



CylanceHYBRID

Administration Guide

2.0.2

Contents

- What is CylanceHYBRID?..... 5**
- CylanceHYBRID architecture..... 6**
- Setting up the CylanceHYBRID application.....7**
- CylanceHYBRID system requirements..... 8**
 - Firewall configuration.....9
 - Considerations for managing CylanceHYBRID..... 10
- Installing the CylanceHYBRID application.....12**
 - CylanceHYBRID files and license..... 12
 - Importing a CylanceHYBRID configuration..... 12
 - Export a CylanceHYBRID 1.x configuration..... 12
 - Configuration settings exported from CylanceHYBRID 1.x..... 12
 - Install Kubernetes and the container environment for CylanceHYBRID while connected to the Internet..... 13
 - Install Kubernetes and the container environment for CylanceHYBRID using a downloaded setup file..... 14
 - Install the CylanceHYBRID application..... 15
- Upgrading your CylanceHYBRID version.....17**
 - Upgrade a CylanceHYBRID version 2.x to a higher version..... 17
 - Upgrade a CylanceHYBRID version 1.x to version 2.x..... 17
- Configuring the CylanceHYBRID application.....19**
 - Configure DNS..... 19
 - Configure CylanceHYBRID..... 19
 - Active Directory sign-in types.....21
- Use the CylanceHYBRID console.....23**
 - CylanceHYBRID log files..... 23
 - Download a support bundle from the CylanceHYBRID console.....24
 - Download a support bundle from the command line on the CylanceHYBRID instance.....24
- Using the CylanceHYBRID Status page..... 25**
 - Sign in to the Status page.....25
 - Update an SSL certificate.....25
 - Change the SSL Certificate Cipher mode..... 25
 - Configure a proxy server..... 26

Enable or disable Maintenance Mode.....	26
Enable or disable the cache.....	26
Change the logging level.....	26
Change the password of the local user account.....	27

Installing the agents that communicate with CylanceHYBRID..... 28

Steps to install the device agents that communicate with CylanceHYBRID.....	28
Installing agents on Windows devices.....	29
Import the CylanceHYBRID CA certificate.....	29
If you will install CylanceOPTICS, add registry entries on the Windows device.....	29
Install the CylancePROTECT Desktop agent on the Windows device.....	30
Install the CylanceOPTICS agent on the Windows device.....	31
Installing agents on macOS devices.....	32
Install the CylanceHYBRID CA certificate on the macOS device.....	32
Create a macOS configuration file.....	33
Install the CylancePROTECT Desktop agent for macOS.....	33
Install the CylancePROTECT Desktop agent for macOS from the command line.....	34
Install the CylanceOPTICS agent for macOS.....	34
Installing agents on Linux devices.....	35
Convert and distribute the CylanceHYBRID CA certificate.....	35
Create the config_defaults.txt file.....	38
Install the Linux agent.....	38
Install the CylanceOPTICS agent on the Linux device.....	39

Troubleshooting..... 41

The CylancePROTECT Desktop agent is not communicating with CylanceHYBRID.....	41
The CylanceOPTICS agent is not communicating with CylanceHYBRID.....	41
The CylanceHYBRID application is not communicating with the Cylance Endpoint Security management console.....	42
The browser is reporting an insecure webpage.....	42

Third-party products and licenses..... 43

Legal notice..... 45

What is CylanceHYBRID?

CylanceHYBRID offers next-generation protection to organizations with restricted Internet access. Some organizations operate with limited Internet access due to design or operational circumstances. These organizations use restricted networks, a private cloud, or operate in remote areas with limited connectivity.

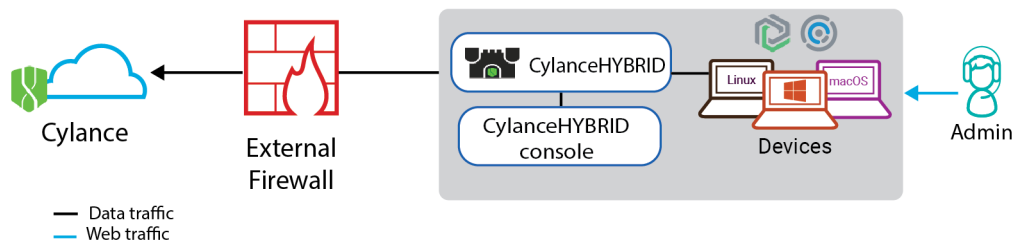
CylanceHYBRID facilitates security-related communication between the cloud and local infrastructure without exposing the local network to the wider Internet. The standard configuration of CylancePROTECT Desktop and CylanceOPTICS requires devices to individually communicate with the cloud. CylanceHYBRID requires only a single connection to the cloud.

CylanceHYBRID is deployed as a single instance. CylanceHYBRID does not currently support multi-node clusters for load balancing or high availability.

This guide covers installing, configuring, and monitoring your CylanceHYBRID application. This guide also covers the installation parameters required to configure your CylancePROTECT Desktop and CylanceOPTICS agents to communicate with your CylanceHYBRID application. All other CylancePROTECT Desktop and CylanceOPTICS related information for the management console are provided in the [documentation for Cylance Endpoint Security](#). For more information about installing the agents for CylancePROTECT Desktop and CylanceOPTICS, see the [Cylance Endpoint Security Setup Guide](#).

CylanceHYBRID architecture

The CylanceHYBRID architecture is designed to help protect your private network with restricted internet access.



Component	Description
CylanceHYBRID	CylanceHYBRID is deployed as a single instance that provides security protection to organizations with restricted Internet access. CylanceHYBRID secures communications between the Cylance cloud and your local infrastructure.
CylanceHYBRID console	The Cloud-based CylanceHYBRID console allows you to view the version history, set certain configuration parameters (for example, set the number of CylanceOPTICS agents), perform troubleshooting steps, view license information and configuration yaml files of the Kubernetes pods, and deploy CylanceHYBRID app updates.
Devices with the CylancePROTECT Desktop agent and CylanceOPTICS agent	<p>The CylancePROTECT Desktop agent and CylanceOPTICS agent must be installed on a device (endpoint) to protect the device. CylancePROTECT Desktop and CylanceOPTICS support Windows, macOS, and Linux operating systems.</p> <p>The CylanceOPTICS agent deploys sensors to the device OS to monitor and collect data that is used to identify threats and trigger automated responses.</p>

Setting up the CylanceHYBRID application

Step	Action
1	Review the CylanceHYBRID system requirements .
2	Install the CylanceHYBRID application .
3	Configure the CylanceHYBRID application .
4	Install the CylancePROTECT Desktop and CylanceOPTICS agents on the devices.

CylanceHYBRID system requirements

Some requirements vary depending on the number of agents that are installed in your environment. For example, if you have both CylancePROTECT Desktop and CylanceOPTICS agents, you will need 8 CPU cores and 12 GB of RAM.

Item	Description
Operating systems	<p>Ubuntu</p> <ul style="list-style-type: none">• 18.04*• 20.04 (requires Docker version 19.03.10 or higher)• 22.04 (requires Containerd 1.5.10 or higher, or Docker version 20.10.17 or higher)• 24.04 (requires Containerd package pre-installed) <p>Red Hat Enterprise Linux (RHEL)</p> <ul style="list-style-type: none">• 7.4*, 7.5*, 7.6*, 7.7*, 7.8*, 7.9• 8.0*, 8.1*, 8.2*, 8.3*, 8.4*, 8.5*, 8.6, 8.7*, 8.8, 8.9• 9.0, 9.1*, 9.2, 9.3, 9.4, 9.5 <p>Note:</p> <ul style="list-style-type: none">• *This version is deprecated because it is no longer supported by its creator. We continue to support it, but support will be removed in the future.• RHEL 8.x and 9.x require Containerd.
CPU cores	<p>3.0 GHz processor (Intel Xeon or later)</p> <ul style="list-style-type: none">• 4 cores - Supports up to 10,000 CylancePROTECT Desktop agents only; no CylanceOPTICS agents• 8 cores - Supports up to 10,000 CylancePROTECT Desktop and CylanceOPTICS agents
RAM	<ul style="list-style-type: none">• 8 GB RAM - Supports up to 10,000 CylancePROTECT Desktop agents only; no CylanceOPTICS agents• 12 GB RAM - Supports up to 10,000 CylancePROTECT Desktop and CylanceOPTICS agents
Disk space	100 GB of space specifically for CylanceHYBRID, not including operating system
root or sudo	Use root or sudo access to install CylanceHYBRID.
Internet connection	The CylanceHYBRID application requires an Internet connection. Devices that communicate with CylanceHYBRID do not need an Internet connection.
Web browser support	<ul style="list-style-type: none">• Google Chrome (latest 2 versions)• Mozilla Firefox (latest 2 versions)• Safari (latest 2 versions)• Microsoft Edge (latest version)

Item	Description
Certificate for HTTPS communication	Use a certificate from a certificate authority (CA) to ensure a secure connection between your CylanceHYBRID console and your devices. While a self-signed certificate will work with CylanceHYBRID, this is less secure than a CA certificate. If you must use a self-signed certificate, BlackBerry recommends using it for testing environments only, and not for production environments.
DNS entry	DNS entry for the CylanceHYBRID application.
IP Address	The IP address of the CylanceHYBRID host must be a static IP address and not changed after installation.

