BlackBerry Syslog Guide

Contents

Overview

You can configure Cylance to forward events to a Syslog server. The content of each event is Unicode plain text consisting of key-value pairs, separated by commas. Due to the size limitations of most syslog servers, the details of each message (Cylance-specific payload) is limited to 2048 characters. Syslog messages are sent from the following Cylance IP addresses, based on the login URL for your region:

Asia-Pacific Northeast (protect-apne1.cylance.com):

- 13.113.53.36
- 13.113.60.107

Asia-Pacific Southeast (including Australia; protect-au.cylance.com):

- 52.63.15.218
- 52.65.4.232

Europe Central (protect-euc1.cylance.com):

- 52.28.219.170
- 52.29.102.181
- 52.29.213.11

North America (protect.cylance.com):

- 52.2.154.63
- 52.20.244.157
- 52.71.59.248
- 52.72.144.44
- 54.88.241.49

South America East (protect-sae1.cylance.com):

- 52.67.244.213
- 52.67.252.42

Undeliverable messages

If the Cylance syslog/SIEM integration cannot successfully deliver syslog messages to a syslog/SIEM server, an email notification will be sent to administrators (built-in role) with a confirmed email address within an organization. The email notification alerts administrators about this syslog issue.

The maximum number of undelivered messages before the syslog/SIEM integration is disabled is 400. The first warning email is sent after 1/3 of the maximum number of undelivered messages are sent. Each message attempts to be sent 10 times before it fails to forward to a syslog/SIEM server and then transitions to a dead-letter queue.

Delayed events

BlackBerry and Cylance products can be configured to forward event data to a syslog server. Though delivered in a timely manner, it should not be used for real time or near real-time monitoring. Due to various factors, potential delays can occur when it comes to reporting of events. Cylance syslog integration cannot guarantee an exact time for the delivery of events.

Configure Syslog settings

1. In the console, Select **Settings > Application**.
2. Click the **Syslog/SIEM** checkbox.
3. Select the Event Types for which you want to receive messaging.
4. Select or type in the information for your Syslog or SIEM integration. The other sections in this guide provide details and descriptions for each Syslog/SIEM option.
5. Click **Test Connection** to verify that your settings are correct.
6. Click **Save**.

Configuration

Syslog configuration is done on the Application page, on the Settings tab.

Feature	Description
Events	Select the Cylance event types you want to receive Syslog messaging for.
Custom Token	Some log management services, like SumoLogic, might need a custom token included with syslog messages to help identify where those messages should go. The custom token is provided by your log management service. **Example Token:** 4uOHzVv+ZKBheckRJouU3+XojMn02Yb0DOKlYwTZuDU1K +PsY27+ew== **Note:** The Custom Token field is available with all Syslog/SIEM options, not just SumoLogic. It is possible to type any information as a custom tag to the syslog information.
Facility	This is the type of application that is logging the message. The default is Internal (or Syslog). This is used to categorize the messages when they are received by the Syslog server.
IP/Domain	This is the IP address or fully-qualified domain name of the Syslog server that the customer has set up. Consult with your internal network experts to ensure firewall and domain settings are properly configured.
Port	This is the port number on the machines that the Syslog server will listen to for messages. It must be a number between 1 and 65535. Typical values are: 512 for UDP, 1235 or 1468 for TCP, and 6514 for Secured TCP (example: TCP with TLS/SSL enabled).
Protocol	This must match what you have configured on your Syslog server. The choices are UDP or TCP. UDP is generally not recommended as it does not guarantee message delivery. You should use the default setting, TCP.
Security Information and Event Management (SIEM)	This is the type of Syslog server or SIEM to which events are to be sent.

Feature	Description
Severity	This is the severity of the messages that should appear in the Syslog server. This is a subjective field, and you may set it to whatever level you like. The value of severity does not change the messages that are forwarded to Syslog.
TLS/SSl	This option is only available if the Protocol specified is TCP. TLS/SSL ensures the Syslog message is encrypted in transit from Cylance to the Syslog server. You should checkmark this option. Be sure your Syslog server is configured to listen for TLS/SSL messages.

BlackBerry Protect Desktop event types

Syslog events have standard fields like timestamp, severity level, facility, and a Cylance-specific payload (message). Examples provided in this section only contain the Cylance-specific message.

Application control

This option is only visible to users who have the Application Control feature enabled. Application control events represent actions occurring when the device is in application control mode. Selecting this option will send a message to the syslog server whenever an attempt is made to modify or copy an executable file, or when an attempt is made to execute a file from an external device or network location.

Field	Value	Description
Action	Allow	The event was allowed.
	Deny	The event was denied.
Action Type	Execution	An attempt to execute a file from the local drive was detected.
	ExecutionFromExternalDrive	An attempt to execute from an external drive or USB drive was detected.
	PEFileChange	An attempt to change a portable executable (PE) file on the file system was detected. This includes copying files onto the file system.
	Unknown	The action type could not be determined.
Device Name	[varies]	This is the name of the device.
Event Name	Execution	An attempt to execute a file from a local drive was detected.
	ExecutionFromExternalDrive	An attempt to execute from an external drive or USB drive was detected.
	PEFileChange	An attempt to change a portable executable (PE) file on the file system was detected. This includes copying files onto the file system.
	Unknown	The event name could not be determined.
Event Type	AppControl	This is an application control event.
File Path	[varies]	This is the path to the file.
IP Address	[varies]	This is the IP address for the device. Multiple IP addresses are comma separated values.

Field	Value	Description
SHA256	[varies]	This is the SHA256 hash for the file.
Zone Names	[varies]	This is the zones to which the device belongs.

Example message for deny PE file changes

```
BlackBerry Protect Desktop: Event Type: AppControl, Event Name: pechange, Device
 Name: WIN-7entSh64, IP Address: (192.168.119.128), Action: PEFileChange, Action
 Type: Deny, File Path: C:\Users\admin\AppData\Local\Temp\MyInstaller.exe, SHA256:
 04D4DC02D96673ECA9050FE7201044FDB380E3CFE0D727E93DB35A709B45EDAA), Zone Names:
 (Script Test,Server Test)
```

Example message for deny executions from external drive

```
BlackBerry Protect Desktop: Event Type: AppControl, Event
 Name: executionfromexternaldrives, Device Name: WIN-7entSh64,
 IP Address: (192.168.119.128), Action: PEFileChange, Action
 Type: Allow, File Path: \\shared1\psexec.exe, SHA256:
 F8DBABDFA03068130C277CE49C60E35C029FF29D9E3C74C362521F3FB02670D5), Zone Names:
 (Script Test,Server Test)
```

Audit log

Selecting this option will send the audit log of user actions performed in the Cylance console (website) to the syslog server. Audit log events will always appear in the Audit Log screen, even when this option is unchecked.

Field	Value	Description
Eco Id	[varies]	The user's EcoID, if available.
Event Name	AuditLog	This is an Audit Log event.
	AcceptEula	The user accepted the End-User License Agreement (the first user to log in to a newly created tenant).
	AgentUpdate	The user updated the Agent.
	ApplicationAdd	The user created a Custom Application (on the Integration page). This includes the name of the application.
	ApplicationEdit	The user updated the Custom Application name.
	ApplicationEdit	The user changed the permissions for a Custom Application.
	ApplicationEdit	The user regenerated the credentials for the Custom Application.

Field	Value	Description
	ApplicationRemove	The user removed a Custom Application.
	CertificateRepositoryAddItem	The user added a certificate. Includes the name and thumbprint for the certificate.
	CertificateRepositoryDeleteItem	The user deleted a certificate. Includes the name and thumbprint for the certificate.
	CertificateRepositoryEditItem	The user edited a certificate. Includes the name and thumbprint for the certificate.
	CertificateSafelistAddItem	The user added a certificate to the Safe List.
	CertificateSafelistDeleteItem	The user removed a certificate from the Safe List.
	CustomAuthenticationDisable	The user disabled Custom Authentication.
	CustomAuthenticationSave	The user saved Custom Authentication settings.
	DeleteAllQuarantinedFiles	The user issued a command from the Console to delete all quarantined files on a device.
	DeleteTokenThreatDataReport	The user deleted the Threat Data Report Token.
	DetectionExceptionAdd	The user added an Optics detection exception.
	DetectionExceptionEdit	The user edited an Optics detection exception.
	DetectionExceptionRemove	The user removed an Optics detection exception.
	DetectionRuleAdd	The user added an Optics detection rule.
	DetectionRuleEdit	The user edited an Optics detection rule.
	DetectionRuleRemove	The user removed an Optics detection rule.
	DetectionRuleSetAdd	The user added an Optics detection rule set.
	DetectionRuleSetEdit	The user edited an Optics detection rule set.
	DetectionRuleSetRemove	The user removed an Optics detection rule set.
	DetectionsChangeStatus	The user changed the status of an Optics detection.
	DetectionsRemove	The user removed an Optics detection.
	DeviceAdd	The user registered a device.

Field	Value	Description
	DeviceEdit	The user edited a device.
	DeviceFileDownload	The user download a file that Optics identified as a potential threat.
	DeviceLock	The user locked a device.
	DeviceRemove	The user removed a device.
	DeviceShowUnlockKey	The user revealed the unlock key for a device.
	DownloadThreatDataReport	The user downloaded the deprecated Threat Data Report.
	EndUserAssignPolicy	The user assigned a Protect Mobile policy to one or more users. The message indicates the assigned users and policy.
	EndUserAdd	The user added a Protect Mobile user. The message includes the Protect Mobile user's email address and name.
	EndUserImport	The user imported Protect Mobile users. The message includes the Protect Mobile user email addresses and names.
	EndUserRemove	The user removed a Protect Mobile user. The message includes the Protect Mobile user's email address and name.
	EndUserSendInvitation	The user sent an activation password and QR code to one or more Protect Mobile devices. The message includes the Protect Mobile user email addresses, a success count, and a failure count.
	FocusDataAdd	The user retrieved focus data.
	GenerateTokenThreatDataReport	The user generated a new token for the Threat Data Report.
	GhostLoginSettingChange	The user enabled or disabled the Enable Support Login feature.
	GlobalListAdd	The user added a file to the Global List.
	GlobalListRemove	The user removed a file from the Global List.
	InstallationTokenDelete	The user deleted the Installation Token.

Field	Value	Description
	InstallationTokenRegenerate	The user generated a new Installation Token.
	InstaQueryAdd	The user added an InstaQuery.
	InstaQueryRemove	The user removed an InstaQuery.
	InvitationUrlGenerate	The user generated an Invitation URL.
	JobServiceStop	The user stopped a package deploy job.
	LoginFailure	The user failed to log in to the Cylance Console.
	LoginSuccess	The user successfully logged in to the Cylance Console.
	MobileAlertsExport	The user exported Protect Mobile alert information from the console. The message indicates any filters that were applied.
	MobileAlertsIgnore	The user selected and ignored a Protect Mobile alert. The message indicates the type and name of the mobile alert.
	MobileDeviceExport	The user exported Protect Mobile device information from the console. The message indicates any filters that were applied.
	MobileDeviceRemove	The user removed a Protect Mobile device. The message indicates the removed user and device details.
	MobileExclusionsAdd	The user added an app or developer certificate to the Protect Mobile safe or unsafe list.
	MobileExclusionsRemove	The user removed an app or developer certificate from the Protect Mobile safe or unsafe list.
	MobilePolicyAdd	The user added a Protect Mobile policy. The message indicates the policy name and settings.
	MobilePolicyEdit	The user edited a Protect Mobile policy. The message indicates the policy name and changes.
	MobilePolicyRemove	The user removed a Protect Mobile policy. The message indicates the removed policy.

Field	Value	Description
	NightlyThreatDataReportChange	The user enabled or disabled the Threat Data Report (on the Applications page).
	PackageDeployAdd	The user added a package deploy.
	PackageDeployRemove	The user removed a package deploy.
	PackagePlaybookAdd	The user added an Optics package playbook.
	PackagePlaybookEdit	The user edited an Optics package playbook.
	PackagePlaybookRemove	The user removed an Optics package playbook.
	PlaybookResultRemove	The user removed an Optics package playbook result.
	PolicyAdd	The user added a policy. Includes the policy name.
	PolicyEdit	The user edited a policy. Includes the policy name.
	PolicyRemove	The user removed a policy. Includes the policy name.
	PolicySafeListAdd	The user added a file to the Policy Safe List. Includes the SHA256 hash that was added.
	PolicySafeListRemove	The user removed a file from the Policy Safelist. Includes the SHA256 hash that was removed.
	RemoteResponseConnect	The user opened an Optics remote response session with a device.
	RemoteResponseDisconnect	The user closed an Optics remote response session.
	RequestToGenerateThreatDataReport	The user enabled or disabled the Threat Data Report (on the Application page).
	ScriptControlExclusionListAdd	The user added a script to the Global Safe List.
	ScriptControlExclusionListRemove	The user removed a script from the Global Safe List.
	SyslogDisable	The user disabled the syslog feature.
	SyslogSettingSave	The user saved the syslog settings.

Field	Value	Description
	ThreatGlobalQuarantine	The user added a file to the Global Quarantine List.
	ThreatQuarantine	The user quarantined a file for an endpoint.
	ThreatSafeList	The user added a file to the Global Safe List.
	ThreatWaive	The user waived a file for an endpoint.
	UninstallAgentPasswordSave	The user saved a password, after checking Require Password to Uninstall Agent.
	UninstallAgentRequirePasswordDisable	The user disabled Require Password to Uninstall Agent.
	UserAdd	The user created a user.
	UserEdit	The user edited a user.
	UserRemove	The user removed a user.
	ZoneAdd	The user added a zone.
	ZoneAddDevice	The user added a device to a zone.
	ZoneEdit	The user edited a zone.
	ZoneRemove	The user removed a zone.
	ZoneRemoveDevice	The user removed a device from a zone.
	ZoneRuleAdd	The user added a zone rule.
	ZoneRuleEdit	The user edited a zone rule.
	ZoneRuleRemove	The user removed a zone rule.
Message	[varies]	The message contains information related to the action. Example: When a file is added to the Global Quarantine List, the message might include the file hash and the reason given for adding it to the Global List.
User	[varies]	The user who logged in and triggered this audit log event.

Example message for audit log events being forwarded to syslog

```
BlackBerry Protect Desktop: Event Type: AuditLog,
 Event Name: ThreatGlobalQuarantine, Message: SHA256:
 A1E92E2E84A1321F499A5EC500E8B9A9C0CA28701668BF13EA56D3995A96153F,
```

```
 1CCC95B7B2F781D55D538CA01D6049762FDF6A75B32A06DF3CC2EDC1F1573BFA; Reason:
 Manually blacklisting these 2 threats., User: (johnsmith@contoso.com)
```

Example message for audit log events being forwarded to syslog with Eco Id

```
BlackBerry Protect Desktop: Event Type: AuditLog, Event Name: ZoneEdit, Message:
 Example message, User: (johnsmith@contoso.com, Eco Id: Bn6ZX201mlPgFzl/M9njAPI4=
```

Example message for API events in audit log

API create/add, update, and delete events are captured in the audit log. In the example below, the term “user” appears twice. The first user is the name of the user being edited. The second user is the name of the console user who triggered the audit event, and for an API event, this field is empty. The information on the user who performed the API event is not captured because the event was performed using an authentication token, not by a user logged in to the Cylance console.

```
BlackBerry Protect Desktop: Event Type: AuditLog, Event Name: UserEdit, Message:
 User: Jane Smith, User: (janesmith@contoso.com)
```

Devices

Selecting this option sends device events to the syslog server.

Field	Value	Description
Agent Version	[varies]	This is the version of the BlackBerry Protect Desktop agent installed on the device.
CylanceOPTICS Version	[varies]	If BlackBerry Optics is enabled, this is the version of the BlackBerry Optics agent installed on the device.
Device Message	[varies]	The message is populated when the device details are changed by the user. This can include: name change, policy change, zone changes, log level change, and self-protection level change.
Device Name	[varies]	This is the name of the device.
Event Type	Device	This is a device event.
Event Name	Device Policy Assigned	A policy was assigned to the device.
	Device Removed	The device was removed from the console.
	Device Updated	The device was updated.
	Device Assigned to Zone	The device was assigned to a zone or zones.
	Registration	A new device was registered with the console.

Field	Value	Description
	System Security	A message that is logged after a new device is registered and when a user logs on to the device.
IP Address	[varies]	This is the IP address for the device.
Kernel Version	[varies]	This is the operating system's running kernel version on the device.
Logged On Users	[varies]	These are the users currently logged on to the device. This could be the email address and/or user's name.
MAC Address	[varies]	This is the MAC address for the device.
OS	[varies]	This is the operating system used on the device.
Policy Change	[varies]	This shows the previous policy and the new policy assigned to the device.
Policy Name	[varies]	This is the name of the policy assigned to the device.
Renamed	"device_name" to "device_name"	This shows the previous name and the new name for the device.
User	[varies]	This is the name of the user updating the device.
Zones Added	[varies]	These are the zone names to which the device has been added.
Zone Name	[varies]	These are the zone names to which the device is assigned.

