CylanceHYBRID
Administration Guide

1.4.15

Contents

Overview

CylanceHYBRID offers next-generation protection to organizations with restricted Internet access. Some companies operate with limited Internet access due to design or operational circumstances. Such businesses 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 BlackBerry Protect Desktop requires devices to individually communicate with the cloud. CylanceHYBRID requires only a single connection to the cloud.

This guide covers installing, configuring, and monitoring your CylanceHYBRID virtual appliance. This guide also covers the BlackBerry Protect Desktop agent installation parameter required to configure your agents to communicate with your CylanceHYBRID virtual appliance. All other BlackBerry Protect Desktop-related information for the console is provided in the BlackBerry Protect Desktop Administrator Guide (separate document). Additional agent information is provided in the BlackBerry Protect Desktop Installation Guide.

Note:

CylanceHYBRID requires BlackBerry Protect Desktop agent version 1480 or later to be installed on the devices.

Virtual appliance system requirements

The CylanceHYBRID virtual appliance minimum, dedicated system requirements are:

System requirement	Description
Hypervisor support	CylanceHYBRID is a virtual appliance and supports VMware ESXi version 6.5 and later.
RAM	4 GB (See CylanceHYBRID agent capacity for specific RAM requirements for running BlackBerry Protect Desktop + BlackBerry Optics agents simultaneously)
CPU	3.0 GHz two-cores (Intel Xeon processors or later)
Free disk space	100 GB **Note:** CylanceHYBRID virtual appliance RAM and CPU settings are configurable in VMware. Disk space is not configurable.
Internet connection	The CylanceHYBRID virtual appliance requires an Internet connection. Endpoints that communicate with CylanceHYBRID do not need an Internet connection.
Web browser support	• Google Chrome (latest 2 versions) • Mozilla Firefox (latest 2 versions) • Apple Safari (latest 2 versions) • Microsoft Edge (latest version) • Microsoft Internet Explorer 11 (with latest updates, Compatibility Mode disabled)
Certificate for HTTPS communication	Use a certificate from a certificate authority (CA) to ensure a secure connection between your CylanceHYBRID console and your endpoints. 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, not production environments.
DNS entry	DNS entry for the CylanceHYBRID virtual appliance

Note:

• CylanceHYBRID requires BlackBerry Protect Desktop agent version 1480 or later to be installed on the endpoints.
• The CylanceHYBRID.ova file displays as a Red Hat Enterprise Linux 7 (64-bit) Guest operating system when imported into VMware ESXi. This is by design and the Guest operating system should not be changed to any other operating system, such as CentOS 7 (64-bit).

CylanceHYBRID agent capacity

One CylanceHYBRID virtual appliance with the minimum system requirements can support:

• A maximum of 10,000 devices running BlackBerry Protect Desktop only

- A maximum number of devices running both BlackBerry Protect Desktop and BlackBerry Optics simultaneously based on the following RAM requirements (available in v1.4.7 and later):

CylanceHYBRID Virtual Appliance RAM Allocated	Supports up to...
4 GB RAM	2,000 endpoints
8 GB RAM	5,000 endpoints
16 GB RAM	10,000 endpoints

CylanceHYBRID considerations

Item	Description
CylanceHYBRID local user account password	Currently there is no mechanism to reset or recover the password unless you have configured CylanceHYBRID to use Microsoft Active Directory. If Active Directory is not configured, losing a password will require reinstalling CylanceHYBRID. If Active Directory is configured, an authorized CylanceHYBRID user using their corporate credentials can log in and change the CylanceHYBRID local user account password. See Change the local user account password for more information.
Communicate through another CylanceHYBRID application	A CylanceHYBRID application cannot communicate to or through another CylanceHYBRID application.
Static IP address	CylanceHYBRID does not support Cylance console static IP addresses.
Cylance API	The Cylance API cannot be used to modify the CylanceHYBRID application.
Cylance console	A CylanceHYBRID application appears on the Cylance console, but currently cannot be managed from the console.
Devices connected to CylanceHYBRID	Devices configured to communicate with a CylanceHYBRID must be able to communicate with the DNS host name you created for CylanceHYBRID over TCP port 443. After a device is registered with the console, removing a device, like 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	If your virtualization application has a high availability feature, you should use it to provide failure protection against hardware and operating system outages for your CylanceHYBRID environment. For example, see VMware's article here.

Import and configure the CylanceHYBRID virtual appliance

The CylanceHYBRID virtual appliance must be configured for your Cylance console by using the same installation token used for installing the BlackBerry Protect Desktop agent. This will register CylanceHYBRID as a device in your console and this will appear as a device in your Device list.

Note:

CylanceHYBRID requires an Internet connection. Endpoints that communicate with CylanceHYBRID do not need an Internet connection.

Configure DNS

For your CylanceHYBRID virtual appliance, create a DNS entry on your network (work with your IT department, if necessary).

- Create a hostname for the virtual appliance. Example: login.hybrid-cylance.com
- The DNS entry will also need the IP address of the OVA operating system.

  - **DHCP:** If you use DHCP, the IP address for CylanceHYBRID displays on the login page of the virtual appliance.

    Note: After importing the OVA file, if the IP address does not appear, try restarting the virtual appliance. In VMware vSphere, click the Restart icon, or select **Actions > Power > Restart**.

  - **Static IP:** If you use a static IP address, use that in the DNS entry. Also follow the Import OVA and Configure Static IP Address task.

Import OVA and configure static IP address

This task is for CylanceHYBRID instances that need to use a static IP address. If DHCP is used, see Import OVA and configure DHCP.

Note: This example procedure uses the VMware vSphere Client to import the OVA and configure a static IP address. If you are using VMware ESXi 6.7 or later, or are using VMware ESXi 6.5 managed by vCenter Server 6.x, you can use the following procedure or the VMware OVF tool to import the OVA and configure a static IP address. If you are using a stand-alone version of VMware ESXi 6.5, the Customize Template screen in this procedure does not display so you will need to use the VMware OVF Tool to import the OVA and configure a static IP address. For information about using the VMware OVF Tool, see Configure a Static IP using the OVF Tool.

1. In VMware vSphere, select **Actions > Deploy OVF Template**. The Deploy OVF Template window displays.
2. Select the OVA file. Click **Next**.
3. Type a name for the virtual machine, and select a location. Click **Next**.
4. Select a computer resource.Click **Next**.
5. Review the details. Click **Next**.
6. Select storage and other settings. Click **Next**.
7. Select a network. Click **Next**.
8. On Customize Template, type in the IP Address, Network Mask, Default Gateway, and DNS information.
9. Click **Next**. Review the settings.
10. Click **Finish**.