Firewall configuration

During installation, configure the following domains for your firewall so that your online installation of the CylanceHYBRID application succeeds. All outbound connections are using TCP port 443.

For an online installation, you must make the `amazonaws.com` domain accessible. For an offline installation, you can only configure the `amazonaws.com` domain for your firewall. You can copy the IP ranges to allow from [this JSON file](#). For more information, see [AWS IP address ranges](#).

You must also make the following domains accessible for an online installation:

- `hub.docker.com`
- `k8s.gcr.io`
- `registry.k8s.io`

Domain	IP Address
kurl.sh	162.159.135.41
	162.159.136.41
k8s.kurl.sh	50.19.197.213
	54.236.144.143
	162.159.135.41
	162.159.136.41
replicated.app	162.159.133.41
	162.159.134.41
	2606:4700:7::a29f:8529
	2606:4700:7::a29f:8629
api.replicated.com	162.159.137.43
	162.159.138.43
	2606:4700:7::a29f:892b
	2606:4700:7::a29f:8a2b

Domain	IP Address
get.replicated.com	34.194.217.225 34.200.116.158 162.159.137.43 162.159.138.43 2606:4700:7::a29f:892b 2606:4700:7::a29f:8a2b
proxy.replicated.com	162.159.137.43 162.159.138.43 2606:4700:7::a29f:892b 2606:4700:7::a29f:8a2b
registry.replicated.com	162.159.137.43 162.159.138.43 2606:4700:7::a29f:892b 2606:4700:7::a29f:8a2b
registry-data.replicated.com	This domain resolves to Amazon CloudFront addresses which may change periodically.

Considerations for managing CylanceHYBRID

CylanceHYBRID is deployed as a single instance. CylanceHYBRID does not currently support multi-node clusters for load balancing or high availability.

Item	Description
CylanceHYBRID local user account password	<p>Currently, there is no mechanism to reset or recover the password unless you have configured CylanceHYBRID to use Microsoft Active Directory.</p> <ul style="list-style-type: none"> • If Active Directory is not configured and you lose the password, you must reinstall CylanceHYBRID. • If Active Directory is configured, an authorized CylanceHYBRID user can use their work credentials to sign in and change the CylanceHYBRID local user account password. <p>For more information, see Change the password of the local user account.</p>
Communication through another CylanceHYBRID application	A CylanceHYBRID application cannot communicate to or through another CylanceHYBRID application.
Static IP address	CylanceHYBRID does not support management-console static IP addresses.

Item	Description
Cylance API	The Cylance API cannot be used to modify the CylanceHYBRID application.
Cylance Endpoint Security management console	A CylanceHYBRID application appears in the Cylance Endpoint Security management console, but currently it cannot be managed from the console.
Devices connected to CylanceHYBRID	Devices configured to communicate with CylanceHYBRID must be able to communicate with the DNS host name that you created for CylanceHYBRID over TCP port 443. After a device is registered with the CylanceHYBRID console, disconnecting the device from the corporate network (for example, taking a laptop home), results in the device being offline. In offline mode, agents will continue to function as designed, using the last policy update received while the device was online.
Virtualization high availability	<p>If your virtualization application has a redundancy feature, you should use it to provide failure protection against hardware and operating-system outages for your CylanceHYBRID environment. As an example, see VMware's article on high availability on their website.</p> <p>However, the active node and redundant node(s):</p> <ul style="list-style-type: none"> • must have the same fully qualified domain name (FQDN) and IP address • cannot be running at the same time

Installing the CylanceHYBRID application

The CylanceHYBRID 2.0 application uses Kubernetes and containers so that you can deploy it using a variety of virtual-machine software, such as VMware ESXi, Microsoft Hyper-V, Citrix Xen, and Nutanix AHV. CylanceHYBRID requires a virtual machine running the Ubuntu operating system. This allows you to deploy operating-system updates (for example, security updates) as needed and gives you more control over the virtual machines that run CylanceHYBRID.

CylanceHYBRID files and license

You can download the CylanceHYBRID files and license from the Cylance Endpoint Security management console.

Item	Description
Installation bundle	You require this installation bundle if you want to install the CylanceHYBRID application using a downloaded setup file . Bundle name: cylance-hybrid-2004.tgz
License	BlackBerry provides this license and it is available in the Cylance Endpoint Security management console.

Importing a CylanceHYBRID configuration

CylanceHYBRID 2.0 allows you to import configurations from previous versions of CylanceHYBRID when you migrate to CylanceHYBRID 2.0. The export option is available in CylanceHYBRID versions 1.4.15 and later. CylanceHYBRID 2.0 will import all settings from the configuration file, including the hostname, certifications, and LDAP settings. If any of the settings are different or have been changed in the new instance, the import will fail. For agents that were connected to your previous CylanceHYBRID virtual appliance to connect to the new CylanceHYBRID instance, the hostname, certificates, and name of the new CylanceHYBRID instance must all be the same as the previous instance.

To install CylanceHYBRID 2.0, see [Install Kubernetes and the container environment for CylanceHYBRID while connected to the Internet](#) or [Install Kubernetes and the container environment for CylanceHYBRID using a downloaded setup file](#).

Export a CylanceHYBRID 1.x configuration

If you are migrating to the CylanceHYBRID 2.0 application, you can export your configuration settings from the Status page of a CylanceHYBRID 1.x installation.

You can import the configuration when you install the CylanceHYBRID 2.0 application. For more information, see [Configure CylanceHYBRID](#).

1. On the Status page, click the **Export** link. An alert message appears.
2. Click **Export**. The CylanceHYBRID configuration file is saved to your computer.

Configuration settings exported from CylanceHYBRID 1.x

When you export a CylanceHYBRID 1.x configuration, the configuration file includes the following settings.

Component	Settings exported
CylanceHYBRID Info	<ul style="list-style-type: none"> • Device name • SSL certificate • SSL certificate ciphers
Network Settings	<ul style="list-style-type: none"> • Appliance proxy • Proxy host • Proxy port • Proxy username • Proxy password
Cache Settings	<ul style="list-style-type: none"> • Cache the following files
Active Directory Integration	<ul style="list-style-type: none"> • Connection • Base DN • Group DN • CA certificate

Note: When you export a CylanceHYBRID 1.x configuration, the configuration file does *not* include the following settings.

Component	Settings not exported
CylanceHYBRID Info	<ul style="list-style-type: none"> • Cache space • CylanceHYBRID version
Network Settings	<ul style="list-style-type: none"> • IP assignment • IP address • Subnet mask • Default gateway • DNS servers
Maintenance Mode	<ul style="list-style-type: none"> • Maintenance mode (the default setting is Off)
Logs	<ul style="list-style-type: none"> • Logging level (the default setting is Informational Only)

Install Kubernetes and the container environment for CylanceHYBRID while connected to the Internet

To install CylanceHYBRID, you need to follow these steps to download and install the Kubernetes and container environment. The installation process can take more than 40 minutes to complete.

The following example installation uses the Ubuntu 20.04 OS.

The installation of CylanceHYBRID includes some third-party components and applications. See our [Third-party products and licenses](#).

Before you begin:

- Review the [CylanceHYBRID system requirements](#).
 - Verify that you have root or sudo access to the virtual machine that you will install the CylanceHYBRID application on.
1. In the Cylance Endpoint Security management console, on the menu bar, click **Settings > Deployments**.
 2. In the **Product** drop-down list, select CylanceHYBRID.
Download buttons for a license key file and installation script file appear below.
 3. Download the license key file (`license.yaml`) and the installation script file (`hybrid-online-install.txt`).
 4. Sign in to the virtual machine. You must have root or sudo access.
 5. Open a command prompt. The command prompt should have a buffer of at least 50 lines to see the CylanceHYBRID console address and password that is automatically generated during installation.
 6. Copy the commands from the installation script file into your command prompt and press **Enter**.
 7. A series of questions is displayed. Answer yes (**Y**) to all questions. If no action is taken, the installation process automatically accepts the default settings.
 8. If multiple network interfaces are detected, select the one that CylanceHYBRID will use and press **Enter**. The installation process fetches the required packages and installs CylanceHYBRID. You might see NOKEY warnings. You can ignore them.

Important:

When the installation completes, save the Kotsadm address and the login password that are displayed in the terminal window. These are required when you sign in to the CylanceHYBRID console on the virtual machine, but they will not be shown again.

After you finish: Using the Kotsadm address displayed when the installation completes, [Install the CylanceHYBRID application](#).

Install Kubernetes and the container environment for CylanceHYBRID using a downloaded setup file

You can install Kubernetes and the container environment for CylanceHYBRID using a setup file that you download from the Cylance Endpoint Security management console. The installation process can take 10 minutes or more to complete.

The installation of CylanceHYBRID includes some third-party components and applications. See our [Third-party products and licenses](#).

Before you begin:

- Review the [CylanceHYBRID system requirements](#).
 - Verify that you have root or sudo access to the virtual machine that you will install the CylanceHYBRID application on.
 - Ensure that you have a stable Internet connection.
1. In the Cylance Endpoint Security management console, on the menu bar, click **Settings > Deployments**.
 2. In the **Product** drop-down list, select CylanceHYBRID.
 3. In the **OS** drop-down list, select your Linux distribution.
 4. In the **Version** drop-down list, select your version of CylanceHYBRID.
 5. In the **Format** drop-down list, select the .tgz file that corresponds to your Linux distribution.
 6. Click **Download** to download the file and make note of the file name. It might take several minutes to download.