New device

When a new device is registered, you will receive two messages for this event: Registration and SystemSecurity.

Note: SystemSecurity messages are also generated when a user logs on to a device. Therefore, this message may occur more often, not just during registration.

Example Messages for Device Registration Events

```
BlackBerry Protect Desktop: Event Type: Device, Event Name: Registration, Device
 Name: WIN-55NATVQHBUU
```

```
BlackBerry Protect Desktop: Event Type: Device, Event Name: SystemSecurity, Device
 Name: WIN-55NATVQHBUU, Agent Version: 1.1.1270.58, IP Address: (10.3.0.154), MAC
```

```
 Address: (005056881877), Logged On Users: (WIN-55NATVQHBUU\Administrator), OS:
 Microsoft Windows Server 2008 R2 Standard Service Pack 1 x64 6.1.7601
```

Remove device

When a device is removed, you will receive the following message for this event: Device Removed.

Example Message for Device Removed Events

```
BlackBerry Protect Desktop: Event Type: Device, Event Name: Device Removed, Device
 Names: (jsmithxp-test), User: (jsmith@contoso.com)
```

Updated device

When a device's policy, zone, name, or logging level has changed, you will receive the following message for this event: Device Updated.

Example Message for Device Updated Events

```
BlackBerry Protect Desktop: Event Type: Device, Event Name: Device Updated,
 Device Message: Renamed: 'WIN-55NATVQHBUU' to 'WIN-2008R2-IRV1'; Policy
 Changed: 'Default' to 'IRVPolicy1'; Zones Added: 'IRV1', User: John Smith
 (johnsmith@contoso.com)
```

Device control

When this option is selected, any device control events will be logged to the syslog server.

Field	Value	Description
Device Name	[varies]	Name of the device associated with the Device Control event
Event Type	DeviceControl	Type of event
Event Name	Block	A USB mass storage device cannot be used on the device (set in Policy).
	Fullaccess	A USB mass storage device can be used on the device (set in Policy).
External Device Type	AndroidUSB	Android device
	iOS	iOS device
	StillImage	Still image device, like a camera
	USBCDDVDRW	USB disc drive (CD, DVD, Blu-ray)
	USBDrive	USB drive, like a thumb drive
	VMWareMount	VMware USB PassThrough
	WPD	Windows Portable Device

Field	Value	Description
External Device Name	[varies]	The name given to the external device
External Device Product ID	[varies]	Varies by manufacturer
External Device Serial Number	[varies]	Varies by manufacturer
External Device Vendor ID	[varies]	Varies by manufacturer
Zone Names	[varies]	Zones to which the device belongs

Example message for device control events

BlackBerry Protect Desktop: Event Type: DeviceControl, Event Name: fullaccess, Device Name: Test_Device_1, External Device Type: iOS, External Device Vendor ID: 1953, External Device Name: Generic USB Drive - 2017/02/16-01, External Device Product ID: 0202, External Device Serial Number: 575833314133343210041246, Zone Names: (test_zone_02)

Note: For Windows, Android devices may be identified as Still Image or Windows Portable Device.

Memory protection

Selecting this option will log any Memory Exploit Attempts that might be considered an attack from any of the Tenant's devices to the syslog server. For full descriptions of each violation type, see Memory Protection violation types in the BlackBerry Protect Desktop Administration Guide.

Field	Value	Description
Action	Allowed	The event is allowed because of a policy.
	Blocked	The event is blocked because of a policy.
	None	The event is allowed because no policy has been defined for this violation.
	Terminated	The process has been terminated.
Device ID	[varies]	The unique ID for the device.
Device Name	[varies]	The name of the device.
Event Type	ExploitAttempt	A Memory Protection event is known as an exploit attempt.

Field	Value	Description
Event Name	Allowed	The file was allowed to run, either because it was added to an exclusion or the action was set to None (Ignore).
	Blocked	The Exploit Attempt was blocked. However, if a process was started before the Exploit was blocked (example: process was started before Memory Protection was enabled), the process will continue to run.
	None	This is an alert only. No actions were taken on the Exploit Attempt.
	Terminated	The Exploit Attempt was blocked, and any processes were terminated.
IP Address	[varies]	The IP address or IP addresses for the device.
Process ID	[varies]	The Process ID for the event.
Process Name	[varies]	The fully qualified path of the process
User Name	[varies]	The name of the user currently logged in to the device
Violation Type	DyldInjection	The memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords.
	LsassRead	The memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords.
	MaliciousPayload	A generic shellcode and payload detection associated with exploitation has been detected.

Field	Value	Description
	OutOfProcessAllocation	Remote Allocation of Memory: A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system.
	OutOfProcessApc	Remote APC Scheduled.
	OutOfProcessCreateThread	Remote Thread Creation: A process has created a new thread in another process. A process's threads are usually only created by that same process. This is generally used by an attacker to activate a malicious presence that has been injected into another process.
	OutOfProcessMap	Remote Mapping of Memory: A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system.
	OutOfProcessOverwriteCode	Remote Overwrite Code: A process has modified executable memory in another process. Under normal conditions executable memory will not be modified, especially by another process. This usually indicates an attempt to divert execution in another process.
	OutOfProcessUnmapMemory	Remote Unmap of Memory: A process has removed a Windows executable from the memory of another process. This may indicate an intent to replace the executable image with a modified copy for the purpose of diverting execution.

Field	Value	Description
	OutOfProcessWrite	Remote Write to Memory: A process has modified memory in another process. This is usually an attempt to store code or data in previously allocated memory (see OutOfProcessAllocation) but it is possible that an attacker is trying to overwrite existing memory in order to divert execution for a malicious purpose.
	OutOfProcessWritePe	Remote Write PE to Memory: A process has modified memory in another process to contain an executable image. Generally this indicates that an attacker is attempting to execute code without first writing that code to disk.
	OverwriteCode	The code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass Data Execution Prevention (DEP).
	RamScraping	A process is trying to read valid magnetic stripe track data from another process. Typically related to point of sale systems (POS).
	StackPivot	A generic shellcode and payload detection associated with exploitation has been detected.
	StackProtect	The memory protection of a thread's stack has been modified to enable execution permission. Stack memory should not be executable, so usually this means that an attacker is preparing to run malicious code stored in stack memory as part of an exploit, an attempt which would otherwise be blocked by Data Execution Prevention (DEP).

Field	Value	Description
	ZeroAllocate	A null page has been allocated. The memory region is typically reserved, but in certain circumstances it can be allocated. Attacks can use this to setup privilege escalation by taking advantage of some known null de-reference exploit, typically in the kernel.
Zone Names	[varies]	The zones associated with the device.

Example message for memory protection events

BlackBerry Protect Desktop: Event Type: ExploitAttempt, Event Name: blocked, Device Name: WIN-7entSh64, IP Address: (192.168.119.128), Action: Blocked, Process ID: 3804, Process Name: C:\AttackTest64.exe, User Name: admin, Violation Type: LSASS Read, Zone Names: (Script Test,Server Test), Device ID: e378dacb-9324-453a-b8c6-5a8406952195

Script control

Selecting this option will log any newly found scripts, convicted by BlackBerry Protect Desktop, to the syslog server.

Syslog script control events contain the following properties:

- Alert: The script is allowed to run. A script control event is sent to the Console.
- Block: The script is not allowed to run. A script control event is sent to the Console.

Reporting frequency

The first time a Script Control event is detected, a message is sent via syslog with full event information. Each subsequent event that is deemed a duplicate will not be sent via syslog for the remainder of the day (based on Cylance's server time). At the end of the day, if the counter for a specific Script Control event is greater than one, an event will be sent via syslog with the count of all duplicate events that have transpired that day. If the counter equals one at the end of the day, no additional message will be sent via syslog.

Determining if a Script Control event is a duplicate uses the following logic:

- Look at key information: Device, Hash, Username, and Block/Alert.
- For the first event received in a day, set a counter value to 1. There are separate counters for Block and Alert.
- All subsequent events with the same key increment the counter.
- The counter resets each calendar day, according to Cylance's server time.

Example: If Script A runs on Device 1 at 11:59PM on 9/20/18 and then again at 12:05AM, 12:10AM, and 12:15AM on 9/21/18 will result in the following:

- One syslog message will be sent on 9/20/18 for the one Script Control event for that day.
- One syslog message will be sent on 9/21/18 for the two duplicate Script Control events for that day.