Import OVA and configure DHCP

This task is for CylanceHYBRID instances that use DHCP. If a static IP address is used, go to the Import OVA and Configure Static IP Address task.

1. In VMware vSphere, select **Actions > Deploy OVF Template**. The Deploy OVF Template window displays.
2. Select the OVA file. Click **Next**.
3. Type a name for the virtual machine, and select a location. Click **Next**.
4. Select a computer resource. Click **Next**.
5. Review the details. Click **Next**.

6. Select storage and other settings, Click **Next**.
7. Select a network. Click **Next**.
8. Click **Next**. Leaving the Custom Template fields blank will enable DHCP on the virtual appliance. Review the settings.
9. Click **Finish**.

Configure CylanceHYBRID

1. Log in to the Cylance console and copy your Installation Token. The token is on the Application page (**Settings > Application**).
2. Start the CylanceHYBRID file (OVA). In VMware vSphere, click the Power On icon, or select **Actions > Power > Power On**.

   Note: It is recommended to take a snapshot of the virtual appliance in the event configuration fails, including invalid SSL certificate uploads. This will allow reverting back to the snapshot instead of reimporting the appliance.
3. Open a web browser and go to the following URL. Replace `<fqdn>` with the fully qualified domain name (FQDN) from the DNS entry. Example: `https://login.hybrid-cylance.com/configui/config`. For a web browser, use a system that can communicate with the CylanceHYBRID virtual appliance.

   • `https://<fqdn>/configui/config`
4. From the welcome screen, click **Let's Get Started**. The Secure Your Connection page displays with Generate a CSR enabled by default.
5. To generate a certificate signing request (CSR) that will be submitted to a certificate authority (CA) to use with the CylanceHYBRID virtual appliance:

   Note:

   To use an SSL certificate and key generated on a computer other than CylanceHYBRID, go to step 6.

   • Fill out the form.
     a. **Common Name:** Derived from the fully qualified domain name (FQDN) for the virtual appliance. For example, if the FQDN is `https://hybrid.cylance.com`, then the common name is `hybrid.cylance.com`.
     b. **Subject Alternative Name:** Any alternative names to use for the virtual appliance, such as *hybrid-alt.cylance.com*. Please note that the Common Name will be added automatically as a Subject Alternative Name. Click **Add** after typing an alternative name to add it.
     c. **Organization Name:** Enter the legal name of the organization.
     d. **Organizational Unit:** This could be a department name.
     e. **City:** Enter the city where the organization is located.
     f. **State / Province:** Enter the state or province where the organization is located. Do not use an abbreviation.
     g. **Country:** Enter the two letter ISO abbreviation for the country.
   • Click **Generate CSR**. This creates a `cert_request.csr` file in the Downloads folder. Send this to your CA who should then send back an SSL certificate.

     Example: `hybrid.cylance.crt.`

     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.

     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.
   • Upload the SSL certificate to the **Step 2: Upload certificate from CA** box.

- Continue to step 7.

6. To upload an SSL certificate and key generated on a computer other than CylanceHYBRID, turn off the **Generate a CSR** toggle.

   Note: To generate a certificate signing request (CSR), go to step 5.

   - Drag the certificate to the **Upload certificate** box or click **Browse for a file** and select the certificate.
   - Drag the key to the **Upload key** box or click **Browse for a file** and select the key.

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

8. To add Active Directory/LDAP Integration, enter your AD information.

   Note: To disable Active Directory Integration, click the **Use Active Directory** toggle (green = enabled, grey = disabled). If needed, you can configure Active Directory after initial setup of the virtual appliance. For more information, see CylanceHYBRID Status page.

   - **Active Directory Host:** Active Directory configuration requires the FQDN due to a TLS requirement. Using an IP address for LDAP server configuration will fail. The FQDN must be configured on the Domain Server.
   - **Port:** The port number of the LDAP server.
   - **Base DN:** The base distinguished name (DN) used as a base for the LDAP search to look for the user DN.
   - **Group DN:** The group DN used to perform an LDAP search to check if the user is a member of the group DN.
   - **Upload certificate to enable TLS:** The secure socket layer (SSL) certificate used to perform a transport layer security (TLS) connection when binding to the LDAP server. The certificate must be Base64 encoded.

9. Click **Test Connection**. A Test Active Directory Connection dialog displays.

10. Enter a username and password in the fields, then 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. A description of common configuration error messages and their meaning is available on the Knowledge Base at CylanceHybrid Active Directory Configuration Error Messages.

    Note:

    To test the connection, use either the UPN Login or SAM Account Login:

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

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

11. Click **Save & Continue**. The Set a password to access CylanceHYBRID page displays.

12. Type and confirm your new password, then click **Save & Continue**. Follow the password requirements. The Configuration Step 1 of 2: Enter CylanceHYBRID Info page displays.

13. Type or paste your Installation Token.

14. Type a Device Name. This name will appear in the console as a device. Allowed characters include letters, numbers, -, _, ., !, @, #, $, %, ^, &, *, (,), {, }, [,], +, $.

15. Type in a fully qualified domain name (FQDN) for the CylanceHYBRID. The FQDN must match the one in the DNS entry. For example, a fully qualified domain name could be `login.hybrid.com` **or** `hybrid.com`.

16. To include a proxy server, click the **Connect Appliance to Proxy** toggle to enable it. Enter the proxy server information, including a proxy username and password.

    Note: CylanceHYBRID uses Tinyproxy for the web proxy server. Tinyproxy only supports lowercase letters, numbers, periods, dashes, and underscores for the proxy username and password.

17. Click **Save & Continue**. The Configuration Step 2 of 2: Confirm Info page displays.

18. If your CylanceHYBRID setup information is correct, click **Confirm & Finish**. The CylanceHYBRID Setup Complete page displays.

19. Click **Go to Status Page**. You are automatically logged in to the CylanceHYBRID Status page. For future log ins, the CylanceHYBRID username is `cylance`.

After you finish:

When configuring the CylanceHYBRID virtual appliance is complete, it will appear in your console, under Devices, with the Device Name you assigned in step 12.

CylanceHYBRID console login using Active Directory

Users can authenticate to the CylanceHYBRID console using a UPN logon or a SamAccountName logon (if supported by the AD server).

Login Type	Description
UPN login	To authenticate using a UPN login, use an email logon. In the following example, username is the User UPN login and email.com is the domain name.
	username@email.com (*Example:* hadmin@onprem-cylance.com)
SamAccountName login	To authenticate using SamAccountName, using the following format:
	domain\username (*Example:* onprem-cylance\hadmin)
Local user account	Using the cylance user account to authenticate to the CylanceHYBRID console is supported. When LDAP/AD is enabled, log in using the local account using the following username:
	.\cylance
	Note: .\cylance can also be used when LDAP/AD is not enabled.

