System	5/17/2017 2:42:45 PM	8000
09/18/2017 02:45:29 PM	DBMaintenanceInProgress	0	System	9/18/2017 12:00:51 AM	59116311
09/18/2017 02:45:29 PM	ParityServerOSDescription	Microsoft Windows Server 2012 R2 x64 Server Datacenter (6.3.9600)	System	2/1/2016 1:14:33 PM	2729
09/18/2017 02:45:29 PM	ParityServerOSVersion	100859904	System	2/1/2016 1:14:33 PM	100859904
09/18/2017 02:45:29 PM	ParityServerProcessorCount	4	System	2/1/2016 1:14:33 PM	2731
09/18/2017 02:45:29 PM	ParityServerProcessorSpeedMHz	2295	System	2/1/2016 1:14:33 PM	2732
09/18/2017 02:45:29 PM	ParityServerProcessorDescription	Intel(R) Xeon(R) CPU E5-2670 v3 @ 2.30GHz	System	2/1/2016 1:14:33 PM	2733
09/18/2017 02:45:29 PM	API_UploadsAvailable	true	System	2/1/2016 1:14:39 PM	3250
09/18/2017 02:45:29 PM	API_NotificationsAvailable	true	System	2/1/2016 1:14:39 PM	3251
09/18/2017 02:45:29 PM	BackupRequested	Feb 1 2016 2:14PM	System	2/1/2016 1:14:39 PM	3252
09/18/2017 02:45:29 PM	ReporterMetadataLookupCount	1000	System	2/1/2016 1:13:52 PM	2460
09/18/2017 02:45:29 PM	adLoginBaseDomain	LEC.com	admin	2/1/2016 1:25:23 PM	3285

Log Considered

id : 1

name : syslogFormat

value : enhanced

modifiedBy : System

dateModified : 2/1/2016 1:13:31 PM

version : 2102

- **Carbon Black Protection - Application details:** This report provides details regarding various installed applications across the network.

LogTime	Application Name	Enabled	Created By	Creation Date	Modified By	Modification Date	Application Version
09/18/2017 02:45:29 PM	Adobe Reader	False	System	2/1/2016 1:14:28 PM	System	5/17/2017 2:42:47 PM	4
09/18/2017 02:45:29 PM	Linux Self Protection	True	System	5/17/2017 2:43:04 PM	System	5/17/2017 2:43:04 PM	1
09/18/2017 02:45:29 PM	Google Drive	False	System	2/1/2016 1:14:29 PM	System	2/8/2016 1:27:36 PM	6
09/18/2017 02:45:29 PM	Google Chrome	False	System	2/1/2016 1:14:29 PM	System	3/1/2016 3:10:10 PM	18
09/18/2017 02:45:29 PM	Symantec Endpoint Protection for Mac	False	System	2/1/2016 1:14:29 PM	System	2/1/2016 1:14:29 PM	2
09/18/2017 02:45:29 PM	Flowdock	False	System	2/1/2016 1:14:29 PM	System	2/29/2016 3:05:03 PM	2
09/18/2017 02:45:29 PM	Mac System Updates	False	System	2/1/2016 1:14:29 PM	System	5/17/2017 2:42:48 PM	7

Log Considered

id : 1

name : Adobe FrameMaker

enabled : False

createdBy : System

dateCreated : 2/1/2016 1:14:25 PM

modifiedBy : System

dateModified : 2/1/2016 1:14:25 PM

version : 9

clVersion : 0

platformFlags : 1

createdByUserId : 32768

modifiedByUserId : 32768

- **Carbon Black Protection - User details:** This report provides details regarding user registered on Carbon Black Protection.