Note: Only one syslog message is sent on 9/21/18 because the events are duplicates of the event that occurred on 9/20/18.

Field	Value	Description
Device ID	[varies]	The unique ID for the device.
Device Name	[varies]	This is the name of the device.
Event Type	ScriptControl	This is a Script Control event.
Event Name	Alert	This is an alert only. No actions were taken on the Script Control event.
	Blocked	The Script Control event was blocked.
	None	No action was taken on the Script Control event.
	Unknown	It could not be determined if any action was taken on the Script Control event.
File Path	[varies]	This is the path to the file.
Interpreter	ActiveScript	This is the interpreter that detects VBScript and Jscript that run from the Windows Script Host (WSH).
	MacroScript	This is the interpreter that detects macros in Microsoft Office documents.
	Powershell	This is the interpreter that detects PowerShell scripts.
Interpreter Version	[varies]	This is the version number of the interpreter.
Policy Name	[varies]	The name of the policy assigned to the device.
SHA256	[varies]	This is the SHA256 hash for the file.
Zone Names	[varies]	These are the names of the zones to which the device belongs.

Example message for script control events

BlackBerry Protect Desktop - - - Event Type: ScriptControl, Event Name: Blocked, Device Name: Fake_Device, File Path: d:\windows\system32\windowspowershell\v2.1\newlyMade.vbs, SHA256: FE9B64DEFD8BF214C7490BB7F35B495A79A95E81F8943EE279DC99998D3D3440, Interpreter: active, Interpreter Version: 6.1.7600.16385 (win7_rtm.090713-1255), Zone Names: (Script Test,Server Test), Device ID: e378dacb-9324-453a-b8c6-5a8406952195, Policy Name: Default

Threats

Selecting this option will log any newly found threats, or changes observed for any existing threat, to the syslog server. Changes include a threat being removed, quarantined, waived, or executed.

Field	Value	Description
Auto Run	False	The threat is not set to automatically run when the system starts.
	True	The threat is set to automatically run when the system starts.
	Unknown	It cannot be determined if the threat is set to Auto Run or not.
Cylance Score	Ranges from 1 to 100	A file with a score ranging from 1 to 59 is considered Abnormal. A file with a score ranging from 60 to 100 is considered Unsafe.
Detected By	ExecutionControl	Execution Control
	BackgroundThreatDetection	Background Threat Detection
	FileWatcher	Watch for New Files
	NotAvailable	Not Available
	RunningModuleScan	Running Module Scan
Device Name	[varies]	This is the name of the device on which the threat was found.
Drive Type	[varies]	This is the type of drive or storage device the threat originated from, if known. The drive type includes: CDROM, Fixed, Network, None, No Root Directory, RAM, and Removable.
Event Name	threat_found	A new threat has been found in an Unsafe state.
	threat_cleared	An existing threat has been cleared (removed). This occurs when a threat_removed event is generated.
	threat_quarantined	A new threat has been found in the Quarantined status.
	threat_waived	A new threat has been found in the Waived status.
	threat_changed	The behavior of an existing threat has changed (examples: score, quarantine status, running status).

Field	Value	Description
	corrupt_found	A file is classified as corrupt because the file appears to be malformed and cannot run, or the file may contain a malformed file structure.
Event Type	Threat	This is a Threat event.
File Name	[varies]	This is the name of the threat (file).
File Owner	[varies]	This is the owner of the threat (file).
File Type	Archive	The file is an archive file.
	Executable	The file is a Windows executable.
	Linuxexe	The file is a Linux executable.
	MacOSExe	The file is a macOS executable.
	Ole	The file is a Microsoft Office file.
	Pdf	The file is a PDF (Portable Document Format).
	Unknown	The file type could not be determined.
Found Date	[varies]	This is the date and time the threat was found on the device.
IP Address	[varies]	This is the IP address or IP addresses for the device.
Is Malware	False	The threat is not classified as malware (Threat Classification).
	True	The threat is classified as malware (Threat Classification).
Is Running	False	The threat is not running.
	True	The threat is currently running.
Is Unique to	False	The threat is not unique to Cylance.
	True	The threat is unique to Cylance (has not been identified by other antivirus products).
MD5	[varies]	This is the MD5 hash for the file.
Path	[varies]	This is the path to the file.
SHA256	[varies]	This is the SHA256 hash for the file.

Field	Value	Description
Status	Abnormal	The threat is considered Abnormal.
	Cleared	The threat was cleared by deleting the threat, either using the Console or on the endpoint.
	Corrupt	The file is corrupt or otherwise invalid.
	Quarantined	The file has been quarantined by either adding it to the Global Quarantine List or quarantining it on a specific endpoint.
	Unsafe	The threat is considered Unsafe.
	Waived	The file has been waived by either adding it to the Global Safe List or allowing it to run on a specific endpoint.
Threat Classification	File Unavailable	The file is unavailable due to an upload constraint (example: file is too large to upload), the file is unavailable for analysis.
	Malware	The file is classified as malware.
	Possible PUP	The file might be a potentially unwanted program (PUP).
	PUP	The file is considered a potentially unwanted program (PUP).
	Trusted	The file is considered trusted.
	Unclassified	Cylance has not analyzed this file.
Zone Names	[varies]	These are the names of the zones where the threat was found.

Example message for threat events

BlackBerry Protect Desktop: Event Type: Threat, Event Name: threat_found, Device Name: SH-Win81-1, IP Address: (10.3.0.132), File Name: virusshare_00fbc4cc4b42774b50a9f71074b79bd9, Path: c:\ruby \host_automation\test\data\test_files\, Drive Type: None, File Owner: SH-Win81-1\Exampleuser, SHA256: 1EBF3B8A61A7E0023AAB3B0CB24938536A1D87BCE1FCC6442E137FB2A7DD510B, MD5: , Status: Unsafe, Cylance Score: 100, Found Date: 6/1/2015 10:57:42 PM, File Type: Executable, Is Running: False, Auto Run: False, Detected By: FileWatcher), Zone Names: (Script Test,Server Test), Is Malware: False, Is Unique to Cylance: False, Threat Classification: File Unavailable

Threat classifications

Each day, Cylance will classify hundreds of threats as either malware or potentially unwanted programs (PUPs). By selecting this option, you are subscribing to be notified when these events occur. For full descriptions of each threat class and subclass, read the Threat Classification FAQ knowledge base article.

Field	Value	Description
Event Name	ResearchSaved	Threat classification additions and changes from the Cylance Threat Research Team.
	ThreatUpdated	The threat details have been updated.
Event Type	ThreatClassification	This is a threat classification event.
MD5	[varies]	The MD5 hash for the file.
SHA256	[varies]	The SHA256 hash for the file.
Threat Class	Dual Use	The file can be used for malicious and non-malicious purposes.
	File Unavailable	The file is unavailable for analysis. **Example:** The file is too large to upload.
	Malware	The file has been identified as malicious.
	Possible PUP	The file might be a potentially unwanted program (PUP).
	PUP	The file has been identified as a possible potentially unwanted program (PUP).
	Trusted	The file has been identified as Safe.
Threat Subclass	Adware	Annoying advertisements or unwanted bundled add-ons
	Backdoor	Provides unauthorized access
	Bot	Malware that connects to a botnet server
	Corrupt	Malformed or unable to run
	Crack	Altered to bypass licensing
	Downloader	Malware that downloads data
	Dropper	Malware that installs other malware
	Exploit	Attacks a specific vulnerability

Field	Value	Description
	Fake Alert	Malware that appears to be legitimate security software
	Fake AV	Malware that appears to be legitimate security software
	Game	A game file
	Generic	Does not fit into any existing category
	Hacking Tool	A hacking tool
	Infostealer	Records login credentials and other sensitive information
	Keygen	Generates product keys
	Monitoring Tool	Track user's activities
	Other	A category used for PUPs that don't fit anything else
	Parasitic	Spread by attacking to other programs
	Pass Crack	Used to reveal passwords
	Portable Application	Designed to run without needing installation
	Ransom	Restricts access
	Remnant	Remnants post removal
	Remote Access	Access another system remotely
	Rootkit	Avoids detection
	Scripting Tool	Any script that can run as if it were an executable
	Tool	Administrative features used to attack or intrude
	Toolbar	Any technology that places additional buttons or input boxes on-screen within a UI
	Trojan	Disguises itself as legitimate software
	Virus	Inserts or appends itself to other files
	Worm	Propagates by copying itself to another device

Example message for threat classifications

BlackBerry Protect Desktop: Event Type: ThreatClassification, Event Name: ResearchSaved, SHA256: 1218493137321C1D1F897B0C25BEF17CDD0BE9C99B84B4DD8B51EAC8F9794F65, Threat Classification: Malware - Worm

Note: The Threat Classification and Threat Subclass are provided as Threat Classification in the syslog message. In the above example, the Threat Classification contains the Threat Class (Malware) and the Threat Subclass (Worm). If a Threat Subclass is not available, then only the Threat Class will display.