7. Below the drop-down lists, download the license key file (`license.yaml`).
8. Sign in to the virtual machine. You must have root or sudo access.
9. Open a command prompt and change the directory to the location of the downloaded file.
10. Enter `tar xf <downloaded_file_name>.tar.tgz` and press **Enter**. This extracts the contents of the tar file.
11. Enter `cat install.sh | sudo bash -s airgap` and press **Enter**.
12. A series of questions displays. Answer yes (**Y**) to all questions. If no action is taken, the installation process will automatically accept the defaults.
13. If multiple network interfaces are detected, select the one that CylanceHYBRID will use and press **Enter**. The installation process fetches the required packages and installs the CylanceHYBRID application. You might see NOKEY warnings; these can be ignored.

Important:

When the installation completes, save the Kotsadm address and the login password that are displayed in the terminal window. These are required when you sign in to the CylanceHYBRID console on the virtual machine, but will not be shown again.

After you finish: Using the Kotsadm address displayed when the installation completes, perform [Install the CylanceHYBRID application](#).

Install the CylanceHYBRID application

After you have installed Kubernetes and the container environment on the VM, you are ready to install the CylanceHYBRID application on it.

Before you begin:

- You must [Install Kubernetes and the container environment for CylanceHYBRID while connected to the Internet](#) or [Install Kubernetes and the container environment for CylanceHYBRID using a downloaded setup file](#) and obtain the Kotsadm address and password displayed at the end of the installation.
 - Verify that you have root or sudo access to the virtual machine where you will install the CylanceHYBRID application.
1. In a browser, enter the Kotsadm address and press **Enter**. An example address could be `http://192.0.2.124:8800`.
 2. Click **Continue to Setup**. You might receive a connection warning.
 3. On the CylanceHYBRID console certificate and key upload page, you can configure secure communication with the CylanceHYBRID console. You can upload your own SSL certificate and private key, or you can use the self-signed TLS certificate provided by the console. Do one of the following:
 - If you want to use the self-signed TLS certificate provided by the console, click **Skip & continue**.
 - If you want to use your own SSL certificate and private key, specify the host name, private key, and SSL certificate, and click **Upload & continue**. The host name should be the fully qualified domain name that matches the SSL certificate (for example: `login.hybrid.com`). The certificate and key can be the same one that is used to install Kubernetes and the container environment.
 4. Enter the Kotsadmin login password that you obtained at the end of the container environment installation and click **Log in**.

If you want to change your password, use the `kubectl kots reset-password default` command.
 5. Drag and drop your license file (`.yaml`), or browse and select it.
 6. Click **Upload license**.
 7. Select your CylanceOPTICS client option and click **Continue**.

8. Verify your preflight checks and click **Continue**.

The Application page is displayed. Your CylanceHYBRID application is installed.

9. To see the status of the installation, check the readiness status in the Application information card. When the CylanceHYBRID application is ready, click the CylanceHYBRID button to launch the Status page.

After you finish: To configure the CylanceHYBRID application, see [Configuring the CylanceHYBRID application](#).

Upgrading your CylanceHYBRID version

You can upgrade your current version of CylanceHYBRID to the most recent version.

Upgrade a CylanceHYBRID version 2.x to a higher version

This task applies only to upgrading your installation from one version of the CylanceHYBRID 2.x application to a higher 2.x version.

To upgrade your installation from a version of CylanceHYBRID 1.x to a version of CylanceHYBRID 2.x, see [Upgrade a CylanceHYBRID version 1.x to version 2.x](#).

Before you update the CylanceHYBRID application, you must put the CylanceHYBRID application into maintenance mode.

Before you begin: As a best practice, it is recommended that you take a snapshot of your CylanceHYBRID application in case you need to revert back to it.

1. Update the Kubernetes and the container environment by following the same steps as the installation, except you do not need the `license.yaml` file because it is already in the environment and you do not need to reconfigure secure communication.
 - [Install Kubernetes and the container environment for CylanceHYBRID while connected to the Internet](#)
 - [Install Kubernetes and the container environment for CylanceHYBRID using a downloaded setup file](#)
2. In a browser, enter the Kotsadm address and press **Enter**. For example: `https://<Kotsadm_address>:8000`.
3. Verify the version that you're upgrading from and readiness status of the installation in the Application information card.
4. Sign in to your CylanceHYBRID Status page (for example: `https://login.hybrid.com`).
5. In the Maintenance Mode section, enable **Maintenance Mode**.
6. Sign in to the CylanceHYBRID console (for example, `https://login.hybrid.com:8800/app/hybrid`).
7. Click the **Version history** tab.
8. Click **Check for update**. The page displays details about available releases.
9. Click **Deploy** for the release that you want to upgrade to.
10. Verify your preflight checks and click **Continue**.

The "Maintenance Mode Enabled Check" will fail if CylanceHYBRID is not in maintenance mode. When you have enabled maintenance mode, click **Re-run** to re-run the preflight checklist.

Upgrade a CylanceHYBRID version 1.x to version 2.x

You cannot upgrade in place an installation of CylanceHYBRID version 1.x to a CylanceHYBRID version 2.x; architectural changes in the application prevent this type of upgrade.

Instead, you will need to install CylanceHYBRID version 2.x on a new server. For more information, see [Installing the CylanceHYBRID application](#).

Before you begin:

You can perform this upgrade with or without migrating the settings from the previous server to the new server. Regardless of the method chosen:

- The new instance of CylanceHYBRID 2.x must have the same hostname as the original CylanceHYBRID 1.x server.
- On each managed device, you must add the certificate for the CylanceHYBRID 2.x instance to the keystore so that the agent will trust the CA that issues the certificate.

Do one of the following:

Task	Steps
Install a new instance of CylanceHYBRID and migrate the settings from a previous instance.	<p>You can migrate a configuration from an instance of CylanceHYBRID version 1.4.15 and later to a new instance of CylanceHYBRID version 2.x without having to re-register the CylancePROTECT Desktop or CylanceOPTICS agents.</p> <p>The option to migrate a configuration was not available prior to CylanceHYBRID version 1.4.15.</p> <p>For more information, see Importing a CylanceHYBRID configuration.</p>
Install a new instance of CylanceHYBRID without migrating the settings from a previous instance.	<p>You can manually set up the a new instance of CylanceHYBRID version 2.x.</p> <p>However, to ensure that this new instance will properly manage your current devices without having to re-install on each device the CylancePROTECT Desktop agent, and (optionally) the CylanceOPTICS agent, you must configure the new server with the same settings, display name and installation key as the existing CylanceHYBRID 1.x server.</p>

Configuring the CylanceHYBRID application

The CylanceHYBRID application and your CylancePROTECT Desktop agents that will connect through CylanceHYBRID should be registered to the same tenant. This will register CylanceHYBRID as a device in your Cylance Endpoint Security management console so that it appears as a device in your Devices list.

Note: The CylanceHYBRID application requires an Internet connection. Devices that communicate with CylanceHYBRID do not need an Internet connection.

Note: The CylanceHYBRID application is deployed as a single instance. The application does not currently support multi-node clusters for load balancing or high availability.

Configure DNS

For the virtual machine that hosts your CylanceHYBRID application, create a DNS entry on your network. Work with your IT department, if necessary.

- Create a hostname for the application (for example, login.hybrid.com).
- The DNS entry also requires the IP address of the virtual machine that hosts your CylanceHYBRID application.

Configure CylanceHYBRID

Before you begin:

Take a snapshot of the virtual machine that hosts the application in case the configuration fails, including invalid SSL certificate uploads. This will allow you to revert to the snapshot instead of having to reinstall the application.

1. In the Cylance Endpoint Security management console, click **Settings > Application**.
2. In the **Installation Token** field, copy the token.
3. In the CylanceHYBRID console (for example, login.hybrid.com:8800), in the **Application** section, click **CylanceHYBRID**. Make sure that the status is Ready.
4. On the Welcome screen, click **Let's Get Started**. The Import Hybrid Config page displays.
5. If you want to import a CylanceHYBRID configuration file from an existing CylanceHYBRID instance, do the following sub-steps. For more information, see [Importing a CylanceHYBRID configuration](#). Otherwise, continue to Step 6.
 - a) Enable **Import**.
 - b) Drag and drop your CylanceHYBRID configuration file, or browse to the file and select it.
 - c) Click **Save & Continue**.
6. Perform one of the following tasks:

Task	Steps
Generate a certificate signing request (CSR) that will be submitted to a certificate authority (CA) to use with the CylanceHYBRID application.	<p>a. Fill in the form:</p> <ol style="list-style-type: none"> 1. In the Common Name field, enter the common name, derived from the fully qualified domain name (FQDN) for the application. For example, if the FQDN is <code>https://hybrid.cylance.com</code>, the common name is <code>hybrid.cylance.com</code>. 2. In the Subject Alternative Name field, enter any alternative names to use for the application, such as <code>hybrid-alt.cylance.com</code>. The Common Name will be added automatically as a Subject Alternative Name. 3. In the Organization Name field, enter the legal name of the organization. 4. In the Organizational Unit field, enter the unit name. This could be a department name. 5. In the City field, enter the city where the organization is located. 6. In the State / Province field, enter the state or province where the organization is located. Do not use an abbreviation. 7. In the Country field, enter the two-letter ISO abbreviation for the country. <p>b. Click Generate CSR. This creates a <code>cert_request.csr</code> file in the Downloads folder. Send this file to your CA who should then send back an SSL certificate.</p> <p>Example: <code>hybrid.cylance.crt</code>.</p> <p>After you generate the CSR, the text at the top of the page changes to a pending status and includes a link where you can re-download the CSR and Step 2 displays at the bottom of the page.</p> <p>Note: If you click Generate CSR again, a new private key will be generated, and you will need to provide the latest CSR to the CA.</p> <p>c. In the Step 2: Upload certificate from CA box, upload your SSL certificate.</p> <p>Note: For more information on a possible certificate issue, visit support.blackberry.com/community to read article 98224.</p>
Upload an SSL certificate and key generated on a computer other than the one that hosts the CylanceHYBRID application.	<p>a. Turn off Generate private key and CSR. For more information on certificate guidelines, see our Certificate Guidelines.</p> <p>b. Drag and drop the certificate in the Upload certificate box, or click Browse for a file and select the certificate.</p> <p>c. Drag and drop the key in the Upload key box, or click Browse for a file and select the key.</p> <p>(Optional) To have the CylanceHYBRID application and status page use the same certificate as the CylanceHYBRID admin console:</p> <ol style="list-style-type: none"> a. Turn off Generate private key and CSR. b. Turn on Use CylanceHYBRID admin console TLS certificate and key. c. Click Save.

7. Click **Save & Continue**. The Active Directory Integration page displays.

8. To disable Active Directory Integration or to configure it after the initial setup of the CylanceHYBRID application, turn off **Use Active Directory** and go to step 11. For more information, see [Using the CylanceHYBRID Status page](#).

To add Active Directory/LDAP Integration, do the following:

- a) In the **Active Directory Host** field, enter the FQDN of the server that hosts Active Directory. This is a TLS requirement. If you enter an IP address for an LDAP server or the hostname instead of an FQDN, the configuration will fail. The FQDN must be configured in DNS.
- b) In the **Port** field, enter the port number of the LDAP server.
- c) In the **Base DN** field, enter the base distinguished name (DN) used as a base for the LDAP search to look for the user DN.
- d) In the **Group DN** field, enter the group DN used to perform an LDAP search to check if the user is a member of the group DN.
- e) In the **Upload certificate to enable TLS** field, upload the SSL certificate used to perform a TLS connection when binding to the LDAP server. The certificate must be Base64 encoded.
- f) Click **Test Connection**. A Test Active Directory Connection dialog displays.
- g) Enter a username and password and click **Test Connection**. A message displays informing you that the connection was successful. If the connection failed, use the red text that appears on the dialog to troubleshoot and resolve the issue.

To test the connection, use either the UPN login or sAMAccountName login:

UPN Login Example: *username@domainname.com* (hadmin@onprem-cylance.com)

sAMAccountName Login Example: *domain\username* (onprem-cylance\hadmin)

9. Click **Save & Continue**. The Set a password to access the CylanceHYBRID Status page displays.
10. Enter and confirm your new password, and click **Save & Continue**. Follow the password requirements. The **Configuration Step 1 of 2: Enter Info** page displays.



Warning: Ensure that you note down this password. Currently, there is no mechanism to reset or recover the password.

11. Enter or paste your Installation Token.
12. Enter a Device Name. This name will appear in the Cylance Endpoint Security console as a device.
13. Type an FQDN for the virtual machine that hosts the CylanceHYBRID application. The FQDN must match the one in the DNS entry. For example, an FQDN could be login.hybrid.com or hybrid.com.
14. To include a proxy server, turn on **Connect Appliance to Proxy**. Enter the proxy-server information, including a proxy username and password.
15. Click **Save & Continue**. The **Configuration Step 2 of 2: Confirm Info** page displays.
16. If your CylanceHYBRID setup information is correct, click **Confirm & Finish**. The CylanceHYBRID Setup Complete page displays.
17. Click **Go to Status Page**. You are automatically signed in to the CylanceHYBRID Status page. For future sign ins, the CylanceHYBRID username is *cylance*.

When you have finished configuring the CylanceHYBRID application, it will appear in your Cylance Endpoint Security management console, under Devices, with the Device Name that you assigned in Step 12.

Active Directory sign-in types

Users can authenticate to the CylanceHYBRID console using a User Principal Name (UPN) login or a sAMAccountName login (if supported by the Active Directory server).

Login Type	Description
UPN login	To authenticate with the user's UPN, the format of the username is <i>username@domain.com</i> (for example: hadmin@onprem-cylance.com).
sAMAccountName login	To authenticate with the user's sAMAccountName, the format of the username is <i>domain\username</i> (for example: onprem-cylance\hadmin).
Local user account	<ul style="list-style-type: none"> • When LDAP/AD is enabled, you must sign in using the local account with the following username: <code>.\cylance</code>. • When LDAP/AD is not enabled, you can sign in using the local account with one of the following usernames: <code>.\cylance</code> or <code>cylance</code>.

Use the CylanceHYBRID console

You can use the CylanceHYBRID console to see the version history, set certain configuration parameters, perform troubleshooting steps, view licenses, files, and registry settings, and deploy updates.

To sign in to the console, use <https://<fqdn>:8800>. Replace <fqdn> with the IP address or the fully qualified domain name of your virtual machine that hosts the CylanceHYBRID application.

In the CylanceHYBRID console, do any of the following:

Task	Tab	Step
View the CylanceHYBRID Status page.	Dashboard	In the Application section, click CylanceHYBRID . Because you are already signed in to the console, you will pass directly into the status page.
Check for updates of the CylanceHYBRID application.	Dashboard or Version history	Click Check for Update .
Deploy an update of the application.	Version history	See Upgrade a CylanceHYBRID version 2.x to a higher version .
Set the total number of CylanceOPTICS agents.	Config	Click an option and click Save config .
Download support bundles for troubleshooting.	Troubleshoot	See CylanceHYBRID log files .
View License details and synchronize license.	License	To synchronize your license, click Sync license .
View the configuration yaml files of the Kubernetes pods.	View files	To view a file: a. Click one of three sections: upstream, base, or overlays. b. Click a file name to display the file contents in the window.
Change the Registry settings.	Registry settings	This feature is not currently supported. BlackBerry does not recommend changing these values.
Add a node.	Cluster Management	Currently, this feature is not supported and the user should not use this button.
Drain a node.	Cluster Management	Currently, this feature is not supported and the user should not use this button.

CylanceHYBRID log files

You can use the CylanceHYBRID log files to troubleshoot issues.

To change the logging level, see [Change the logging level](#).

Download a support bundle from the CylanceHYBRID console

A support bundle contains the log files for the CylanceHYBRID application and the platform that the application is built on.

1. In the CylanceHYBRID console, click the **Troubleshoot** tab.
2. If you have generated previous support bundles, those bundles appear in a list. To generate a new bundle, do the following:
 - a) Click **Generate a support bundle**.
 - b) Click **Analyze CylanceHYBRID**.
3. If you have not generated previous support bundles, click **Analyze CylanceHYBRID**.
4. After the log collection has completed, click the support bundle to view it in the console or click **Download bundle** to download it.

Download a support bundle from the command line on the CylanceHYBRID instance

A support bundle contains the log files for the CylanceHYBRID application and the platform that the application is built on. If you do not have access to the console, a support bundle can be obtained from the command prompt.

Before you begin:

Install the support-bundle packages on the virtual machine that hosts the CylanceHYBRID application.

```
curl https://krew.sh/support-bundle | bash
```

1. Open the command prompt.
2. Run the following command in your cluster to generate the support bundle: `kubectl support-bundle secret/default/kotsadm-hybrid-supportbundle --redactors=configmap/default/kotsadm-redact-spec/redact-spec,configmap/default/kotsadm-hybrid-redact-spec/redact-spe`
3. After the command has completed, a high-level support bundle analysis is displayed. Click **s** to save the high-level analysis. This saves only the high-level analysis as a .txt file.
4. Click **q** to quit.

The full support bundle is saved in the working directory that was present when you ran the command. You can download the support bundle .tar.gz and the .txt file from that location.

Using the CylanceHYBRID Status page

The CylanceHYBRID Status page displays system information, provides an interface for modifying network settings, turning Maintenance Mode on or off, changing the logging level, and allowing you to clear or disable the cache. You can also configure Active Directory integration from this page.

Sign in to the Status page

If you are already signed in to the console, you can access the Status page directly from the CylanceHYBRID console. On the Dashboard tab, in the Application section, click **CylanceHYBRID**.

To sign in to the CylanceHYBRID Status page directly, without first signing in to the console, go to <https://<fqdn>/configui/status> and use the same credentials that you use to sign in to the console. Replace [<fqdn>](#) with the fully qualified domain name of your virtual machine that hosts the CylanceHYBRID application.

Note:

The username, cylance, and the password was set during the installation process for CylanceHYBRID. For more information, see [Install Kubernetes and the container environment for CylanceHYBRID while connected to the Internet](#) or [Install Kubernetes and the container environment for CylanceHYBRID using a downloaded setup file](#).

Update an SSL certificate

For more information on certificate guidelines, see [Certificate Guidelines](#).

For more information on a possible certificate issue, visit support.blackberry.com/community to read article 98224.