LogTime	User Name	Email ID	First Name	Last Name	Title	Department	Registration Date	Enabled	User Group Id
09/18/2017 02:45:29 PM	admin	it.support@contoso.com					2/1/2016 1:13:31 PM	True	3,4
09/18/2017 02:45:29 PM	dott.it@jla.com	dott.it@contoso.com	Daniel	Ott			2/1/2016 1:29:13 PM	True	4
09/18/2017 02:45:29 PM	tellyw@jla.com	tellyw@contoso.com	Telly	Williams	Help Desk	IT	2/25/2016 3:46:33 PM		
09/18/2017 02:45:29 PM	tellyw.it@jla.com		Telly	Williams			2/26/2016 10:13:04 AM	True	4
09/18/2017 02:45:29 PM	miket.it@jla.com	miket.it@contoso.com	Mike	Tucker			3/9/2016 7:14:15 AM	True	4
09/18/2017 02:45:29 PM	michaelt@jla.com	michaelt@contoso.com	Mike	Tucker	Help Desk	IT	3/30/2016 4:25:21 PM		
09/18/2017 02:45:29 PM	dott@jla.com	dott@contoso.com	Daniel DFO	Ott	Systems Analyst	IT	8/22/2016 11:09:31 AM		

Log Considered

id : 0

name : admin

apiToken : A54F5BF8-0E86-4CFE-8BBA-95EB0FA226E6

passwordHash :

passwordSalt :

eMailAddress : itsupport@contoso.com

firstName :

lastName :

title :

salutation :

department :

homePhone :

cellPhone :

backupCellPhone :

pager :

backupPager :

comments :

adminComments :

registrationDate : 2/1/2016 1:13:31 PM

readOnly : False

external : False

automatic : True

enabled : True

unified :

userGroupIds : 3,4

- **Carbon Black Protection - User group details:** This report provides details regarding user groups created on Carbon Black Protection.

LogTime	Group Name	User Permissions	Enabled	Editable	Creation Date	Created By	Modification Date	Modified By	Modification Count
09/18/2017 02:45:29 PM	ReadOnly	00408202028a0491	True	True	2/1/2016 1:13:30 PM	System	2/1/2016 1:13:30 PM	System	0
09/18/2017 02:45:29 PM	PowerUser	0042c71e1fffffff	True	True	2/1/2016 1:13:30 PM	System	2/1/2016 1:13:30 PM	System	0
09/18/2017 02:45:29 PM	Administrator	007aff7f7fffffff	True	True	2/1/2016 1:13:30 PM	System	2/1/2016 1:28:36 PM	admin	1
09/18/2017 02:45:29 PM	Administrator (Unified Management)	01faff7f7fffffff	True	True	5/17/2017 2:40:39 PM	System	5/17/2017 2:40:39 PM	System	4
09/18/2017 02:45:29 PM	User (Unified Management)	00c08202028b04f1	True	True	5/17/2017 2:40:39 PM	System	5/17/2017 2:40:39 PM	System	0

Log Considered

id : 1

name : ReadOnly

permissions : 00408202028a0491

enabled : True

editable : True

description :

dateCreated : 2/1/2016 1:13:30 PM

createdByUserId : 32768

createdBy : System

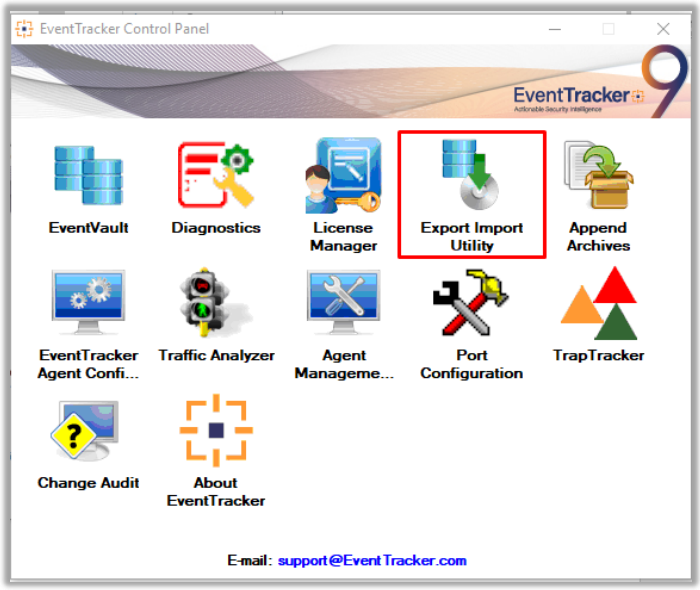
```
dateModified    : 2/1/2016 1:13:30 PM
modifiedByUserId : 32768
modifiedBy      : System
automaticCount  : 0
manualCount     : 0
policyIds       :
```

6. Importing knowledge pack into EventTracker

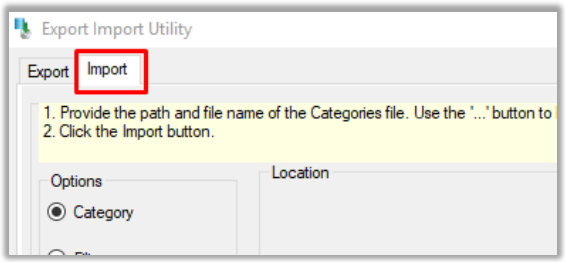
NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.