BlackBerry Optics detection events

This option is visible only to users who have BlackBerry Optics enabled. Optics events represent malicious or suspicious events detected by the Optics Context Analysis Engine (CAE). Selecting this option will send a message to the syslog server whenever an applicable Optics detection rule or threat detection module is triggered on an Optics device. Selecting this option will enable syslog messages for the following detection event types: process events, file events, registry events, network events, and memory events.

Due to the volume of information included in Optics detection events, the syslog representation of a detection event is reduced in size and does not contain the full set of information that is available from the management console or the API.

BlackBerry Optics process-based detection events

These events occur when a Detection Event that includes a Target Process artifact is triggered.

Field	Value	Description
Description	[varies]	Name of the Detection Rule that was triggered
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaeProcessEvent	Detection Event involved a Target Process
Event Type	OpticsCaeProcessEvent	Detection Event involved a Target Process
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Target Process ImageFileSha256	[varies]	SHA256 hash of the process that was started or terminated

Field	Value	Description
Target Process Name	[varies]	Name of the process that was started or terminated
Target Process Owner	[varies]	User who owns the process that was started or terminated
Zone Names	[varies]	Zones that the device belongs to

Example message for process-based detection events

Event Type: OpticsCaeProcessEvent, Event Name: OpticsCaeProcessEvent, Device Name: OPTICS-DEMO-2, Zone Names: (Zone1, Zone2), Event Id: 471a31e0-1c94-4c69-8e71-687514f8adaf, Severity: Low, Description: Office DDE to Script Interpreter (MITRE), Instigating Process Name: POWERPNT.EXE, Instigating Process Owner: CYLANCE/mmorin, Instigating Process ImageFileSha256: AFFABA38032700FE50C70B352ACE10F1A07D170B07CDFED10ECF2C1706A9C8BC, Target Process Name: csc.exe, Target Process Owner: CYLANCE/mmorin, Target Process ImageFileSha256: 6E24B58A16510E2135EABCF181B43B0CBF215451ACA9BA8F8CB9A5B87C231908, Device Id: e378dacb-9324-453a-b8c6-5a8406952195

BlackBerry Optics file-based detection events

These events occur when a Detection Event that includes a target-file artifact is triggered.

Field	Value	Description
Description	[varies]	Name of the Detection Rule that was triggered
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaeFileEvent	Detection Event involved a Target File
Event Type	OpticsCaeFileEvent	Detection Event involved a Target File
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action

Field	Value	Description
Severity	[varies]	Severity of the event.: • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Target File Sha256	[varies]	SHA256 hash of the file that was acted upon (created, written, overwritten, or deleted) SHA256 hashes are not available for all file types
Target File Path	[varies]	Path of the file that was acted upon (created, written, overwritten, or deleted)
Target File Owner	[varies]	Owner of the file that was acted upon (created, written, overwritten, or deleted)
Zone Names	[varies]	Zones that the device belongs to

Example message for file-based detection events

Event Type: OpticsCaeFileEvent, Event Name: OpticsCaeFileEvent, Device Name: OPTICS-DEMO-2, Zone Names: (Zone1, Zone2), Event Id: b401cb01-ee5e-44af-b094-fa9777c2975a, Severity: Low, Description: Microsoft Office WLL/XLL RCE, Instigating Process Name: WINWORD.EXE, Instigating Process Owner: CYLANCE/mmorin, Instigating Process ImageFileSha256: 5BBCF5C59544169FB1C199525BBF57A5BBD827202EA2C68D3143130AB2D60A88, Target File Path: c:\users\mmorin\appdata\local\microsoft\office\suspect.wll, Target File Owner: CYLANCE/mmorin, Target File Sha256: 5BBCF5C59544169FB1C199525BBF57A5BBD827202EA2C68D3143130AB2D60A88, Device Id: e378dacb-9324-453a-b8c6-5a8406952195

BlackBerry Optics registry-based detection events

These events occur when a Detection Event that includes a Registry Process artifact is triggered.

Field	Value	Description
Description	[varies]	Name of the detection rule that was triggered
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred

Field	Value	Description
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaeRegistryEvent	Detection Event involved a Target Registry item
Event Type	OpticsCaeRegistryEvent	Detection Event involved a Target Registry item
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Target Registry KeyPath	[varies]	Path of the registry key that was acted upon (created, written, overwritten, or deleted)
Target Registry ValueName	[varies]	Value name of the registry item that was acted upon (created, written, overwritten, or deleted)
Zone Names	[varies]	Zones that the device belongs to

Example message for registry-based detection events

Event Type: OpticsCaeRegistryEvent, Event Name: OpticsCaeRegistryEvent, Device Name: OPTICS-DEMO-2, Zone Names: (Zone1, Zone2), Event Id: b70da00c-78f4-400f-9b81-25aee339c4ed, Severity: Low, Description: Detect Suspect_Key Persistence, Instigating Process Name: reg.exe, Instigating Process Owner: CYLANCE/mmorin, Instigating Process ImageFileSha256: 4E66B857B7010DB8D4E4E28D73EB81A99BD6915350BB9A63CD86671051B22F0E, Target Registry KeyPath: HKLM\software\microsoft\windows\currentversion\run, Target Registry ValueName: suspect_key, Device Id: e378dacb-9324-453a-b8c6-5a8406952195

BlackBerry Optics network-based detection events

These events occur when a Detection Event that includes a Network Process artifact is triggered.

Field	Value	Description
Description	[varies]	Name of the Detection Rule that was triggered
Destination IP	[varies]	Destination IP address involved with a Detection Event. This is typically a resource external to your environment
Destination Port	[varies]	Network port on the destination IP address involved with a Detection Event
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaeNetworkEvent	Detection Event involved a network connection
Event Type	OpticsCaeNetworkEvent	Detection Event involved a network connection
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action
Severity	[varies]	Severity of the event • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Zone Names	[varies]	Zones that the device belongs to

Example message for network-based detection events

Event Type: OpticsCaeNetworkEvent, Event Name: OpticsCaeNetworkEvent, Device Name: OPTICS-DEMO-2, Zone Names: (Zone1, Zone2), Event Id: f3cc2742-34f8-4374-9231-d59350b10ecc, Severity: Low, Description: Unsigned Application Network Beaconing, Instigating Process Name: myapp.exe, Instigating Process Owner: CYLANCE/mmorin, Instigating Process ImageFileSha256:

4E66B857B7010DB8D4E4E28D73EB81A99BD6915350BB9A63CD86671051B22F0E, Destination IP: 95.85.19.151, Destination Port: 443, Device Id: e378dacb-9324-453a-b8c6-5a8406952195

BlackBerry Optics memory-based detection events

These events occur when a Detection Event that includes a macOS Memory Event (such as changing an area of memory marked as read/write to execute.)

Field	Value	Description
Description	[varies]	Name of the Detection Rule that was triggered
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaeMemoryEvent	Detection Event involved a memory event
Event Type	OpticsCaeMemoryEvent	Detection Event involved a memory event
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Zone Names	[varies]	Zones that the device belongs to

Example message for memory-based detection events

Event Type: OpticsCaeMemoryEvent, Event Name: OpticsCaeMemoryEvent, Device Name: OPTICS-DEMO-2, Zone Names: (Zone1, Zone2), Event Id: 26874384-989c-4962-bc5f-bca0da4b8bb1, Severity: Low, Description: Read/Write Memory Changed to Executable, Instigating Process Name: memory-mapper.app, Instigating Process Owner: CYLANCE/mmorin, Instigating Process ImageFileSha256:

4E66B857B7010DB8D4E4E28D73EB81A99BD6915350BB9A63CD86671051B22F0E, Device Id: e378dacb-9324-453a-b8c6-5a8406952195

BlackBerry Optics DNS-based detection events

These events occur when a Detection Event that includes a DNS-based artifact is triggered.

Field	Value	Description
Description	[varies]	Name of the Detection Rule that was triggered
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaeDNSEvent	Detection Event involved a DNS-based connection
Event Type	OpticsCaeDNSEvent	Detection Event involved a DNS-based connection
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action
Resolved Address	[varies]	Resolved IP address for the domain
Resolved Address Count	[varies]	Number of resolved IP addresses for the domain
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Target Domain Name	[varies]	Target domain that was attempted to be resolved

Field	Value	Description
Zone Names	[varies]	Zones that the device belongs to

Example message for DNS-based detection events

9/27/19 0:31:07 Syslog.Warning 10.6.27.126 1 2019-09-27T00:31:04.2540000Z sysloghost CylanceOPTICS - - [Optics2.4SyslogTesting] Event Type: OpticsCaeDnsEvent, Event Name: OpticsCaeDnsEvent, Device Name: DEV-01, Zone Names: (Windows 10,10.45.*), Event Id: 7cd37028-4cba-4a81-b9bb-c1ebbef9a0a3, Severity: Informational, Description: v1-dnsrequest_tld2, Instigating Process Name: ICreateDnsRequests.exe, Instigating Process Owner: DEV-01//DevUser, Instigating Process ImageFileSha256: 839459355BC41EA0F85F1D15868DD6576C510677DA7DF4DFC00E317FE4C2C7F5, Target Domain Name: test.test, Resolved Address: Unknown, Resolved Address Count: 0, Device Id: 340d587c-1bbe-41d0-a330-24b12584fadc

BlackBerry Optics log-based detection events

These events occur when a detection event that includes a log-based artifact is triggered.

Field	Value	Description
Description	[varies]	Name of the Detection Rule that was triggered
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaeLogEvent	Detection Event involved a Log-based connection
Event Type	OpticsCaeLogEvent	Detection Event involved a Log-based connection
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action
Security Provider	[varies]	Name of the service which generated the Windows Event Log message

Field	Value	Description
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Windows Event ID	[varies]	Numerical Windows Event ID associated with the Windows Event
Zone Names	[varies]	Zones that the device belongs to

Example message for log-based detection events

9/27/19 0:30:29 Syslog.Warning 10.6.27.126 1 2019-09-27T00:30:26.9950000Z sysloghost CylanceOPTICS - - [Optics2.4SyslogTesting] Event Type: OpticsCaeLogEvent, Event Name: OpticsCaeLogEvent, Device Name: DEV-01, Zone Names: (Windows 10,10.45.*), Event Id: 3b53b1d1-f23b-46b3-a6b4-b1547a4461c7, Severity: Informational, Description: WindowsEvent Rule - Logon, Instigating Process Name: services.exe, Instigating Process Owner: NT AUTHORITY//SYSTEM, Instigating Process ImageFileSha256: BE42E4A901D6AC8885882D2CD9372A64023794428E0AC8CC87EE3121DD5DC402, Windows Event Id: 4624, Security Provider: SecurityAuditProvider, Device Id: 340d587c-1bbe-41d0-a330-24b12584fadc

BlackBerry Optics Powershell trace detection events

These events occur when a Detection Event that includes a Powershell Trace artifact is triggered.

Field	Value	Description
Description	[varies]	Name of the Detection Rule that was triggered
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaePowershellTraceEvent	Detection Event involved a Powershell trace
Event Type	OpticsCaePowershellTraceEvent	Detection Event involved a Powershell trace
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action

Field	Value	Description
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action
Payload	[varies]	Powershell modules and/or arguments that were passed into the Powershell interpreter
Payload Length	[varies]	Length of the observed Powershell Payload field
Script Block Length	[varies]	Length of the observed Powershell Script Block Text field
Script Block Text	[varies]	Content of a Powershell script or module that was loaded or executed by the Powershell interpreter
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Zone Names	[varies]	Zones that the device belongs to

Example message for Powershell trace detection events

9/27/19 0:31:10 Syslog.Warning 10.6.27.126 1 2019-09-27T00:31:06.3840000Z sysloghost CylanceOPTICS - - [Optics2.4SyslogTesting] Event Type: OpticsCaePowershellTraceEvent, Event Name: OpticsCaePowershellTraceEvent, Device Name: DEV-01, Zone Names: (Windows 10,10.45.*), Event Id: 11fbfe57-364d-48bb-a0c5-291d69e1b1c3, Severity: Informational, Description: Basic PowerShell ScreenShot Rule, Instigating Process Name: powershell.exe, Instigating Process Owner: DEVICE-01//DeviceUser, Instigating Process ImageFileSha256: D3F8FADE829D2B7BD596C4504A6DAE5C034E789B6A3DEFBE013BDA7D14466677, Script Block Text: function screenshot([Drawing.Rectangle]$bounds, $path){ $bmp = New-Object Drawing.Bitmap $bounds, Script Block Length: 320, Payload: None, Payload Length: 0, Device Id: 340d587c-1bbe-41d0-a330-24b12584fadc

BlackBerry Optics WMI-based detection events

These events occur when a Detection Event that includes a Windows Management Instrumentation (WMI) Process artifact is triggered.

Field	Value	Description
Consumer Text	[varies]	Text (commonly the command to be executed) associated with a WMI event
Consumer Text Length	[varies]	Length of the observed Consumer Text field
Description	[varies]	Name of the Detection Rule that was triggered
Device Id	[varies]	Unique ID for the device
Device Name	[varies]	Name of the device on which the Detection Event occurred
Event Id	[varies]	Unique ID for the Detection Event
Event Name	OpticsCaeWmiEvent	Detection Event involved a WMI connection
Event Type	OpticsCaeWmiEvent	Detection Event involved a WMI connection
Instigating Process ImageFileSha256	[varies]	SHA256 hash of the process that instigated the action
Instigating Process Name	[varies]	Name of the process that instigated the action
Instigating Process Owner	[varies]	User who owns the process that instigated the action
Operation	[varies]	WMI operation that was executed. Commonly a binding creation, a filter creation, or a consumer creation
Operation Length	[varies]	Length of the observed Operation field
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention. • Medium: A suspicious event that should be reviewed. • Low: An important event, but may not be malicious. • Info: An observed event.
Zone Names	[varies]	Zones that the device belongs to

Example message for WMI-based detection events

9/27/19 0:45:43 Syslog.Warning 10.6.27.126 1 2019-09-27T00:45:39.6710000Z sysloghost CylancePROTECT - - [Optics2.4SyslogTesting] Event Type: OpticsCaeWmiEvent, Event Name: OpticsCaeWmiEvent, Device Name: DEV-01, Zone Names: (Windows 10,10.45.*), Event Id: 65e46a05-181a-4d87-adef-b84f4732031a, Severity: Informational, Description: Basic WMI Permanent Subscriber Rule, Instigating Process Name: svchost.exe, Instigating Process Owner: NT AUTHORITY//SYSTEM, Instigating Process ImageFileSha256: 29F04D5F4B8D798038CB9647178A8B9C68E16DC50DA850937F6E993FC7967B75, Consumer Text: "E:\\\ \Test.vbs";, Consumer Text Length: 17, Operation: Binding EventFilter: instance of __EventFilter{ CreatorSID = {1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, Operation Length: 731, Device Id: 340d587c-1bbe-41d0-a330-24b12584fadc

BlackBerry Protect Mobile event types

If BlackBerry Protect Mobile is enabled for your organization, you can choose to send the alerts that are detected by the Protect Mobile app on users' devices to your organization's syslog server. This section provides details about the mobile alert events that are sent to the syslog server.

Mobile alerts

This option is visible only if Protect Mobile is enabled. When this option is turned on, the mobile alerts that are detected by the Protect Mobile app on users' devices are sent to your organization's syslog server.

Field	Value	Description
Alert Id	[varies]	This is the unique ID associated with the mobile alert.
Alert Name	maliciousApplication: [app name]	This is the name of the malicious app that the Protect Mobile app detected.
	sideLoadedApplication for Android: [app name]	This is the name of the sideloaded app that the Protect Mobile app detected.
	sideLoadedApplication for iOS: [signing ID]	This is the signing ID of the sideloaded app that the Protect Mobile app detected.
	jailbrokenOrRooted for Android: Rooted	The Protect Mobile app detected that the device is rooted.
	jailbrokenOrRooted for iOS: Jailbroken	The Protect Mobile app detected that the device is jailbroken.
	deviceEncryption: Encryption disabled	The Protect Mobile app detected that encryption is not enabled on the device.
	deviceScreenlock: Screenlock disabled	The Protect Mobile app detected that a screen lock is not enabled on the device.
	iOsIntegrityFailure: iOS App Integrity Check	The Protect Mobile app failed an integrity check.
	androidSafetyNetFailure: Android SafetyNet	The Protect Mobile app failed a SafetyNet attestation check.
	androidHWFailure: Android Hardware	The Protect Mobile app failed hardware certificate attestation.

Field	Value	Description
	unsupportedOS: Unsupported OS	Based on the administrator configuration of the Protect Mobile policy, the Protect Mobile app detected that the device has an unsupported OS.
Alert Status	New	The mobile alert is not yet resolved.
	Resolved	The mobile alert is resolved.
Alert Type	maliciousApplication	The Protect Mobile app detected a malicious app.
	sideLoadedApplication	The Protect Mobile app detected a sideloaded app.
	jailbrokenOrRooted	The Protect Mobile app detected that the device is jailbroken or rooted.
	deviceEncryption	The Protect Mobile app detected that encryption is not enabled on the device.
	deviceScreenlock	The Protect Mobile app detected that a screen lock is not enabled on the device.
	iOsIntegrityFailure	The Protect Mobile app failed an integrity check.
	androidSafetyNetFailure	The Protect Mobile app failed a SafetyNet attestation check.
	androidHWFailure	The Protect Mobile app failed hardware certificate attestation.
	unsupportedOS	Based on the administrator configuration of the Protect Mobile policy, the Protect Mobile app detected that the device has an unsupported OS.
ApplicationSha256	[SHA256 hash]	This is the SHA256 hash of a malicious or sideloaded Android app that the Protect Mobile app detected.
ApplicationName	[app name]	This is the name of a malicious or sideloaded Android app that the Protect Mobile app detected.

Field	Value	Description
AttestationRuleFailure	[attestation rules]	These are the rules that failed when an attestation check occurred for the Protect Mobile app.
AttestationState	[attestation state]	This is the attestation state of the Protect Mobile app.
AttestationSubType	[attestation sub-type]	This is the sub-type of the attestation check for the Protect Mobile app.
Description	maliciousApplication: [package name], [package version], [SHA256 hash]	These are the details of the malicious app that was detected.
	sideLoadedApplication for Android: [package name], [package version], [installer source], [SHA256 hash]	These are the details of the sideloaded app that was detected.
	sideLoadedApplication for iOS: empty string	This field is not supported for iOS.
	jailbrokenOrRooted: [OS name], [OS version]	This is the OS name and version of the jailbroken or rooted device.
	deviceEncryption: [OS name], [OS version]	This is the OS name and version of the device that does not have encryption enabled.
	deviceScreenlock: [OS name], [OS version]	This is the OS name and version of the device that does not have a screen lock enabled.
	iOsIntegrityFailure: [attestation type], [attestation state]	These are the details of the failed iOS integrity check.
	androidSafetyNetFailure: [attestation type]	These are the details of the failed SafetyNet attestation check.
	androidHWFailure: [attestation type], [attestation state], [rule failure]	These are the details of the failed hardware certificate attestation.
	unsupportedOS: [OS name], [OS version]	This is the OS name and version of the device with an unsupported OS.
Detected	[varies]	This is the date and time the alert was detected.
Device Id	[varies]	This is the unique ID of the user's device.

Field	Value	Description
Device Name	[varies]	This is the name of the user's mobile device.
Event Type	MobileAlert	This is the defined event type for mobile alerts.
Event Name	ProtectMobileAlert	This is the defined event name for mobile alerts.
First Name	[varies]	This is the first name of the device user.
InstallerSource	[package name]	This is the package name of a sideloaded Android app that the Protect Mobile app detected.
Last Name	[varies]	This is the last name of the device user.
OsName	[OS name]	This is the OS of the device.
OsVersion	[OS version]	This is the device's OS version.
PackageName	[package name]	This is the package name of a malicious or sideloaded Android app that the Protect Mobile app detected.
PackageVersion	[package version]	This is the package version of a malicious or sideloaded Android app that the Protect Mobile app detected.
SigningIdentity	[signing ID]	This is the signing ID of a sideloaded iOS app that the Protect Mobile app detected.
SigningIdentitySha256	[signing ID hash]	This is the signing ID hash of a sideloaded iOS app that the Protect Mobile app detected.

Example syslog message

```
May 31 17:34:04 sysloghost CylancePROTECT Event Type: MobileAlert,
 Event Name: ProtectMobileAlert, Alert Type: sideLoadedApplication,
 Alert Name: Protect, Description: com.blackberry.protect,
 1.4.397 (Installer Source: com.google.android.packageinstaller),
 1234ABCD5678EFGH1234ABCD5678EFGH1234ABCD5678EFGH1234ABCD5678EFGH, Detected:
 5/31/2021 2:32:12 PM, Alert Status: New, Device Name: Galaxy S9 SM-G960F,
 First Name: John, Last Name: Smith, Device Id: 1abc2345-67d8-9123-45ef-
g45hi67j8kl9, Alert Id: a1b23456-789c-12d3-e45f-g6h7i8jk9123, Application Sha245:
 1234ABCD5678EFGH1234ABCD5678EFGH1234ABCD5678EFGH1234ABCD5678EFGH, Application
```

```
Name: Protect, Installer Source: com.google.android.packageinstaller, Package
Name: com.blackberry.protect, Package Version: 1.4.397
```

BlackBerry Persona Desktop event types

If BlackBerry Persona Desktop is enabled for your organization, you can choose to send the alerts that are detected by the Persona Desktop agent on users' devices to your organization's syslog server. This section provides details about the mobile alert events that are sent to the syslog server.

Persona Desktop events

This option is visible only if Persona Desktop is enabled. When this option is turned on, the events that are detected by the Persona Desktop agent on users' devices are sent to your organization's syslog server.

Note: Trust scores and model scores are displayed as N/A in the syslog message when Persona Desktop is in training mode.

Field	Value	Description
Alert ID	[varies]	This is the unique ID associated with the Persona Desktop event.
Alert Severity	[varies]	This is the severity of the alert.
Alert Time	[varies]	This is the event Action Type and it is used as the name for the alert. See Persona Desktop event types for more information.
Alert Type	Failed 2FA	The user failed to pass the two-factor authentication (2FA) logon.
	Failed Logon	The user failed to enter the correct username and password when logging into the device.
	Forced Step-Up Authentication	The user was required to enter their username and password or pass a 2FA challenge to continue using the device.
Device ID	[varies]	This the unique device ID associated with the event.
Device Name	[varies]	This is the device name associated with the event.
Event Name	Persona Event	This is the defined event name for Persona Desktop events.
Event Type	PersonaEvent	This is the defined event type for Persona Desktop events.
IP Address	[varies]	This is the IP address for the device.
Keyboard Model Score	[varies]	This is a model score based on the way the user types on the keyboard.
Logon Model Score	[varies]	This is a model score based on when the user logs on or when the user fails at logging on.
Meta Model Score	[varies]	This is a combined score from the keyboard, mouse, and conduct models.

Field	Value	Description
Mouse Model Score	[varies]	This is a model score based on the way the user moves and clicks the mouse or trackpad.
Network Model Score	[varies]	This is a model score based on the IP addresses and ports the user accesses.
Process Model Score	[varies]	This is a model score based on the applications the user launches.
Tenant ID	[varies]	This is the unique tenant ID.
User ID	[varies]	This is the unique user ID associated with the event.
User Name	[varies]	This is the username associated with the event.
User Trust Score	[varies]	This is the user's trust score.

Example syslog message

```
May 31 17:34:04 sysloghost CylancePROTECT: Event Type: PersonaEvent, Event Name:
 Persona Event, Tenant ID: 572d08ac-3232-41d8-a0fd-59a8db8d603d, Alert ID: 0d10cf3a-
dfb9-4c6f-932b-550bf2d53ad7, Alert Type: Failed Logon, Alert Severity: High, User
 ID: 41577746-8260-30ac-35b2-e41c34c7ac6b, User Name: test10, Device ID: 58d0329c-
eb73-4a54-9ca5-6dcb4e23746c, Device Name: PDTESTAGENT1, IP IpAddress: 82.45.6.13,
 Alert Time: 2/18/2021 1:22:02 AM, User Trust Score: 81, Meta Model Score: 82,
 Keyboard Model Score: 83, Mouse Model Score: 84, Logon Model Score: 85, Process
 Model Score: N/A, Network Model Score: 87
```

BlackBerry Gateway event types

If BlackBerry Gateway is enabled for your organization, you can choose to send the alerts that are detected by Gateway to your organization's syslog server. This section provides details about the network threat events that are sent to the syslog server.

Network threats

This option is visible only if Gateway is enabled. When this option is turned on, the events that are detected by Gateway are sent to your organization's syslog server.

Field	Value	Description
Eco Id	[varies]	The user's EcoID, if available.
Event Name	Blocked Connection Allowed Connection	This is the defined event name for network alerts: • Allowed connections: a detection happened and a syslog event was generated; but the connection was allowed based on the applied risk criteria. • Blocked connections: a detection happened and a syslog event was generated; and the connection was blocked based on the applied risk criteria.
Event Type	NetworkThreat	This is the defined event type for network alerts.
GhostUserEmail	[varies]	The email address of the support user.
Message	[varies]	The message contains information related to the event, in JSON string format.
Source	big.blackberry.com	The BlackBerry product generating the event.
Timestamp	[varies]	The date and time the event occurred.

Message descriptions

Field	Value	Description
action	string	The action performed against this traffic. Unique to the associated event.

Field	Value	Description
alertType	string	The alert type associated with the event. The supported types are: • ipReputation - event triggered due to destination risk. • signature - event triggered due to inspection of packets. • accessControl - event triggered due to user's network access rules.
signature	string	The Packet Inspection Rule details of the identified network threat, if applicable.
category	string	The Packet Inspection Rule category of the identified network threat, if applicable.
policyName	string	The name of the user's policy that triggered the event, if applicable.
appName	string	The name of the application or network service associated with the blocked event, if applicable.
mitre	string	The MITRE information related to the event. Additional details are provided below. **Name** / **Notes** techniqueId — The MITRE technique ID techniqueName — The MITRE technique name tacticId — The MITRE tactic ID tacticName — The MITRE tactic name
endpointId	string	The Gateway installation ID of the endpoint as it is registered in UES.
venueEndpointId	string	The ID of the BlackBerry Protect Desktop service if it is installed on the same device.
dOsVers	string	The OS version of the device.
dId	string	The UES ID of the device.
dPlat	string	The platform of the device.
dManuf	string	The manufacturer of the device.
dModel	string	The model of the device.

Field	Value	Description
flowId	string	The ID of the Gateway access control engine flow that this event is associated with.
correlationId	string	The correlation ID assigned to the event.
sourceIp	string	The packet source IP address.
sourcePort	string	The packet source port.
dstAddress	string	The destination IP address of the IP packet that triggered the event. Can be IPv4 or IPv6.
destPort	string	The packet destination port.
protocol	string	The protocol used to transit the packet.
endpointIp	string	The public source IP associated with the endpoint. This IP is assigned by the network itself.

Example syslog message - Access control policy (blocked)

```
Event Type: NetworkThreat, Event Name: blocked connection, Eco Id:
 Am6XZ102m1PgFzI/N8mjANP4=, User: John Smith (jsmith@example.com),
 User Name: jsmith, Message: {"endpointId":"6c726244-ad1d-4ff4-922b-
cbaf8ab3c6c2", "flowId":3190005035111956, "endpintIp":"99.250.195.118:39867",
 "dstAddress":"10.10.10.129", "action":"blocked", "dManuf":"Google",
 "category":"Access Control Blocked", "key":"", "correlationId":"4ddb23a8-
defa-4a17-b549-4c36ed193954", "sourcePort": 31637, "destPort":53,
 "alertType":"accessControl", "policyName":"E2E Auto Block Saas Apps",
 "dId":"821f57dc-d7d6-4907-90ba-c6d7b0bca943", "venueEndpointId":"",
 "dOsVers":"11", "appName":"Slack", "protocol":"UDP", "signature":"Access Control
 Blocked - DNS", "dPlat":"Android", "sourceIp":"10.10.10.137", "dModel":"Pixel 4",
 "mitreData":""}
```

Example syslog message - Signature detection (blocked)

```
Event Type: NetworkThreat, Event Name: blocked connection, Eco Id:
 Am6XZ102mlPgFzI/N8mjANP4=, User: John Smith (jsmith@example.com),
 User Name: jsmith, Message: {"endpointId":"7c726244-ad1d-4ff4-922b-
cbaf8ab3c6c1", "flowId":1975772272249751, "endpointIp":"99.250.195.118:49713",
 "dstAddress":"10.10.10.1", "action":"blocked", "dManuf":"Google", "category":"A
 Network Trojan was detected", "key":"", "correlationId":"6df43c40-5bad-40d1-
b081-7882cb28d330", "sourcePort":28945, "destPort":53, "alertType":"signature",
 "policyName":"E2E Auto Block Saas Apps", "dId":"812f57dc-d7d6-4907-90ba-
c6d7b0bca943", "venueEndpointId":"", "dOsVers":"11", "appName":"",
 "protocol":"UDP", "signature":"ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY
 DNS Lookup 1 (tp/emerging-threats/emerging-mobile_malware/2025014)",
 "dPlat":"Android", "sourceIp":"10.10.10.9", "dModel":"Pixel 4", "mitreData":""}
```

Example syslog message - Signature detection (allowed)

```
Event Type: NetworkThreat, Event Name: allowed connection, Eco Id:
 Am6XZ102mlPgFzI/N8mjANP4=, User: John Smith (jsmith@example.com), User Name:
```

```
 jsmith, Message: {"policyName":"E2E Auto FQDN Block", "flowId":788929250499854,
 "sourceIp":"10.10.10.22", "dId":"5e2ae619-8116-4f0e-b233-91eeec15c9c4",
 "sourcePort":41236, "destPort":80, "endpointId":"f9963a84-9311-42c7-b251-
c4dd97ed2bd6", "dOsVers":"0", "mitreData":"", "appName":"", "endpointIp":"",
 "correlationId":"883d6505-2cd5-4872-98b0-570cf2bdf24b", "dManuf":"generic",
 "venueEndpointId":"", "dModel":"Generic Device", "action":"allowed",
 "alertType":"signature", "dstAddress":"69.16.231.150", "signature":"ET POLICY
 curl User-Agent Outbound (tp/emerging-threats/emerging-policy/2013028)",
 "key":"", "category":"Attempted Information Leak", "dPlat":"Windows",
 "protocol":"TCP"}
```

Example syslog message - IP reputation (blocked)

```
Event Type: NetworkThreat, Event Name: blocked connection, Eco Id:
 Am6XZ102mlPgFzI/N8mjANP4=, User: John Smith (jsmith@example.com), User Name:
 jsmith, Message: {"sourceIp":"10.10.10.18", "protocol":"TCP", "dModel":"Nexus
 6", "policyName":"IP Reputation Policy", "appName":"", "mitreData":"", "key":"",
 "dstAddress":"195.110.46.232", "alertType":"ipReputation", "dPlat":"Android",
 "venueEndpointId":"", "destPort":80, "category":"Access Control Blocked",
 "endpointId":"e017bd79-69e5-4a4f-af26-f295b0d28e78", "signature":"Access Control
 Blocked", "flowId":801786180096101, "sourcePort":39240, "action":"blocked",
 "dId":"fe9fd95d-76c4-410f-997f-7c76e8741b0f", "dManuf":"motorola",
 "correlationId":"d773b803-9333-4851-85ed-ae5165e83f93", "dOsVers":"7.1.1",
 "endpointIp":"173.33.81.137:41890"}
```

Example syslog message - IP reputation (allowed)

```
Event Type: NetworkThreat, Event Name: allowed connection, Eco Id:
 Am6XZ102mlPgFzI/N8mjANP4=, User: John Smith (jsmith@example.com), User Name:
 jsmith, Message: {"dPlat":"Windows", "destPort":443, "dId":"a58a0ce5-d94f-472e-
ab57-574fc807119e", "policyName":"allow_all", "flowId":1139639166113122,
 "dstAddress":"odc.officeapps.live.com", "endpointIp":"172.29.139.30:35068",
 "dOsVers":"Windows 10 Enterprise 2009", "category":"Access Control
 Allowed", "mitreData":"", "protocol":"TCP", "dManuf":"VMware, Inc.",
 "dModel":"VMware Virtual Platform", "appName":"", "endpointId":"96551433-
b13d-423b-8157-d8854f82a8cb", "key":"", "signature":"Access Control
 Allowed - TLS", "venueEndpointId":"c303f4e7-8377-4a6d-9849-19b8cf811e9f",
 "correlationId":"210cc54b-8624-4d18-9ca8-3af1335500bd", "action":"allowed",
 "alertType":"ipReputation", "sourceIp":"10.10.10.133", "sourcePort":58111}
```

Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada