BeyondTrust

Privilege Management Cloud 23.7 Elastic Common Schema (ECS) Events Reference Guide

TC:8/28/2023

PM Cloud ECS Event Reference

Why Change to ECS?

PM Cloud is developing a more scalable data infrastructure to better support your reporting, analytics, and insights needs.

We're using the elastic stack to provide scale and speed in ingesting and searching the millions of events we process every day.

To enable better correlation of our data with others sources and make our events easier to work with, we have adopted the well known open source schema that was built for Elastic: the Elastic Common Schema (ECS).

> *For more information, please see Elastics Docs at https://www.elastic.co/guide/en/ecs/current/ecs-reference.html.*

What Does it Mean For Me?

There is no change in your existing analytics or SIEM integrations in PM Cloud.

A new API is exposed to extract the events in bulk.

```
get /v{version}/Events/FromStartDate
```

The following is an example PowerShell usage script.

> ***Note:** PowerShell 7 is required.*

```
param (
  [Parameter(mandatory = $true)] $nextDate,
  [Parameter(mandatory = $true)] $tenantName,
  [Parameter(mandatory = $true)] $apiClientId,
  Parameter(mandatory = $true)] $apiClientSecret,
  $resource = 'domains',
  $lookupCache = 'false',
  $pageSize = 100,
  $pageNumber = 1
)



$_baseUrl = "https://$tenantName-services.epm.btrusteng.com"

function Get-AccessToken(
  [Parameter(mandatory = $true)][string] $apiClientId,
  [Parameter(mandatory = $true)][string] $apiClientSecret) {

  $authBody = @{
    client_id     = "$apiClientId"
    client_secret = "$apiClientSecret"
    scope         = "urn:management:api"
```

```
    grant_type    = "client_credentials"
    }
  $tokenUrl = "$_baseUrl/oauth/token"
  Write-Host "Requesting $tokenUrl"
  $response = Invoke-WebRequest -Uri $tokenUrl `
    -ContentType "application/x-www-form-urlencoded" `
    -Body $authBody `
    -Method Post `
    -ErrorAction Stop
  $accessToken = $response.content | ConvertFrom-Json
  return $accessToken
}

function Get-AllPages( [Parameter(mandatory = $true)][System.Object] $accessToken,
  [Parameter(mandatory = $true)][string] $nextDate) {
  $page = 1;
  while ($true) {
    if (($accessToken.expires_in - $TotalStopwatch.Elapsed.Seconds ) -lt 10) {
       Write-Host "******* AccessToken Expiring in 10 Sec So Re-Requesting New Accesstoken
********"
       $accessToken = Get-AccessToken $apiClientId $apiClientSecret
    }
    $headers = @{
       'Authorization'     = "Bearer " + $accessToken.access_token
       'Content-Type'      = 'application/json'
       'ExpiresOn'         = $accessToken.expires_in
       'client-request-id' = New-Guid
    }
    $Stopwatch = [System.Diagnostics.Stopwatch]::StartNew()
    $resourceUrl = "$_baseUrl/management-
api/v1/Events/FromStartDate?StartDate=$nextDate&RecordSize=1000"
    $Response = Invoke-WebRequest -Uri $resourceUrl -Headers $headers -Method Get -ErrorAction
Stop
    $Stopwatch.Stop()

    $jsonObj = ConvertFrom-Json $([String]::new($Response.Content))
    $lastTimeStamp = $jsonObj.events[$jsonObj.events.Count - 1].event.ingested.ToUniversalTime
().ToString('o')
    $timetake = $Stopwatch.ElapsedMilliseconds
    $line = "$page*1000 -- $nextDate  TimeTake: $timetake"
    $line | Out-File -FilePath .\fetchResult.txt -Append
    # $Response.Content| Out-File -FilePath .\fetchResult.txt -Append

    Write-Host $line
    $page++
    $nextDate = $lastTimeStamp
    if ($jsonObj.events.Count -lt 1000) { break; }

    }

}

$TotalStopwatch = [System.Diagnostics.Stopwatch]::StartNew()
$accessToken = Get-AccessToken $apiClientId $apiClientSecret
Get-AllPages $accessToken $nextDate
```

```
$TotalStopwatch.Stop()
$sec = $TotalStopwatch.Elapsed.TotalSeconds
$finishLine = "Total Time Taken To Fetch All Pages $sec Seconds"
$finishLine | Out-File -FilePath .\fetchResult.txt -Append
Write-Host
Write-Host $finishLine
exit(0);
```