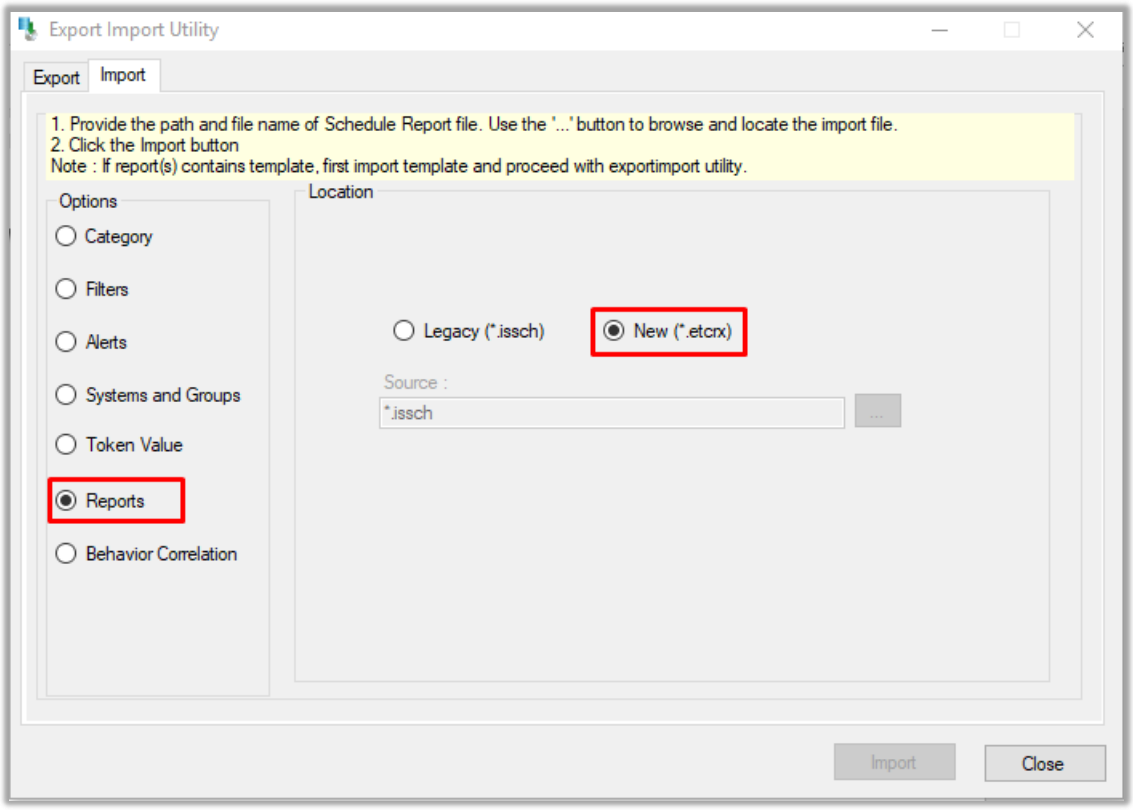
Export-Import Utility window opens.



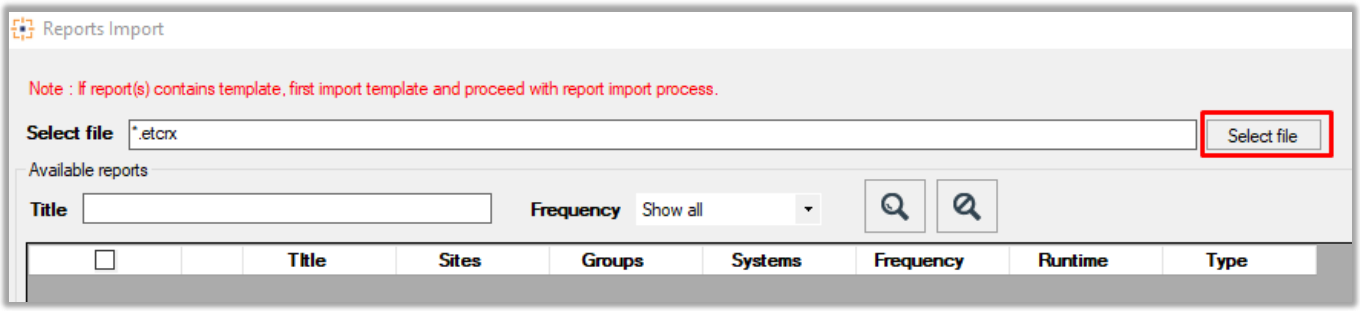
3. Click the **Import** tab.

6.1 Flex Reports

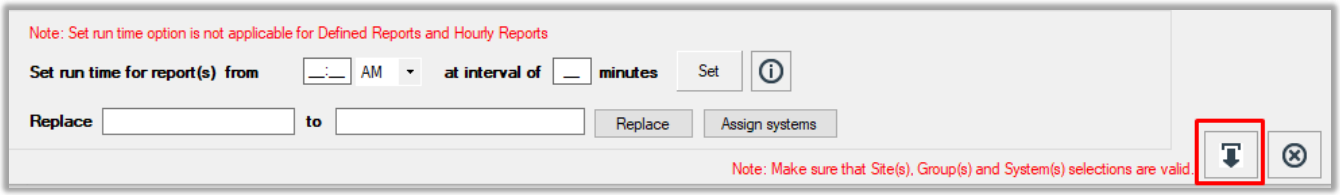
1. In **Export-Import Utility** window, select the **Import tab**. Click the **Reports** option, and choose **New (*.etcrx)**.



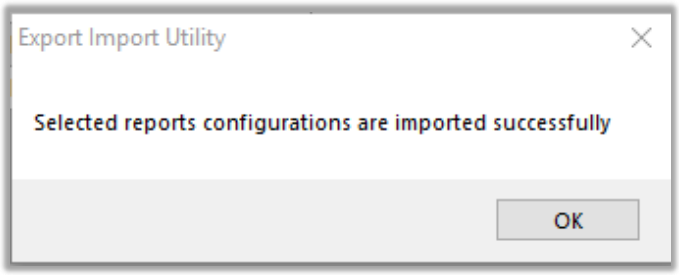
2. A new pop-up window appears. Click the **Select File** button and navigate to the knowledge pack folder and select file with the extension **".etcrx", e.g., Reports_Carbon Black Protection.etcrx.**



3. Wait while reports populate. Select all the relevant reports and click **Import** .



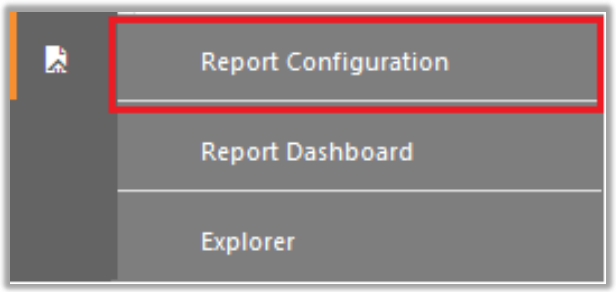
EventTracker displays a success message.



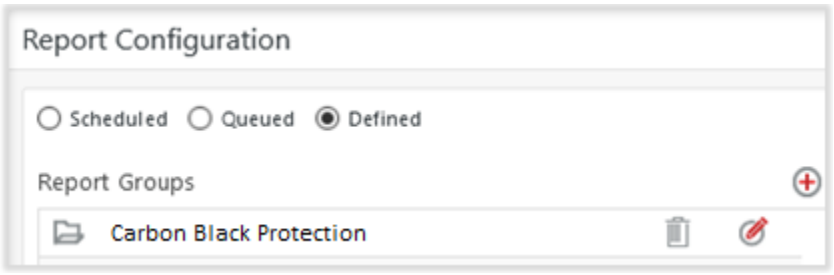
7. Verifying knowledge pack in EventTracker

7.1 Flex Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.



2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Carbon Black Protection** group folder to view the imported reports.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support