CylanceHYBRID Status page

The CylanceHYBRID Status page displays system information, provides an interface for modifying network settings, the ability to turn on Maintenance Mode, provides some logging features (enable Debug and download), and allows you to clear or disable the cache. You can also configure Active Directory integration from this page.
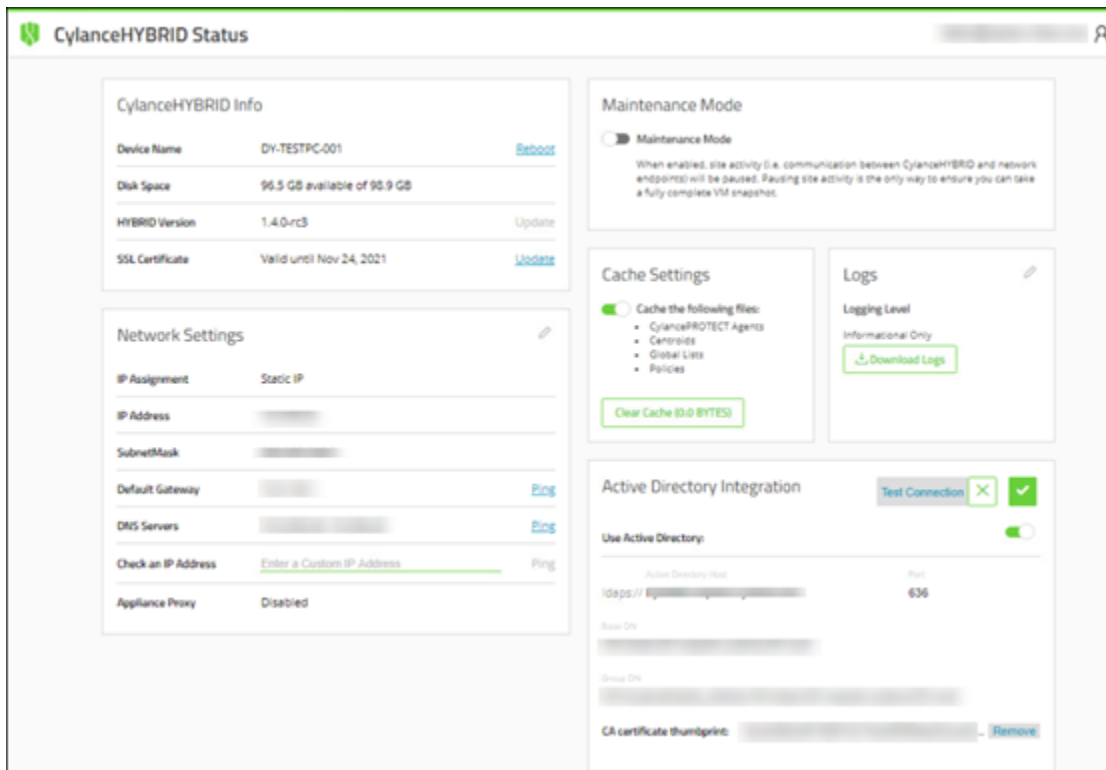
Log in to the Status page

To log in to the CylanceHYBRID status page, use https://<fqdn>/configui/status. Replace <fqdn> with the FQDN of your CylanceHYBRID virtual appliance.

Note:

The username cylance and the password was set during the Configuring CylanceHYBRID process.

Status page field definitions

CylanceHYBRID Info	
Device Name	This is the name of the device where the CylanceHYBRID virtual appliance is installed. Click **Reboot** to restart the virtual appliance. See Reboot the virtual appliance for more information.
Disk Space	This is the disk space available and the total disk space allotted to the virtual appliance.
HYBRID Version	This is the version for CylanceHYBRID. Click **Update** to update the virtual appliance using a CylanceHYBRID update package. See Update CylanceHYBRID for more information.
SSL Certificate	This is the expiration date for the certificate. Click **Update** to update the SSL certificate and key. See Update SSL certificate for more information.

SSL Certificate Ciphers	This indicates whether the certificate is running using strict mode of TLS 1.2+ (default) or the legacy TLS 1.0+ mode. See Change the Certificate Cipher mode for more information.
Network Settings	
IP Assignment	This indicates where the IP address for the virtual appliance is DHCP or Static. See for more information.
IP Address	This is the IP address for the virtual appliance.
Subnet Mask	This is the subnet mask.
Default Gateway	This is the IP address for the default gateway CylanceHYBRID is communicating with. Click **Ping** to test the connection between CylanceHYBRID and the default gateway.
DNS Servers	This is the IP addresses for the DNS servers CylanceHYBRID communicates with.
Check an IP Address	Ping an IP address to test the connection between CylanceHYBRID and the device.
Appliance Proxy	Configure the CylanceHYBRID virtual appliance to communicate through a proxy server. • **Proxy Host:** The fully qualified domain name (FQDN) or IP address for the proxy server. • **Proxy Port:** The port number used to communicate with the proxy server. • **Proxy Username:** Username used to authenticate to the proxy server. • **Proxy Password:** Password used to authenticate to the proxy server.
Maintenance Mode	
Maintenance Mode	Pause activity between CylanceHYBRID and BlackBerry Protect Desktop devices to allow updating the virtual appliance without interruption. When disabling Maintenance Mode, you must confirm that you want to disable it. **Note:** It is recommended to take a snapshot of the CylanceHYBRID virtual appliance before updating.
Cache Settings	
Cache Settings	This indicates whether cache is Enabled or Disabled. The cache includes the following files: • Files to update the Cylance agent • Centroids • Global lists • Policies

Clear Cache	Clear the cache. Use this if you suspect items stored in cache could be corrupt or incomplete.
	⚠️ **CAUTION:** Clearing cache removes all Cylance agent updates, Centroids, Global lists, and Policies.
Logs	
Logging Level	Enable or disable debug logging for the CylanceHYBRID virtual appliance.
	Note:
	Debug logging can consume a high amount of storage space. Only enable debug logging when troubleshooting CylanceHYBRID issues. Otherwise, debug logging should be disabled.
Download Logs	Download the log files for the CylanceHYBRID virtual appliance.
Active Directory Integration	
Use Active Directory	This indicates whether Active Directory is enabled. Click ✎ to enable or disable Active Directory.
Connection	This can be on of the following: • **Active Directory Host:** Active Directory configuration requires the FQDN due to a TLS requirement. Using an IP address for LDAP server configuration will fail. • **Port:** The port number of the LDAP server.
Base DN	This is the base distinguished name (DN) used as a base for the LDAP search to look for the user DN.
Group DN	This is the group DN that performs an LDAP search to check if the user is a member of the group DN.
CA Certificate/ Upload certificate to enable TLS	This is the thumbprint of the secure socket layer (SSL) certificate used to perform a transport layer security (TLS) connection when binding to the LDAP server. Click **Remove** to delete the SSL certificate and upload a different one.
Test Connection	Test a connection to the LDAP server.

