Contents

Cylance Endpoint Security service updates................................................................. 4

Management console and platform services.............................................................. 5
  Management console and platform services fixed issues........................................... 9
  Management console and platform services known issues.................................... 9

CylancePROTECT Desktop release notes............................................................... 11
  What's new in the CylancePROTECT Desktop agent for Windows.......................... 12
    Fixed issues in the Windows agent................................................................. 15
    Known issues in the Windows agent............................................................. 18
  What's new in the CylancePROTECT Desktop agent for Linux.............................. 19
    Fixed issues in the Linux agent................................................................. 22
    Known issues in the Linux agent............................................................. 23
  What's new in the CylancePROTECT Desktop agent for macOS............................ 23
    Fixed issues in the macOS agent............................................................... 24
    Known issues in the macOS agent........................................................... 25

CylancePROTECT Mobile release notes.............................................................. 26
  CylancePROTECT Mobile fixed issues................................................................. 27
  CylancePROTECT Mobile known issues............................................................. 29

CylanceOPTICS release notes............................................................................. 31
  CylanceOPTICS fixed issues.............................................................................. 34
  CylanceOPTICS known issues........................................................................ 36

CylanceGATEWAY release notes........................................................................... 38
  CylanceGATEWAY fixed issues.......................................................................... 42
  CylanceGATEWAY known issues.................................................................... 42

CylanceAVERT release notes................................................................................... 47
  CylanceAVERT fixed issues.............................................................................. 48
  CylanceAVERT known issues........................................................................ 49

Legal notice............................................................................................................ 51
Cylance Endpoint Security service updates

The latest releases of the Cylance Endpoint Security services are listed in the following table. For information about previous releases, refer to KB89592.

<table>
<thead>
<tr>
<th>Product</th>
<th>Latest release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management console and platform services</td>
<td>July 2023</td>
</tr>
<tr>
<td>CylancePROTECT Desktop</td>
<td>May 2023</td>
</tr>
<tr>
<td>CylancePROTECT Mobile</td>
<td>May 2023</td>
</tr>
<tr>
<td>CylanceOPTICS</td>
<td>April 2023</td>
</tr>
<tr>
<td>CylanceGATEWAY</td>
<td>July 2023</td>
</tr>
<tr>
<td>CylanceAVERT</td>
<td>April 2023</td>
</tr>
</tbody>
</table>
Management console and platform services

This section contains information about updates to the management console and platform services that impact more than one Cylance Endpoint Security service or the general experience of the console. Console changes that impact specific Cylance Endpoint Security services are described in the respective sections of this guide.

What's new in the management console

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date added</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts view enhancements</td>
<td>For CylanceGATEWAY threat alerts, the Alerts view now supports alerts that are based on the network protection settings that you set. Detections such as IP Reputation, Zero-Day, Signature, and DNS Tunneling alerts might be generated and displayed in the Alerts view. This provides a comprehensive way to review the alerts that are detected by CylanceGATEWAY and makes it easier for you to identify and track threats in your environment and resolve collections of alerts more efficiently. The priority for the alerts is determined by your Network Protection settings. For more information, see Managing aggregated alerts in the Cylance Endpoint Security Administration content.</td>
<td>July 2023</td>
</tr>
<tr>
<td>Tenant identifier</td>
<td>You can now specify whether the tenant ID, name or both should appear in the SIEM solution or syslog server. This value allows you to easily identify the source tenant in a multiple tenant environment. For more information, see &quot;Configure Cylance Endpoint Security to send events to a SIEM solution or syslog server&quot; in the Syslog content.</td>
<td>June 2023</td>
</tr>
<tr>
<td>Syslog enhancements</td>
<td>The syslog message delivery is now using an updated platform for message delivery. The updated platform will provide improved stability and a basis for future enhancements. To ensure uninterrupted delivery of syslog messages to your SIEM solution or syslog server, you must configure them to allow connections from new source IP addresses. For more information, see Source IP addresses for a SIEM solution or syslog server messages.</td>
<td>May 2023</td>
</tr>
<tr>
<td>Notifications for disabled services</td>
<td>You can now view your notifications for expiring and disabled services in the management console. A notification prompt for new and non-dismissed notifications will display upon login and a message banner will be shown at the top of the console if there are any expiring services. You can view all of your notifications in the new Notifications tab located in the bottom-left corner of the console.</td>
<td>May 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date added</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Configure console session timeout</td>
<td>You can specify how long an administrator can remain logged in to the management console before they are signed out, even if the session is active. For more information, see Configure the session timeout limit in the Cylance Endpoint Security Setup content.</td>
<td>May 2023</td>
</tr>
<tr>
<td>Alerts view changes</td>
<td>• CylancePROTECT Desktop threat alerts displayed in Protection &gt; Threats with an Unsafe, Abnormal, or Quarantined status now have a New status in the Alerts view. Alerts displayed in Protection &gt; Threats with a Waived status now have a Closed status in the Alerts view. • The Detection Detail link that allows you to access more information and actions for an individual alert in other areas of the console will now remain active for 60 days for CylancePROTECT Desktop threat alerts and for 30 days for other types of alerts. For more information, see View and manage aggregated alerts in the Cylance Endpoint Security Administration content.</td>
<td>March-April 2023</td>
</tr>
<tr>
<td>Update client credentials for Microsoft Azure Directory Connections</td>
<td>You can now update the client secret or add both a new client ID and client secret after you have set up a directory connection to Microsoft Azure Active Directory. For more information, see Update the Microsoft Azure Active Directory connection credentials in the Cylance Endpoint Security Setup content.</td>
<td>March 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date added</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| Alerts view             | The new alerts view gives you a comprehensive way to review the alerts that are detected and correlated across Cylance Endpoint Security services, making it easier for you to identify and track prevailing threat patterns in your corporate ecosystem and resolve collections of alerts more efficiently. The correlation of alerts across services offers a more complete view of potential threats and contributes to a more holistic approach to protecting your organization's employees and data.  
  **Note:** To view and use the new alerts view, you currently must have an entitlement for CylancePROTECT Desktop or CylanceOPTICS. Future updates will extend the Alerts view to customers with entitlements for other Cylance Endpoint Security services.  
  The initial release of the alerts view supports alerts from the CylanceOPTICS agent on desktop devices and threat alerts from CylancePROTECT Desktop devices. Future updates will add support for alerts from additional Cylance Endpoint Security services.  
  For more information, see Managing aggregated alerts in the Cylance Endpoint Security Administration content. | Feb 2023   |
| Evaluate the risk level of a file | You can use the management console to evaluate the risk level of a file, as analyzed and determined by the CylancePROTECT cloud services. This feature gives you insight into how the CylancePROTECT Desktop agent would classify a file that it identifies on a device.  
  For more information, see Evaluate the risk of a file in the Cylance Endpoint Security Administration content. | Feb 2023   |
| Share dashboards        | You can now share dashboards that you create in the management console with other administrators.  
  For more information, see Share a dashboard in the Cylance Endpoint Security Administration content. | Feb 2023   |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date added</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator controls for discovery of devices not protected by CylancePROTECT Desktop</td>
<td>Previously, the discovery of devices not protected by CylancePROTECT Desktop was enabled and you did not have the option to disable it. In this release, the management console now includes the option to enable or disable this feature. If you enable the feature, you can discover unprotected devices in your environment for your Microsoft Azure Active Directory, Microsoft Active Directory, and LDAP directory connections. When the feature is enabled, all of the known devices that are not protected by CylancePROTECT Desktop are displayed on the Assets &gt; Unprotected Devices page. Enabling or disabling this feature applies to all of the directory connections that you have connected to Cylance Endpoint Security. For more information, see Discover unprotected devices in the Cylance Endpoint Security Administration content.</td>
<td>Jan 2023</td>
</tr>
<tr>
<td>Default authentication</td>
<td>To enhance security, the default authenticator for all apps and services except the Cylance console, CylanceGATEWAY agent, and CylancePROTECT Mobile app has been changed from Enterprise password to Deny authentication. Users that do not have an authentication policy assigned to them are presented with an error message when they try to access apps or services and cannot sign in.</td>
<td>Dec 2022</td>
</tr>
<tr>
<td>FIDO authenticator</td>
<td>You can now add FIDO as an authenticator in authentication policies. Users can register one or more FIDO2 devices during sign in and use them to verify their identity.</td>
<td>Dec 2022</td>
</tr>
<tr>
<td>Identify devices not protected by CylancePROTECT Desktop</td>
<td>The new Unprotected Devices page (Assets &gt; Unprotected Devices) displays a list of known devices that are not protected by CylancePROTECT Desktop. Administrators can export the device list and take action to protect those devices and their network from potential threats. This feature requires BlackBerry Connectivity Node 2.12.1 or later. For more information, see Discover unprotected devices in the Cylance Endpoint Security Administration content.</td>
<td>Oct 2022</td>
</tr>
<tr>
<td>BlackBerry Connectivity Node enhancements</td>
<td>The BlackBerry Connectivity Node now supports identifying devices that are not protected by CylancePROTECT Desktop.</td>
<td>Oct 2022</td>
</tr>
</tbody>
</table>
### Feature

**New SAML and Deny authenticators and skip OTP option**

Cylance Endpoint Security now supports integration with third-party IDPs that support SAML (Azure, Okta, Ping Identity) for use in authentication policies. Administrators can migrate existing SAML configurations from Custom Authentication settings to the new Enhanced Authentication framework.

A new a “Deny” authenticator can be added to authentication policies to explicitly deny authentication to a product or service. During authentication, if the Deny Authenticator is found, authentication will be rejected for the user and an error message is presented.

Administrators can allow users to skip OTP setup for a specified number of times without losing access to the console. Any existing polices that include the one-time password authenticator will automatically use the default setting of zero skips allowed.

For more information, see [Add an authenticator](https://support.cylance.com) in the Cylance Endpoint Security Setup content.

**Date added**: August 2022

---

### BlackBerry Connectivity Node version

BlackBerry Connectivity Node version 2.12.1 (bundle 28.11.0). To download the latest version of the BlackBerry Connectivity Node, click [here](https://www.blackberry.com).

---

### Management console and platform services fixed issues

#### Azure Active Directory Synchronization

You could not authenticate users synchronized from Azure Active Directory if the user’s email address and UPN did not match. (EID-16967)

#### Authentication

If the maximum session age specified in a client was less than the default setting used by Okta, users that completed Okta authentication were not prompted to reauthenticate until the session age set in Okta was reached. This was due to a known Okta issue. (EID-17965)

#### BlackBerry Connectivity Node

BlackBerry Router and proxy settings displayed in the BlackBerry Connectivity Node were not applicable to CylanceGATEWAY. (UES-6396)

---

### Management console and platform services known issues

---

### Management console
In Google Chrome version 105.0.5195.102 and later, the "Block third-party cookies" option is enabled by default for incognito mode. If you try to log in to the management console while this option is enabled, you may receive a "Sign-in failed" error. (UES-9770)

**Workaround:** Change your Chrome privacy and security settings to allow all cookies, or in the browser settings add [*.]cylance.com as a site that can always use cookies.

**Dashboards**

The management console user details (Assets > Users) does not display the TLS version in the CylanceGATEWAY event details screen when the CylanceGATEWAY agent is installed and activated. For more information, visit support.blackberry.com to read article 99220. (BIG-6300)

The management console unprotected devices screen (Assets > Unprotected devices) displays devices that do not have the BlackBerry Protect Desktop agent installed. After a device has the BlackBerry Protect Desktop agent installed and is flagged as protected, the device is no longer displayed on the screen. If a user then uninstalls the BlackBerry Protect Desktop agent, the device is not displayed again on the unprotected devices screen. (UES-213)

The management console unprotected devices screen (Assets > Unprotected devices) occasionally may display incorrect device OS and OS versions. For example,

- On Mac devices, supported OS and OS versions may display as unknown and unsupported, respectively. (UES-9904)
- On Windows devices, unsupported OS versions (for example, Windows Server 2008 and Windows 8) may display as supported. (UES-9903)

For information about the operating systems that each of BlackBerry Protect Desktop agents supports, see the Cylance Endpoint Security compatibility matrix.