1. On the Status page, beside SSL Certificate, click **Update**.

2. Do one of the following:

- Download the CSR for the current key and upload the updated certificate from the Certificate Authority.
- Generate a new CSR and upload the certificate you receive from the Certificate Authority. For steps to generate a CSR, see [Configure CylanceHYBRID](#).

Note: If you complete the form and click **Generate CSR**, the generated CSR will be bound to a new private key and your original certificate will no longer work.

- Upload an SSL certificate and key. For steps to upload the certificate and key, see [Configure CylanceHYBRID](#).

Change the SSL Certificate Cipher mode

By default, CylanceHYBRID uses TLS 1.2+ (Strict Mode) to secure its communications over computer networks. If you need to support legacy operating systems that require TLS 1.0, TLS 1.1, or TLS 1.2, you can revert to TLS 1.0+ (Legacy Mode).



1. On the Status page, beside SSL Certificate Ciphers, click **Change**. If you are switching to Legacy Mode, a dialog prompts you before the change is made.

2. Select whether to enable the change.

- If you want to change back to Strict Mode, you can click **Change** again.

Configure a proxy server

You can configure the CylanceHYBRID application to communicate through a proxy server.

1. On the Status page, in the Network Settings section, click .
2. Turn on **Appliance Proxy**.
3. Configure the settings for the proxy server:
 - a) In the **Proxy Host** field, enter the FQDN or IP address for the proxy server.
 - b) In the **Proxy Port** field, enter the port number used to communicate with the proxy server.
 - c) In the **Proxy Username** field, enter the username used to authenticate to the proxy server.
 - d) In the **Proxy Password** field, enter the password used to authenticate to the proxy server.
4. Click .

Enable or disable Maintenance Mode

You can pause activity between the CylanceHYBRID application and the CylancePROTECT Desktop devices so that you can update the application without interruption.

1. On the Status page, in the Maintenance Mode section, turn Maintenance Mode on or off.
2. If you turned Maintenance Mode off, click **Yes, Turn Maintenance Mode Off**.

Enable or disable the cache

You can enable or disable the caching function. The cache includes the following files:

- CylancePROTECT agents
- Centroids
- Global lists
- Policies

If you suspect that items stored in cache are corrupt or incomplete, you can clear the cache.





CAUTION: Clearing the cache removes all Cylance agent updates, Centroids, Global lists, and Policies.

1. On the Status page, in the Cache Settings section, turn caching on or off.
2. If you turned caching off, click **Disable caching**.
3. To clear the cache:
 - a) Click **Clear Cache**.
 - b) Click **Clear the cache**.

Change the logging level

Logging is enabled automatically and cannot be disabled. By default, the logging level is set at the "Informational Only" level.

Note: Debug logging can consume a large amount of storage space. Select the Debug (verbose logging) level only when troubleshooting CylanceHYBRID issues.

1. On the Status page, in the Logs section, click .
2. In the **Logging Level** drop-down list, select the logging level.
3. Click  to save the setting.

Change the password of the local user account

An authorized user can change the password for the CylanceHYBRID local user account (cylance).

1. In the top-right corner of the Status page, click the user profile icon next to the user name.
2. Click **Change password**.
3. Enter a new password and confirm it in the fields.
4. Click **Submit**.

Installing the agents that communicate with CylanceHYBRID

When you use CylanceHYBRID, the CylancePROTECT Desktop agent requires installation parameters to configure the agent to communicate with your CylanceHYBRID application. For information about legacy Windows OS support, see the [Legacy OS Support for CylancePROTECT](#) page.

The following list provides information that you should know about using the CylancePROTECT Desktop agent and the CylanceOPTICS agent with CylanceHYBRID. All other agent features are described in the [Cylance Endpoint Security documentation](#).

- Use the most recent versions of the CylancePROTECT Desktop agent and the CylanceOPTICS agent, if CylanceOPTICS will also be installed. For more information, see the [compatibility information](#) for the Cylance Endpoint Security desktop agents.
- The following minimum versions of the agents are required on the devices:
 - CylancePROTECT Desktop version 1574/1578 or later
 - CylanceOPTICS version 2.5.2100 or later

Note:

- CylanceHYBRID 2.0 does not support devices that are running Windows XP, Windows 2003, or Windows Server 2012 R2 due to a lack of AES cipher support on these operating systems. For more information, visit support.blackberry.com/community to read article 95914.
- Currently, CylanceHYBRID 2.0 does not support the CylanceOPTICS agent on macOS devices.
- You must install the CylancePROTECT Desktop agent on the device before you install the CylanceOPTICS agent.
- When you use CylanceHYBRID, the CylancePROTECT Desktop agent requires installation parameters to configure the agent to communicate with your CylanceHYBRID application.
 - For Windows, use the command line.
 - For macOS, create a cyagent_install_token file.
 - For Linux, create the config_defaults.txt file.
- The CA certificate that is used to sign the certificate and key used on your CylanceHYBRID application must be installed on each device in the appropriate keystore for secure HTTPS communication.
- The CylancePROTECT Desktop agent communicates with the CylanceHYBRID application over TCP port 443.
- The CylanceOPTICS agent for Windows communicates with the CylanceHYBRID application over TCP port 8888.

Steps to install the device agents that communicate with CylanceHYBRID

For each device that you will install the CylancePROTECT Desktop agent and (optionally) the CylanceOPTICS agent on:

Step	Action
1	Install the CA certificate that was used to sign the certificate and key used on the virtual machine that hosts the CylanceHYBRID application.

Step	Action
2	Gather the installation parameters for the CylancePROTECT Desktop agent and the CylanceOPTICS agent.
3	Install the CylancePROTECT Desktop agent on the device. For instructions, see: <ul style="list-style-type: none"> • Install the CylancePROTECT Desktop agent on the Windows device • Install the macOS agent or Install the CylancePROTECT Desktop agent for macOS from the command line • Install the Linux agent
4	(Optional) Install the CylanceOPTICS agent on the device. For instructions, see: <ul style="list-style-type: none"> • Install the CylanceOPTICS agent on the Windows device • Install the CylanceOPTICS agent on the Linux device <p>Note: Currently, CylanceHYBRID 2.0 does not support the CylanceOPTICS agent on macOS devices.</p>

Installing agents on Windows devices

This section explains how to install the CylancePROTECT Desktop agent and the CylanceOPTICS agent on Windows devices.

Import the CylanceHYBRID CA certificate

To ensure secure communication between your CylanceHYBRID server and your devices, the CA certificate used to sign the certificate and key used on the server must be installed (trusted) on every device with an agent.

1. Click **Start** and type `mmc`.
2. Press **Enter** and click **Yes**. This starts the Microsoft Management Console.
3. Select **File > Add/Remove Snap-in**.
4. Under **Available snap-ins**, select **Certificates**. Click **Add**.
5. Select **Computer account** and click **Next**.
6. Click **Finish** and click **OK**.
7. Right-click on Trusted Root Certification Authority to expand Certificates.
8. Select **All Tasks > Import** and click **Next**.
9. Click **Browse** and select your CA certificate. Click **Open**.
10. Click **Next > Next > Finish**.
11. When **The import was successful** message displays, click **OK**.
12. Select **File > Save** and click **Save**.
13. Close the console.

If you will install CylanceOPTICS, add registry entries on the Windows device

On Windows devices, you must add two registry entries:

- The first entry configures CylancePROTECT Desktop and CylanceOPTICS to use the CylanceHYBRID proxy server, running on port 8888. The CylanceHYBRID application uses a proxy server to help with communication between CylanceOPTICS devices and the CylanceHYBRID console.
- The second entry disables the CylanceOPTICS cloud fallback feature. By default, CylanceOPTICS attempts to communicate directly with the Cylance cloud when a proxy connection is not available.

Note: You may need to run the command prompt as an administrator.

1. On the device, open a command prompt.
2. To configure CylancePROTECT Desktop and CylanceOPTICS to use the CylanceHYBRID proxy server, running on port 8888, type the following command:

```
reg add HKLM\software\Cylance\Desktop /v ProxyServer /t REG_SZ /d
http://<CylanceHYBRID FQDN>:8888 /f
```

Use `http://` and port 8888 in the command.

3. Press **Enter**. This adds your CylanceHYBRID application information that is used when CylancePROTECT Desktop and CylanceOPTICS are installed.
4. To disable the CylanceOPTICS cloud fallback feature, type the following command:

```
reg add HKLM\software\Cylance\Optics /v DisableProxyBypass /t REG_SZ /d True /f
```

Note: If this key is present, the CylanceOPTICS agent will always attempt to establish a connection through the configured proxy server.

5. Close the command prompt.

Install the CylancePROTECT Desktop agent on the Windows device

You can install the CylancePROTECT Desktop agent from the command line using the "msiexec" or ".exe" installer.

Before you begin:

- Download the CylancePROTECT Desktop installation files from the management console. Click **Settings > Deployments**. From the **Product** drop-down list, select **CylancePROTECT**, and set the target operating system, the agent version, and the file type. Click **Download**.
 - In the management console, copy the installation token from **Settings > Application**.
1. Use the following parameters when you install the CylancePROTECT Desktop agent on Windows devices. These parameters are required to ensure that all agents properly communicate with CylanceHYBRID. Use the DNS name for your CylanceHYBRID application.

Parameter	Example
Example of third-level domain name (login.hybrid.com):	
InstallRegistrationURL=<hybridurl>	InstallRegistrationURL=https://login.hybrid.com
InstallTrustedSuffix=<hybridurlsuffix>	InstallTrustedSuffix=hybrid.com
InstallInfinityURL=<hybridurl>	InstallInfinityURL=https://login.hybrid.com
Example of second-level domain name (hybrid.com):	
InstallRegistrationURL=<hybridurl>	InstallRegistrationURL=https://hybrid.com

Parameter	Example
InstallTrustedSuffix=<hybridurlsuffix>	InstallTrustedSuffix=hybrid.com
InstallInfinityURL=<hybridurl>	InstallInfinityURL=https://hybrid.com

2. Open the command prompt.
3. Run one of the following commands and use your installation parameters for the options:

Task	Steps
msiexec installer	<pre>msiexec /i CylanceProtect_x64.msi /qn PIDKEY=<YourInstallationToken> LAUNCHAPP=1 InstallRegistrationURL=<hybridurl> InstallTrustedSuffix=<hybridurlsuffix> InstallInfinityURL=<hybridurl></pre> <p>For examples on editing the MSI installation file for deployment through Group Policy, see the Editing the MSI Installer using Orca article.</p>
.exe installer	<pre>CylanceProtectSetup.exe /s PIDKEY=<YourInstallationToken> LAUNCHAPP=1 InstallRegistrationURL=<hybridurl> InstallTrustedSuffix=<hybridurlsuffix> InstallInfinityURL=<hybridurl></pre>

Install the CylanceOPTICS agent on the Windows device

CylancePROTECT Desktop must be installed and properly communicating with CylanceHYBRID before you install CylanceOPTICS.

Before you begin: If you did not add the two registry entries before installing CylancePROTECT Desktop, you must do so now.

- First, perform the steps in [Take ownership of the CylancePROTECT Desktop registry folder for Windows](#).
 - Next, perform the steps in [If you will install CylanceOPTICS, add registry entries on the Windows device](#).
 - Finally, return to this procedure.
1. Download the CylanceOPTICS setup file to the device. You can either sign in to the Cylance Endpoint Security management console from the device, or transfer the installation file from an external source (like a USB flash drive) to the device. You can also deploy CylanceOPTICS using a group policy or other software management system.
 2. Double-click **CylanceOPTICSSetup.exe**.
 3. Click **Install**.
 4. When the installation is complete, click **Close**.
 5. Reboot the device.

Take ownership of the CylancePROTECT Desktop registry folder for Windows

Note: Follow this procedure only if you need to make changes to the registry entries after you have installed CylancePROTECT Desktop.

If CylancePROTECT Desktop is already installed, the HKLM\SOFTWARE\Cylance\Desktop folder is not accessible. Use the following procedure to take ownership of the folder and add the registry entries.

1. Open the Registry Editor.
2. Navigate to HKEY_LOCAL_MACHINE > SOFTWARE > Cylance, and right-click the **Desktop** folder.
3. Select **Permissions**.
4. On the **Security** tab, under **Permissions for**, click **Advanced**.
5. For Owner, click **Change**.
6. Type the name of the new owner and click **Check Names**. If the user is an administrator for the device, select Administrators as the new owner.
7. Click **OK**.
8. Click **Replace owner on subcategories and objects**. Make sure the checkbox is selected.
9. Click **OK**.
10. Under **Group or user names**, make sure that the new owner is selected. If the new owner is not visible, refresh the screen. If the new owner is still not visible:
 - a) Click **Add** and add the user.
 - b) Under **Group or user names**, verify that the new owner is visible.
 - c) If the newly added name is not selected as the owner, return to Step 5 to select again the new owner.
11. Under **Permissions**, make sure **Allow** is selected for **Full Control**.
12. Click **OK**. The new owner should now be able to add registry entries. For more information, see [If you will install CylanceOPTICS, add registry entries on the Windows device](#).

Installing agents on macOS devices

This section explains how to install the CylancePROTECT Desktop agent and the CylanceOPTICS agent on macOS devices.

Install the CylanceHYBRID CA certificate on the macOS device

To ensure the secure communication between your CylanceHYBRID server and your devices, the CA certificate used to sign the certificate and the key used on the server must be installed (trusted) on every device with an agent.

1. On the macOS device, copy to or download the root CA certificate. In this example, the file is in the Downloads folder. If you save it to a different folder, you must navigate to that folder in the Terminal and then run the command to add the certificate.
2. Click **Launchpad**.
3. In the search field, type `terminal` and click the Terminal icon.
4. In Terminal, type `cd ./Downloads` and press **Return**.
5. Type `sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain rootCA.crt` and press **Return**. In this example, the root CA certificate is named `rootCA.crt`. If your certificate has a different file name, be sure to type the correct file name in the command before you run it.
6. Type your password and press **Return**.

Create a macOS configuration file

Use the following parameters to create the `cyagent_install_token` plain-text file that is used to configure the agent on your macOS devices. This is required to ensure that all agents properly communicate with CylanceHYBRID. Use the DNS name for your CylanceHYBRID application.

Parameter	Example
Example of third-level domain name (login.hybrid.com):	
<code>InstallRegistrationURL=<hybridurl></code>	<code>InstallRegistrationURL=https://login.hybrid.com</code>
<code>InstallTrustedSuffix=<hybridurlsuffix></code>	<code>InstallTrustedSuffix=hybrid.com</code>
<code>InstallInfinityURL=<hybridurl></code>	<code>InstallInfinityURL=https://login.hybrid.com</code>
Example of second-level domain name (hybrid.com):	
<code>InstallRegistrationURL=<hybridurl></code>	<code>InstallRegistrationURL=https://hybrid.com</code>
<code>InstallTrustedSuffix=<hybridurlsuffix></code>	<code>InstallTrustedSuffix=hybrid.com</code>
<code>InstallInfinityURL=<hybridurl></code>	<code>InstallInfinityURL=https://hybrid.com</code>

Example:


```
echo YourInstallationToken >> cyagent_install_token
echo InstallRegistrationURL=<hybridurl> >> cyagent_install_token
echo InstallTrustedSuffix=<hybridurlsuffix> >> cyagent_install_token
echo InstallInfinityURL=<hybridurl> >> cyagent_install_token
sudo installer-pkg CylancePROTECT Desktop.pkg -target /
```

The following is a example of a completed `cyagent_install_token` file:

```
InstallToken=YourInstallationToken
InstallRegistrationURL=https://login.hybrid.com
InstallTrustedSuffix=hybrid.com
InstallInfinityURL=https://login.hybrid.com
```

Install the CylancePROTECT Desktop agent for macOS

Before you begin:

- Download the CylancePROTECT Desktop installation files from the management console. Click **Settings > Deployments**. From the **Product** drop-down list, select **CylancePROTECT**, and set the target operating system, the agent version, and the file type. Click **Download**.
 - In the management console, copy the installation token from **Settings > Application**.
- Double-click the CylancePROTECT Desktop installation file (.dmg or .pkg) to mount the installer.
 - Double-click  from the CylancePROTECT Desktop user interface to begin the installation.
 - Click **Continue** to verify that the OS and hardware meet the requirements.
 - Click **Continue**.
 - Type the installation token.
 - Click **Continue**.

7. Optionally, change the installation location.
8. Click **Install**.
9. Type your credentials.
10. Click **Install Software**.
11. On the summary screen, click **Close**.
12. Click **OK > Finish**.
13. If you are installing CylancePROTECT Desktop on macOS Catalina, a notification prompts you to allow CylanceUI to display notifications. Click **Allow**.

Install the CylancePROTECT Desktop agent for macOS from the command line

Before you begin:

- Download the CylancePROTECT Desktop installation files from the management console. Click **Settings > Deployments**. From the **Product** drop-down list, select **CylancePROTECT**, and set the target operating system, the agent version, and the file type. Click **Download**.
- In the management console, copy the installation token from **Settings > Application**.
- To set the installation parameters in the configuration file, see [Create a macOS configuration file](#).

Install the macOS agent without the installation token

```
sudo installer-pkg CylancePROTECT.pkg-target/
```

Install the macOS agent with the installation token

```
echo YOURINSTALLTOKEN >cyagent_install_token
sudo installer -pkg CylancePROTECT.pkg-target/
```

Install the CylanceOPTICS agent for macOS

Before you begin:

- Review the [CylanceOPTICS software requirements](#).
 - You must install the CylancePROTECT Desktop agent on devices before you install the CylanceOPTICS agent.
 - If you want to install the CylanceOPTICS agent on macOS Big Sur (11.x) or later devices, see [Configuration requirements for macOS 11.x and later](#).
1. Before you install the CylanceOPTICS agent on devices, you must configure the following on those devices to disable proxy bypass. This is required for CylanceHYBRID environments, as it ensures that the CylanceOPTICS agent always uses a specified proxy server to connect to the CylanceOPTICS cloud services:
 - a) In /Library/Application Support/Cylance/Desktop/registry/LocalMachine/Software/Cylance/Desktop/, add the following to the values.xml file:


```
<value name="ProxyServer" type="string">http://proxy_server_IP:port</value>
```
 - b) In /Library/Application Support/Cylance/Optics/Configuration, create an ExternalConfig.xml file with the following:


```
<?xml version="1.0" encoding="utf-8"?><EnforceProxyServer>true</EnforceProxyServer>
```
 2. In the management console, on the menu bar, click **Settings > Deployments**.
 3. In the **Product** drop-down list, click **CylanceOPTICS**.