Update CylanceHYBRID

The upgrade path for CylanceHYBRID is sequential. For example, if you have version 1.4.1 installed, you must upgrade to 1.4.2, then 1.4.3, and so on, until you upgrade to the latest release. Exceptions to sequential upgrades are:

• Version 1.4.6 can be upgraded from version 1.4.3 or 1.4.4.

1. Obtain the CylanceHYBRID update file from the CylanceHYBRID Upgrade Packages KB article on the Cylance Support Site. Make sure you can access the CylanceHYBRID update file from the browser you use to log in to your CylanceHYBRID console.
2. Log in to the Status page.
3. Enable **Maintenance Mode**. Maintenance Mode must be enabled before you can update the software.

4. Take a snapshot of your virtual appliance.

5. For HYBRID Version, click **Update**.

6. Select **I have taken a VM snapshot**. Click **Continue to upload update package**.

7. Upload an install package. Either drag-and-drop the install package file into the upload window, or click **Browse For a File**, and select the CylanceHYBRID update file. Click **Open**.

8. Click **Update**. The update will take several minutes. During this time, a green bar displays near the top of the web browser. A message displays when the update is complete. Wait for a few more moments while the virtual appliance restarts.

Reboot the virtual appliance

The CylanceHYBRID Status page allows administrators to restart the virtual appliance, instead of doing it from the virtual console (like VMware vSphere).

1. Log in to the Status page.

2. Beside Device Name, click **Reboot**. A message displays asking you to confirm the request.

CylanceHYBRID Info		
Device Name	DY-HYBRIDTEST-120a2	Reboot
Disk Space	51.4 GB available of 53.7 GB	
HYBRID Version	1.1.4-a2	Update
SSL Certificate	Valid until Jan 25, 2019	Update

3. Click **Reboot Now**. During the reboot process, a Reboot in progress message displays and the Status page is inaccessible during the reboot process.

4. When the reboot completes, a Reboot Successful notification displays, and the Status page is accessible. The notification will disappear after a few moments.

Update SSL certificate

1. Log in to the Status page.

2. Beside SSL Certificate, click **Update**.

3. Do one of the following:

  • Download the CSR for the current key (click here link in step 1), then upload the updated certificate from the Certificate Authority in step 2.

  • Generate a new CSR, then upload the certificate you receive from the Certificate Authority. For steps to generate a CSR, see To generate a certificate signing request (CSR) under 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 To upload an SSL certificate and key under Configure CylanceHYBRID.

Change the Certificate Cipher mode

CylanceHYBRID defaults to using TLS 1.2+ (aka 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 (like Windows XP), you can revert to TLS 1.0+ (aka Legacy Mode).

1. Log in to the Status page.
2. Click **Change** beside Certificate Ciphers. If you are switching to Legacy Mode, a dialog prompts you before the change is made.
3. Select whether to enable the change. If you change the setting, a message displays stating a successful change. If you want to change back to Strict Mode, click **Change**.

Export Hybrid configuration

You can export your configuration settings from the CylanceHYBRID Status Page. This export is used to import your configuration when upgrading to Hybrid 2.0.

1. Log in to the Status page.
2. Click the Export link. An alert message appears regarding the export file.
3. Click Export. The Hybrid configuration file is saved to your computer for use when upgrading.

Change IP assignment

1. Log in to the Status page.
2. Enable **Maintenance Mode**. Maintenance Mode must be enabled before you can edit the Network Settings.
3. Take a snapshot of your virtual appliance.
4. Click the Edit icon for Network Settings. A message displays stating that editing network settings may result in loss of access to the CylanceHYBRID Status Page.
5. Select **I have taken a VM snapshot**. Click **Proceed to Edit Network Settings**.
6. From the IP Assignment drop-down, select the assignment type you want.

   - **DHCP:** Dynamic Host Configuration Protocol. A DHCP server assigns an IP address to the virtual appliance.
   - **Static:** You assign an IP address to the virtual appliance.

     - **IP Address:** The IP address for the virtual appliance
     - **Subnet Mask:** A logical subdivision of your network
     - **Default Gateway:** An access point to another network
     - **DNS Servers:** One or more Domain Name System servers
7. Click the green checkmark to save your settings.
8. Disable **Maintenance Mode**, then confirm that you want to disable it.
9. Restart the virtual appliance.

Configure Active Directory

If Active Directory was not configured during the initial deployment, you can configure it from the CylanceHYBRID Status Page. If Active Directory was configured during the initial deployment, you can also disable it form this page.

1. Log in to the Status page.
2. Click the Edit icon, then click the **Use Active Directory** toggle to enable or disable Active Directory.

   Note:

   If you disable Active Directory:

- You are not automatically logged out; however, the next time you log in, you will need to log in with your local user account.
- After saving the disabled state, previous LDAP configuration information will be removed if you later decide to re-enable Active Directory.

3. Configure Active Directory. For steps to configure Active Directory, see To add Active Directory integration under Configure CylanceHYBRID.

Configure a proxy server

With CylanceHYBRID version 1.2.0 and later, allows administrators to configure the virtual appliance to communicate through a proxy server.

Note: CylanceHYBRID uses Tinyproxy for the web proxy server. Tinyproxy only supports lowercase letters, numbers, periods, dashes, and underscores for the proxy username and password.

1. Log in to the Status page.
2. Enable **Maintenance Mode**. Maintenance Mode must be enabled before you can edit the Network Settings.
3. Take a snapshot of your virtual appliance.
4. Click the Edit icon for Network Settings. A message displays stating that editing network settings may result in loss of access to the CylanceHYBRID Status Page.
5. Select **I have taken a VM snapshot**, then click **Proceed to Edit Network Settings**.
6. Click the Appliance Proxy toggle to enable the feature.
7. Type in the Proxy Host (like IP address), Proxy Port, Proxy Username, and Proxy Password.
8. Click the Save icon.

Start the virtual appliance

- In VMware vSphere, click the Power On icon for the virtual appliance you want to power on, or select **Actions > Power > Power On**.

Stop the virtual appliance

- In VMware vSphere, click the Shut Down icon for the virtual appliance you want to shutdown, or select **Actions > Power > Shut Down Guest OS**.