The management console unprotected devices screen (Assets > Unprotected devices) incorrectly displays devices running Windows 10 Enterprise Insider Preview as Linux (UES-9897)

The management console unprotected devices screen (Assets > Unprotected devices) does not display the device OS and OS version and results in 'insufficient information' to be displayed for the devices. (UES-9574)

**Workaround:** Configure the schema to allow the required attributes to synchronize from the domain controller to the Global Catalog. For instructions, see Configure your environment to view the device OS and OS version of managed unprotected devices in the administration content.

**BlackBerry Connectivity Node**

The BlackBerry Connectivity Node is not compatible with OpenJDK292b10 or ZuluJDK292b10. (UES-3667)

CylancePROTECT Desktop release notes

The following tables provide information about the new features of CylancePROTECT Desktop in the management console. For the agents, information is available in their separate sections:

- Windows agent
- Linux agent
- macOS agent

What's new in the management console for CylancePROTECT Desktop (May 2023)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| DLL exclusions for memory protection (Windows only) | In the device policy, you can now add memory protection exclusions for third-party application DLLs. For example, if you are running third-party security products in addition to CylancePROTECT, you can add an exclusion for the appropriate .dll files so that CylancePROTECT ignores specific violations for those products. This feature supports the Malicious Payload and System DLL Overwrite violation types only. The following rules apply when you specify a DLL exclusion:  
- You must select the **Treat as DLL exclusion** option in the device policy.  
- The device must be running CylancePROTECT Desktop agent version 3.1.1001 or later on a Windows device.  
- The exclusion file path that you specify must be the full, direct path to the .dll file. Wildcards are not allowed.  
- The .dll file must be signed using a certificate that is trusted on the device where CylancePROTECT Desktop is installed. Otherwise, it will not be excluded. |

What's new in the management console for CylancePROTECT Desktop (January 2023)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Script control setting for XLM macros in the device policy (Preview) | Administrators can now configure a script control setting in the device policy for protection against XLM macros. When a macro is executed, the agent responds to the Microsoft anti-malware scanning interface according to the device policy. This feature requires the following:  
- Microsoft Windows 10 or later  
- CylancePROTECT Desktop agent version 3.1  
- VBA macros must be disabled in the Excel **File > Trust Center > Excel Trust Center > Macro Settings** menu. **Note:** This feature is currently available in Preview mode where it might behave unexpectedly. |
What's new in the management console for CylancePROTECT Desktop (November 2022)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-update Linux Driver</td>
<td>The CylancePROTECT Desktop agent 3.1.1000 for Linux devices can now request an update to the latest supported driver when an updated kernel is detected on the system. For example, if the Linux kernel is updated and the current installed driver does not support it, the agent can now automatically update the driver as soon as a compatible driver is released. This feature requires CylancePROTECT Desktop agent version 3.1.1000 and the agent driver version 3.1.1000 or later. To enable this feature, select the Auto-update Linux Driver option in the zone-based update rule from the Settings &gt; Update menu in the management console.</td>
</tr>
</tbody>
</table>

What's new in the management console for CylancePROTECT Desktop (October 2022)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom interval for background threat detection scanning</td>
<td>Administrators can now set a custom interval to run background threat detection scanning from the device policy. The date of the last scan for each device is logged in the management console. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. Note that increasing the frequency of the scans may impact the device performance. You can also start the scan manually from the command line. This feature requires CylancePROTECT Desktop agent 3.1.1000 or later.</td>
</tr>
</tbody>
</table>

What's new in the CylancePROTECT Desktop agent for Windows

What's new in Windows agent version 3.1.1001

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script control improvements</td>
<td>The CylancePROTECT Desktop agent now reports parent and interpreter processes to the Cylance console when a potentially malicious script is executed. Administrators can add exclusions for either a parent process or interpreter process of a script to allow the script to run on a device.</td>
</tr>
</tbody>
</table>
### DLL exclusions for memory protection

The CylancePROTECT Desktop agent for Windows now supports the ability to add exclusions for third-party application DLLs. For example, if you are running third-party security products in addition to CylancePROTECT, you can add an exclusion for the appropriate .dll files so that CylancePROTECT ignores specific violations for those products.

This feature supports the Malicious Payload and System DLL Overwrite violation types only.

The following rules apply when you specify a DLL exclusion:

- You must select the **Treat as DLL exclusion** option in the device policy.
- The device must be running CylancePROTECT Desktop agent version 3.1.1001 or later on a Windows device.
- The file path that you specify must be the full, direct path to the .dll file. Wildcards are not allowed.
- The .dll file must be signed using a certificate that is trusted on the device where CylancePROTECT Desktop is installed. Otherwise, it will not be excluded.

### Improvements to memory protection sensor for malicious payloads

The memory protection sensor for the malicious payload violation type has been improved to help improve accuracy of violation reporting and reduce unnecessary alerts.

### What's new in Windows agent version 3.1.1000

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Execution protection for XLM/XL4 Excel Macros (Preview) | The CylancePROTECT Desktop agent now works with Microsoft's anti-malware scan interface (AMSI) so that when a potentially dangerous XLM macro is executed, threat information is reported to the management console, and the agent responds to the interface according to the device policy rules for script control events. For example, the agent responds whether to allow the macro to run or block it from running. This feature is enabled from the Script Control > XLM Macros settings in the device policy. This feature requires the following:

- Microsoft Windows 10 or later
- CylancePROTECT Desktop agent version 3.1
- VBA macros must be disabled in the Excel **File > Trust Center > Excel Trust Center > Macro Settings** menu. **Note:** This feature is currently available in Preview mode where it might behave unexpectedly. |
### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Antimalware Protected Process Light (AM-PPL)</td>
<td>The CylancePROTECT Desktop agent now runs as a trusted service using Antimalware Protected Process Light (AM-PPL) technology from Microsoft, which protects the agent’s security processes from malicious actions. For example, it helps protect the agent from being terminated. This feature requires the endpoint to be running Windows 10 1709 or later or Windows Server 2019 or later.</td>
</tr>
<tr>
<td>Custom interval for background threat detection scanning</td>
<td>Administrators can now set a custom interval to run background threat detection scanning from the device policy. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. Note that increasing the frequency of the scans might impact the device performance. The scan may also be manually started from the command line. The date of the last scan for each device is logged in the management console.</td>
</tr>
<tr>
<td>Manually start background threat detection scanning</td>
<td>On Windows devices, you can now manually start background threat detection scanning from the command line using the \texttt{backgroundscan} command option. For example, you can run the following command: \texttt{C:\Program Files\Cylance\Desktop\CylanceSvc.exe /backgroundscan}</td>
</tr>
</tbody>
</table>
| Windows OS support                                | • Added support for Windows 365 (Business, Enterprise)  
• Added support for Windows 10 (22H2)  
• Removed support for Windows 10 (2004) |

**What's new in Windows agent version 3.0.1005**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSASS Read violations reporting</td>
<td>LSASS Read violations that are blocked are now reported to the management console.</td>
</tr>
</tbody>
</table>

**Note:** Due to compatibility issues, tenants that have CylanceOPTICS 3.2 for Windows available will not have CylancePROTECT Desktop agent version 3.0.1005 for Windows provisioned to them. The compatibility issues will be resolved in an upcoming release. All other versions of CylanceOPTICS support CylancePROTECT Desktop agent version 3.0.1005 for Windows.

**What's new in Windows agent version 3.0.1000**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LSASS Read violations detection</td>
<td>Detection of LSASS Read violations has been improved in the Windows agent 3.0.1000.</td>
</tr>
<tr>
<td>Exclusions for macro files</td>
<td>For Windows devices running agent 3.0.1000, administrators can now add exclusions in the Memory Protection device policy for macro files that cause Script Control events.</td>
</tr>
<tr>
<td>Read-only access to USB devices</td>
<td>For Windows devices running agent 3.0.1000, administrators can now allow read-only access to external USB devices on Windows devices.</td>
</tr>
<tr>
<td>Detection disabled for embedded VBScripts</td>
<td>Detection of embedded VBScript script control violations is disabled in Windows agent 3.0.1000.</td>
</tr>
</tbody>
</table>

**What's new in Windows agent version 2.1.1584**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory protection enhancements</td>
<td>• Memory Protection now uses a new code base and methodology that generates more events.</td>
</tr>
<tr>
<td></td>
<td>• The Dangerous VBA Macro event (RunMacroScript) is now a memory protection event, not a script control event. This event prevents dangerous implementations within a macro. This event is not related to running scripts.</td>
</tr>
</tbody>
</table>

**What's new in Windows agent version 2.1.1568**

Bug fixes only.

**Note:** The CylancePROTECT Desktop 1568 agent for Windows is the last release that supports endpoints running the Windows XP, Windows Server 2003, and Windows Server 2008 (non-R2) operating systems. The Cylance SHA1 certificate that the agent requires to support these endpoints is due to expire in November 2023. After November 2023, any endpoints that are running this version of the agent may not behave as expected. For endpoints that are running a later version of Windows, you must install a later version of the CylancePROTECT Desktop agent. For more information about CylancePROTECT Desktop support for legacy operating systems, visit support.blackberry.com and read KB 66653.

**Fixed issues in the Windows agent**

**Fixed in Windows agent version 3.1.1001**

When a device could not connect to the Cylance management console, the log line that was associated with the event was only available when verbose logging was enabled. (EPP-3311)
If you installed a version of CylancePROTECT Desktop using a unified installer (version 2.4.x), you were prevented from upgrading the CylancePROTECT Desktop agent individually. You can now upgrade to CylancePROTECT Desktop agent 3.1.1001.17 using the online updater. (EPP-3300)

For more information, visit support.blackberry.com/community to read KB 102884.

When a device connection timed out, the log line that was associated with the event was only available when verbose logging was enabled. (EPP-3294)

Devices that are on networks with higher latency could not connect to Cylance Cloud services. (EPP-3292)

When you opened Microsoft Excel documents through an Outlook attachment or OneNote tab, `OfficeClickToRun.exe` was blocked by the memory protection policy. (EPP-1951)

The `taskkill.exe` process intermittently stopped responding while killing a process. (EUS-1274)

When a memory protection exclusion for Dangerous VBA macros was added for a `.xlsm` file, if file name contained Japanese characters, the file was not excluded properly and was blocked from running. (EUS-1090)

Fixed in Windows agent version 3.1.1000

When Smart App Control was enabled on Windows 11 devices, the installation of the CylancePROTECT Desktop agent 3.1 was not successful if you used the `.exe` installer. (EPP-3194)

When a memory protection violation occurred, there was a delay before the system reported the event to the management console. (CHP-8615)

When some applications caused a memory protection violation, the applications stopped responding due to a "Security check failure or stack buffer overrun" error. (EUS-991)

Microsoft Excel stopped responding due to stack overflow errors when attempting to run a macro with VBA hooking functions. (EUS-664)

When VSTO add-ins are configured in Microsoft Excel, it stopped responding when you opened a file that included various macros even though exclusions were properly set. (EUS-637)

When accessing an ASP-based website that uses an embedded VBScript, the website throws a 500 error on the first attempt to access the site. This error appears if the device is assigned a policy with the Active Script script control setting enabled. (EUS-555)

The memory protection exclusion list did not take effect properly when folders were named using uppercase letters of the Zenkaku Hiragana input method. (EUS-937)

Fixed in Windows agent version 3.0.1005

When “Block PowerShell Console Usage” was selected in the script control policy, and a script that used the `Write-Error` cmdlet was added to the exclusion list (i.e. approved), the script was interrupted when it used the cmdlet. The script can now run as expected without being interrupted by the agent when the cmdlet is used. (EUS-508)
If the CylancePROTECT Desktop agent version 3.0 with memory protection enabled was running on a user’s 64-bit Windows OS, and the user started a 32-bit version of Microsoft Outlook, Outlook closed immediately. (EUS-440)

When a user tried to execute a program file from a network share while the CylancePROTECT Desktop agent version 3.0 was monitoring, Windows might have displayed a blue screen with the following error: "Your PC ran into a problem and needs to restart, Stop code: SYSTEM_SERVICE_EXCEPTION, What failed: CylanceDrv64.sys" (EUS-437)

When memory protection was enabled, redundant information was written to temporary files. The redundant information has been reduced and fewer temporary files are created. (EUS-294)

**Fixed in Windows agent version 3.0.1000**

The CylancePROTECT service did not start on devices that have installed the Arabic version of Windows. (CHP-8512)

When you opened the Windows agent on a Windows 10 device, some options were disabled when you right-clicked a threat in the Threats tab. In Online Mode, the "Show File Properties" option was disabled. In Disconnected Mode, "Show File Properties", "Quarantine File", and "Waive File" options were disabled. (CHP-8357)

The timestamps of events that the agent reported were slightly offset if the device time zone was set to UTC +0100. (CHP-8351)

**Fixed in Windows agent version 2.1.1584**

Microsoft SQL Server 2008 R2 stopped responding on startup. (MEM-847)

Fixed an issue with WideOrbit servers and CylancePROTECT Desktop script control. (MEM-846, MEM-844)

Fixed an issue with Microsoft Dynamics and CylancePROTECT Desktop script control. (MEM-845)

An error occurred when launching VisionApp Remote Desktop 2011 with script control enabled. (MEM-830)

Resolved an issue with LSASS Read for memory protection. (MEM-662)

The 1580 agent did not properly log an action taken for the Remote APC Scheduled violation. (CHP-8534)

**Fixed in Windows agent version 2.1.1568**

When a remote procedure call (RPC) message was larger than 64K and the agent allocated memory, the memory allocation size couldn't be modified. (EPP-1504)

An arbitrary message could have been broadcasted to an Advanced Local Procedure Call (ALPC) port. (EPP-1503)
A user with insufficient privileges could have deleted files in the Cylance directory when using a remote procedure call (RPC) and the Chromium Embedded Framework (CEF) was loaded using a third-party app. (EPP-1236)

A system bugcheck may occur when formatting some Unicode strings for logging. (CHP-8610)

### Known issues in the Windows agent

* On some devices running Windows Server 2012 R2, rundll32.exe stops responding after a memory protection violation. (EUS-1267)

On a device running Windows Server 2012 R2 and CylancePROTECT Desktop agent 2.1.1580 and later, System32\wbem\WmiPrvSE.exe is incorrectly reported as a threat. (EUS-179, EPP-3279)

Each time an executable that’s in the exclusion list is run on a device, there are multiple redundant 'UNKNOWN_FILE' log entries associated with it. If the executable is used frequently, the log file size can grow quickly. (EPP-2828)

The script control policy for XLM macros is not enforced if the Excel Trust Center > Macros Settings is set to "Enable VBA macros". (EUS-1065)

**Workaround:** Verify that one of the "Disable VBA macros" is selected.

If you plug in a UGREEN USB-C hub on a device that's running the CylancePROTECT Desktop agent with a device control policy, a blue screen error occurs. (EUS-934)

When the Windows 8.3 short naming format of a process path is used to execute a file (e.g. C:\PROGRA~1\folder\file.exe) and the memory protection exclusions are defined using the long naming format for that process (e.g. C:\Program Files\folder\file.exe), the exclusions do not apply. (EUS-593)

**Workaround:** Ensure that files are executed using the long path format. Note that adding exclusions using the Windows 8.3 short naming format is not supported.

When trying to launch Microsoft Visual Studio 2022, several System DLL Overwrite violations are reported and it is not launching as expected. (EPP-2312)

**Workaround:** In the device policy, add an exclusion to ignore "System DLL Overwrite" violations for devenv.exe that is located in the installation folder of Visual Studio 2022. For example, set the exclusion to ignore "System DLL Overwrite" violations at \Program Files\Microsoft Visual Studio \2022\Professional\Common7\IDE\devenv.exe. The installation path may differ between editions and locales.

If you assign a device policy with script control set to "Block" but allow PowerShell console usage, scripts run from the PowerShell console are blocked. (CHP-8409)

On the Script tab of the Windows agent, the command line display in the tooltip for a long PowerShell script shows duplicated and overwritten information. (CHP-8349)

In some Windows 10 environments, when attempting to upgrade to the 1580 agent, the automatic uninstallation of the previous agent might not be successful. (CHP-8288)

**Workaround:** Manually uninstall the previous agent and install the 1580 agent.
If the following conditions are met, 32-bit processes that do not have Program Control Flow Guard (CFG) enabled can stop responding:

- Windows Defender is enabled, and the System Control flow guard (CFG) setting is set to on under System Settings (Start menu > Windows Security > App & browser control > Exploit protection settings > System settings).
- CylancePROTECT agent 1580 is installed.
- Memory Protection is enabled.

(CHP-8262)

**Workaround:**

1. Go to **Start > Windows Security > App & browser control > Exploit protection settings > Program settings**.
2. Select the program that stopped responding and click **Edit**.
3. Scroll to Control Flow Guard (CFG) for the program and select the **Override system settings** checkbox.
4. Toggle the setting below the checkbox to **On**.
5. Click **Apply**.
6. Restart your computer.

The Cylance service may intermittently get stuck in a "StopPending" state when cycling between a stopped and running state. (CHP-7174)

When "System DLL Overwrite" is enabled in the memory protection policy, using AutoCad 2022 (S.51.0.0) and trying to log in to an AutoCad account triggers a memory protection event. (COM-3896)

**Workaround:** Add a memory protection exclusion for AutoCad for the System DLL Overwrite violation type.

---

**What's new in the CylancePROTECT Desktop agent for Linux**

**What's new in the Linux agent version 3.1.1001**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Added support for Linux distributions | Added support for the following Linux distributions:  
- Red Hat Enterprise Linux 9 and 9.1  
- Oracle 9 and 9.1  
- Oracle UEK 9 and 9.1  
- Oracle 8.7  
- Oracle UEK 8.7  
- SUSE (SLES) 15 SP4 |
| Updated Linux driver package | The Linux driver package version 3.1.1101 is now available from the management console and is compatible with agent version 2.1.1590 and later. If you are using the Auto-update Linux Driver feature, the agent drivers will be updated automatically to version 3.1.1101.  
The Auto-update Linux Driver feature requires CylancePROTECT Desktop agent version 3.1.1000 and the agent driver version 3.1.1000 or later. |
What's new in the Linux agent version 3.1.1000

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added support for Linux distributions</td>
<td>Added support for the following Linux distributions: Ubuntu 22.04 LTS</td>
</tr>
<tr>
<td>Custom interval for background threat detection scanning</td>
<td>Administrators can now set a custom interval to run background threat detection scanning from the device policy. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. Note that increasing the frequency of the scans may impact the device performance. The scan may also be manually started from the command line. The date of the last scan for each device is logged in the management console.</td>
</tr>
<tr>
<td>Auto-update Linux Driver</td>
<td>The CylancePROTECT Desktop agent 3.1.1000 for Linux devices can now request an update to the latest supported agent driver when an updated kernel is detected on the system. For example, if the Linux kernel is updated and the current installed agent driver does not support it, the agent can now automatically update the driver as soon as a compatible driver is released. This feature requires CylancePROTECT Desktop agent version 3.1.1000 and the agent driver version 3.1.1000 or later. To enable this feature, select the Auto-update Linux Driver option in the zone-based update rule from the Settings &gt; Update menu in the management console.</td>
</tr>
</tbody>
</table>

What's new in the Linux driver version 3.1.1100

The CylancePROTECT 3.1.1100 driver package is now available for Linux endpoints, in advance of an upcoming release of the 3.1 agent. It includes the latest drivers to support the latest OS kernels and is compatible with devices running agent version 2.1.1590 or later. When the driver is used together with the upcoming release of the 3.1 agent, administrators can allow the Linux driver to be automatically updated to support the latest OS kernels. Updating to the latest Linux driver makes sure that CylancePROTECT continues to run as expected while you receive important OS kernel updates.

What's new in the Linux agent version 3.0.1005

Bug fixes only.

If you installed the CylancePROTECT 3.0.1101 or 3.0.1100 driver package for Linux endpoints running the 3.0.1001, 3.0.1000, or 2.1.1590 agents, the drivers are not automatically updated to 3.0.1105 (which includes bug fixes) when the 3.0.1005 agent is deployed from the console or upgraded locally. To update the drivers on endpoints that have the 3.0.1101 or 3.0.1100 driver package installed, manually upgrade to the 3.0.1105 driver package that is available in the Cylance Endpoint Security management console.

What's new in the Linux agent version 3.0.1001

Bug fixes only.
If you installed the CylancePROTECT 3.0.1100 driver package for Linux endpoints running the 3.0.1000, or 2.1.1590 agents, the drivers are not automatically updated to 3.0.1101 (which includes bug fixes) when the 3.0.1001 agent is deployed from the console or upgraded locally. To update the drivers on endpoints that have the 3.0.1100 driver package installed, manually upgrade to the 3.0.1101 driver package that is available in the Cylance Endpoint Security management console.

**What's new in the Linux agent version 3.0.1000**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added support for Linux distributions</td>
<td>Added support for the following Linux distributions:</td>
</tr>
<tr>
<td></td>
<td>• RHEL/CentOS 8.4</td>
</tr>
<tr>
<td></td>
<td>• RHEL 8.5</td>
</tr>
<tr>
<td></td>
<td>• Oracle 8.4</td>
</tr>
<tr>
<td></td>
<td>• SUSE 12 SP5</td>
</tr>
<tr>
<td></td>
<td>• SUSE 15 SP2 and SP3</td>
</tr>
<tr>
<td></td>
<td>To view the full list of supported Linux kernels and drivers, download the</td>
</tr>
<tr>
<td></td>
<td><a href="https://example.com/supported-kernels">Supported Linux Kernels spreadsheet</a>.</td>
</tr>
</tbody>
</table>

**What's new in the Linux agent version 2.1.1590**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added support for Linux distributions</td>
<td>Added support for the following Linux distributions:</td>
</tr>
<tr>
<td></td>
<td>• RHEL/CentOS 7.9, 8.3</td>
</tr>
<tr>
<td></td>
<td>• Ubuntu 20.04 LTS</td>
</tr>
<tr>
<td></td>
<td>• SUSE Linux 15</td>
</tr>
<tr>
<td></td>
<td>• Oracle 6, 7, 8</td>
</tr>
<tr>
<td></td>
<td>• Oracle UEK 6, 7, 8</td>
</tr>
<tr>
<td></td>
<td>• Debian 10</td>
</tr>
<tr>
<td></td>
<td>The Linux driver can be downloaded as a separate installation package.</td>
</tr>
<tr>
<td></td>
<td>This allows users to update the Linux driver without waiting for a new</td>
</tr>
<tr>
<td></td>
<td>release of the CylancePROTECT Desktop Linux agent. This release has the</td>
</tr>
<tr>
<td></td>
<td>latest drivers, so installing the Linux driver package is not needed. If</td>
</tr>
<tr>
<td></td>
<td>a new Linux driver becomes available before the next agent release, you</td>
</tr>
<tr>
<td></td>
<td>can choose to upgrade the Linux driver at that time.</td>
</tr>
<tr>
<td></td>
<td>If the Linux driver is updated manually, the zone-based updating feature</td>
</tr>
<tr>
<td></td>
<td>in the console will not upgrade or downgrade the driver, unless a new</td>
</tr>
<tr>
<td></td>
<td>major version is assigned. This is to prevent the automated system from</td>
</tr>
<tr>
<td></td>
<td>overwriting an action taken by an administrator.</td>
</tr>
</tbody>
</table>
## Fixed issues in the Linux agent

### Fixed in Linux agent version 3.1.1001

When the PID number of a process was greater than 32768, a violation that was related to that process was not detected. The fix is also available using driver package version 3.1.1101 for devices running agent 2.1.1590 and later. (EPP-3214)

### Fixed in Linux agent version 3.1.1000

When you tried to scan a specific directory that had Japanese characters in its name using the command line option, the scan was not successful. (CHP-8700)

### Fixed in Linux agent version 3.0.1005

When the CylancePROTECT driver was extracted from the .tar archive, the folder permissions were unexpectedly changed. The permissions are no longer changed and the folder's original permissions are now properly retained. This issue is fixed in the 3.0.1005 and 3.0.1105 Linux drivers. (EPP-2359)

The deployment of CylanceHYBRID on a host computer was not successful if CylancePROTECT was running with the memory protection policy enabled. (CHP-8676)

High memory usage was identified on Linux devices. This issue is fixed in the 3.0.1005 and 3.0.1105 Linux drivers. (CHP-8661)

If SELinux was disabled after the CylancePROTECT drivers were already loaded, a system kernel panic error occurred. This issue is fixed in the 3.0.1005 and 3.0.1105 Linux drivers. (CHP-8651)

### Fixed in Linux agent version 3.0.1001

There was excessive logging of `CefRPCServerHelper:listenForRequests: Error receiving message from queue using conn=## errno=110 (Connection timed out)` in the system logs. For more information visit support.blackberry.com and read KB 93972. (EPP-2239)

When trying to update or uninstall the CylancePROTECT agent, it stopped responding if any netcore application was running. (EPP-2172)

### Fixed in Linux agent version 3.0.1000

There are no fixed issues in this release.

### Fixed in Linux agent version 2.1.1590

There are no fixed issues in this release.
Known issues in the Linux agent

The agent updater proceeds to install the agent and driver (as if there’s an update) even though the same version was already installed. The agent continues to run as expected and the unnecessary updates do not continue to occur. (EPP-2874)

After the installation of the agent, if the first agent update is not successful, the updater could not roll back the installation because the installation files cannot be found. (EPP-2726)

Workaround: After installation, copy the each of the installation packages (.deb or .rpm) for the agent, drivers, and UI to the /opt/cylance/desktop directory.

On a SUSE 11 system (SLES 11), after upgrading from 1570 to 1580, attempts to downgrade back to 1570 was not successful. (CHP-8341)

On a SUSE 11 SP4 64-bit system (SLES 11), upgrading the agent may result in the exception System.TypeInitializationException appearing multiple times in the log file. (CHP-7916)

On an Ubuntu 14.04 and 16.04 systems, when upgrading from 1570 or 1580 to 1590, and then downgrading from 1590 to 1570 or 1580 results in the agent continuously trying to downgrade to 1570 or 1580. This results in a continuous rollback and failure messages in the agent logs. (EPP-1475, EPP-1477)

On SUSE SLES 11 SP4, if you upgrade from agent 1570/1574 to agent 1580 and then downgrade back to agent 1570/1574, the downgrade is initially successful, but is eventually upgraded back to agent 1580. (CHP-8293)

On Amazon Linux 2, installing the agent on newer kernels is successful, but a "CyProtectDrv: module verification failed: signature and/or required key missing - tainting kernel" error displays because a signature is missing. The agent still runs properly and the error can be ignored. (CHP-7335)

What's new in the CylancePROTECT Desktop agent for macOS

What's new for the macOS agent 3.1.1000.537

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added support for macOS 13</td>
<td>The CylancePROTECT Desktop agent 3.1 now supports devices that are running macOS 13 (Ventura). You must upgrade to CylancePROTECT Desktop agent 3.1 on devices that are running macOS 13, even though agent version 3.0 might continue to run on these devices after upgrading to macOS 13.</td>
</tr>
<tr>
<td>Custom interval for background threat detection scanning</td>
<td>Administrators can now set a custom interval to run background threat detection scanning from the device policy. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. Note that increasing the frequency of the scans might impact device performance. You can also start the scan manually from the command line. The date of the last scan for each device is logged in the management console.</td>
</tr>
</tbody>
</table>
What's new for the macOS agent 3.0.1000.511

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added support for macOS 12</td>
<td>The CylancePROTECT Desktop agent now supports devices that are running macOS 12 (Monterey).</td>
</tr>
</tbody>
</table>

What's new for the macOS agent 2.1.1594.518

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple Mac M1 ARM processor support</td>
<td>The CylancePROTECT Desktop now supports devices that use the Apple Mac M1 ARM processor.</td>
</tr>
</tbody>
</table>

Fixed issues in the macOS agent

Fixed issues in the macOS agent version 3.1.1000.537

The CylancePROTECT Desktop macOS agent did not load proxy auto-configuration (PAC) files properly. (EPP-1978)

When you installed or upgraded to the CylancePROTECT Desktop 3.0.1000 agent on a device running macOS 11 or later, the CyProtectDrvOSX kext was still found on the system, even though it was no longer required. (EPP-2942)

Fixed issues in the macOS agent version 3.0.1000.511

There are no fixed issues in this release.

Fixed issues in the macOS agent version 2.1.1594.518

On macOS Big Sur, a kernel panic would intermittently occur when running the agent. This was related to checking if a file is an executable and has been resolved. (CHP-8535, UD-1626)

On macOS Monterey, the agent stopped responding when closing a file when Memory Protection was enabled. (UD-1616)

On different macOS versions, memory usage increased. (EPP-1708)

On macOS Monterey, the CylanceSvc and CyUpdate services would not run. (EPP-1643)

On macOS Big Sur devices, the CylancePROTECT Desktop agent gave multiple Remote Allocation of Memory (OopAllocate) memory protect alerts for osqueryd. (UD-1266)
Known issues in the macOS agent

On macOS Catalina devices, the Cylance logo might not display on the Cylance UI About page or Installation Token prompt dialog box. (CHP-7509)
# CylancePROTECT Mobile release notes

## What's new in CylancePROTECT Mobile

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date added</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for the Play Integrity API</td>
<td>The May release of the CylancePROTECT Mobile app adds support for the Play Integrity API for attestation of the app on Android devices. Play Integrity attestation replaces SafetyNet attestation. Older versions of the app will continue to support SafetyNet attestation until <a href="https://support.google.com/android-developer/answer/7277380">Google removes support</a>. To ensure that Play Integrity attestation works as expected, instruct users to update to the latest version of Google Play.</td>
<td>May 2023</td>
</tr>
<tr>
<td>Change to Android OS support</td>
<td>The May release of the CylancePROTECT Mobile app removes support for the Android 9 OS.</td>
<td>May 2023</td>
</tr>
</tbody>
</table>
| Record of the most recent device scan        | The Device Health section of the CylancePROTECT Mobile app will indicate when the most recent scan for threats occurred.                                                                                   | December 2022 (Android)  
October 2022 (iOS) | |
| Browser support                              | The CylancePROTECT Mobile app now supports the Firefox and Brave browsers for Android.                                                                                                                                 | December 2022 |
| New name for the app                         | The late July release rebrands the BlackBerry Protect app to the CylancePROTECT Mobile app.                                                                                                                  | July 2022   |
| Samsung Knox Enhanced Attestation            | This release supports the use of Samsung Knox Enhanced Attestation in regular intervals to validate the integrity of users’ Samsung devices. Knox Enhanced Attestation is hardware-based and can detect device tampering, rooting, OEM unlock, and IMEI or serial number falsification, in addition to performing app health checks. | July 2022   |
| Enhancements to SMS monitoring for Android devices | This release introduces new options in CylancePROTECT Mobile policies that allow you to specify an age threshold for SMS messages that can be scanned (up to 7 days old), and the ability to obfuscate certain pieces of data that Cylance Endpoint Security collects, including URLs and the email or phone number of the sender. When a malicious URL is detected in a text message, an alert is reported in the management console on the Protection > Protect Mobile Alerts page. | July 2022   |
Administrator controls for detecting developer mode on Android devices

Previously, the ability to detect developer mode on Android devices was always on and you did not have the option to turn this feature off. In this release, CylancePROTECT Mobile policies now include the option to turn this feature on or off. When developer mode is detected on a device, an alert is reported in the management console on the Protection > Protect Mobile Alerts page.

July 2022

CylancePROTECT Mobile app versions

• CylancePROTECT Mobile app for iOS: 2.16.0.3484
• CylancePROTECT Mobile app for Android: 2.16.0.3484

CylancePROTECT Mobile fixed issues

CylancePROTECT Mobile app (all platforms)

If a user deactivated the CylancePROTECT Mobile app, then changed the device language and activated the app again, the text on the activation screen used the original device language instead of the new device language. (UESAPP-3111)

CylancePROTECT Mobile app for Android

If you added an app to the CylancePROTECT Mobile restricted list in the management console, when the app was detected on devices, the user might have received more than one new threat notification. (MTDLIB-1176)

If the Network protection > Wi-Fi security feature was turned off in the app and the user turned it on and selected "Maybe Later" in the permission prompt, the app indicated that a threat was detected. (MTDPLR-19)

If the CylancePROTECT Mobile app was installed and activated in the Intune portal on an Android OS 13 device, in the App info, the "Pause app activity if unused" option was greyed out and the user could not turn it off. This prevented the user from turning off battery optimization for the app, and they saw a warning message in the Device Health section that they could not dismiss. (UES-10189)

App configurations that you created from the Cylance console did not register successfully for Android devices with the CylancePROTECT Mobile app version 2.2.0.1381. This issue was fixed by a Cylance Endpoint Security update on March 24 2022. (UES-7516)

For CylancePROTECT Mobile devices configured for Intune integration, if the user did not complete Microsoft Online Device Registration, when the user force closed and reopened the CylancePROTECT Mobile app, the Microsoft Online Device Registration banner with the register link did not display as expected. (UES-7243)

In the CylancePROTECT Mobile app, if some device security features were turned off and no device security threats were detected on the device, the text in the Device Health > Device security section of the app displayed in yellow instead of green. (UESAPP-3644)
After a user turned on Wi-Fi protection in the CylancePROTECT Mobile app and granted the required permission, a false "No Wi-Fi connected" threat displayed for a few seconds. (UESAPP-3269)

After a user activated the CylancePROTECT Mobile app, when the user tapped Device Health for the first time, there could be a delay of up to 20 seconds before the UI displayed. (UESAPP-3154)

After a user activated the CylancePROTECT Mobile app and granted permissions for the app to check the security of the Wi-Fi network, for up to 30 seconds, Device Health > Network Protection indicated that network security features were disabled. (UESAPP-3147)

If a user tried to activate the CylancePROTECT Mobile app on a Samsung S20 or S21 device with Android 12 using their activation credentials, the activation failed with the following error: "The specified key does not exist." (UESAPP-2865)

If you removed an app from the CylancePROTECT Mobile safe list or unsafe list, it could take up to 30 minutes for that change to take effect on devices (for example, if an app was removed from the safe list and was considered malicious by the CylancePROTECT cloud services, it could take up to 30 minutes for the CylancePROTECT Mobile app to detect it). If malware detection was turned off on in a CylancePROTECT Mobile policy and you turned it on, it could take up to 30 minutes for the CylancePROTECT Mobile app to start detecting malicious apps. (UESAPP-2547)

If a device was activated on BlackBerry UEM with the Android Enterprise activation type using BlackBerry Secure Connect Plus, when the CylancePROTECT Mobile app was installed in the work space as a required app, a network connection error occurred when the user tried to activate the app. The app did not activate successfully. (UESAPP-2251)

If a user's device was rooted, when the user moved the CylancePROTECT Mobile app from the background to the foreground, a "Threat detected" notification might have displayed on the device. (UESAPP-2210)

CylancePROTECT Mobile app for iOS

On devices with iOS 16.2, if a user enabled SMS message filtering, the feature was turned off after the user upgraded the app. (UESAPP-3764)

If a user sent the CylancePROTECT Mobile app to the background, then brought it to the foreground again, it could take up to 10 minutes for the app to check the device for threats. (UESAPP-3638)

For CylancePROTECT Mobile devices configured for Intune integration, if a user had not completed the Microsoft Online Device Registration process and snoozed the notification for one hour, the notification did not display again after one hour if the CylancePROTECT Mobile app was not running in the background. The user had to wait for the notification that would display every 24 hours. (UESAPP-2583)

If the CylancePROTECT Mobile app detected more than one threat, after you resolved one of the threats, a notification for a new threat still displayed on the device even though no new threats had been detected. (UESAPP-2553)

When a user tried to deactivate the CylancePROTECT Mobile app, in certain circumstances the deactivation could fail and cause the app to stop responding. (UESAPP-2228)

If a device security threat was detected and resolved, the device security section of the app might have still displayed a threat alert. (UESAPP-2224)
When a user deactivated the CylancePROTECT Mobile app, there was no dialogue to indicate that deactivation was in progress. (UESAPP-2167)

When a user activated the CylancePROTECT Mobile app, for the options under the text "No QR code?", the user had to tap the icon for the option and could not tap the text. (UESAPP-1886)

CylancePROTECT Mobile app for Chrome OS

After activating the CylancePROTECT Mobile app, when the user was prompted to ignore battery optimization settings, a "This setting is not supported" error displayed. The user could close the error and allow the app to run in the background, but a message continued to display in the app reminding the user to allow it to run in the background. (UESAPP-3533)

CylancePROTECT Mobile known issues

CylancePROTECT Mobile app for Android

If you turn off hardware attestation, then turn it on again, the previous attestation state will be reported instead of initiating a new attestation check. (MTD-6839)

On Samsung Galaxy S22 devices or later with Android 13 and the December 2022 security patch, Samsung Knox Enhanced Attestation fails and is reported as a threat in the CylancePROTECT Mobile app. (MTDPLR-21)

**Workaround:** Turn off Samsung Knox Enhanced Attestation in the CylancePROTECT Mobile policy assigned to devices until Samsung resolves the issue.

When you navigate to a user's device details in the management console and view Alerts > Protect Mobile Alerts, if you try to filter the results to SafetyNet or Play Integrity attestation failure alerts, the results are not filtered and the following error message displays: "An error occurred. Please try again." (UES-13110)

Some status messages, tooltips, labels, and descriptions in the management console reference SafetyNet attestation when they should reference SafetyNet and Play Integrity attestation. (UES-13010, MTD-7931, MTD-7927)

When Play Integrity or SafetyNet attestation fails, the user receives a notification on their device even if the Protect Mobile policy is not configured to display device notifications for attestation issues. (UESAPP-3962)

If a user's default device browser is Firefox, after the user enters their activation credentials, the activation process does not start. This is due to a known issue with Firefox. (UESAPP-1804)

**Workaround:** Enable the "Open links in app" options in the Firefox settings on the device.

When the CylancePROTECT Mobile app detects a restricted app (an app with a developer certificate that has been added to the malware and sideload detection restricted list in the management console), multiple alerts display in the app instead of a single alert. (UESAPP-1696)

CylancePROTECT Mobile app for iOS

When you navigate to a user's device details in the management console and view Alerts > Protect Mobile Alerts, if you try to filter the results to SafetyNet or Play Integrity attestation failure alerts, the results are not filtered and the following error message displays: "An error occurred. Please try again." (UES-13110)

Some status messages, tooltips, labels, and descriptions in the management console reference SafetyNet attestation when they should reference SafetyNet and Play Integrity attestation. (UES-13010, MTD-7931, MTD-7927)

When Play Integrity or SafetyNet attestation fails, the user receives a notification on their device even if the Protect Mobile policy is not configured to display device notifications for attestation issues. (UESAPP-3962)

If a user's default device browser is Firefox, after the user enters their activation credentials, the activation process does not start. This is due to a known issue with Firefox. (UESAPP-1804)

**Workaround:** Enable the "Open links in app" options in the Firefox settings on the device.

When the CylancePROTECT Mobile app detects a restricted app (an app with a developer certificate that has been added to the malware and sideload detection restricted list in the management console), multiple alerts display in the app instead of a single alert. (UESAPP-1696)
If Work Mode is enabled when the CylancePROTECT Mobile app updates, a "CylanceGATEWAY is disconnected" message is displayed and users are unable to connect to CylanceGATEWAY. (BIG-8649)

**Workaround:** Start the CylancePROTECT Mobile app or tap the pop-up message.

If you turn on Unsupported OS in a Protect Mobile policy and add OS 16.4.1.(a) to the unsupported list, when the policy is applied to a device, the CylancePROTECT Mobile app stops responding and closes instead of displaying an alert that the OS is not supported. Removing 16.4.1.(a) from the unsupported list in the policy does not fix the issue after it has occurred. This issue will be fixed in the next release of the CylancePROTECT Mobile app. (UESAPP-4012)

**Workaround:** Remove 16.4.1.(a) from the unsupported list, then instruct impacted device users to uninstall, reinstall, and reactivate the CylancePROTECT Mobile app.

On certain devices, including iPhone 12 Pro Max and iPhone SE 2020 (iOS 15.2), CylancePROTECT Mobile policy changes that are sent from Cylance Endpoint Security to the CylancePROTECT Mobile app might not apply immediately if the app is running in the background. (UESAPP-2433)

False app integrity alerts might occur on iPhone X iOS 14.6 devices. (UESAPP-2421)

**CylancePROTECT Mobile app for Chrome OS**

If you turn on hardware attestation and set a security patch level for PixelBook devices, an alert is not displayed in the app and management console if a PixelBook Go device does not meet the patch level you specified. (UESAPP-2271)

On certain Chrome OS, after a user enters their activation credentials, the user is not redirected to the CylancePROTECT Mobile app and the activation does not complete successfully. (UESAPP-887)

**Workaround:** In the “Open with” prompt, select Protect and Open. If the prompt does not display, click the square with the arrow icon.

When a user scans their QR code to activate the CylancePROTECT Mobile app and taps Continue, the user is not redirected to the CylancePROTECT Mobile app and activation does not complete successfully. (EID-16707)

**Workaround:** Reload the browser page.
What's new in CylanceOPTICS (April 2023)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| New audit log values for device lockdown configuration in syslog messages | The April update of the CylanceOPTICS cloud services adds new event name values to audit log messages that can be reported to SIEM solutions and syslog servers. The new Event Name fields are associated with the lockdown configuration feature:  
  • LockdownConfigurationAdd  
  • LockdownConfigurationEdit  
  • LockdownConfigurationDelete  
  For more information about audit log events, see the Cylance Syslog Guide. |

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Lockdown configurations API | The Cylance User API now includes the lockdown configurations API. You can use this API to perform actions on partially locked devices, including:  
  • Getting a list of custom partial lockdown profiles  
  • Creating a custom partial lockdown profile  
  • Updating a custom partial lockdown profile  
  • Deleting a custom partial lockdown profile  
  For more information, see the Cylance User API Guide. |

What's new in CylanceOPTICS (December 2022)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| New OS support | This release adds support for the following operating systems:  
  • macOS Ventura (13.x)  
  • SUSE Enterprise Linux 15 SP4  
  • Oracle Linux Server 7 (non-UEK)  
  • Debian 11  
  • Debian 10  
  For more information about supported operating systems, see the Cylance Endpoint Security compatibility matrix. For more information about OS requirements, see CylanceOPTICS requirements in the Cylance Endpoint Security Setup content. |
### CylanceOPTICS agent versions

- Windows: 3.2.1299.0
- macOS: 3.2.1299.5000
- Linux RHEL/CentOS 8: 3.2.1299-23000
- Linux RHEL/CentOS 7: 3.2.1299-7000
- Amazon Linux 2: 3.2.1299-15000
- Linux SLES15: 3.2.1299-29000
- Linux SLES12: 3.2.1299-21000
- Ubuntu 20.04: 3.2.1299-25000
- Ubuntu 18.04: 3.2.1299-17000
- Oracle Linux Server 8 / UEK 8: 3.2.1299-37000
- Oracle Linux Server 7: 3.2.1299-35000
- Debian 11: 3.2.1299-49000
- Debian 10: 3.2.1299-47000

For more information about supported operating systems, see the [Cylance Endpoint Security compatibility matrix](#). For more information about OS requirements, see [CylanceOPTICS requirements](#) in the Cylance Endpoint Security Setup content.

### MSI installer

This release introduces a new MSI installer package that you can use to install the CylanceOPTICS agent version 3.2 on Windows devices.

For more information about the OS commands supported by the MSI installer, see [OS commands for the CylanceOPTICS agent](#) in the Cylance Endpoint Security Setup content.

### What's new in CylanceOPTICS (October 2022)

### New OS support

This release adds support for the following operating systems:

- Windows 11 22H2
- Windows 10 22H2

For more information about supported operating systems, see the [Cylance Endpoint Security compatibility matrix](#). For more information about OS requirements, see [CylanceOPTICS requirements](#) in the Cylance Endpoint Security Setup content.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| CylanceOPTICS agent versions | - Windows: 3.2.1140.0  
- macOS: 3.2.1140.5000  
- Linux RHEL/CentOS 8: 3.2.1140-23000  
- Linux RHEL/CentOS 7: 3.2.1140-7000  
- Amazon Linux 2: 3.2.1140-15000  
- Linux SLES15: 3.2.1140-29000  
- Linux SLES12: 3.2.1140-21000  
- Ubuntu 20.04: 3.2.1140-25000  
- Ubuntu 18.04: 3.2.1140-17000  
- Oracle Linux Server 8 / UEK 8: 3.2.1140-37000  

For more information about supported operating systems, see the [Cylance Endpoint Security compatibility matrix](#). For more information about OS requirements, see [CylanceOPTICS requirements](#) in the Cylance Endpoint Security Setup content. |
| Customized partial lockdown | CylanceOPTICS version 3.1 introduced the [partial lockdown feature for Windows devices](#). This release introduces the ability to create custom partial lockdown configurations that allow you to specify additional communication channels that you want to allow during a partial lockdown.  

For more information, see [Lock a device](#) in the Cylance Endpoint Security Administration content. |
| Additional CylanceOPTICS administrator permissions | The July 2022 update of CylanceOPTICS introduced new administrator permissions that you could assign to roles to control how administrators engage with CylanceOPTICS. This release introduces additional CylanceOPTICS permission groups and sub-permissions, offering a greater level of access control and customization.  

If you previously granted an administrator role a CylanceOPTICS permission that was introduced in the July 2022 update, that role will be granted any associated sub-permissions that are introduced in this update. It is a best practice to review the CylanceOPTICS permissions that are introduced in this update so that you can make any adjustments that are appropriate for your organization's environment.  

For more information, see [Permissions for administrator roles](#) in the Cylance Endpoint Security Setup content. |
| Syslog messages for the API sensor | The late October update of the CylanceOPTICS cloud services will add a new event type that can be reported to SIEM solutions and syslog servers, OpticsCaeApiEvent. This event type is used for events that are detected by the CylanceOPTICS agent’s optional API sensor. For more information about the API sensor, see [CylanceOPTICS sensors](#) in the Cylance Endpoint Security Setup content.  

For more information this new event type, see the [Cylance Syslog Guide](#). |
### Feature Description

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| New audit log values for device lockdown syslog messages | The mid-October update of the CylanceOPTICS cloud services adds new event name values to audit log messages that can be reported to SIEM solutions and syslog servers. The new Event Name fields are associated with the lockdown feature:  
• DeviceUnlock  
• DeviceChangeLockdownProfile  
For more information about audit log events, see the [Cylance Syslog Guide](#). |

### Considerations when upgrading from CylanceOPTICS 2.5.x to 3.x

- For configuration requirements for macOS Big Sur (11.x) or Monterey (12.x), see the setup instructions in the [Cylance Endpoint Security Setup Guide](#).
- If you do not set up a complete MDM profile for the CylanceOPTICS network extension on devices with macOS Big Sur (11.x) or later, data collection might not occur as expected. Verify that you satisfy the configuration requirements for MDM managed devices in the [Cylance Endpoint Security Setup Guide](#).
- BlackBerry recommends installing the latest available version of the CylancePROTECT agent. For more information, see the [CylanceOPTICS requirements](#).
- On macOS devices, after you upgrade the CylanceOPTICS agent you need to restart the device.
- On macOS Catalina, Mojave, and High Sierra devices with the SelfProtection level set to LocalSystem, if you upgrade from CylanceOPTICS agent version 2.5.x to 3.x, the upgrade might not complete successfully. (EDR-7705)  
  **Workaround:** Change the self protection level to LocalAdmin, then update the CylanceOPTICS agent.
- If you upgrade the CylanceOPTICS agent on a CentOS/RHEL 8.0 or 8.1 device, you must restart the device after the upgrade is complete. (EDR-6750)
- Upgrading the CylanceOPTICS agent on Linux from version 2.x to a newer version fails if Security-Enhanced Linux (SELinux) is enabled on the device. (EDR-6264)  
  **Workaround:** Disable SELinux on the device before you upgrade the CylanceOPTICS agent and enable it again after the upgrade is complete.
- When upgrading the CylanceOPTICS agent on Windows, to avoid an issue with the CylanceOPTICS shutdown time taking longer than usual, disable the TDT sensor in the device policy and enable it again after the upgrade is complete. This issue does not occur if you upgrade from CylanceOPTICS agent version 2.5.3010 or from CylanceOPTICS agent 3.0 to a later version. (EDR-6058)

### CylanceOPTICS fixed issues

**Fixed issues in CylanceOPTICS 3.2**

| If you requested and viewed focus data from the device details page (Assets > Devices) before the event data was loaded to the management console, the resulting focus data did not include any results. (EDRRQ-240) |

On Windows 7 devices, if you upgraded to CylanceOPTICS agent 3.1 or later, after you restarted the device the agent did not start as expected. If the user right-clicked the CylancePROTECT icon and clicked System Check, the status of the CyOptics driver was "Not Found". (EDR-14132)
If you created a custom partial lockdown configuration that contained an allowed port value and you assigned it to a CylanceOPTICS device, the allowed port for partial lockdown was not removed when you assigned a different custom configuration. As a result, any ports that you allowed with any partial lockdown configuration remained allowed on the device, regardless of the new configurations that you assigned. (EDR-13243)

In the management console, if you retry a focus data request, the timestamp information is missing. (EDR-10987)

When you scoped an advanced query to specific devices (Search devices > By Device), the Device drop-down listed a maximum of 200 devices. (EDR-10446)

If you deployed a package to CylanceOPTICS devices, when you highlighted a device in the device selection list, you could not see the icon that indicated that the device was online. The color of the icon matched the color of the highlight. (EDR-10224)

When you deployed a package to CylanceOPTICS devices, the status column might have indicated that the job was completed even though the progress bar was not yet full. (EDR-8754)

If you uninstalled the CylanceOPTICS agent using an MDM profile, the network filter CyOpticsESFLoader remained in the system networking on the device. (EDR-7656)

When you viewed focus data and you clicked the path for a file event to create a pivot query, the Search Term field was not pre-populated. (EDR-6785)

On macOS devices, when CylanceOPTICS performed an action on an empty file (for example, a 0 KB .prn file), the event was not included in the datagram file. This is fixed for macOS devices with Big Sur (11.x) or later. (EDR-5545)

**Fixed issues in CylanceOPTICS 3.1**

If you checked the device details in Optics > Devices after you partially locked or remotely unlocked a device, the device status may not have updated as expected. (EDR-9646)

In some advanced query results, the option to globally quarantine a file was not available. (EDR-9534)

If you cloned an existing package deployment job with a status of created, expired, in progress, or stopped, the device information was not prepopulated in the new package deploy. (EDR-7927)

When you created a package deploy, if you added a device to the request then removed it and tried to add it again, the device did not display on the available devices list. (EDR-7847)

Locking down a macOS device did not close the VNC client on that device. (EDR-6971)

If you ran an InstaQuery for a PowerShellTrace artifact and a Payload or Script Blocked Text facet, the search term was case-sensitive. (EDR-6868)

When you created a pivot query from the focus data timeline view, if the artifact was registry key, the artifact and facet fields were not pre-populated. (EDR-6856)

When you viewed focus data in the table view for a registry key artifact, the name and path were not correct. If you created a pivot query, you did not get any results. (EDR-6855)
CylanceOPTICS known issues

Due to a defect in macOS Ventura 13.0.0, if the CylanceOPTICS agent is installed on a device with macOS 13.0.0 or a CylanceOPTICS device is upgraded to macOS 13.0.0, the CylanceOPTICS agent may not be able to detect events. (EDR-14879)

**Workaround:** To prevent this issue from occurring, install the agent on macOS Ventura 13.0.1 or later or upgrade directly to macOS Ventura 13.0.1 or later instead of 13.0.0. If you upgrade from 13.0.0 to 13.0.1 or later, remove the agent and install it again. If installing on 13.0.1 or later or upgrading to 13.0.1 or later is not possible at this time, remove full disk access for CyOptics and CyOpticsESFLoader then add full disk access for both again and restart the device.

If the API Sensor is enabled in the device policy that is assigned to CylanceOPTICS 3.2.x devices with Windows Server 2016 and CylancePROTECT Desktop agent 3.0.1003 or later, some applications such as Chrome and Powershell may stop working. This issue is resolved in the next release of the CylanceOPTICS agent. (EDR-10871)

**Workaround:** Turn off the API Sensor in the device policy.

When you try to unlock a partially locked device from the management console, it may not unlock as expected. This issue occurs intermittently. (EDR-9690)

**Workaround:** Try to unlock the device again from the management console (Select Action > Unlock device), or use the unlock key.

If you run an advanced query and try to generate focus data from the results, the focus description that is used to generate the data does not include the correct artifact information. (EDR-9414)

If you downgrade from CylanceOPTICS agent version 3.1 or later to version 3.0, the lockdown feature stops working. (EDR-9199)

**Workaround:** Uninstall agent version 3.0 and install it again.

If you try to download a large file from InstaQuery results by clicking the Request File Download button, the request might not complete as expected (the button does not change to "Download File"). (EDR-7702)

If a remote session is active when the CylanceOPTICS agent is installed on a macOS Big Sur (11.x) device, the session disconnects when the installation is complete. (EDR-7180)

**Workaround:** Start the remote session again.

When you view the detection details for an event and you request a file download for an instigating process or target file source, the status of the download changes back to "Request File Download" instead of "Download File". (EDR-7007)

The refract package for browser history that is available in the management console does not collect the expected data on Linux devices. (EDR-6917)
If you view the threats and activities for a device and you request data for an event, the focus view status remains at "Data Pending" indefinitely instead of updating to "View Data". (EDR-6779)

**Workaround:** View another tab and return to the device’s threats and activities.

When you view the status of a package deploy job and you filter the results by name, the operator displays as "Equals" even though it works as "Contains", and the filter is case sensitive. (EDR-6689)

When you view the results of an InstaQuery, the count for devices queried and devices responded might not be accurate. This issue occurs intermittently. (EDR-6523)

Performance counters for macOS and Linux do not include system counter data, such as CPU and memory. (EDR-5219)

If you use an ssh session to perform a silent uninstall of the CylanceOPTICS agent on a macOS Big Sur (11.x) device, /Applications/Cylance/ Optics/CyOpticsESFLoader.app remains and the system extension is still active. This issue occurs because Apple has no mechanism to silently uninstall system extensions without explicit confirmation by the end user. To resolve, use the finder to locate CyOpticsESFLoader.app and drag it to the trashcan, then confirm the UI prompt to deactivate and remove the system extension. For more information, see Troubleshooting: Removing the CylanceOPTICS agent from a macOS device.
# CylanceGATEWAY release notes

## What's new in the management console

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date added</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for multiple private network configurations</td>
<td>You can now configure CylanceGATEWAY to allow access to resources on more than one private network (for example, segments, data centers, and VPCs) both in on-premises and cloud environments. You can view the CylanceGATEWAY Connectors that are associated with each specified Connector Group. This feature allows you to deploy multiple CylanceGATEWAY Connectors from one Cylance Endpoint Security tenant and provides an aggregated view of the connectors for each private network. This feature is enabled by default on new tenants. Existing tenants can be upgraded to support multiple private network configurations. You must contact BlackBerry Technical Support if you want to enable this feature.</td>
<td>July 2023</td>
</tr>
</tbody>
</table>

### UI updates

- The left “Network Routing” navigation menu has been renamed to “Connector Groups”.
- The “Health Check” and “Source IP restriction” configuration screens have been moved to “Connector Groups”.
- In the “Gateway Connectors” navigation menu, the “Tunnel”, “DNS”, and “HTTP” columns have been combined into the “Health Check Status” column. You can click the Health Check Status column to view additional connector information (for example, whether a tunnel is established and the DNS server IP address).
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date added</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved control of network traffic settings</td>
<td>The updated Network Protections settings introduce more granular control over the detection and protection mode of features of CylanceGATEWAY, the respective details that you want to have reported and displayed in the Network Events screen, and the level of details shared to your integrated SIEM solution or syslog server, if configured.</td>
<td>July 2023</td>
</tr>
<tr>
<td></td>
<td>• The current &quot;Network Protection&quot; settings have moved to the <strong>Protect</strong> tab. The Network protection action &quot;Enable intrusion protection&quot; has been renamed to &quot;Enable Signature detection&quot;.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The new <strong>Report</strong> tab allows you to specify the details that will appear in the Network Events page as detections or normal traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The new <strong>Share</strong> tab allows you to specify the details that are sent to the SIEM solution or syslog server, if configured. By default, blocked detections are always sent. Optionally, you can choose to also send allowed detections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">Configuring network protection</a> in the Cylance Endpoint Security Setup content.</td>
<td></td>
</tr>
<tr>
<td>Enhancements</td>
<td>On the CylanceGATEWAY Events page,</td>
<td>July 2023</td>
</tr>
<tr>
<td></td>
<td>• <strong>New category:</strong> Previously the &quot;Security Risk&quot; category was applied as both a content category for destinations that were deemed non-malicious (for example, destinations that teach about malware), as well as an anomaly category for destinations that are considered malicious (for example, destinations that distribute malware). Now when CylanceGATEWAY detects an IP reputation, the IP reputation will be categorized as one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Dynamic Risk:</strong> This new category is applied to destinations that are identified to contain potentially malicious threats by using a combination of ML models and IP Reputation database which continuously changes to add or remove destination entries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Security Risk:</strong> This category is now applied only as a content category to non-malicious destinations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>New BlackBerry source IP address filter capability:</strong> You can now filter events based on the CylanceGATEWAY tunnel IP address. The &quot;BlackBerry source IP&quot; identifies the tunnel IP address users used to access external destinations. This feature provides administrators with added visibility in the tunnel that was used when an event has occurred.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date added</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Enable Split DNS</td>
<td>In the Gateway Service policy, you can now enable Split DNS after Split tunneling is enabled. For more information on split DNS tunneling, see &quot;Split tunneling enhancements&quot; below.</td>
<td>June 2023</td>
</tr>
<tr>
<td>HTTP content logging</td>
<td>In the ACL rules, you can now specify whether network events should include unencrypted, plain-text HTTP connection data. When enabled, a summary of the request and response details of an event are displayed in the Events Details page. The Events details page displays the first three HTTP events of the total events. You have the option to view all the events and the details that are associated with each one. This feature allows unencrypted HTTP network traffic to be reviewed and analyzed more deeply while further enabling threat hunting.</td>
<td>June 2023</td>
</tr>
<tr>
<td>Safe Mode DNS protection support on Windows</td>
<td>In the Gateway Service policy, you can configure users to use Safe Mode. This feature extends the tenant’s ACL rules and endpoint protection for devices when Work Mode is not enabled ensuring that devices are always protected. With Safe Mode, CylanceGATEWAY blocks users from accessing potentially malicious destinations and enforces acceptable use policy (AUP) by intercepting DNS requests. The CylanceGATEWAY Cloud services evaluate each DNS query against the configured ACL rules and network protection settings, and then instructs the agent to allow or block the request in real time. If allowed, the network DNS query is allowed to complete over the bearer network. Otherwise, the CylanceGATEWAY agent overrides the normal response and prevents access. When enabled, Safe Mode automatically takes effect when Work Mode is disabled. Enabling Safe Mode does not prevent users from enabling or disabling Work Mode, if the users’ policy allows such operations. Safe Mode events appear in the CylanceGATEWAY Events screen and are sent to the SIEM solution or syslog server, if configured. This feature is not supported in environments that use secure DNS with DoT (DNS-over-TLS) and DoH (DNS-over-HTTPS) protocols. DNS queries sent using DoT or DoH cannot be viewed by CylanceGATEWAY. This feature is supported on CylanceGATEWAY agent for Windows version 2.8 or later. For more information, see the Gateway Service policy parameters in the Cylance Endpoint Security Setup content.</td>
<td>June 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date added</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>OS-specific ACL support</td>
<td>In the ACL rules, you can create rules and specify which OS that the ACL rule applies to must match. This feature allows you to unify the ACL rules. For example, you have content sensitive resources that you only want desktop devices (macOS and Windows) to access. In this scenario, your ACL rule would specify the desktop devices which are allowed access to the resource. For more information, see the ACL parameters in the Cylance Endpoint Security Setup content.</td>
<td>June 2023</td>
</tr>
<tr>
<td>Split tunneling enhancements</td>
<td>Now when you enable split tunneling, split DNS queries allow lookups for the domains that are listed in the Private Network &gt; DNS &gt; Forward Lookup Zone configuration to be performed through the tunnel where network access controls are applied. All other DNS lookups are performed using your local DNS server. Android and 64-bit Chromebook devices do not support split DNS queries and the DNS lookups are performed through the tunnel. This feature allows you to further ensure user traffic privacy and geographical locality of the DNS queries, enhancing the Split Routing feature of Gateway. Split DNS is disabled by default. If you enabled Safe Mode, DNS traffic that does not use the Gateway tunnel is protected by Safe Mode. For more information, see the Gateway Service policy parameters in the Cylance Endpoint Security Setup content.</td>
<td>June 2023</td>
</tr>
<tr>
<td>Enhancements</td>
<td>On the CylanceGATEWAY Events page,</td>
<td>June 2023</td>
</tr>
<tr>
<td></td>
<td>• <strong>UI Update</strong>: The “Platform” column has been renamed to “OS”.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On the Events Details page,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UI Update</strong>: The “Platform” column has been renamed to “OS”.</td>
<td></td>
</tr>
</tbody>
</table>

**CylanceGATEWAY component versions**

- CylanceGATEWAY Connector version 2.8.0.848
- CylanceGATEWAY agent for Windows version 2.8.0.10
- CylanceGATEWAY agent for macOS version 2.8.13

To download the agent, go to the BlackBerry Website and scroll down to the Download CylanceGATEWAY section.
What's new in CylanceGATEWAY Connector 2.8.0.848 (June 2023)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General updates</td>
<td>The June release rebrands the &quot;blackberry-gateway-connector&quot; debian package to &quot;cylance-gateway-connector&quot; installation files. This updated version is required to enable enhanced features in future releases.</td>
</tr>
<tr>
<td>Enhancements</td>
<td>The CylanceGATEWAY Connector now provides additional information on TCP and UDP flows that flow through the tunnel to the private network (for example, the Private NAT source IP and Private NAT Source Port) after the Network Address Translation (NAT) is applied. When events traverse the private network, the Private NAT Source IP and Private NAT Source Port are displayed on the Events Details page for each event. If the Private NAT Source IP and Private NAT Source Port events are not available or the feature is not enabled, the Events Details page displays &quot;Unknown&quot;. Events that are identified as a potentially malicious or blocked based on your network protection settings are sent to the SIEM solution or syslog server, if configured. Health check and DNS events are not sent to SIEM solution or syslog server. This feature is disabled by default. You must contact BlackBerry Technical Support if you want to enable this feature. For more information, see the Viewing the Event Details page in the Cylance Endpoint Security Administration content.</td>
</tr>
</tbody>
</table>

**CylanceGATEWAY fixed issues**

**Fixed issues in the CylanceGATEWAY agent for macOS**

**Fixed issues in the CylanceGATEWAY agent for macOS 2.5.16 (Aug 2022)**

Changes to the local CylancePROTECT Serial Number on macOS devices, when not propagated to the management console by the CylanceGATEWAY client, may have resulted in a failure to activate or enable Work Mode on macOS CylanceGATEWAY endpoints. (BIG-8030)

**Fixed issues in the CylanceGATEWAY agent for macOS 2.0.17 (May 2022)**

When some users that ran the CylancePROTECT agent on macOS devices tried to enable work mode, the client remained at ‘enabling work mode’ and didn’t enable. (BIG-6935)

**CylanceGATEWAY known issues**

Items marked with an asterisk (*) are new for this release.

Access control list (ACL)
In some scenarios, an ACL rule might be expected to block a connection to a destination, but it isn’t when the following combined ACL properties are used to create the rule. (BIG-6511)

Consider the following scenario, this ACL rule will allow users to access to *.example.com when the following ACL properties are specified because the DNS request for http://example.com will be resolved to an IP address (for example, 172.16.10.55) and the request to the IP address on port 80 is not blocked.

In the **Action** section,
- The Action drop-down list displays **Block**.
- The **Ignore port** check box is cleared.

In the **Destination** section,
- The **Target** dropdown list displays **Matches any**.
- In the **Address and Ports** field, you entered *.*example.com with port 80.

To block access to the destination in the above scenario, best practice is to enter the FQDN without a wildcard or enter the FQDN with a wildcard and not specify a port number. To have this rule block access to the destination as expected, you must update the ACL rule to one of the following:

<table>
<thead>
<tr>
<th>Block destination</th>
<th>ACL properties</th>
</tr>
</thead>
</table>
| Specify the destination FQDN and port number. | In the **Action** section,  
- The Action drop-down list displays **Block**.  
- The **Ignore port** check box is cleared.  
In the **Destination** section,  
- The **Target** dropdown list displays **Matches any**.  
- In the **Address and Ports** field, you entered example.com with port 80. |
| Specify the destination FQDN with a wildcard, no port number. | In the **Action** section,  
- The Action drop-down list displays **Block**.  
- The **Ignore port** check box is selected.  
In the **Destination** section,  
- The **Target** dropdown list displays **Does not match**.  
- In the **Address and Ports** field, you entered http://*.example.com. |

The ACL tab is not displayed in the Cylance Endpoint Security console immediately after CylanceGATEWAY is enabled for the tenant. (BIG-7059)

**Workaround:** Log out of the Cylance Endpoint Security console, and log in again.

**Network connections**

* On macOS devices when split tunneling is enabled and a DNS query is made for an unqualified hostname, the DNS suffixes may not be applied or used as defined in Settings > Network > Client DNS. (BIG-11180)

**Workaround:** Complete one of the following:
- Disable split tunneling and users use CylanceGATEWAY to access network resources.
- Instruct users to use the FDQN to access network resources.
When Windows devices are configured to use Safe Mode and Work Mode is not enabled, if third-party solutions that control DNS such as VPN are enabled, they may not work as expected. When enabled, Safe mode intercepts and evaluates all DNS queries and may have conflicts with other solutions that also control DNS. For more information on Safe Mode, see CylanceGATEWAY release notes. (BIG-11098)

If the component that is handling active connections through the CylanceGATEWAY Connector is restarted within the BlackBerry Infrastructure, the number of active connections for the connector may not return to zero when the connector is disabled. (BIG-8614)

Restricted apps can't open loopback sockets when "Block network traffic from restricted apps" is set to "No" in the CylanceGATEWAY service policy, for Windows devices. (BIG-7593)

The Intel Killer Prioritization Engine may drop CylanceGATEWAY traffic. (BIG-5527)

**Workaround:** Give BlackBerryGatewayService.exe a priority of "1" in the Killer Prioritization Engine console.

If a device's local network IP range (for example, a home Wi-Fi network) overlaps with the customer's private network, CylanceGATEWAY work mode does not allow access to the private network resources for the IPs that fall in the overlap range. For example, if a user's home Wi-Fi network range uses 10.0.0.0/24 and the customer’s private network uses 10.0.0.0/8, the user will not be able to access 10.0.0.100 on the private network as it falls under 10.0.0.0/24 and will be routed to the local network. (BIG-5389)

**Workaround:** Complete one of the following actions:

- **User:** If the user can configure their local network, the user could change the local network IP range to a private IP range that does not conflict with the customer's private network IP range.
- **CylanceGATEWAY administrators:** Create and assign a CylanceGATEWAY service policy to the specific user. In the policy, enable split tunneling and add a CIDR address of 0.0.0.0/0 and the IP range of the local network. **Note:** The local network IP range must be added as more specific CIDR addresses (for example, for the local network of 10.0.0.0/24, add 10.0.0.0/25 and 10.0.0.128/25).

**BlackBerry UEM Connector**

* In environments with the following policy settings, the first time that Android users try to Enable Work Mode the attempt fails. (BIG-11454)

  - UEM policy settings
    - Force always-on VPN
    - Force work apps to only use VPN
  - Gateway Service policy setting: Allow Gateway to run only if the device is managed by BlackBerry UEM or Microsoft Intune

**Workaround:** Click Enable Work Mode.

* After upgrading to CylanceGATEWAY agent for Windows version 2.8.0.9, DNS tunneling does not enable split DNS when a Group Policy Object (GPO) that sets a DNS name resolution policy table (NRPT) or an empty NRPT exists. When split DNS is not enabled, all DNS lookups are performed through the tunnel. (BIG-11032)

To confirm if a GPO exists, verify whether the Windows registry key "DnsPolicyConfig" is present at HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\.

* After you connect the Cylance Endpoint Security to your BlackBerry UEM Cloud instance, the status of the BlackBerry UEM Connector remains at "In progress". (UES-12931)

**Workaround:** Refresh the Connectors screen.
On iOS devices that are running CylancePROTECT Mobile app version 2.12.0.3252 or later and BlackBerry UEM Client version earlier than 12.47.3265, and the UEM Client is updated to 12.47.3265 or later the BlackBerry Infrastructure identifies the device as a new activation. (UESAPP-3841)

**Workaround:** Deactivate and reactivate the CylancePROTECT Mobile app.

---

**Device**

* After upgrading to CylanceGATEWAY agent for macOS version 2.8.0.13, Work Mode and Safe Mode may not establish a connection. (BIG-11186)

**Workaround:** Complete one of the following actions:

- Disable Work Mode and then enabled Work Mode.
- Restart the device.

If Work Mode is enabled when the CylancePROTECT Mobile app for iOS updates, a “CylanceGATEWAY is disconnected” message is displayed and users are unable to connect to CylanceGATEWAY. (BIG-8649)

**Workaround:** Start the CylancePROTECT Mobile app or tap the pop-up message.

When you try to reauthenticate the CylanceGATEWAY agent, you might receive a "Sign-in failed" error. (EID-19203)

**Workaround:** Temporarily change your default browser or clear the browser cache.

When environments are configured for device posture validation, macOS users receive an error message when they try to enable work mode if the CylancePROTECT Mobile app is installed but not activated. The CylanceGATEWAY agent log file logs a 403 and the following error message: "error": "NotEntitled", "detail": "Endpoint requires protect". (BIG-7848)

**Workaround:** Complete the following steps:

1. Make sure that the CylancePROTECT Mobile app is installed and activated.
2. Close and open the CylanceGATEWAY agent.
3. Click **Enable Work Mode**.
Users may experience connectivity issues when the CylanceGATEWAY agent is installed on a computer running Windows Subsystem for Linux (WSL) due to a known issue where WSL does not accommodate the MTU of the network interfaces in Windows. (BIG-5509)

**Workaround:** Users with WSL2 can work around this issue using the following commands.

1. Check the MTU WSL2 assigned to the (virtual) "eth0" interface. Note the 1500.

```bash
$ ip link show dev eth0
6: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
```

2. As root in WSL2, set the MTU to match that of CylanceGATEWAY's IPv4 tunnel interface.

```bash
$ sudo ip link set dev eth0 mtu $(powershell.exe -Command "(Get-NetIPInterface -InterfaceAlias "BlackBerry Gateway" -AddressFamily IPv4).NlMtu" | grep -m1 -oE '[0-9]+')
```

3. Confirm that the MTU was changed. Note the 1420.

```bash
$ ip link show dev eth0
6: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1420 qdisc mq state UP mode DEFAULT group default qlen 1000
link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
```

**Agent**

Windows users only receive the Connection Blocked notification popup message the first time they try to access a blocked website. (BIG-8578)
# CylanceAVERT release notes

## What's new in CylanceAVERT 1.2 (April 2023)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for keyword dictionary</td>
<td>You can now upload a keyword dictionary when creating a data type in this release of CylanceAVERT. A keyword dictionary is a text file that contains all of the keywords for an information protection data type. All keywords in a keyword dictionary must be entered on a separate line in the text file. For more information, see <a href="#">Add a data type</a> in the setup guide.</td>
</tr>
<tr>
<td>Alerts view integration</td>
<td>CylanceAVERT alerts can now be surfaced in the Alerts view of the Cylance Endpoint Security console. For more information, see <a href="#">View and manage aggregated alerts</a> in the administration guide.</td>
</tr>
<tr>
<td>CylanceAVERT policy enhancements</td>
<td>You can now view if an assigned user policy has been applied to that user and their devices by selecting the user in the Cylance Endpoint Security console. For more information, see <a href="#">View CylanceAVERT user details</a> in the Administration guide.</td>
</tr>
<tr>
<td>Data collection enhancements</td>
<td>Non-ASCII filenames are now valid in evidence upload headers.</td>
</tr>
<tr>
<td>Dashboard enhancements</td>
<td>You can now select the CylanceAVERT custom dashboard when you are adding a new dashboard. The CylanceAVERT custom dashboard includes all of the supported CylanceAVERT widgets. This release adds the &quot;Evidence Locker files by date added&quot; dashboard widget.</td>
</tr>
</tbody>
</table>
| Support for partially analyzed files | This release adds the following support for partially analyzed files:  
  - You can use the Partially Analyzed Files view to view a list of files that have been partially analyzed and no sensitive information was detected. The file will display in this view with an alert stating that the file was only partially analyzed.  
  - If a file is partially analyzed and sensitive information is detected, it will be treated the same as a fully analyzed file and will display in the File Inventory, Events view, and Evidence Locker. However, an icon displays beside the file in the tables and detailed views with an alert stating that the file was only partially analyzed. |
| File inventory enhancements | You can now group files in the file inventory based on the following parameters:  
  - Group by users  
  - Group by devices  
  - Group by data types  

Using these group parameters will display the users, devices, or data types name as well as the number of sensitive files associated with that group in the file inventory. This list is sorted by the number of sensitive files in descending order. You can click on the users, devices, or data types name to view detailed information about the sensitive files. |
# What's new in CylanceAVERT 1.0 (January 2023)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive data scanning</td>
<td>CylanceAVERT can scan files uploaded to USB drives, internet browsers, and email attachments, as well as scan the body content of an email message for company data that the administrator defined as sensitive in the information protection policies. An email notification will be sent for data exfiltration events.</td>
</tr>
<tr>
<td>Information protection policies</td>
<td>Administrators can specify the conditions that must be met to trigger the policy violation, the allowed domains for the policy, and the actions to take when a policy has been violated. See Information Protection in the BlackBerry Avert Administration and Overview Guide for more information.</td>
</tr>
<tr>
<td>CylanceAVERT events</td>
<td>When the conditions are met to trigger a policy violation, information about that data exfiltration event display in the CylanceAVERT events view. The events view shows detailed information about the event including the data and time of the event, the location that the file was exfiltrated to, the number of policies that were violated, and the user of the device where the event occurred. See BlackBerry Avert Events in the BlackBerry Avert Administration and Overview guide for more information.</td>
</tr>
<tr>
<td>Information protection settings</td>
<td>Administrators can use the information protection settings to configure the sensitive data that they want to monitor for by adding templates and data types to use in an information protection policy. Administrators can also define the browser and email domains that will be allowed and trusted, manage the evidence that they want to collect for data exfiltration events, and specify how long the evidence should be available. Specified email addresses can also be sent notifications of data exfiltration events. See Information protection settings in the BlackBerry Avert Administration and Overview guide for more information.</td>
</tr>
<tr>
<td>File inventory</td>
<td>The CylanceAVERT file inventory creates a record of all the sensitive files in an organization through a file trawling process. See File Inventory in the BlackBerry Avert Administration and Overview Guide for more information.</td>
</tr>
<tr>
<td>Evidence locker</td>
<td>Administrators can use the evidence locker to view details of the files that have been involved in exfiltration events and download the files to their local storage for auditing purposes. See Evidence locker in the BlackBerry Avert Administration and Overview guide for more information.</td>
</tr>
</tbody>
</table>

# CylanceAVERT fixed issues

## Fixed issues in CylanceAVERT 1.2

- The Custom Time function on the "Information Exfiltration Events" widget was still usable when the function was turned off. (DLP-7663)
- Read-only users will now see "No permission" when they are viewing information protection widgets that they are not authorized to see. (DLP-7489)
If you clicked on some items on the Data Types tab for the "Top exfiltration events by category" widget, you were redirected to an empty events table. (DLP-7603)

If you clicked on a removable media device from the "Top Exfiltration Events by Location" widget, you were redirected to an empty events table. (DLP-7294)

### Fixed issues in CylanceAVERT 1.0

<table>
<thead>
<tr>
<th>Issue</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you saved an information protection policy, you were redirected to the Cylance Endpoint Security dashboard page.</td>
<td>(DLP-6573)</td>
</tr>
<tr>
<td>The information protection user and devices policies are now applied every hour, instead of every 24 hours.</td>
<td>(DLP-6102)</td>
</tr>
<tr>
<td>Only domains with 2 or 3 characters (for example .ca or .com) were accepted when adding allowed domains in the information protection settings.</td>
<td>(DLP-6097)</td>
</tr>
<tr>
<td>The file inventory will now only detect and display files that include sensitive data types that were specified in the information protection policies, instead of all of the sensitive files on the endpoint. This will reduce the number of sensitive files in the file inventory.</td>
<td>(DLP-5978)</td>
</tr>
<tr>
<td>The CylanceAVERT icon on the management console menu bar was replaced with a question mark on some occasions.</td>
<td>(DLP-5549)</td>
</tr>
</tbody>
</table>

### CylanceAVERT known issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>If a user that has not been added to Cylance Endpoint Security logs in to a computer that has CylanceAVERT installed, the user will be automatically added to Cylance Endpoint Security.</td>
<td></td>
</tr>
<tr>
<td>If a user attaches a sensitive file to an email message in Gmail and cancels the email message before sending it, an exfiltration event will still be triggered because Google will upload the file to a web server regardless of the email that is being sent.</td>
<td></td>
</tr>
<tr>
<td>If a user quits the CylanceAVERT app from the Windows system tray, they will not receive a Windows notification when an exfiltration event occurs.</td>
<td></td>
</tr>
<tr>
<td>If a Microsoft Outlook personal folder file (.pst) is stored in a network drive, CylanceAVERT will cause your desktop to shut down or restart unexpectedly (BSOD).</td>
<td>(DLP-8698)</td>
</tr>
<tr>
<td><strong>Workaround:</strong> The .pst file should be moved to a location on the desktop.</td>
<td></td>
</tr>
<tr>
<td>Filtering predefined templates does not display the proper results.</td>
<td>(DLP-8285)</td>
</tr>
<tr>
<td>CylanceAVERT does not support local users (non Active Directory users).</td>
<td>(DLP-8262)</td>
</tr>
<tr>
<td>The Custom Time function on the &quot;Information Exfiltration Events&quot; widget is still usable when the function is disabled.</td>
<td>(DLP-7663)</td>
</tr>
</tbody>
</table>
The following are known issues that relate to widgets:

- If you click on some items on the Data Types tab for the "Top exfiltration events by category" widget, you will be redirected to an empty events table. (DLP-7603)
- If you click on an removable media device from the "Top Exfiltration Events by Location" widget, you will be redirected to an empty events table. (DLP-7294)

During an exfiltration event involving a USB drive, the temporary copy of the sensitive file is a different size than the original file. (DLP-7494)

If CylanceAVERT is reinstalled on an endpoint, the device information displays the incorrect enrollment date and time. (DLP-7278)

In Firefox, developer tools are disabled. (DLP-6302)

If a user sets a USB or shared folder as the default location for downloads in a browser, the user may receive an exfiltration event notification even if the location where the file will be saved has not been specified. This is due to the browser creating a temp file on the USB or shared folder. (DLP-5399)

**Workaround:** Do not configure a USB device or a shared folder as the default location for all browser downloads. For example, in Chrome, do the following:

1. Open Chrome browser.
2. In the search bar, type `chrome://settings/downloads`.
3. Under the Location section, click "Change" and choose a location that is not a USB device or shared folder.

CylanceAVERT does not support directly synchronizing with Microsoft Azure Active Directory for user onboarding. As of the 1.0 beta release, CylanceAVERT only supports user onboarding using on-premises Active Directory through the BlackBerry Connectivity Node. (DLP-5366)

A custom data type cannot be deleted if it is used in an information protection policy. (DLP-5319)

If policies are assigned to a user, and then all of those policies are removed, the user will be deleted from CylanceAVERT. (DLP-5253)

You will receive an error when you check the access status of a file with a path longer than 260 characters. (DLP-5050)

The CylanceAVERT extension for Google Chrome is not immediately added after CylanceAVERT is installed. CylanceAVERT will prompt you to close the Chrome browser during installation. (DLP-2182)

When an administrator deletes a file from the Evidence Locker, they cannot see that the files have been removed until the file service updates the Evidence Locker. This can take up to 24 hours to complete. UI enhancements are planned for a future release to communicate this to the administrator when files are deleted. (DLP-2115)

Sensitive data is not detected when it is used in the file name. (DLP-1221)
Legal notice

©2023 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible “AS IS” and “AS AVAILABLE” and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the “Third Party Products and Services”). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, WARRANTIES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, WARRANTIES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED.

YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES
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 HEREBIN; 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.