CylanceMDR Pro

Integration Guide

Third-party Log Sources

Contents

Integrating third-party log sources

When you integrate third-party log sources with CylanceMDR, you unify endpoint detection and response (EDR) with other security and business tools for improved visibility and control of security incidents across the business in a single console. Related telemetry data from various tools across the environment are automatically associated with a single incident, reducing manual effort and unnecessary context switching. Based on the efficacy, correlation, and actions of incidents from the various telemetry sources, CylanceMDR can be optimized to automatically take action against security incidents in real time.

A CylanceMDR Pro subscription is required to support the integration of third-party log sources.

For a list of third-party log sources that can be integrated with CylanceMDR so that suspicious activities can be reported and tracked from the Cylance console, see Supported third-party log sources for telemetry data ingestion.

Steps for integrating third-party log sources

Step	Action
1	If you have a Windows Server and you want to forward its event data to CylanceMDR, you need to install the sensor. • Review the Windows Server Sensor requirements • Install the Windows Server Sensor
2	If you want to forward logs from third-party application (such as from a firewall or VPN application) to CylanceMDR, you need to install a modular sensor. • Review the Modular Sensor requirements • Install a Modular Sensor in VMware • Install a Modular Sensor in Azure
3	Configure devices to Forward log messages to the Modular Sensor.
4	Configure CylanceMDR to Collect logs using connectors.

Installing the Windows Server Sensor

The Windows Server Sensor (agent) runs as a Windows service in a compatible Windows Server system. It observes events within the Windows Server system and sends data records to CylanceMDR. The sensor captures the following events:

- Hardware
- Security
- System
- Windows Firewall
- Windows Defender
- PowerShell
- File Integrity Monitoring

The Windows Server Sensor provides the following key capabilities:

- If the sensor is installed on the same network as the domain controller, CylanceMDR enriches data with the relationship between users and IP addresses.
- If the sensor is installed on the same network as the DHCP server, CylanceMDR enriches data with the relationship between hostnames and IP addresses, so assets can be tracked even when the IP address changes.

Windows Server Sensor requirements

The host Windows Server into which the Windows Server Sensor is installed must meet the following minimum requirements, regardless of whether it is a physical or virtual server:

Component	Specification
Host requirements	• CPU: Xeon Core 2 virtual cores (2.0 GHz or more) • RAM: 8 GB • Disk space (SSD): 64 GB
OS version	Windows Server 2008 R2 (or later)
OS updates	As a best practice, use Windows Update to ensure that the Windows Server software is up-to-date and all pending updates are complete before installing the Windows Server Sensor. The Windows Server Sensor includes the **AI_ChainedPackageFile.vc_redist.x64.exe** redistributable from Microsoft which requires the following packages: • KB2919355 • KB2999226
Firewall ports	Open TCP port 8889 to receiver-cylancemdr.stellarcyber.cloud

Component	Specification
Other software considerations	To avoid potential conflicts with antivirus or EDR software, configure any such software that's installed on the same host as the Windows Server Sensor to exclude the server sensor installation directories from scanning. Exclude the following directories on the Windows Server Sensor host: • `C:\ProgramData\Stellarcyber` • `C:\Program Files\Aella`

Install the Windows Server Sensor

Before you begin:

- Review the Windows Server Sensor requirements.
- Obtain the token for Windows Server Sensor from the CylanceMDR onboarding team.
- Download the Windows Server Sensor installation (.msi) file.

1. Some Windows systems automatically block files you download from running. To unblock the .msi file:
   a) Right-click the .msi file > **Properties**.
   b) In the **Security** section, click **Unblock** .
   c) Click **OK**.
2. To start the installation, double-click the .msi file. If you see a dialog box asking you to verify that you want to run this file, click **Run**.
3. Choose the following installation path for the agent installation: `C:\Program Files\Aella`. An error message occurs if you try to install at a different path.
4. Specify the following:
   - **Token**: Specify the installation token which is provided by the CylanceMDR onboarding team to register your Windows Server Sensor with your CylanceMDR tenant.
5. Click **Install**.
   The installer installs the Windows Server Sensor.
6. When the installation completes, click **Finish**. The sensor is installed as a service.

After you finish:

- To verify the installation, on the Windows Server Sensor host, open the **Services** app and look for **Windows Agent Sensor Ctrl**.
- To verify the connection to the tenant, open **Windows Agent Sensor CLI** and enter `show cm` in the command line.

Installing a Modular Sensor

You can install a Modular Sensor to collect and forward logs to CylanceMDR. For example, you can set up your organization's firewall syslogs, DHCP/DNS/IP network syslogs, and syslogs from other applications to forward log entries to the Modular Sensor. The sensor collects the entries and forwards them to CylanceMDR.

Modular Sensor requirements

Item	Description
Host requirements	• CPU: 4 cores • RAM: 8 GB • Disk space (SSD): 64 GB
Firewall ports	Open TCP port 8889 to receiver-cylancemdr.stellarcyber.cloud

Install a Modular Sensor in VMware

When you install a Modular Sensor in VMware, you also need to create and specify a port group as well as apply a token to associate it with your CylanceMDR tenant.

Before you begin:

- Review the Modular Sensor requirements.
- Obtain a token for the Modular Sensor from the CylanceMDR onboarding team.
- Download the .ova file for the Modular Sensor.

1. Log in to the vSphere client.
2. Right-click the VM host on which you want to install the port group and click **Add Networking**.
3. Select the **Virtual Machine Port Group for a Standard Switch** option.
4. Click **Next**.
5. Enter the following:
   - **Name**: The name for this port group.
   - **vLAN ID**: 4095
   - **Virtual switch**: Select an existing virtual switch that you want to use.
   - **Promiscuous mode**: Accept
   - **MAC Address changes**: Inherit from vSwitch
   - **Force transmits**: Inherit from vSwitch
6. In the vSphere client, on the VM host where you want install and deploy the Modular Sensor, specify the following settings.
   - **OVF template**: Specify the Modular Sensor .ova file.
   - **Virtual machine name**: Specify a name for the Modular Sensor VM.
   - **Compute resource**: Specify the compute resource to use for the Modular Sensor VM.
   - **Storage**: Specify the datastore drive to use for VM storage and its configuration.
   - **Provisioning type**: Specify `Thick`.
   - **Network mappings**: Select the VM network that you want to use.

- **Power On automatically**: Deselected.

7. Verify the settings and click **Finish**.
   The deployment completes. This might take several minutes.
8. After successful deployment, click the VM.
9. Click **Edit**.
10. Click **Add network adapter**.
11. Beside the **New adapter** field, select the port group that you created earlier.
12. Click **Save**.
13. Power on the VM.
14. Do the following to set a static IP address for the Modular Sensor and apply the token to associate it with CylanceMDR:
    a) Open the VM for your Modular Sensor. A command line appears.
    b) Enter your login information. The default username/password is aella/changeme. You are prompted to change the password immediately.
    c) Set a static IP address for the modular sensor using the following commands:
       - `set interface management ip <ip_address>`
       - `set interface management gateway <gateway_ip_address>`
       - `set interface management dns <dns_ip_address>`
    d) Enter `set token string <token>`, where *<token>* is the token provided by the CylanceMDR onboarding team.
       The message "Sensor token is successfully set" appears.

After you finish:

- To verify the connection with CylanceMDR use the following commands:
  - `show interface`
  - `show cm`
  - `show version`
- The CylanceMDR onboarding team completes the configuration for your CylanceMDR tenant to receive logs from your Modular Sensor.

Install a Modular Sensor in Azure

Depending on your Microsoft Azure subscription, installing and using the Modular Sensor in Azure may incur additional costs. After you install the sensor, you need to apply a token to associate it with your CylanceMDR tenant.

Before you begin:

- Review the Modular Sensor requirements.
- Obtain a token for the Modular Sensor from the CylanceMDR onboarding team.

1. Log in to your Azure portal at https://portal.azure.com/.
2. On the **Dashboard** screen, Click **Azure Active Directory**.
3. Click **Properties**.
4. Copy the **Tenant ID** field.

5. Copy and paste the following URL into your browser address bar and replace <*tenant_id*> with the Tenant ID that you copied.

```
https://login.microsoftonline.com/<tenant_id>/oauth2/authorize?
client_id=58238038-43b4-4446-8260-0fa97ace1085&response_type=code&redirect_uri=https
%3A%2F%2Fwww.microsoft.com%2F
```

6. In the **Permissions requested** dialog, select **Consent on behalf of your organization**.
7. Click **Accept**.
8. Click **Enterprise Applications**.
9. On the **Enterprise applications | All applications** screen, search for `Stellar`.
   A list of applications appear. If you don't see a list of applications, contact CylanceMDR support.
10. If necessary, create a new resource group. If you want to use an existing resource group, proceed to the next step.
    a) Click **Resource Groups**.
    b) Click **Add**.
    c) In the **Subscription** field, choose your subscription.
    d) In the **Resource group** field, enter a name of your group.
    e) In the **Region** field, choose the region where you want to deploy the resource.
    f) Click **Review + create**.
    g) Click **Create**.
11. On the **Resource Groups** screen, click the name of the resource group where you want to deploy the sensor.
12. Click **Access control (IAM)**.
13. Click **Add role assignments**.
14. Click the**Privileged administrator roles** tab.
15. Select the **Contributor** option.
16. In the **Assign access to** drop-down list, keep the default selection of **User, group, or service principal**.
17. In the **Select** field, type `Stellar`.
18. Choose **Stellar Cyber Software Packages**.
19. Click **Save**.
20. In the left pane, click **Home**. The Azure services screen appears.
21. On the **Azure services** screen, click **Subscriptions**.
22. Click the subscription that you want to use.

    Note: Depending on your Azure subscription, you may incur additional costs.
23. Click **Resource providers**.
24. Click **Microsoft.Network**.
25. Click **Register**.
26. Click **Microsoft.Compute**.
27. Click **Register**.
28. On the top right of the screen, click the **Cloud Shell** icon.
29. Enter the following commands to retrieve an access token (each command should be one line):

```
az account clear

az login --service-principal -u '58238038-43b4-4446-8260-0fa97ace1085'
 -p '3238Q~KMtVAIyuC6gDVMhboKEW7w6W~bXYQhFcZx' --tenant
 '2f580e30-1cc1-4c08-9e80-704999508e1a'
```

```
az account get-access-token
```

30. Enter the following commands to retrieve and access token using the Tenant ID that you copied earlier (each command should be one line).

```
az login --service-principal -u '58238038-43b4-4446-8260-0fa97ace1085' -p
 '3238Q~KMtVAIyuC6gDVMhboKEW7w6W~bXYQhFcZx' --tenant '<Tenant ID>'

az account get-access-token
```

31. Use the following one-line command to output a list of Azure subscriptions:

```
az account list --output table
```

32. Make sure that the subscription that you want to deploy the sensor to is the default (i.e. IsDefault=True). Use the following one-line command to set it:

```
az account set --subscription <subscription>
```

33. Enter the following one-line command to create a Modular Sensor VM. Replace <*resource-group*> with an existing resource group in your deployment and <*version*> with the version of software you want to install (for example, 5.2.0)

```
az vm create --size Standard_B12ms --resource-group <resource-group>
 --name StellarModularSensor --image "/subscriptions/0e28f851-
f477-4f2d-94bc-35c00d3d5fd8/resourceGroups/Stellar/providers/
Microsoft.Compute/galleries/StellarCyberSoftwares/images/Stellar-ModularSensor/
versions/<version>" --admin-username azureuser --admin-password P@ssw0rd#2022
 --os-disk-size-gb 128
```

Note that you can specify the virtual network and subnet by including the `--vnet-name <vnet-name>` and `--subnet <subnet-name>` parameters. The networks must exist in the same resource group as the VM.

34. Do the following to set a static IP address for the Modular Sensor and apply the token to associate it with CylanceMDR:
    a) Open the VM for your Modular Sensor. A command line appears.
    b) Enter your login information. The default username/password is aella/changeme. You are prompted to change the password immediately.
    c) Set a static IP address for the modular sensor using the following commands:
        - `set interface management ip <ip_address>`
        - `set interface management gateway <gateway_ip_address>`
        - `set interface management dns <dns_ip_address>`
    d) Enter `set token string <token>`, where <*token*> is the token provided by the CylanceMDR onboarding team.
    The message "Sensor token is successfully set" appears.

After you finish: The CylanceMDR onboarding team completes the configuration for your CylanceMDR tenant to receive logs from your Modular Sensor.

Forwarding log messages to the Modular Sensor

You can configure devices (for example, firewall) in your environment to forward log messages (for example, syslog) to the Modular Sensor so that CylanceMDR analysts can track suspicious activity.

You need to forward log messages from your device (for example, firewall) to the Modular Sensor from a specific port so that the Modular Sensor receives the messages successfully. Follow the instructions from your vendor to set up your device to forward the logs messages. For the list of ports that you need to open in your environment, see Supported third-party log sources for telemetry data ingestion.

Collect logs using connectors

You can allow CylanceMDR to collect logs from various sources by providing the necessary information to the CylanceMDR onboarding team to configure it in your tenant.

The following table lists some example log sources that can use connectors. For more information, contact the CylanceMDR onboarding team.

Log source	Required information
HIBUN	Provide the following information (obtained from Hitachi Solutions) to the CylanceMDR team: • Customer Code • Username • Password The password should not contain non-ASCII special characters.

Log source	Required information
Microsoft Active Directory	Provide the following information to the CylanceMDR team: • The Active Directory domain to be monitored • The fully qualified domain name (FQDN) or IP address for an Active Directory Server configured as a Domain Controller • The protocol type (LDAP, LDAPS, or LDAPS with certificate validation disabled) • Active Directory username and passwords with appropriate permissions • If you want to collect Active Directory logs from the Modular Sensor, you need to add the Active Directory server domain and domain controller to the same DNS where the Modular Sensor is installed. For **Collect only** configurations, the username and password needs to be a standard Active Directory user who is a member of the domain to be monitored. The password should not include non-ASCII special characters. For **Respond** configurations (if you want to also allow CylanceMDR to respond to a detected threat by disabling an Active Directory user account), do the following: 1. Launch **Active Directory Users and Computers** with administrative credentials. 2. Right-click on the **Organizational Unit** with the user account for which you want to enable the respond action authority, and select **Delegate Control**. 3. Select the user or group to which you want to delegate the authority, then click **Next**. 4. Select **Create Custom Task to Delegate** and click **Next**. 5. In the **Delegation of Control Wizard**, select the **Only the following objects in the folder** radio button. 6. Select **User objects** and click **Next**. 7. In the **Show these permissions** section, select only the **Property-specific** option. Deselect the **General** and **Creation/Deletion of specific child objects** options. 8. In the specific permissions section, select the checkboxes for **Read userAccountControl** and **Write userAccountControl**. 9. Click **Next**. 10. Click **Finish**.

Log source	Required information
Microsoft Azure Active Directory / Entra ID	Provide the following information to the CylanceMDR team: • Application (client) ID • Directory (tenant) ID • Secret Key (password) To obtain this information for configuring CylanceMDR, you need to: • In the Azure AD portal, register the CylanceMDR application. • In the AD manifest, set allowPublicClient to "true". • Create a new client secret (password) for CylanceMDR. • Set the API permissions (application permissions) for Microsoft Graph and specify the logs that you want to collect. A super admin must grant admin consent. For more information, see the Microsoft documentation.
Microsoft Azure Event Hub	Event Hub Name: The name of the Event Hub Connection String: Find the connection string in Azure. You must use a unique connection string for each instance Consumer Group: The consumer group for the Event Hub Event Source: The source of the events you want to collect from Event Hub. You must configure log sources to send data to the Event Hub. • AzureActivityLog • AzureBastion • AzureFirewall • AzureKeyVault • AzureSecurityCenter • AzureSecurityGroups • AzureSQLServer (includes AuditEvent log) • AzureStorage • AzureSynapseWorkspace • AzureWebApplicationFirewall

Supported third-party log sources for telemetry data ingestion

The following table lists the third-party products that can be integrated with CylanceMDR as a log source for telemetric data ingestion. Beside each log source is the port that needs to be opened in your organization's environment so that CylanceMDR can collect and ingest the log data, and the data fields that will be collected and indexed in CylanceMDR.

Device	Port	Index
HTTP JSON	5200 (TCP only)	Syslog
JSON	5142	Syslog
(OpnSense) Zenarmor plugin logs	5604	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
AAA - Core (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Accops	5526	Traffic (srcip), Syslog (otherwise)
Ahnlab AIPS	5647	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Ahnlab EMS	5657	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Ahnlab EPP	5640	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
AhnLab Policy Center	5571	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
AhnLab TrusGuard	5558	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
AirGap Ransomware Kill Switch	5602	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
AIX	5523	Traffic (event_time: time format of hour:minute:second), Syslog (otherwise)
Alcatel Lucent Switch	5677	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Aliyun / AliCloud	5545	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Android	5605	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Apache HTTP Server (httpd)	5663	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
AQTRONiX WebKnight	5658	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Aqua Cloud Native Application Protection Platform (CNAPP 2022.4)	5656	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Arbor Peakflow SP	5598	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Array Networks APV Series Load Balancing & App Delivery	5680	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Array Networks ASF 1800	5675	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Array Networks Secure Access Gateway	5537	Traffic (srcip), Syslog (otherwise)
Aruba ClearPass Policy Manager (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Aruba Switch	5577	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Automox	5183	Syslog
Avanan	5681	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Avanan (HTTP JSON)	5200 (TCP only)	Syslog
Avaya Switch	5607	Traffic (srcip, srcport, dstip, dstport, and proto) Syslog (otherwise)
AWS WAF	5200 (TCP only)	Syslog
Azure ATP (CEF)	5143	Traffic (srcip, srcport, dstip, dstports, and proto), Syslog (otherwise)
Azure MFA	5528	Traffic (srcip), Syslog (otherwise)
Barracuda email	5559	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Barracuda firewall	5524	ML IDS/Malware (sub_dev_type: fw_threat or fw_av), Traffic (srcip), Syslog (otherwise)
Barracuda WAF	5524	ML IDS/Malware (sub_dev_type: fw_threat or fw_av), Traffic (srcip), Syslog (otherwise)
BeyondTrust BeyondInsight	5621	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
BeyondTrust PasswordSafe	5692	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Bitdefender (HTTP JSON)	5200 (TCP only)	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
BlackBerry CylancePROTECT & CylanceOPTICS	5177	Traffic (srcip), Syslog (otherwise)
BlueCoatProxySG	5576	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Brocade switch (system & admin logs)	5548	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Calyptix UTM	5161	ML IDS/Malware (ids.signature), Traffic (srcip), Syslog (otherwise)
Centos Audit	5673	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Centrify	5165	Syslog
Cerberus FTP Logs	5635	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Check Point - Application Control (CEF)	5143	ML IDS/Malware (threat, normalized from attack_information), Traffic (srcip, srcport,dstip,dstport, and proto), Syslog (otherwise)
Check Point - URL Filtering (CEF)	5143	ML IDS/Malware (threat, normalized from attack_information), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
CheckPoint appliance	5174	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
CheckPoint firewall	5519	Traffic (srcip), Syslog (otherwise)
CheckPoint Harmony EP	5618	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
CheckPoint VPN-1 & FireWall-1 (CEF)	5143	ML IDS/Malware (threat, normalized from attack_information), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Cisco ASA	5518	Traffic (srcip), Syslog (otherwise)
Cisco CUCM	5532	Syslog
Cisco ESA	5562	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Cisco ESA	5164 (deprecated)	Syslog
Cisco Firepower	5168	Traffic (srcip), Syslog (otherwise)
Cisco IKE	5176	Syslog
Cisco IronPort	5163	Syslog
Cisco ISE	5157	Syslog
Cisco MDS	5563	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Cisco Meraki	5172	Traffic (srcip), Syslog (otherwise)
Cisco Netflow	2055 (UDP only)	Traffic
Cisco routers and switches	5158	Syslog
Cisco UCS	5579	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Cisco Umbrella	5521	Syslog
Cisco VPN	5156	Syslog
Cisco WLC	5531	Syslog
Citrix Access Gateway	5688	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Citrix NetScaler	5166	Syslog
Citrix NetScaler (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Comodo- CIS CCS (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
CoreLight Sensor	5575	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
CoSoSys Endpoint Protection	5654	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Cribl / NXLog	5142	Windows Events
Cribl default (Syslog JSON)	5142	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
CrowdStrike (beats)	5044	Syslog
CrowdStrike (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
CyberArk PTA (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Cynet (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
D-Link	5189	Traffic (srcip), Syslog (otherwise)
DBSafer	5181	Syslog
Deep Instinct	5628	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Dell EMC Powerstore	5683	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Dell iDRAC	5566	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Dell Switch	5578	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
DHCP (beats)	5044	Traffic (srcmac), Syslog (otherwise)
DHCPD (IS DHCP)	5554	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
DNSVault RPZdb	5639	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Dragos (CEF)	5539	Traffic (srcip), Syslog (otherwise)
DrayTek Firewall	5593	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
eDictionary - eDictionary (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Egnyte (Syslog JSON)	5142	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Ericom ZTEdge	5603	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
ESET PROTECT	5655	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
ExtraHop (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Extreme AirDefense	5612	Traffic (srcip, srcport, dstip, dstport, and proto) Syslog (otherwise)
Extreme Controller	5666	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
ExtremeCloud IQ Site Engine	5614	Traffic (srcip, srcport, dstip, dstport, and proto) Syslog (otherwise)
F5 - ASM (CEF)	5143	ML IDS/Malware (threat, normalized from attack_type), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
F5 BIG-IP	5162	ML IDS/Malware (IDS signature), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
F5 BIG-IP Telemetry (HTTP JSON)	5200 (TCP only)	Syslog
F5 IPI	5536	ML IDS/Malware (dev_type: /threat/), Traffic (dstip), Syslog (otherwise)
F5 iRule	5536	ML IDS/Malware (dev_type: /threat/), Traffic (dstip), Syslog (otherwise)
F5 L7 DDOS	5536	ML IDS/Malware (dev_type: /threat/), Traffic (dstip), Syslog (otherwise)

Device	Port	Index
F5 Mitigation	5536	ML IDS/Malware (dev_type: /threat/), Traffic (dstip), Syslog (otherwise)
F5 NGINX	5151	Syslog
F5 Silverline	5536	ML IDS/Malware (dev_type: /threat/), Traffic (dstip), Syslog (otherwise)
F5 VPN	5187	Syslog
F5 WAF	5536	ML IDS/Malware (dev_type: /threat/), Traffic (dstip), Syslog (otherwise)
FatPipe Networks SD-WAN	5583	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
FluentD (HTTP JSON)	5200 (TCP only)	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Forcepoint	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Forcepoint - Firewall (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Forcepoint -DLP (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Forcepoint -Firewall (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Forcepoint Web Security (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
ForeScout	5154	Syslog
Fortinet FortiAnalyzer	5542	ML IDS/Malware (vendor.attack_name), Traffic (dstip), Syslog (otherwise)
Fortinet FortiAuthenticator	5671	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Fortinet Forticloud FortiClient EMS Cloud Endpoint Management Services	5682	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Fortinet FortiEDR	5661	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Fortinet FortiGate	5517	Traffic (action), Syslog (otherwise)

Device	Port	Index
Fortinet Fortigate (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Fortinet FortiMail	5616	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Fortinet FortiSandbox	5648	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Fortinet FortiWeb	5642	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
FutureSystems WeGuardia SSL plus (SSL VPN)	5651	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Graylog format	5569	Windows Events (winlogevent), ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Guardicore (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
HanDreamnet VIPM	5676	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Hewlett Packard UNIX	5585	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Hillstone	5514	ML IDS/Malware log_type: threat), Traffic (log_type: traffic),
HPE Switch	5595	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
IBM AS400	5632	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Impero ContentKeeper	5670	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Imperva - SecureSphere (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Incapsula SIEM Integration (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Indusface Web Application Firewall	5582	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Infoblox Data Connector (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Infoblox Network Identity OS (NIOS)	5587	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Infocyte HUNT (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
IPFIX	4739 (UDP only)	Traffic (srcip, srcport, dstip, dstport, and proto)
IronScales (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Jsonar Database Security Tool	5586	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Juniper SRX	5173	Traffic (srcip), Syslog (otherwise)
Juniper SSG	5516	Traffic (srcip), Syslog (otherwise)
Juniper Switch	5591	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
KasperskyLab (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Kemp Technologies Load Master LB	5695	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Keycloak	5653	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Lancope - StealthWatch (LEEF)	5522	Traffic (srcip), Syslog (otherwise)
LanScope Cat	5588	Syslog
Lepide	5607	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Linux Syslog	5555	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Logstash Suricata	5629	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Mailboarder Agent	5580	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Mako Networks firewall	5547	Traffic (dstip), Syslog (otherwise)
ManageEngine ADAudit Plus	5679	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
ManageEngine ADAuditPlus (CEF)	5143	Windows Events
McAfee (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
McAfee Advanced Threat Defense	5584	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
McAfee ePolicy Orchestrator	5533	Traffic (srcip), Syslog (otherwise)
McAfee Firewall	5169	Traffic (srcip), Syslog (otherwise)
McAfee Network Security	5527	Traffic (srcip), Syslog (otherwise)
MCAS SIEM Agent (CEF)	5143	Windows Events
Medigate	5631	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Menlo Security MS-XL50M	5630	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Microsoft IIS	5636	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Microsoft IIS (Syslog JSON)	5142	Syslog
Microsoft Office 365	5627	Windows Events
Microsoft Windows Event	5646	Windows Events (winlogevent), Syslog (otherwise)
Microsoft Windows via Graylog	5569	Windows Events (winlogevent)
MicroWorld eScan	5645	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
MikroTik firewall and router	5553	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
MONITORAPP AI WAF 4.1	5613	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
MONITORAPP WAF 1.0	5535	Traffic (srcip), Syslog (otherwise)
Nasuni	5592	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
NetApp	5608	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Netfilter	5544	Traffic (dstip), Syslog (otherwise)
NetIQ - Identity Manager (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
NetIQ Access Manager	5167	Syslog
NetIQ SSO	5171	Syslog
Netman Smart NAC	5650	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
NetMotion	5641	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
NXLog	5601	Windows Events (winlogevent), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
OneLogin	5581	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Open LDAP	5164	Syslog
OpenCanary	5638	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
OpenShift	5573	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
OpenVPN	5643	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
OPNsense	5660	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Oracle DB	5170	Traffic (srcip), Syslog (otherwise)
Oracle Solaris	5664	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Ordr Connected Device Security	5622	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
PacketFence	5686	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Palo Alto Networks - Next Generation Firewall (LEEF)	5522	Traffic (srcip), Syslog (otherwise)
Palo Alto Networks - Traps Agent (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Palo Alto Networks firewall	5515	Traffic (type: traffic), ML IDS/Malware (type: threat), Syslog (otherwise)
Palo Alto Networks Firewall via Graylog	5569	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Penta Security WAPPLES WAF	5560	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Peplink XDR	5665	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Perception Point X-Ray	5667	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
pfSense Firewall	5543	Syslog
PIOLINK WEBFRONT-K	5617	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
PrintChaser	5179	Syslog
Privacy-i	5178	Syslog
Proofpoint	5596	Syslog
Pulse Secure	5534	Syslog
Radware DefensePro	5619	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Rapid7	5153	Syslog
RazLeeSecurity - Audit (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
RSA Authentication Manager	5184	Syslog

Device	Port	Index
Ruckus ZoneDirector	5662	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
RuiJie Switch	5689	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SafePC	5180	Syslog
Sangfor NGAF	5637	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SECUI Firewall	5561	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SECUI MF2 Firewall	5570	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SECUI MFD	5611	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Secureki APPM 6	5693	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Security Strategy Research (SSR) Metieye	5572	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Secuway SSLVPN	5652	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SentinelOne (CEF2)	5175	Traffic (srcip), Syslog (otherwise)
SentinelOne Mgmt (CEF)	5143	ML IDS/Malware (threat, normalized from classification), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SentinelOne Security Center (CEF)	5143	ML IDS/Malware (threat, normalized from classification), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SentinelOne Singularity Mobile	5623	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
ServiceNow Now Platform	5668	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
ShareTech Firewall	5609	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Snare Agent	5590	Windows Events (winlogevent), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Sniper IPS	5182	Traffic (srcip), Syslog (otherwise)
SonicWall - NSA 2400 (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SonicWall (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
SonicWall Firewall	5152	ML IDS/Malware (IDS signature), Traffic (srcip), Syslog (otherwise)
SonicWall VPN	5556	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Sophos (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Sophos (JSON)	5530	Traffic (endpoint_type: traffic), ML IDS/ Malware (endpoint_type: threat), Syslog (endpoint_type: computer)
Sophos endpoint	5565	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Sophos endpoint (beats)	5044	Traffic (srcip), Syslog (otherwise)
Sophos firewall	5520	Data goes to the indicated index based on the log_type:
Sophos Web Appliance	5626	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Splunk Heavy Forwarder	5188	Syslog
Stormshield Net Security Firewall	5625	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Symantec (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Symantec Endpoint Protection	5525	Traffic (dstip), Syslog (otherwise)
Symantec Firewall	5155	Syslog
Symantec Messaging Gateway	5567	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Synology Directory Server	5597	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Thales Group CipherTrust Manager	5674	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Trellix FireEye HX	5644	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Trend Micro - Deep Security Agent (LEEF)	5522	Traffic (srcip), Syslog (otherwise)
Trend Micro (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Trend Micro Apex Central (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Trend Micro Interscan Messaging	5678	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Trend Micro Proxy	5540	Traffic (dstip), Syslog (otherwise)
Trend Micro TippingPoint Intrusion Prevention System (IPS)	5672	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Tripwire Enterprise	5186	Syslog
Ubiquiti	5552	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Unix	5633	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Untangle Firewall (Syslog JSON)	5142	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Varonis DatAdvantage (CEF)	5143	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Versa Networks Firewall	5568	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
VMware - Carbon Black (LEEF)	5522	Traffic (srcip), Syslog (otherwise)
VMware ESXi	5600	Syslog
VMWare Horizon	5687	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
VMware NSX-T Data Center	5574	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
VMware UAG	5620	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
VMware Vcenter	5615	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
VMWare VeloCloud SD-WAN	5685	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
WatchGuard - XTM (LEEF)	5522	Traffic (srcip), Syslog (otherwise)
WatchGuard firewall security appliance	5557	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Wazuh	5634	Windows Events (winlogevent) , Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Windows DNS Server	5599	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Windows Event NXLog	5601	Windows Events (winlogevent), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Windows System Security	5610	Windows Events (winlogevent), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Wins IPS ONE-1 / Wins DDX	5538	ML IDS/Malware (vendor.attack_name), Syslog (otherwise)
WINS Sniper NGFW	5649	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Zix Mail	5185	Traffic (srcip), Syslog (otherwise)
Zscaler NSSWeblog (CEF)	5143	Syslog
Zscaler ZIA Firewall	5549	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Zscaler ZIA Web	5550	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

Device	Port	Index
Zscaler ZPA	5551	ML IDS/Malware (threat), Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)
Zyxel Firewall	5594	Traffic (srcip, srcport, dstip, dstport, and proto), Syslog (otherwise)

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