ECS Based Events

The following tables indicate the presence of field sets for each event type currently raised.

The *Field Sets* tables contain the following:

- Some field sets are always present.
- Some are always present for that event type.
- Some always present for a given application type.
- Some are always optional, present when a particular rule configuration drives them.

The *Fields Sets Details* tables contain fields within a field set and whether they are mandatory or optional (within that field set).

Some ECS field sets are extended with custom fields where necessary. For those properties specific to Privilege Management, there is a EPMWinMac field set too.

- Field Sets
  - Windows Processes - Field Sets
  - Mac Processes - Fields Sets
  - Other - Field Sets
- Fields Sets Detail
  - Common
  - User
  - Configuration
  - Process
  - Windows Process
  - macOS Process
  - File
  - Windows Executable File
  - macOS Executable File
  - Hosted File
  - macOS Hosted File
  - Windows COM
  - Windows ActiveX
  - Windows Store Apps
  - Windows Remote PowerShell
  - Windows Installers
  - Uninstallers
  - Services
  - PPAM
  - DLL
  - User Session

- EPM Start
- EPM Stop
- Authorizing User
- Rule Script
- Trusted Application Protection

For more information on Elastic custom fields, please see Custom Fields at https://www.elastic.co/guide/en/ecs/current/ecs-custom-fields-in-ecs.html.

Field Sets

Key for Field Sets

Cell Value	Definition	Description
m	mandatory	Field set will always be populated.
o	optional	Field set populated if the feature was used on that rule. Configuration driven.

Windows Processes - Field Sets

Event Action (event.action)	process-start-*process requires-elevation						process-start-*
Event Code(s)	*100-120*	*100-120*	*100-120*	*100-120*	*100-120*	*100-120*	*100-120*
Application Types	exe	unin, unex'	cpl, msc, msi, wsh, ps1, bat, reg	unin, unex^	com	ocx	appx
Common	m	m	m	m	m	m	m
User	m	m	m	m	m	m	m
Configuration	m	m	m	m	m	m	
Process	m	m	m	m	m	m	
Win Process	m	m	m	m			
File	m	m					m
Win Exe File	m	m					m
Win Hosted File			m	m			
Win Installers				m			
Win Uninstallers		m		m			
COM					m		
ActiveX						m	
Store Apps							m
Authorizing User	o	o	o	o	o	o	o

Event Action (event.action)	process-start-*process requires-elevation						process-start-*
Event Code(s)	*100-120*	*100-120*	*100-120*	*100-120*	*100-120*	*100-120*	*100-120*
Application Types	exe	unin, unex'	cpl, msc, msi, wsh, ps1, bat, reg	unin, unex^	com	ocx	appx
Rule Script	o	o	o	o	o	o	
TAP	o	o	o	o			

'- when Parent Process *is not* msiexec.exe

^- when Parent Process *is* msiexec.exe

Mac Processes - Field Sets

Event Action (event.action)	process-start-*	process-start-*	bundle-*
Event Code(s)	*100-120*	*100-120*	*130,131*
Application Types	bin, bund, pref, pkg	sudo, scr	bund
Common	m	m	m
User	m	m	m
Configuration	m	m	m
Process	m	m	m
mac Process	m	m	
File	m		
mac Exe File	m		
mac Hosted File		m	
Authorizing User	o	o	o

Other - Field Sets

Event Action (event.action)	license-unlicensed	service-*	privileged-group-modification-blocked	challenge-response-authorization-failed-process-blocked	user-logon	epm-service-start	epm-service-stop	file-*	dll-load-*
Operating System	*Win, Mac*	*Win*	*Win*	*Win, Mac*	*Win*	*Win*	*Win*	*Win*	*Win*
Event Code(s)	10	150-162	198	199	300	400	401	600-606	706,716,720
Application Types	*-*	*svc*	*-*	*-*	*-*	*-*	*-*	*cont*	*dll*
Common	m	m	m	m	m	m	m	m	m
User		m	m	m	m			m	m

Event Action (event.action)	license-unlicensed	service-*	privileged-group-modification-blocked	challenge-response-authorization-failed-process-blocked	user-logon	epm-service-start	epm-service-stop	file-*	dll-load-*
Operating System	*Win, Mac*	*Win*	*Win*	*Win, Mac*	*Win*	*Win*	*Win*	*Win*	*Win*
Event Code(s)	10	150-162	198	199	300	400	401	600-606	706,716,720
Application Types	*-*	*svc*	*-*	*-*	*-*	*-*	*-*	*cont*	*dll*
EPM Start						m			
EPM Stop							m		
User Session					m				
Configuration		m		m				m	m
Process			m	m				m	m
Win Process									m
File								m	m
Services		m							
PPAM			m						
DLL									m
Authorizing User		o						o	
TAP									m

Field Sets Detail

Key for Field Sets Detail

Cell Value	Definition	Description
m	mandatory	Field will always be populated
o	optional	Field populated if the data exists and can be sourced for this event

Common

All events raised will have these fields.

Field ECS	ECS Type	Required	Examples
@timestamp	date	m	2023-03-16T08:05:34.853Z
agent.id	keyword	m	4965825c-0da2-4cce-a99e-af655d1fcc0d
agent.version	keyword	m	23.1.0.1
event.action	keyword	m	process-start-blocked, privileged-group-modification-blocked

Field ECS	ECS Type	Required	Examples
event.code	keyword	m	100, 116, 400
event.id	keyword	m	a5239a3a-e352-416d-9927-708d7ef65910
host.domain	keyword	o	StanLand
host.hostname	keyword	m	Stan-Win-PC
host.id	keyword	m	S-1-5-21-995079707-3417812545-548763902-4783
host.DomainIdentifier	keyword	o	S-1-5-21-995079707-3417812545-548763902
host.os.type	keyword	m	windows, macos
host.os.version	keyword	m	12.4
EPMWinMac.Event.Type	keyword	m	Process, Content
EPMWinMac.GroupId	keyword	m	099ce279-5d33-4331-8a94-2b1c76073085
EPMWinMac.SchemaVersion	keyword	m	4.4.0

User

Field ECS	ECS Type	Required (when this field is present)	Examples
user.name	keyword	m	Stan
user.domain	keyword	o	StanLand
user.id	keyword	m	S-1-5-21-1234567890-1212121212-635717638-56524798
user.DomainIdentifier	keyword	o	S-1-5-21-1234567890-1212121212-635717638
user.LocalIdentifier	keyword	o	501

Configuration

Any event raised by a Privilege Management for Windows or Privilege Management for Mac rule match has these fields.

Field ECS	ECS Type	Required (when this field set is present)	Examples
EPMWinMac.Configuration.Application.Type	keyword	m	exe, bund, svc, bat
EPMWinMac.Configuration.Identifier	keyword	m	3732243d-6206-4c6c-8a17-bb60c1235b52
EPMWinMac.Configuration.Message.Name	keyword	o	Allow Message (enter Reason)
EPMWinMac.Configuration.Message.Type	keyword	o	Prompt, Notification
EPMWinMac.Configuration.Message.Identifier	keyword	o	efa4004d-e1b7-4f85-a49a-375160aa65fc
EPMWinMac.Configuration.Workstyle.Name	keyword	m	All Users
EPMWinMac.Configuration.Workstyle.Identifier	keyword	m	8506a411-979d-4f14-aee4-1fb65a8e68ea

Field ECS	ECS Type	Required (when this field set is present)	Examples
EPMWinMac.Configuration.ApplicationGroup.Name	keyword	m	(Default) Any UAC Prompt
EPMWinMac.Configuration.ApplicationGroup.Identifier	keyword	m	a875788d-bcbc-4d63-b43d-d6224a50ea7b
EPMWinMac.Configuration.Application.Description	keyword	m	Any COM Class
EPMWinMac.Configuration.Application.Identifier	keyword	m	9d541a2f-3347-448f-8146-797a833c62ed
EPMWinMac.Configuration.Rule.Identifier	keyword	m	b70bb7cb-6202-440e-abe0-f6a93b6ebc39
EPMWinMac.Configuration.Rule.Action	keyword	o	allow, block
EPMWinMac.Configuration.Rule.OnDemand	boolean	o	true
EPMWinMac.Configuration.Token.Identifier	keyword	o	f8d4ce02-e95d-4700-b69a-957dc5c1de6f
EPMWinMac.Configuration.Token.Name	keyword	o	Add Basic Admin Rights, Passive (No Change)
EPMWinMac.Configuration.Token.Description	keyword	o	Privilege Management Support Token
EPMWinMac.Configuration.Message.UserReason	keyword & text	o	Other: Reason not listed
EPMWinMac.Configuration.Message.AuthMethods	keyword	o	
EPMWinMac.Configuration.Message.Authentication.User	keyword & text	o	
EPMWinMac.Configuration.Message.Authorization.ChallengeCode	keyword	m	123456
EPMWinMac.Configuration.Message.Authorization.ResponseStatus	keyword	m	
EPMWinMac.Event.Action	keyword	m	Allowed, Cancelled, Blocked, Elevated

Process

Field ECS	ECS Type	Required (when this field set is present)	Examples
process.start	date	m	2023-03-16T08:05:34.853Z
process.command_line	keyword & text	o	"C:\Program Files\Google\Chrome\Application\chrome.exe"
process.pid	keyword	m	17501
process.executable	keyword & text	m	c:\windows\system32\svchost.exe
process.parent.executable	keyword & text	o	c:\windows\explorer.exe
process.parent.pid	keyword	o	6332

Field ECS	ECS Type	Required (when this field set is present)	Examples
process.user.DomainIdentifier	keyword	o	S-1-5-21-1234567890-1212121212-635717638
process.user.domain	keyword	o	StanLand
process.user.id	keyword	o	S-1-5-21-1234567890-1212121212-635717638-56524798
process.user.name	keyword	o	Stan

Windows Process

Field ECS	ECS Type	Required (when this field set is present)	Examples
process.entity_id	keyword	m	248d7b79-73df-4478-9328-84f1b9e04e52
process.parent.entity_id	keyword	o	bce44920-8c58-4282-a2a4-90d21664d8de
EPMWinMac.ElevationRequired	boolean	m	true, false
client.Name	keyword	m	

macOS Process

Field ECS	ECS Type	Required (when this field set is present)	Examples
process.name	keyword	m	DateAndTime
EPMWinMac.AuthorizationRequest.AuthRequestURI	keyword	o	system.install.software

File

Field ECS	ECS Type	Required	Examples
file.code_signature.subject_name	keyword	o	Microsoft Windows
file.DriveType	keyword	m	Fixed Disk
file.hash.sha1	keyword	m	acf9e85f6a590925c13bb2bced82978a431d706e
file.hash.sha256	keyword	m	c3eb055c9bc5b53d16be3cc7fc7ac27cefa553ed5612738e568869fe0cf28e8e
file.hash.md5	keyword	o	5DA8C98136D98DFEC4716EDD79C7145F
file.Owner.Identifier	keyword	m	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
file.owner	keyword	m	TrustedInstaller, Stan
file.Owner.DomainIdentifier	keyword	o	S-1-5-80
file.Owner.DomainName	keyword	o	NT SERVICE

Field ECS	ECS Type	Required	Examples
file.path	keyword & text	m	c:\program files\windows nt\accessories\wordpad.exe
file.SourceUrl	keyword	o	https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.4.9/npp.8.4.9.Installer.x64.exe

Windows Executable File

Field ECS	ECS Type	Required	Examples
file.pe.description	keyword	o	Paint
file.pe.product	keyword	o	Microsoft® Windows® Operating System
file.pe.file_version	keyword	o	10.0.19041.1766 (WinBuild.160101.0800)
file.pe.ProductVersion	keyword	o	10.0.19041.1766
file.Owner.DomainNetBIOSName	keyword	o	NT SERVICE
file.ZoneTag	keyword	o	3

macOS Executable File

Field ECS	ECS Type	Required	Examples
file.Bundle.Creator	keyword	m	
file.Bundle.InfoDescription	keyword	o	
file.Bundle.Name	keyword	m	Notes
file.Bundle.Type	keyword	m	APPL, BNDL,
file.Bundle.Uri	keyword	o	com.apple.Notes
file.Bundle.Version	keyword	m	4.9
file.gid	keyword	m	
file.group	keyword	m	

Hosted File

Field ECS	ECS Type	Required	Examples
process.HostedFile.code_signature.subject_name	keyword	o	Microsoft Windows
process.HostedFile.DriveType	keyword	m	Fixed Disk
process.HostedFile.hash.sha1	keyword	m	acf9e85f6a590925c13bb2bced82978a431d706e
process.HostedFile.hash.sha256	keyword	m	c3eb055c9bc5b53d16be3cc7fc7ac27cefa553ed5612738e568869fe0cf28e8e
process.HostedFile.hash.md5	keyword	o	5DA8C98136D98DFEC4716EDD79C7145F

Field ECS	ECS Type	Required	Examples
process.HostedFile.Owner.Identifier	keyword	o	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
process.HostedFile.owner	keyword	o	TrustedInstaller
process.HostedFile.Owner.DomainIdentifier	keyword	o	S-1-5-80
process.HostedFile.Owner.DomainName	keyword	o	NT SERVICE
process.HostedFile.path	keyword & text	m	c:\program process.HostedFiles\windows nt\accessories\wordpad.exe
process.HostedFile.SourceUrl	keyword	o	https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.4.9/npp.8.4.9.Installer.x64.exe

macOS Hosted File

Field ECS	ECS Type	Required	Examples
process.HostedFile.gid	keyword	m	20
process.HostedFile.group	keyword	m	staff

Windows COM

Field ECS	ECS Type	Required	Examples
EPMWinMac.Com.ClsIdentifier	keyword	m	
EPMWinMac.Com.AppIdentifier	keyword	m	
EPMWinMac.Com.DisplayName	keyword	m	

Windows ActiveX

Field ECS	ECS Type	Required	Examples
EPMWinMac.ActiveX.Codebase	keyword & text	m	"https://qa-webserver-01/ActiveX/JONTESTOCX.ocx"
EPMWinMac.ActiveX.CLSID	keyword	m	{5A2BF647-7719-4A60-BD9B-E86F4E262312}
EPMWinMac.ActiveX.Version	keyword	m	"0.0.0.0"

Windows Store Apps

Field ECS	ECS Type	Required	Examples
EPMWinMac.StoreApp.Name	keyword	m	
EPMWinMac.StoreApp.Publisher	keyword	m	
EPMWinMac.StoreApp.Version	keyword	m	

Windows Remote PowerShell

Field ECS	ECS Type	Required	Examples
EPMWinMac.RemotePowerShell.Command	keyword	m	

Windows Installers

Field ECS	ECS Type	Required	Examples
EPMWinMac.Installer.ProductCode	keyword	m	
EPMWinMac.Installer.UpgradeCode	keyword	m	

Uninstallers

Field ECS	ECS Type	Required	Examples
EPMWinMac.Installer.Action	keyword	m	Uninstall, Remove, Repair

Services

ECS Field	ECS Type	Required	Examples
EPMWinMac.ServiceControl.Service.Action	keyword	m	Start, Stop, Configure
EPMWinMac.ServiceControl.Service.DisplayName	keyword	m	Microsoft Intune Management Extension
EPMWinMac.ServiceControl.Service.Name	keyword	m	IntuneManagementExtension

PPAM

ECS Field	ECS Type	Required	Examples
EPMWinMac.PreventPrivilegedGroup.Access	keyword	m	Write General Information Attributes, Read Account Attributes, Write Account Attributes, Set User's Password, Query Membership
EPMWinMac.PreventPrivilegedGroup.Name	keyword	m	Administrators
EPMWinMac.PreventPrivilegedGroup.Rid	keyword	m	544

DLL

ECS Field	ECS Type	Required	Examples
dll.code_signature.subject_name	keyword & text	o	

User Session

Field ECS	ECS Type	Required	Examples
EPMWinMac.Session.Administrator	boolean	m	true, false
EPMWinMac.Session.Locale	keyword	m	en-GB
EPMWinMac.Session.Identifier	keyword	m	25194188-61fe-4e51-9015-330c5a2f44fc
EPMWinMac.Session.PowerUser	boolean	m	true, false
EPMWinMac.Session.WindowsSessionId	keyword	m	8
EPMWinMac.Session.UILanguage	keyword	m	en-GB

EPM Start

Field ECS	ECS Type	Required (when this field set is present)	Examples
agent.ephemeral_id	keyword	m	043AB647-338D-4A89-BF4C-61019DBC9AEE
host.os.version	keyword	m	10.14.1
host.uptime	number	m	63579
host.ChassisType	keyword	m	Desktop, Laptop, Rack Mount Chassis
host.DefaultLocale	keyword	m	eb-GB
host.DefaultUILanguage	keyword	m	eb-GB
host.geo.TimezoneOffset	keyword	m	+120, -60
host.os.ProductType	keyword	m	Workstation, Server

EPM Stop

Field ECS	ECS Type	Required (when this field set is present)	Examples
agent.ephemeral_id	keyword	m	043AB647-338D-4A89-BF4C-61019DBC9AEE

Authorizing User

Field ECS	ECS Type	Required	Examples
EPMWinMac.AuthorizingUser.Identifier	keyword	m	
EPMWinMac.AuthorizingUser.Name	keyword & text	m	
EPMWinMac.AuthorizingUser.DomainIdentifier	keyword	o	
EPMWinMac.AuthorizingUser.DomainName	keyword & text	o	
EPMWinMac.AuthorizingUser.DomainNetBIOSName	keyword & text	o	

Rule Script

Field ECS	ECS Type	Required	Examples
EPMWinMac.Configuration.RuleScript.FileName	keyword	m	
EPMWinMac.Configuration.RuleScript.Outcome.Name	keyword	o	
EPMWinMac.Configuration.RuleScript.Outcome.Output	keyword	o	
EPMWinMac.Configuration.RuleScript.Publisher	keyword & text	o	
EPMWinMac.Configuration.RuleScript.Outcome.Result	keyword & text	o	
EPMWinMac.Configuration.RuleScript.Outcome.RuleAffected	boolean	m	
EPMWinMac.Configuration.RuleScript.Outcome.Version	keyword & text	o	

Trusted Application Protection

These fields are populated when the Trusted Application Workstyles are enabled and a Trusted Application has a child process launch or DLL load blocked.

Field ECS	ECS Type	Required	Examples
EPMWinMac.TrustedApplication.Name	keyword	m	Adobe Acrobat Reader DC
EPMWinMac.TrustedApplication.Version	keyword	m	20.6.20042.371103