4. Select the OS, version, and format, and click **Download**.
5. Using your organization's preferred software distribution method, deploy and run the installation file on devices.

If you want to install the CylanceOPTICS agent using OS commands, see [OS commands for the CylanceOPTICS agent](#).

Installing agents on Linux devices

This section explains how to install the CylancePROTECT Desktop agent and the CylanceOPTICS agent on Linux devices.

Convert and distribute the CylanceHYBRID CA certificate

CylancePROTECT Desktop agents must trust the certificate that the CylanceHYBRID application has been configured with to communicate with the application. Linux agents do not use a central certificate store like Windows or macOS systems. Instead, the Linux agent uses the certificate store from the Mono framework. These certificates must be formatted in a Mono-specific format.

After the x509 certificate is converted into the Mono format, the certificate files can be distributed to Linux devices.

By converting the certificates, you do not need to install Mono on each CylancePROTECT Desktop agent on a Linux device.

Mono for Linux steps

Before you begin:

- You must complete the following steps in a root shell.
 - Install either the **mono-devel** or **mono-complete** package. For instructions, see [the information on the Mono Project website](#). Either Mono package will allow you to complete the steps below.
1. Open Terminal and change directories to the location where your certificate is stored.

Note:

- The certificate must be in Privacy-Enhanced Mail (PEM) format.
- The certificate required is the one that was used to sign the certificate and the key for your CylanceHYBRID application.

2. After you change directories, enter the cert-sync command:

```
cert-sync <YOURCERTIFICATE>
```

where <YOURCERTIFICATE> is your certificate.

Example Output: cert-sync rootCA.crt

```
[root@Example Example]# cert-sync rootCA.crt
Mono Certificate Store Sync - version 6.6.0.161
Populate Mono certificate store from a concatenated list of certificates.
Copyright 2002, 2003 Motus Technologies. Copyright 2004-2008 Novell. BSD licensed.
```

Importing into legacy system store:

I already trust 133, your new list has 1

Certificate added: C=US, 

1 new root certificates were added to your trust store.

Import process completed.

Importing into BTLS system store:

I already trust 133, your new list has 1

Certificate added: C=US, 

1 new root certificates were added to your trust store.

Import process completed.

3. Mono stores the synced certificate to `/usr/share/.mono/new-certs/Trust`.

Note: When you install Mono for Linux, Mono automatically inserts its own certificates into the `/new-certs/Trust` directory.

To locate your target certificate, you can use `ls -ltr` to display the latest modified file at the bottom of the Terminal output. You can use your method of choice to differentiate your target certificate from the other previously inserted certificates.

Example: The certificate highlighted in the red box is the certificate that was synchronized using the above steps. All other certificates were inserted upon installation of Mono.

```
...
...
-rw-r--r--. 1 root root 7223 Dec 10 14:29 ca6e4ad9.0
-rw-r--r--. 1 root root 3033 Dec 10 14:29 c089bbbd.0
-rw-r--r--. 1 root root 4767 Dec 10 14:29 2e4eed3c.0
-rw-r--r--. 1 root root 4793 Dec 10 14:29 c089bbbd.0
-rw-r--r--. 1 root root 4540 Dec 10 14:31 44ff1262.0
```

4. To confirm that a Mono certificate is the correct certificate, view the contents of the certificate file using the following command:

```
cat /usr/share/.mono/new-certs/Trust/<filename>
```

For example:

```
cat /usr/share/.mono/new-certs/Trust/44ff1262.0
```

Confirm that the subject and the fingerprint in the output match the subject and the fingerprint or thumbprint of the correct CA certificate.

5. In each Linux device that will use the application, create the following directory:

```
/usr/share/.mono/new-certs/Trust
```

Note that there is a period (.) before "mono".

This step does not install Mono on the target machine; you are just manually creating the directory.

Example method to create the directory:

```
mkdir -p /usr/share/.mono/new-certs/Trust
```

6. For all Linux devices, copy the synced certificate to the directory that you created in the previous step.

Mono for Windows steps

The following steps use Windows 10 as an example.

Before you begin: Install Mono for Windows. For instructions, see [the information on the Mono Project website](#).

1. In the Start menu, right-click **Open Mono x64 Command Prompt** and select **More > Run as administrator**. For instructions, see the Mono documentation [here](#).
2. Change directories to the location where your certificate is stored.

Note:

- The certificate must be in Privacy-Enhanced Mail (PEM) format.
- The certificate required is the one that was used to sign the certificate and the key for your CylanceHYBRID application.

3. After you change directories, enter the cert-sync command:

```
cert-sync <YOURCERTIFICATE>
```

where <YOURCERTIFICATE> is your certificate.

Example Output: cert-sync rootCA.crt

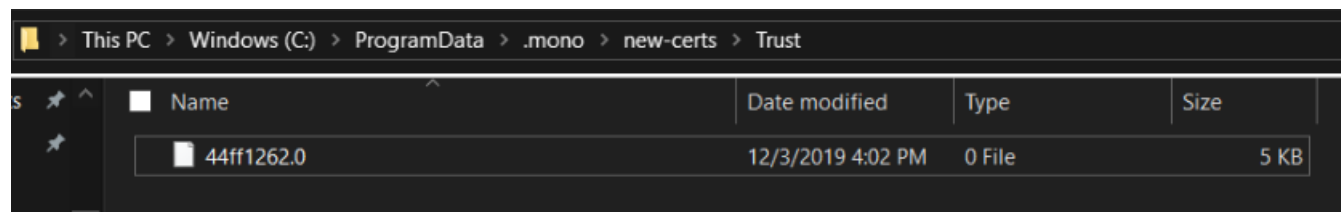
```
C:\Example>cert-sync rootCA.crt
Mono Certificate Store Sync - version 6.4.0.0
Populate Mono certificate store from a concatenated list of certificates.
Copyright 2002, 2003 Motus Technologies. Copyright 2004-2008 Novell. BSD licensed.

Importing into legacy system store:
I already trust 0, your new list has 1
Certificate added:
1 new root certificates were added to your trust store.
Import process completed.

Importing into BTLS system store:
I already trust 0, your new list has 1
Certificate added:
1 new root certificates were added to your trust store.
Import process completed.
```

Mono stores the synced certificates in the ProgramData directory: **C:\ProgramData\.mono\new-certs\Trust**

The Mono certificate will look like this:



To confirm that a Mono certificate is the correct certificate, open the file in a text editor and confirm that the subject and the fingerprint in the output match the subject and the fingerprint or thumbprint of the correct CA certificate.

4. On each Linux device that will use the application, create the following directory:

```
/usr/share/.mono/new-certs/Trust
```

Note that there is a period (.) before "mono".

This step does not install Mono on the target machine; you are just manually creating the directory.

Example method to create the directory:

```
mkdir -p /usr/share/.mono/new-certs/Trust
```

5. For all Linux devices, copy the synced certificate to the directory that you created in the previous step.

Create the config_defaults.txt file

Create the config_defaults.txt file and include the CylanceHYBRID installation parameters.

Before you begin: Before you create the config_defaults.txt file:

- Verify that you have root or sudo access to the device that you will install the agents on. Beginning with Step 1 below, you need to be logged in as root or run the commands as sudo.
1. Enter `sudo bash` and press **Enter**. This launches a shell as root. You can use a different installed shell other than bash if you choose.
 2. Enter `mkdir /opt/cylance` and press **Enter**. This creates the Cylance installation folder. You need to be logged in as root when you run this command, or run it as sudo; otherwise, the command will fail.
 3. Enter `cd /opt/cylance` and press **Enter**.
 4. Enter `echo InstallToken=YourInstallationToken >> config_defaults.txt` and press **Enter**. Replace *YourInstallationToken* with the installation token from the management console.
 5. Enter `echo InstallRegistrationURL=<hybridurl> >> config_defaults.txt` and press **Enter**. Replace *<hybridurl>* with the FQDN for the CylanceHYBRID server (for example, `https://login.hybrid.com`).
 6. Enter `echo InstallTrustedSuffix=<hybridsuffix> >> config_defaults.txt` and press **Enter**. Replace *<hybridsuffix>* with the URL suffix for the CylanceHYBRID server (for example, `hybrid.com`).
 7. Enter `echo InstallInfinityURL=<hybridurl> >> config_defaults.txt` and press **Enter**. Replace *<hybridurl>* with the FQDN for the CylanceHYBRID server (for example, `https://login.hybrid.com`).

Example:

```
echo InstallToken=YourInstallationToken >> config_defaults.txt
echo InstallRegistrationURL=https://login.hybrid.com >> config_defaults.txt
echo InstallTrustedSuffix=hybrid.com >> config_defaults.txt
echo InstallInfinityURL=https://login.hybrid.com >> config_defaults.txt
```

Install the Linux agent

Note: The following steps use a CentOS 7.4 virtual machine and logged in as the root user.

1. Copy synced certificates to the proper directory for all target Linux machines. See [Configure CylancePROTECT Desktop Linux agents](#) for more information.
2. Create the config_defaults.txt file and include the CylanceHYBRID installation parameters.
 - Enter `mkdir /opt/cylance`, then press **Enter**. This creates the Cylance installation folder.

- Enter `cd /opt/cylance`, then press **Enter**.
 - Enter `echo InstallToken=YourInstallationToken > config_defaults.txt`, then press **Enter**. Replace *YourInstallationToken* with the installation token from the Cylance console.
 - Enter `echo InstallRegistrationURL=<hybridurl> >> config_defaults.txt`, then press **Enter**. Replace *<hybridurl>* with the fully-qualified domain name for the CylanceHYBRID server. Example: `https://login.hybrid.com`. See [Examples for the Linux Configuration File](#).
 - Enter `echo InstallTrustedSuffix=<hybridsuffix> >> config_defaults.txt`, then press **Enter**. Replace *<hybridsuffix>* with the URL suffix for the CylanceHYBRID server. Example: `hybrid.com`. See [Examples for the Linux Configuration File](#).
 - Enter `echo InstallInfinityURL=<hybridurl> >> config_defaults.txt`, then press **Enter**. Replace *<hybridurl>* with the fully-qualified domain name for the CylanceHYBRID server. Example: `https://login.hybrid.com`. See [Examples for the Linux Configuration File](#).
3. Navigate to the folder with the CylancePROTECT Desktop Linux agent installation file. For example, if the installation file is in the Downloads folder and you are logged on as root: enter `cd /root/Downloads`, then press **Enter**.
 4. Install the CylancePROTECT drivers and agent software.
Note: This example installs the Linux agent for RHEL 7 / CentOS 7 (el7). Change the RPM file name as needed during installation.
 - a) Type `rpm -ivh CylancePROTECTOpenDriver-<version>.rpm`, then press **Enter**. This installs the CylancePROTECT open driver.
 - b) Type `rpm -ivh CylancePROTECTDriver-<version>.rpm`, then press **Enter**. This installs the CylancePROTECT agent driver.
 - c) Type `rpm -ivh CylancePROTECT.el7.rpm`, then press **Enter**. This installs the CylancePROTECT Desktop Linux agent.
 - d) Optionally, type `rpm -ivh CylancePROTECTUI.el7.rpm`, then press **Enter**. This installs the CylancePROTECT Desktop UI for the Linux agent. The UI is not required to run the agent.

Install the CylanceOPTICS agent on the Linux device

Complete the following steps if the CylancePROTECT Desktop agent is already installed on the Linux device and the device is already communicating with the CylanceHYBRID application.

Before you begin:

- Verify that you are running CylanceHYBRID version 2.0 or later.
 - Verify that the CylancePROTECT Desktop agent is installed and properly communicating with CylanceHYBRID before you install the CylanceOPTICS agent on the device.
 - Use the most recent versions of the CylancePROTECT Desktop agent, and the CylanceOPTICS agent if you will also install CylanceOPTICS. For more information, see the [compatibility information](#) for the Cylance Endpoint Security desktop agents.
1. Download the CylanceOPTICS setup file to the Linux device. You can either sign in to the Cylance Endpoint Security management console from the device, or transfer the installation file from an external source (like a USB flash drive) to the device. You can also use a group policy or other software-management system to deploy the CylanceOPTICS installer.
 2. Configure CylanceHYBRID as the proxy server for CylanceOPTICS. On each CylanceOPTICS endpoint, run the following commands as root or using a root shell:

Task	CLI command
Make the cyoptics.service.d directory	<code>mkdir /etc/systemd/system/cyoptics.service.d</code>
Add the CylanceHYBRID instance to the proxy.conf file	<pre>echo "[Service]" > /etc/systemd/system/cyoptics.service.d/proxy.conf echo "Environment=http_proxy=http:// <cylancehybrid.domain.local>:8888" >> /etc/systemd/system/ cyoptics.service.d/proxy.conf echo "Environment=https_proxy=http:// <cylancehybrid.domain.local>:8888" >> /etc/systemd/system/ cyoptics.service.d/proxy.conf</pre>

3. Use the following command to verify the contents of the file:

```
cat /etc/systemd/system/cyoptics.service.d/proxy.conf
```

The following is a sample output for that command:

```
[Service]
Environment=http_proxy=http://cylancehybrid.domain.local:8888
Environment=https_proxy=http://cylancehybrid.domain.local:8888
```

4. If you make changes to the proxy.conf file after you install CylanceOPTICS, you must restart the cyoptics service for the changes to take effect. Run the following commands as root:
- `systemctl stop cyoptics`
 - `systemctl daemon-reload`
 - `systemctl start cyoptics`
5. Perform one of the following tasks:

Task	Steps
Use the GUI.	<ol style="list-style-type: none"> Double-click the CylanceOPTICS installer. No other parameters or configuration are required. Click Continue. Click Close when the installation is complete.
Use the terminal commands.	<p>Note: Make sure that your version of Linux meets the requirements for CylanceOPTICS. See Requirements: CylanceOPTICS.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> On RHEL/CentOS, SUSE, or Amazon Linux 2, open a terminal window and run the following command: <code>yum install CylanceOPTICS-<version>.rpm</code>, where <code><version></code> is the version of the .rpm file. On Ubuntu, run the following command: <code>dpkg -i cylance-optics-<version>-amd64.deb</code>, where <code><version></code> is the version of the .deb file.


After you finish: For additional information and troubleshooting suggestions, see [Troubleshooting](#).

Troubleshooting

This section provides a list of questions to answer and files to collect when you troubleshoot issues with CylanceHYBRID. This information will help BlackBerry Technical Support to resolve issues.

The CylancePROTECT Desktop agent is not communicating with CylanceHYBRID


Verify the following:

- Make sure that the CylancePROTECT Desktop agent version 1574/1578 or later is installed on the device. To do so, locate the Cylance icon () in the system tray or check the list of apps installed on the device. For more information, see the [compatibility information](#) for the Cylance Endpoint Security desktop agents.
- Make sure the CA certificate used to sign the certificate and key used on your CylanceHYBRID application is installed on the device in the Local Machine Certificate Store.
- Confirm that the device can reach the CylanceHYBRID application over port 443.

The CylanceOPTICS agent is not communicating with CylanceHYBRID

Verify the following items.

For all platforms:

- Make sure that the CylanceOPTICS agent version 2.5.2100 or later is installed on the device. To do so, locate the Cylance icon () in the system tray or check the list of apps installed on the device. For more information, see the [compatibility information](#) for the Cylance Endpoint Security desktop agents.
- Confirm that the device can reach the CylanceHYBRID application over port 8888.

For Windows:

- Make sure the agent is configured to communicate with your CylanceHYBRID application. In the command prompt, run this command to check the registry key on the device:

```
reg query HKLM\software\Cylance\Desktop /v ProxyServer
```

The value should show the CylanceHYBRID DNS name and port number. For example:

```
HKEY_LOCAL_MACHINE\software\Cylance\Desktop ProxyServer REG_SZ http://login.hybrid.com:8888
```

For Linux:

- Confirm that you have configured CylanceOPTICS to use CylanceHYBRID as a proxy. See [Install the CylanceOPTICS agent on the Linux device](#).
- After performing the steps in that procedure, run the following command as root to verify whether CylanceOPTICS has established a connection to CylanceHYBRID over port 8888:
 - `ss -ano | head -1 ; ss -ano | grep :8888`

- The expected output is:

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
tcp	ESTAB	0	0	<Local IP>:46170	<CylanceHYBRID IP>:8888	

The CylanceHYBRID application is not communicating with the Cylance Endpoint Security management console

- Make sure the CylanceHYBRID application is running.
- If your network uses a firewall or proxy, make sure to allow all Cylance hosts for proper communication. For a list of Cylance hosts to allow, based on your region, visit support.blackberry.com to read KB-66572.

The browser is reporting an insecure webpage

If the browser generates an error for an insecure web page when you try to sign in to the CylanceHYBRID console, install the CA certificate that is used to sign the certificate and the key used on your CylanceHYBRID application in the Local Machine Certificate Store on the device.

Third-party products and licenses

CylanceHYBRID includes third-party code licensed to BlackBerry for redistribution under open-source licenses. This list of licenses for the open-source software packages refers to the third-party software incorporated into the CylanceHYBRID application.

Package Type	Third-Party Software
OS packages	<ul style="list-style-type: none">• containerd• docker registry• ekco• kotsadm• kubernetes• minio• openebs• weave
Python	<ul style="list-style-type: none">• aioredis• aioredlock• async-timeout• asynccpg• attrs• bcrypt• blinker• certifi
	<ul style="list-style-type: none">• cffi• chardet• click• cryptography: Apache license or BSD license• Flask• Flask-Bcrypt• Flask-Cors• Flask-login
	<ul style="list-style-type: none">• gunicorn• hiredis• idna• itsdangerous• jinja2• MarkupSafe• marshmallow

Package Type	Third-Party Software
	<ul style="list-style-type: none"> • psycpg2 • pyasn1 • pyasn1-modules • pycparser • pycurl: Copying-LGPL or Copying-MIT • pyOpenSSL • python-ldap
	<ul style="list-style-type: none"> • redis • requests • six • tornado • urllib3 • werkzeug
JavaScript	<ul style="list-style-type: none"> • axios • babel-polyfill • classnames • form-data • lodash • material-ui • normalize.css
	<ul style="list-style-type: none"> • pretty-bytes • prop-types • react • react-dom • react-dropzone • react-tippy • toastr • whatwg-fetch

Legal notice

©2024 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, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE 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 HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

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

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

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

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

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

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

Published in Canada