Change the local user account password

If Active Directory is configured, an authorized CylanceHYBRID user using their corporate credentials can log in and change the CylanceHYBRID local user account password.

1. In the top-right of the CylanceHYBRID web browser, click the user profile icon. C
2. Click **Change password**. Then, Set a local password to access CylanceHYBRID in the future page displays.
3. Enter a new password and confirm it in the fields.
4. Click **Submit**.

Configure a Static IP using the OVF Tool

The CylanceHYBRID OVA supports using the VMware OVF Tool to configure the static IP address. The following information is just an example for using the OVF Tool. For more in-depth information about the OVF Tool, please refer to the VMware documentation (OVF Tool Documentation).

1. Download and install the VMware OVF Tool.
2. Open the Command Prompt (Windows) or Terminal (macOS).
3. Navigate to the folder containing the CylanceHYBRID OVA file.
4. Type the following: `ovftool -ds=datastore1 -n=CylanceHYBRID1.1.0 --X:injectOvfEnv --powerOn --prop:ip=123.45.67.89 --prop:netmask=255.255.255.0 --prop:gateway=123.45.67.2 --prop:dns=123.45.67.2,8.8.8.8 CylanceHYBRID_1.1.0.ova vi://test_user@10.60.41.80`
5. Press **Enter**. The OVA file is imported into vSphere.

Things to know about CylanceHYBRID agents

When you use CylanceHYBRID, the BlackBerry Protect Desktop agent requires an installation parameter to configure the agent to communicate with your CylanceHYBRID application.

The following list describes information you should know about using the BlackBerry Protect Desktop agent with CylanceHYBRID. All other agent features are described in the BlackBerry Protect Desktop Installation Guide and the BlackBerry Optics Administrator Guide. This includes all Installation Parameters for the agent.

- CylanceHYBRID requires BlackBerry Protect Desktop agent version 1480 or later. For BlackBerry Optics, use version 2.3.2020 or later (only supports Windows). BlackBerry Protect Desktop must be installed on the endpoint before you install BlackBerry Optics.
- When you use CylanceHYBRID, the Cylance agent requires installation parameters to configure the agent to communicate with your CylanceHYBRID application.

  - For Windows, this is done using the command line.
  - For macOS, create a cyagent_install_token file.
  - For Linux, create the config_defaults.txt file.
  - All other console and agent features are described in the BlackBerry Protect Desktop Administrator Guide.
- When installing BlackBerry Protect Desktop and BlackBerry Optics on a Windows device, there are slightly different workflows:

  - Installing BlackBerry Protect Desktop and BlackBerry Optics on a device for the first time.
  - If BlackBerry Protect Desktop is already installed and communicating with CylanceHYBRID when you try to install BlackBerry Optics.
- The CA certificate used to sign the certificate and key used on your CylanceHYBRID application must be installed on each endpoint in the Local Machine Store for secure HTTPS communication.
- The BlackBerry Protect Desktop agent communicates with the CylanceHYBRID virtual appliance over TCP port 443.

Configure the BlackBerry Protect Desktop Windows agent

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

1. Click **Start**, type `mmc`. Press **Enter**.
2. 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**. Click **Next**.
6. Click **Finish**. Click **OK**.
7. Expand Certificates, right-click Trusted Root Certification Authority. Click **All Tasks > Import**.
8. Click **Next**.
9. Click **Browse**, select your CA certificate. Click **Open**.
10. Click **Next**. Click **Next**. Click **Finish**.
11. When **The import was successful** message displays. Click **OK**.
12. Select **File > Save**. Click **Save**.
13. Close the console.

Configure BlackBerry Protect Desktop Windows agents (without BlackBerry Optics)

Use the following parameters when you install the Windows agent. This is required to ensure all Agents properly communicate with CylanceHYBRID. Use the DNS for your CylanceHYBRID application.

Example of third-level domain name (login.hybrid.com):

InstallRegistrationURL=<hybridurl> **Example: https://login.hybrid.com**

InstallTrustedSuffix=<hybridurlsuffix> **Example: hybrid.com**

InstallInfinityURL=<hybridurl> **Example: https://login.hybrid.com**

Example of second-level domain name (hybrid.com):

InstallRegistrationURL=<hybridurl> **Example: https://hybrid.com**

InstallTrustedSuffix=<hybridurlsuffix> **Example: hybrid.com**

InstallInfinityURL=<hybridurl> **Example: https://hybrid.com**

MSI example

```
msiexec /i CylanceProtect_x64.msi /qn PIDKEY=YourInstallationToken LAUNCHAPP=1
  InstallRegistrationURL=<hybridurl> InstallTrustedSuffix=<hybridurlsuffix>
  InstallInfinityURL=<hybridurl>
```

For examples on editing the MSI installation file for deployment through Group Policy, see the Editing the MSI Installer using Orca article.

EXE example

```
CylanceProtectSetup.exe /s PIDKEY=YourInstallationToken LAUNCHAPP=1
  InstallRegistrationURL=<hybridurl> InstallTrustedSuffix=<hybridurlsuffix>
  InstallInfinityURL=<hybridurl>
```

Configure BlackBerry Protect Desktop and BlackBerry Optics Windows Agents

Follow this procedure if BlackBerry Protect Desktop and BlackBerry Optics are being installed for the first time on the device.

CylanceHYBRID version 1.2.0, or later, supports the BlackBerry Optics agent, version 2.3.2020, or later.

Prerequisites

- CylanceHYBRID version 1.2.0 or later
- BlackBerry Protect Desktop version 1480 or later
- BlackBerry Optics version 2.3.2020 or later
- Available for Windows endpoints only

- See the Support article links below for additional information and troubleshooting suggestions.

Summary:

- On the endpoint, add two registry entries. One to configure BlackBerry Protect Desktop and BlackBerry Optics to use the CylanceHYBRID v1.2.0 proxy server, running on port 8888. The second to disable the BlackBerry Optics cloud fallback feature.
- Add the CA certificate to the endpoint.
- Install BlackBerry Protect Desktop.
- Install BlackBerry Optics. Launch the EXE installer. No other parameters or configuration is required.

Adding registry entries on the endpoint

CylanceHYBRID v1.2.0 uses a proxy server to help with communication between BlackBerry Optics devices and the Cylance console. Also disable the BlackBerry Optics cloud fallback feature. (By default, BlackBerry Optics will attempt to communicate directly with the Cylance cloud when a proxy connection is not available.)

Note: You may need to run the Command Line as an administrator.

1. On the endpoint, open the Command Prompt.
2. Type in the following command. This will configure BlackBerry Protect Desktop and BlackBerry Optics to use the CylanceHYBRID proxy server, running on port 8888.

   reg add HKLM\software\Cylance\Desktop /v ProxyServer /t REG_SZ /d http://hybrid.cylance.com:8888 /f

   Note: Replace `hybrid.cylance.com` with FQDN for your CylanceHYBRID virtual appliance.

   Use `http://` and port `8888` in the command.
3. Press **Enter**. This adds your CylanceHYBRID virtual appliance information that is used when installing BlackBerry Protect Desktop and BlackBerry Optics.
4. Type in the following command. This will disable the BlackBerry Optics cloud fallback feature.

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

   Note:

   If this key is present, the BlackBerry Optics agent will always attempt to establish a connection through the configured proxy server.
5. Close the Command Prompt.

After you finish:

After the registry entry has been added, install the BlackBerry Protect Desktop agent (version 1480 or later).

Configure BlackBerry Protect Desktop

Use the following parameters when you install the Windows agent. This is required to ensure all Agents properly communicate with CylanceHYBRID. Use the DNS for your CylanceHYBRID virtual appliance.

Example of third-level domain name (login.hybrid.com):

InstallRegistrationURL=<hybridurl> **Example: https://login.hybrid.com**

InstallTrustedSuffix=<hybridurlsuffix> **Example: hybrid.com**

InstallInfinityURL=<hybridurl> **Example: https://login.hybrid.com**

Example of second-level domain name (hybrid.com):

InstallRegistrationURL=<hybridurl> Example: https://hybrid.com

InstallTrustedSuffix=<hybridurlsuffix> **Example: hybrid.com**

InstallInfinityURL=<hybridurl> **Example: https://hybrid.com**

MSI example

```
msiexec /i CylanceProtect_x64.msi /qn PIDKEY=YourInstallationToken LAUNCHAPP=1
InstallRegistrationURL=<hybridurl> InstallTrustedSuffix=<hybridurlsuffix>
InstallInfinityURL=<hybridurl>
```

EXE example

```
CylanceProtectSetup.exe /s PIDKEY=YourInstallationToken LAUNCHAPP=1
  InstallRegistrationURL=<hybridurl> InstallTrustedSuffix=<hybridurlsuffix>
  InstallInfinityURL=<hybridurl>
```

Install BlackBerry Optics for CylanceHYBRID Windows

BlackBerry Protect Desktop must be installed and properly communicating with CylanceHYBRID before you install BlackBerry Optics.

1. Download the BlackBerry Optics installer to the endpoint. This can be done by logging into the Cylance console from the endpoint or transferring the installation file from an external source (like a USB flash drive). BlackBerry Optics can also be deployed using a group policy or other software management system.
2. Double-click **CylanceOPTICSSetup.exe**.
3. Click **Install**.
4. Click **Close** when the installation is complete.

Configure BlackBerry Optics Windows agent (BlackBerry Protect Desktop already installed)

Note: Follow this procedure if the BlackBerry Protect Desktop Windows agent is already installed on the device, you did not set the registry to communicate to the CylanceHYBRID proxy server, and the device is already communicating with the CylanceHYBRID virtual appliance.

CylanceHYBRID version 1.2.0, or later, supports the BlackBerry Optics agent, version 2.3.2020, or later.

Prerequisites

- CylanceHYBRID version 1.2.0 or later
- BlackBerry Protect Desktop version 1480 or later
- BlackBerry Optics version 2.3.2020 or later
- Supports Windows endpoints only
- See Support article links below for additional information and troubleshooting suggestions.

Summary

- Take ownership of the Cylance Desktop registry folder. See Take ownership of the Cylance Desktop registry.
- On the endpoint, add two registry entries. One to configure BlackBerry Protect Desktop and BlackBerry Optics to use the CylanceHYBRID v1.2.0 proxy server, running on port 8888. The second to disable the BlackBerry Optics cloud fallback feature.
- Install BlackBerry Optics. Just launch the EXE installer. No other parameters or configuration is required.
- After you install BlackBerry Optics, the Cylance service must be restarted. See Restart the Cylance service Windows.

Take ownership of the Cylance Desktop registry

Only the Cylance\Desktop folder is protected. The `Optics` folder and the `DisableProxyBypass` registry entry can be added to the `HKLM\SOFTWARE\Cylance` folder.

Note: If BlackBerry Protect Desktop is already installed, the `HKLM\SOFTWARE\Cylance\Desktop` folder is not accessible. Use the following to take ownership of the folder, then add the registry entries.

1. Open the Registry Editor.
2. Right-click the **Desktop** folder. This folder is located under HKEY_LOCAL_MACHINE > SOFTWARE > Cylance.
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, then click **Check Names**. Example: If the user is an administrator for the endpoint, select Administrators as the new owner.
7. Click **OK**. This closes the Select User or Group window.
8. Click **Replace owner on subcategories and objects**. Make sure the checkbox is selected.
9. Click **OK**. This closes the Advanced Security Settings for Desktop window.
10. Under Group or user names, make sure the new owner is selected.
11. Under Permissions, make sure **Allow** is selected for **Full Control**.
12. Click **OK**. This closes the Permission for Desktop window. The new owner should now be able to add registry entries. See Add registry entries on the endpoint.

Add registry entries on the endpoint

CylanceHYBRID v1.2.0 and later uses a proxy server to help with communication between BlackBerry Optics devices and the Cylance console. Also disable the BlackBerry Optics cloud fallback feature. (By default, BlackBerry Optics will attempt to communicate directly with the Cylance cloud when a proxy connection is not available.)

Note: You may need to run the Command Line as an administrator.

1. On the endpoint, open the Command Prompt.
2. Type in the following command. This will configure BlackBerry Protect Desktop and BlackBerry Optics to use the CylanceHYBRID proxy server, running on port `8888`.

   ```
   reg add HKLM\software\Cylance\Desktop /v ProxyServer /t REG_SZ /d http://
   hybrid.cylance.com:8888 /f
   ```

   Note: Replace `hybrid.cylance.com` with the FQDN for your CylanceHYBRID virtual appliance.

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

3. Press **Enter**. This adds your CylanceHYBRID virtual appliance information that is used when installing BlackBerry Protect Desktop and BlackBerry Optics.
4. Type in the following command. This will disable the BlackBerry Optics cloud fallback feature.

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

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

5. Close the Command Prompt.

Install BlackBerry Optics for CylanceHYBRID Windows

BlackBerry Protect Desktop must be installed and properly communicating with CylanceHYBRID before you install BlackBerry Optics.

1. Download the BlackBerry Optics installer to the endpoint. This can be done by logging into the Cylance console from the endpoint or transferring the installation file from an external source (like a USB flash drive). BlackBerry Optics can also be deployed using a group policy or other software management system.
2. Double-click **CylanceOPTICSSetup.exe**.
3. Click **Install**.
4. Click **Close** when the installation is complete.

Restart the Cylance service Windows

After you install BlackBerry Optics, you must restart the Cylance service.

1. Open the Device Details page (Devices > select the device) in the Cylance console, then change the **Self Protection Level** to *Local Admin* and click **Save**.
2. Edit the policy for the device (Settings > Device Policy > select the policy):
   a) Select the Protection Settings tab and uncheck **Prevent service shutdown from device**.
   b) Click **Save**.
3. To stop the Cylance service and driver, open the Command Prompt as an administrator, and execute the following commands:

```
net stop cylancesvc
net stop cylancedrv
```

4. To start the Cylance service and driver, execute the commands (in the following order) in the Command Prompt:

```
net start cylancedrv
net start cylancesv
```

Configure BlackBerry Protect Desktop macOS agents

Add a CA certificate to macOS

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

Create a macOS configuration file

Use the following parameters to create the cyagent_install_token plain text file used to configure the agent on your macOS devices. This is required to ensure all Agents properly communicate with CylanceHYBRID. Use the DNS for your CylanceHYBRID virtual appliance.

Example of third-level domain name (login.hybrid.com):

InstallRegistrationURL=<hybridurl> Example: *https://login.hybrid.com*

InstallTrustedSuffix=<hybridurlsuffix> Example: *hybrid.com*

InstallInfinityURL=<hybridurl> Example: *https://login.hybrid.com*

Example of second-level domain name (hybrid.com):

InstallRegistrationURL=<hybridurl> Example: *https://hybrid.com*

InstallTrustedSuffix=<hybridurlsuffix> Example: *hybrid.com*

InstallInfinityURL=\<hybridurl\> Example: *https://hybrid.com*

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 BlackBerry Protect Desktop.pkg -target /
```

Configure BlackBerry Protect Desktop Linux agents

Convert and distribute certificates

BlackBerry Protect Desktop Agents must trust the certificate that the CylanceHYBRID virtual appliance has been configured with to communicate with the virtual appliance. 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. Once the x509 certificate is converted into the Mono format, the certificate files can be distributed to Linux endpoints.

By converting the certificates, you do not need to install Mono on each BlackBerry Protect Desktop Linux agent endpoint.

Mono for Linux steps

The following steps use a CentOS 7.6 virtual machine with a user logged in as the root user.

1. Follow the instructions on Mono Project's website: https://www.mono-project.com/download/stable/#download-lin. Install either the **mono-devel** or **mono-complete** package. Either mono package will allow you to complete the steps below.

2. Open Terminal and change directories to the location where your certificate is stored.

   The certificate needs to be in PEM format.

   Note: The certificate required is the one used to sign the certificate and key for your CylanceHYBRID virtual appliance.

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

   `cert-sync <YOURCERTIFICATE>`

   where <YOURCERTIFICATE> should be replaced with 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.
```

4. Mono stores the synced certificate to **/usr/share/.mono/new-certs/Trust**.

   Note: When you install Mono for Linux, Mono will automatically insert its own certificates into the **/new-certs/ Trust** directory. Because of this, it may be confusing which mono certificate is your newly synced certificate.

   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 versus the other previously inserted certificates.

   Example: The red boxed certificate is the certificate that was synced using the above steps. All other certificates were inserted upon installation of Mono.

```
-rw-r--r--. 1 root root 6863 Dec 10 14:29 5f15c80c.0
-rw-r--r--. 1 root root 4355 Dec 10 14:29 b7a5b843.0
-rw-r--r--. 1 root root 7088 Dec 10 14:29 6410666e.0
-rw-r--r--. 1 root root 6979 Dec 10 14:29 5cd81ad7.0
-rw-r--r--. 1 root root 4855 Dec 10 14:29 7aaf71c0.0
-rw-r--r--. 1 root root 4891 Dec 10 14:29 5d3033c5.0
-rw-r--r--. 1 root root 7620 Dec 10 14:29 3e44d2f7.0
-rw-r--r--. 1 root root 4386 Dec 10 14:29 d853d49e.0
-rw-r--r--. 1 root root 4922 Dec 10 14:29 7992b8bb.0
-rw-r--r--. 1 root root 3032 Dec 10 14:29 f30dd6ad.0
-rw-r--r--. 1 root root 7337 Dec 10 14:29 fc5a8f99.0
-rw-r--r--. 1 root root 3646 Dec 10 14:29 7d0b38bd.0
-rw-r--r--. 1 root root 5219 Dec 10 14:29 b204d74a.0
-rw-r--r--. 1 root root 5165 Dec 10 14:29 c01cdfa2.0
-rw-r--r--. 1 root root 4524 Dec 10 14:29 c0ff1f52.0
-rw-r--r--. 1 root root 4484 Dec 10 14:29 a760e1bd.0
-rw-r--r--. 1 root root 4979 Dec 10 14:29 706f604c.0
-rw-r--r--. 1 root root 4262 Dec 10 14:29 8d86cdd1.0
-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 ba89ed3b.0
-rw-r--r--. 1 root root 4540 Dec 10 14:31 44ff1262.0
```

5. On each Linux device that will use the appliance, create the following directory:

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

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

Please be aware that there is a period, ".", in front of ".mono".

Example method to create the directory:

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

6. Copy the synced certificate to the directory you created in the previous step for all target Linux machines.

Mono for Windows steps

The steps below use Windows 10 as an example.

1. Install Mono for Windows from: https://www.mono-project.com/download/stable/#download-win.
2. In the Start menu, right-click **Open Mono x64 Command Prompt** and select **More > Run as administrator**. Please refer to Mono's documentation here for more information.
3. Change directories to the location where your certificate is stored.

   Note: The certificate needs to be in PEM format.

   Note: The certificate required is the one used to sign the certificate and key for your CylanceHYBRID virtual appliance.

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

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

where <YOURCERTIFICATE> should be replaced with 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.
```

5. Mono stores the synced certificates in the ProgramData directory:

   C:\ProgramData\.mono\new-certs\Trust

   The mono certificate will look like this:

6. On each Linux device that will use the appliance, create the following directory:

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

   Note: This does not install mono on the target machine; you are just manually creating the directory.

   Please be aware that there is a period, ".", in front of ".mono".

   Example method to create the directory:

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

7. Copy the synced certificate to the directory you created in the previous step for all target Linux machines.

Install the Linux agent

Note: The following was done using a CentOS 7.4 virtual machines and logged in as the root user.

1. Copy synced certificates to the proper directory for all target Linux machines. See Configure BlackBerry Protect 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 more examples in the next section.
- Enter `echo InstallTrustedSuffix=<hybridsuffix> >> config_defaults.txt`, then press **Enter**. Replayce <hybridsuffix> with the URL suffix for the CylanceHYBRID server. Example: hybrid.com. See more examples in the next section.
- 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 more examples in the next section.

3. Navigate to the folder with the BlackBerry Protect 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. Type `rpm -ivh CylancePROTECT.el7.rpm`, then press **Enter**. This installs the BlackBerry Protect Desktop Linux agent.

   Note: This example installs the Linux agent for RHEL 7 / CentOS 7 (el7). Change the RPM file name as needed during installation.

5. Optionally, type `rpm -ivh CylancePROTECTUI.el7.rpm`, then press **Enter**. This installs the BlackBerry Protect Desktop UI for the Linux agent. The UI is not required to run the agent.

   Note: This example installs the Linux agent for RHEL 7 / CentOS 7 (el7). Change the RPM file name as needed during installation.

Examples for the Linux Configuration File

Use the following parameters in the plain text file used to configure the agent on your Linux devices. This is required to ensure all Agents properly communicate with CylanceHYBRID. Use the DNS for your CylanceHYBRID virtual appliance.

Example of third-level domain name (login.hybrid.com):

InstallRegistrationURL=<hybridurl> Example: *https://login.hybrid.com*

InstallTrustedSuffix=<hybridurlsuffix> Example: *hybrid.com*

InstallInfinityURL=<hybridurl> Example: *https://login.hybrid.com*

Example of second-level domain name (hybrid.com):

InstallRegistrationURL=<hybridurl> Example: *https://hybrid.com*

InstallTrustedSuffix=<hybridurlsuffix> Example: *hybrid.com*

InstallInfinityURL=<hybridurl> Example: *https://hybrid.com*

Example:

```
echo InstallToken=YourInstallationToken > config_defaults.txt
echo InstallRegistrationURL=<hybridurl> >> config_defaults.txt
echo InstallTrustedSuffix=<hybridurlsuffix> >> config_defaults.txt
echo InstallInfinityURL=<hybridurl> >> config_defaults.t
```

Support article links

The following Support knowledge base articles are related to Proxy Servers or BlackBerry Optics and might help with deployment.

- Authenticated Proxy Configuration: Suggestions for authenticating proxies when a user is not logged in.
- CylanceOPTICS Proxy Support: Configuration and troubleshooting for using BlackBerry Optics with a proxy server.
- How to alter MSI Installers and include proxy settings and verbose logging:

    - Using Orca
    - Using Instedit
- Unauthenticated Proxy Configuration: Configuring proxy settings using a registry entry.

Troubleshooting

This section provides a list of questions to answer and files to collect when troubleshooting issues with CylanceHYBRID. This information will enable Support to assist in resolving any issues.

Agent not communicating with CylanceHYBRID

Verify the following:

- Make sure the agent (version 1480 or later) is installed on the endpoint. To do so, locate the Cylance icon ( ) in the system tray or check the list of apps installed on the endpoint.
- Make sure the agent is configured to communicate with your CylanceHYBRID virtual appliance. For example, check for the registry entry on the device.
- Ensure the CA certificate used to sign the certificate and key used on your CylanceHYBRID virtual appliance is installed on the endpoint in the Local Machine Certificate Store.

CylanceHYBRID not communicating with Cylance console

- Make sure the CylanceHYBRID virtual appliance 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, read this KB article.

Web browser reporting an insecure webpage

When attempting to log in to the CylanceHYBRID console, the web browser displays an error, reporting an insecure webpage.

- Install the CA certificate used to sign the certificate and key used on your CylanceHYBRID virtual appliance on to the endpoint in the Local Machine Certificate Store.

Contact Cylance support

If the above troubleshooting suggestions do not resolve your issue, before you contact Cylance Support, enable Debug logging on the CylanceHYBRID Status page, wait for at least 20 minutes, then download the log file and submit it to Cylance Support.

To Enable Verbose Logging

1. Log in to the Status page
2. Beside Logs, click   .
3. Click the **Logging Level** dropdown arrow, then select **Debug** (verbose logging).
4. Click the checkmark to save the Logging Level.
5. Wait at least 20 minutes to collect a sufficient amount of log information.
6. Click **Download Logs**. The log file is saved as a compressed file to your local disk drive.
7. Create a Cylance Support ticket and include the CylanceHYBRID log file.

- Log in to myAccount.
- Click **Get Help Now**, under Submit a Case.
- Submit your case.

Third-party products and licenses

CylanceHYBRID includes third-party code licensed to Cylance for redistribution under open-source licenses. This list of open-source software packages was complied with reference to third-party software incorporated into the CylanceHYBRID application.

Operating System: CentOS (license)

OS Packages: bzip2 (license); epel-release (license, source); miniconda3 (license); nginx (license); postgresql-contrib (license); postgresql-server (license); redis (license); supervisor (license); tinyproxy (license, source); unzip (license); vim (license).

Python: aiopg (license); aioredis (license); aioredlock (license); aiosqlite (license); aniso8301 (license); async-timeout (license); asn1crypto (license); attrs (license); blinker (license); bcrypt (license); certifi (license); cffi (license); chardet (license, source); click (license); cryptography (Apache license, BSD 3-Clause license); Flask (license); Flask-bcrypt (license); Flask-Cors (license); Flask-login (license); gunicorn (license); Hiredis (license); idna (license); itsdangerous (license); jinja2 (license); MarkupSafe (license); marshmallow (license); pycurl (COPYING-LGPL license, source, COPYING-MIT license); psycopg2 (license, source); pyasn1 (license); pyasn1-modules (license); pycparser (license); pyOpenSSL (license); python-ldap (license); pytz (license); requests (license); six (license); tornado (license); urllib3 (license); werkzueg (license).

JavaScript: axios (license); babel-polyfill (license); classnames (license); clipboard (license, readme); d3 (license); deepmerge (license); form-data (license); formik (license); lodash.debounce (license); lodash.filter (license); lodash.get (license); lodash.isequal (license); lodash.map (license); lodash.mapkeys (license); lodash.reduce (license); lodash.snakecase (license); lodash.some (license); lodash.uniqueid (license); material-ui (license); moment (license); normalize.css (license); pretty-bytes (license); prop-types (15.6.0 license, 15.6.1 license); rc-slider (license); react (license); react-copy-to-clipboard (license); react-datepicker (license); react-dom (license); react-dropzone (license); react-popper (license); react-responsive (license); react-tippy (license); toastr (license, readme); url-polyfill (license); url-search-params-polyfill (license); whatwg-fetch (license).

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada