CylanceON-PREM

Administration Guide

1.8

Contents

Troubleshooting.. 91

Legal notice.. 94

Overview

CylanceON-PREM offers next generation protection to organizations with networks where Internet access is severely restricted or not allowed (air-gapped environments).

CylanceON-PREM facilitates security-related communication between a virtual server that acts as the Cylance console and local infrastructure (endpoints with CylancePROTECT agents installed) without exposing the local network to the wider internet. The standard configuration of CylancePROTECT requires endpoints to individually communicate with the cloud. CylanceON-PREM allows organizations to manage their agents without connecting to the Cylance console.

High-level installation and configuration

The following flowchart shows the high-level steps for installing and configuring CylanceON-PREM.
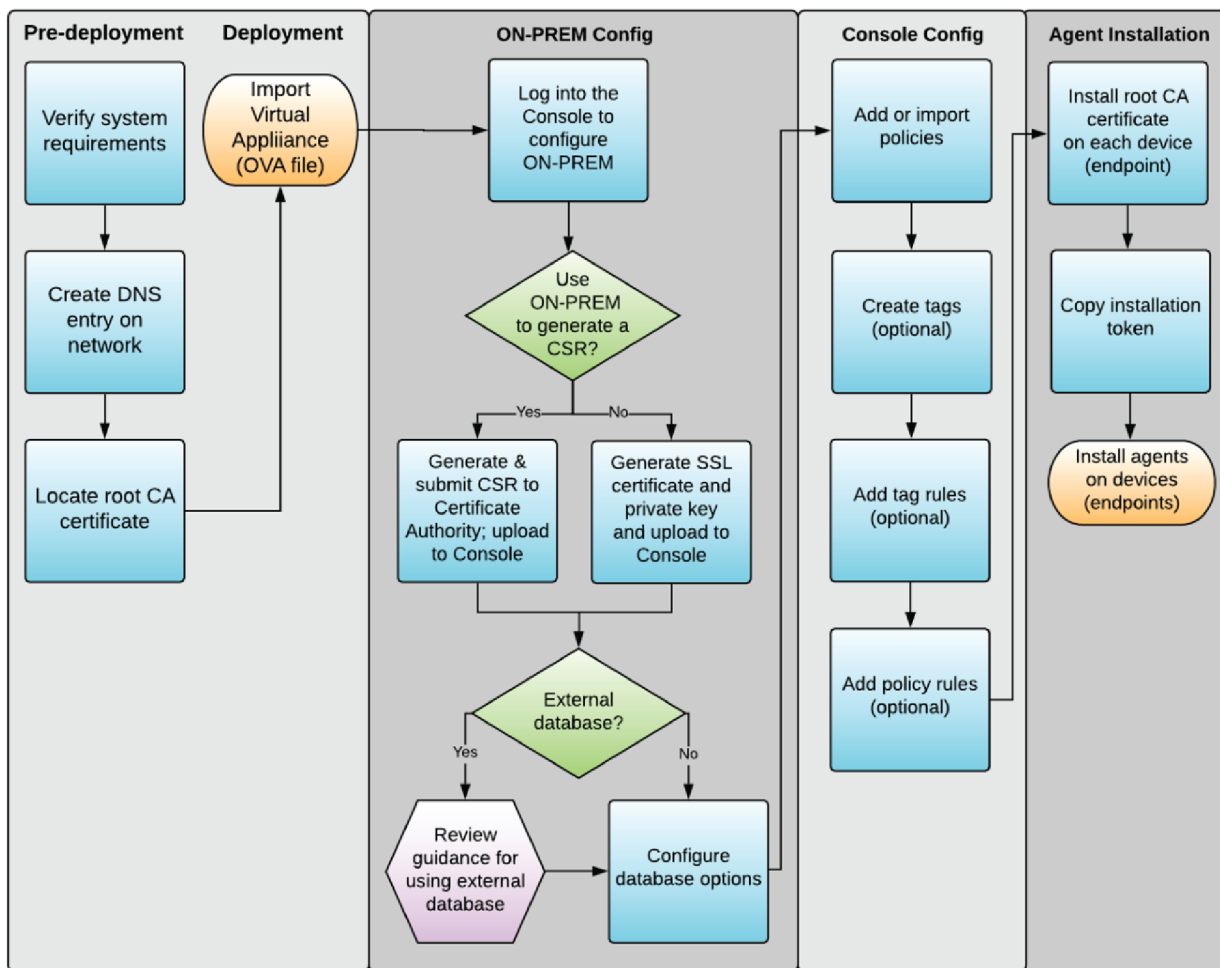
Pre-deployment steps

1. Verify system requirements:
    - CylanceON-PREM OVA requirements

- Virtual appliance system requirements
- Other requirements
- Web browser support
- Things to know about CylanceON-PREM

2. Create a DNS Entry on the Network. See Prerequisites for more information.
3. Locate the root CA certificate. See Prerequisites for more information.

Deployment steps

Import the CylanceON-PREM virtual appliance (OVA file):

- Import the OVA and configure a static IP address
- Import the OVA and configure DHCP

CylanceON-PREM configuration steps

1. Log in to the console to configure CylanceON-PREM. See Configure CylanceON-PREM for more information.
2. Select a certificate option:

   - Generate and submit a CSR from CylanceON-PREM
   - Generate an SSL certificate and private key using a different computer, then upload to CylanceON-PREM

3. Select a database option:

   - If you use an external database, see External database overview before continuing.
   - Configure database options. See Configure CylanceON-PREM for more information.

Console configuration steps

1. Add or import a policy:

   - Add a policy
   - Import a policy

2. (Optional) Add a device tag.
3. (Optional) Add a tag rule.
4. (Optional) Add a policy rule .

Agent installation steps

1. Add Root CA certificate to every endpoint
2. Copy installation token
3. Install agents on devices (endpoints):

   - Install the Windows agent
   - Install the macOS agent

CylanceON-PREM OVA requirements

CylanceON-PREM is provided as an OVA (virtual appliance) and supports VMware ESXi 6.5 or later.

Virtual appliance system requirements

All-in-one virtual appliance

The CylanceON-PREM virtual appliance includes a database and can support up to 10,000 endpoints. This is an all-in-one option. Cylance recommends this option to support up to 10,000 endpoints because it does not require setting up a PostgreSQL database.

The following are the CylanceON-PREM virtual appliance minimum, dedicated hardware requirements:

System requirement	Description
RAM	16 GB
CPU	2.2 GHz quad-core (Intel Xeon processors or later)
Free disk space	1 TB
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)

Endpoint management virtual appliance (up to 50,000 endpoints)

The virtual appliance can communicate with an external database and support up to 50,000 endpoints. With an external database, the CylanceON-PREM virtual appliance uses the Console and other Cylance components necessary to support an on-premises solution.

External database hardware requirements

If an external database is used with the CylanceON-PREM virtual appliance, the following are the minimum, dedicated hardware requirements are:

System requirement	Description
RAM	16 GB
CPU	2.2 GHz quad-core (Intel Xeon processors or later)
Free disk space	500 GB
Database	PostgreSQL version 10.4 (or higher)

When you connect the endpoint management virtual appliance with the external database for the first time, CylanceON-PREM will create the necessary tables in the database.

Note: Setting up, maintaining, and troubleshooting an external database is not supported by Cylance. Organizations must have a dedicated database administrator (DBA) for configuring and maintaining their database.

Other requirements

- CylancePROTECT Agent version 1480 or higher installed on the endpoints
- Root certificate authority (CA) certificate, installed (trusted) on each endpoint
- To obtain a server certificate, submit a certificate-signing request (CSR) generated by CylanceON-PREM or on another server to your CA of choice. The server certificate must be installed on CylanceON-PREM, and if the latter method was used to obtain the certificate, the private key will also need to be installed on CylanceON-PREM.

Things to know about CylanceON-PREM

- Currently, there is no mechanism for a user to reset or recover their password on their own. A CylanceON-PREM administrator can set a new password for the user.

  Note: Administrators should generate a random password when they change or reset a user's password. Do not use a generic password because the password may already be in the user's history (last 10 passwords) so it will be prohibited.
- A CylanceON-PREM virtual appliance cannot communicate to or through another CylanceON-PREM virtual appliance.
- CylanceON-PREM currently does not support BlackBerry Optics.
- CylanceON-PREM does not support command line access to the virtual appliance.CylanceON-PREM was purposefully hardened to prevent any tampering with the virtual appliance because it is a proprietary system. Cylance does not support modifying anything on the virtual appliance or gaining access to it.
- Devices configured to communicate with CylanceON-PREM must be able to communicate with the DNS hostname you created for CylanceON-PREM. Removing a device from that network 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.
- There are currently no migration options to go from an all-in-one virtual appliance to an endpoint management virtual console with an external database (PostgreSQL), or vice versa. This includes upgrading the virtual appliance. After a virtual appliance is deployed, with an internal database or an external database, it cannot be changed to the other.
- When you deploy CylanceON-PREM for the first time, it creates a system account (First Name=system and Email=system@onprem.local) that is used in Audit Logs to identify actions taken by the system versus actions taken by a CylanceON-PREM user. For example, the system account is used when the system applies a policy to a device as a result of a policy rules match.
- You should use the VMware vSphere high-availability feature to provide failure protection against hardware and operating system outages for your CylanceON-PREM environment. For more information, see VMware's article here.

Item	Description
Password reset	Currently, there is no mechanism for a user to reset or recover their password on their own. A CylanceON-PREM administrator can set a new password for the user.
	Note: Administrators should generate a random password when they change or reset a user's password. Do not use a generic password because the password may already be in the user's history (last 10 passwords) so it will be prohibited.
No communication through another CylanceON-PREM virtual appliance	A CylanceON-PREM virtual appliance cannot communicate to or through another CylanceON-PREM virtual appliance.
BlackBerry Optics not supported	CylanceON-PREM currently does not support BlackBerry Optics.
No command line access	CylanceON-PREM does not support command line access to the virtual appliance.CylanceON-PREM was purposefully hardened to prevent any tampering with the virtual appliance because it is a proprietary system. Cylance does not support modifying anything on the virtual appliance or gaining access to it.
Devices must communicate with CylanceON-PREM DNS hostname	Devices configured to communicate with CylanceON-PREM must be able to communicate with the DNS hostname you created for CylanceON-PREM. Removing a device from that network 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.
No database migration	There are currently no migration options to go from an all-in-one virtual appliance to an endpoint management virtual console with an external database (PostgreSQL), or vice versa. This includes upgrading the virtual appliance. After a virtual appliance is deployed, with an internal database or an external database, it cannot be changed to the other.
Virtualization high availability	If your virtualization application has a high availability feature, it is recommended to use it to provide failure protection against hardware and operating system outages for your CylanceON-PREM environment. For example, see VMware's article here.

Configuring the CylanceON-PREM virtual appliance

The CylanceON-PREM virtual appliance must be configured with a certificate and key, generated from a root CA certificate. This ensures secure communication between your CylanceON-PREM appliance and your devices (endpoints with a Cylance Agent installed).

Prerequisites

- Create a DNS entry on your network (work with your IT department, if necessary).
  - Create a fully qualified domain name (FQDN) for the virtual appliance. For example, a fully qualified domain name could be `login.onprem.com` **or** `onprem.com`.
  - The DNS entry will also need the IP address of the OVA operating system.

- **DHCP:** If you use DHCP, the IP address for CylanceON-PREM can be seen on the login screen of the virtual appliance.
  - **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.
- Have a root CA certificate. This is installed (trusted) on every endpoint.
- Obtain a server certificate by submitting a CSR generated by CylanceON-PREM or on another server to your Certificate Authority of choice. The server certificate must be installed on CylanceON-PREM, and if the latter method was used to obtain the certificate, the private key will also need to be installed on CylanceON-PREM.

Import the OVA and configure a static IP address

This task is for CylanceON-PREM instances that need to use a static IP address.

If DHCP is used, go to the Import the OVA and configure DHCP task.

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 higher, or are using VMware ESXi 6.5 managed by vCenter Server 5.1 or higher, 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 is not displayed, 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 static IP using the OVF tool.

1. In VMware vSphere, select **Actions > Deploy OVF Template**. The Deploy OVF Template window is displayed.
2. Select the OVA file. Click **Next**.
3. Type a name for the virtual machine, 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 the OVA and configure DHCP

This task is for CylanceON-PREM instances that use DHCP. This example uses the VMware vSphere Client.

If a static IP address is used, go to the Import the OVA and configure a 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, 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 Customize Template field blank will enable DHCP on the virtual appliance.
9. Click **Next**. Review the settings.
10. Click **Finish**.

Configure CylanceON-PREM

This task is for all CylanceON-PREM instances, either DHCP or Static IP.

Note:

- If you are using a static IP address, Import the OVA and configure a static IP address first.
- If you are using an external database, read the External database overview for an overview of the setup.

1. Start the CylanceON-PREM virtual appliance. In VMware vSphere, click the Power On icon, or select **Actions > Power > Power On**.

2. Open a web browser and go to `https://<fqdn>`.

   - Replace `<fqdn>` with the fully qualified domain name (FQDN) from the DNS entry. Examples: *https:// login.onprem.com* **or** *https://onprem.com*.
   - For a web browser, use a system that can communicate with the CylanceON-PREM virtual appliance.

3. To generate a CSR from CylanceON-PREM that will be submitted to a CA to use with the CylanceON-PREM virtual appliance:

   To use an SSL certificate and key generated on a computer other than CylanceON-PREM, go to step 4.

   - Fill out the form.

   a) **Common Name:** The common name is derived from the fully qualified domain name (FQDN) for the virtual appliance. For example, if the FQDN is `https://onprem.cylance.com`, then the common name is `onprem.cylance.com`.

   b) **Subject Alternative Name:** Enter any alternative names to use for the virtual appliance, such as *onprem-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: onprem.cylance.crt.

     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 Certificate Authority.

4. Click **Upload Cert and Key**. The Webserver Configuration page is displayed. For more information on certificate guidelines, refer to the Certificate Guidelines.

5. In the **Hostname** field, enter in the FQDN (Common Name) or Subject Alternative Name for the virtual appliance. The FQDN must match the DNS entry. For example, the FQDN/Common name could be `login.onprem.com` **or** `onprem.com`.

6. Drag the SSL Certificate to the **Upload certificate** box or click **Browse for a file** and select the certificate. If you generated the CSR using Cylance, you do not have to upload a private key. Skip the remaining steps below and continue to Step 7. If you generated a CSR on a different computer than Cylance, upload a Private Key:

   a) Enable the **Upload Private Key** toggle.

   b) Drag the private key to the **Upload Key** box or click **Browse for a file** and select the private key.

     Note: If your CA provides you a .pfx file (combined site certificate and private key), they will need to separate it into two separate files. In addition, the private key file cannot be password protected.

7. Click **Save and Continue**. SSL is configured on the virtual appliance.

8. Choose a database option:

Item	Configuration
Database connection settings disabled	No configuration required
Database connection settings are enabled	**a.** Enter the hostname or IP address for the external database (for example, `database.com` **or** `123.45.67.89`) **b.** Enter the port number for the external database (for example, `5432`) **c.** Enter the database user name and password (this database user must be able to add tables to the database) **d.** Enable TLS/SSL to use an SSL connection to the external database. If TLS/SSL is enabled, you can also specify the following: • Enable Verify Peer Mode to authenticate the external Postgres DB server certificate, and the communications channel is encrypted. Verify Peer Mode=disabled means CylanceON-PREM will not authenticate the external Postgres DB server certificate but the communications is still encrypted. • Click **Install Postgres SSL Certificate**, then drag the certificate file to the Install Postgres SSL Certificate dialog box or click **Browse for a file** and select the certificate. • Click **Install Certificate**. **e.** Click **Test Connection** to ensure the virtual appliance can communicate with the database. **f.** Click **Save and Continue**.

Note: Setting up, maintaining, and troubleshooting an external database is not supported by Cylance. Organizations must have a dedicated database administrator (DBA) for configuring and maintaining their database.

9. Type in your login information, then click **Save and Finish**. This user will be added as an Administrator in your CylanceON-PREM Console. The login screen displays.

External database overview

This is a simple overview of possible steps for setting up an external database to connect to the CylanceON-PREM virtual appliance. This is not a list of requirements because configuring an external database depends on your environment. This list is simply provided as guidance and could help if you have issues connecting the database to the virtual appliance.

- Install PostgreSQL and PostgreSQL server
- Initialize the PostgreSQL database
- Start and enable autostart postgres service to start the database when the server starts
- Force postgres to listen on all ports in postgresql.conf
- Allow postgres port through firewall
- Enable the pgcrypto extention
- Create a postgres user

  - If the database is dedicated to CylanceON-PREM, using the default postgres user is an option
  - If the database is shared, then you should create a new postgres user for the CylanceON-PREM database

    Note: A shared database is not recommended for CylanceON-PREM
- Authorize remote postgres authentication in pg_hba.conf file

- Generate SSL certificates for postgres server connection
- Configure SSL in postgresql.conf file

When you connect the external database to CylanceON-PREM:

- Use the fully qualified domain name (FQDN) of the external database
    - Using the external database IP address is an option
- The default port for PostgreSQL is 5432
- TLS/SSL requires uploading the external database certificate to CylanceON-PREM
    - During initial configuration, enable Verify Peer Mode, upload the certificate, then disable Verify Peer Mode
- Verify Peer Mode requires configuring certificates on the host and client

Configuring the console

This section includes information about using the console dashboard, filtering lists, and using policies.

Log in to CylanceON-PREM

To log in to CylanceON-PREM, use https://<fqdn>. Replace <fqdn> with the fully qualified domain name (FQDN) of your CylanceON-PREM virtual appliance. **Example:** `https://login.onprem.com` **or** `https://onprem.com`.

For security, CylanceON-PREM will require a user to log in again after 10 minutes of non-activity.

Log in using identity provider credentials

To configure CylanceON-PREM to use an external identity provider, such as Okta, refer to Configure identity provider settings.

1. On the CylanceON-PREM login page, click **Sign in with SSO**. The Identity Provider's login page displays. If you have already authenticated with your identity provider, the CylanceON-PREM dashboard should display.
2. Log in to your Identity Provider's website and go through any validation processes (like two factor authentication). If you are authenticated by your identity provider, your browser will redirect to the CylanceON-PREM Dashboard.

Log in using certificate-based authentication

For more information about certificate-based authentication, refer to Using certificate-based authentication.

Before you begin: The administrator must have a common access card (CAC).

1. On the computer that you are going to log in to, insert your CAC.
2. Select your certificate.
3. On the CylanceON-PREM login page, click **Certificate-based Sign in.** The administrator is logged into the console.

Note that you are automatically logged out of the console if you remove your CAC.

Administrative dashboard

The CylanceON-PREM administrative dashboard displays when you first log into the Console. This page provides an overview of threat events on devices and quick links to frequently used features in the product.

Property	Description
Access Management	Clicking this widget opens the **User Management > Users** page.
Acknowledged	This drop-down list filters the event widgets to display events as follows: • No - Only displays events that have not been acknowledged by a user (manually quarantined or safelisted or from clicking Acknowledge on the Events page) • All - Displays all events including acknowledged and unacknowledged **Note:** If you set this filter and then navigate to an Events page using a widget, the filter is applied to that Events page and any filters previously set on that page will be overridden.
Application Events	This panel displays the total number of application events in your organization. Application Control must be enabled in at least one policy and at least one event of trying to change something on an Application Control device must have occurred. Clicking this widget opens the **Events > Application Events** page.
Configuration	Clicking this widget opens the **Configuration > Settings** page.
Device Events	This panel displays the total number of USB mass storage device events in your organization. Clicking this widget opens the **Events > Device Events** page.
Devices	This panel displays the total number of devices communicating with this CylanceON-PREM virtual appliance. Clicking this widget opens the **Device List** page.

Property	Description
Global Lists	The Global Lists page displays events that were added to the Global Quarantine or Global Safe lists. Clicking this widget opens the **Global Lists** page.
Memory Events	This panel displays the total number of malicious memory events in your organization. Clicking this widget opens the **Events > Memory Events** page.
Policies	Clicking this widget opens the **Policies** page.
Reported On	Filters the event widgets based on a date/time or date range set in this filter. If you set this filter and then navigate to an Events page using a widget, the filter is applied to that Events page and any filters previously set on that page will be overridden.
Script Events	This panel displays the total number of malicious script events in your organization. Clicking this widget opens the **Events > Script Events** page.
Threat Events	This panel displays the total number of malicious file events in your organization. Clicking this widget opens the **Events > File Events** page.

Filter lists

On any page that contains a list of items, you can filter those items to quickly locate the information you need.

1. Click ≡ on the right side above the list to expand the list of filters available.
2. Set one or more filters from the following types.

   - **Quick Search field:** Search across all items listed in the hint text of the field.

     > 🔍 Search by hash, file name, file path, and interpreter
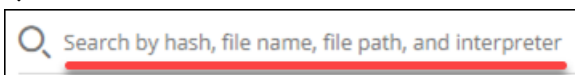
   - **Text Entry fields:** Enter a full or partial name of the term you are searching for in the column, such as the full file name, then click the ✔.

     Note: Wildcards are not supported.
   - **Date Range fields:** Enter a date range or select a range by clicking on the date entry region. To remove a date range, click **Clear**.
   - **Selectable fields:**Click one or more options from a list. To remove a selected option, click the X to the right of the selected option.

   Any filters you add display in the Quick Search field above the filter options.

3. Click ≡ again to hide the filter options. A green circle appears on the icon 🗎 to indicate that filters are applied.

To remove a filter from a list

1.
    Click ![filter icon] on the right side above the list to view the filters applied.

2. Click the X beside the applied filters to remove in the Quick Search field:

🔍 Acknowledged: NO ✕	Last Reported: TO 02/12/2020 ✕	Drive Type: Fixed ✕	Search by hash, file name, file path, and interpreter
Safe	**Acknowledged**	**Hash**	**File Name**
YES	NO ✕	🔍 Enter term...	🔍 Enter term...
NO	YES		
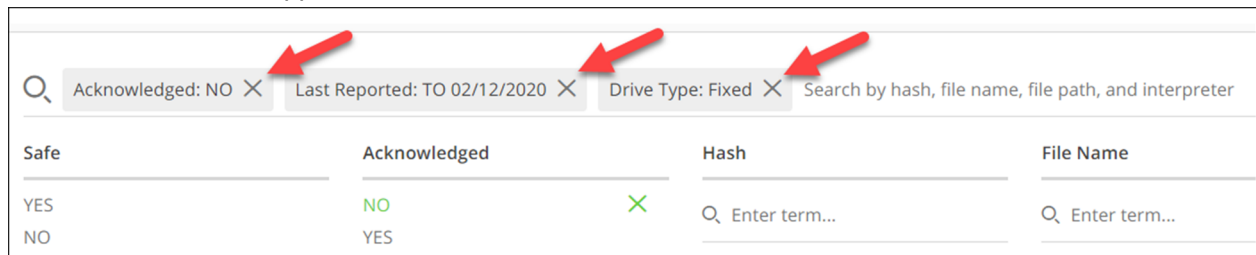
Export lists

On any page that contains a list of items, you can export the current page or all pages in the list as a .csv file for use in other applications.

1. Click ![export icon] on the List page.
2. Select whether to export entries on the current page (**Current View**) or all entries in the list (**Everything**).
3. Click **Export**.

Policies

A policy defines how the Agent handles threats (malware) it encounters – automatically quarantine, ignore if in a specified folder, block a specific type of script, etc. Every device must be in a policy. If no policy is assigned, the device is placed in the Default policy.

You can assign a policy to a device manually or automatically, but not both. For information about manually assigning policies to devices, see Assign a policy. For information about automatically assigning policies to devices, see Add a policy rule.

Add a policy

1. Log in to CylanceON-PREM as an administrator. Only administrators can create policies.
2. Select **Policies**, then click **Add New Policy**.
3. Type a name for the policy and select policy options. Descriptions for each policy option are listed below.
4. Click **Save**.

Threat settings

Threat settings provide different options for handling files detected by the agent. Threats are classified as either Unsafe or Abnormal.

Threat Setting	Description
Allow Execution in Threat Exclusion Folders	Use this option to allow execution of files in Threat Exclusion folders in addition to exclusion of threats found during File Watcher and Background Threat Detection.

Threat Setting	Description
Auto Delete Quarantine	Use this option to automatically delete quarantined files after a specified number of days This applies to all devices assigned to the policy. The minimum number of days is one.
	The number of days starts when the file was first quarantined. This action is included in the Agent log file for verification.
	If this feature is not enabled, the quarantined files will remain on the device until the quarantined files are manually deleted.
Auto Quarantine Abnormal Files	Use this option to quarantine an abnormal file to prevent it from executing. On a device, quarantining a file will move the file from its original location to the Cylance Quarantine directory.
	• **For Windows:** C:\ProgramData\Cylance\Desktop\q
	• **For macOS:** /Library/Application Support/Cylance/Desktop/q
	Some malware is designed to drop other files in certain directories. This malware will continue to do so until the file is successfully dropped. To stop the malware from continually dropping the removed file, the Agent will modify the dropped file so it won't execute and leave it in the folder.
	Note: Auto Quarantine Unsafe Files must be selected for Auto Quarantine Abnormal Files to be available.
Auto Quarantine Unsafe Files	Use this option to quarantine an unsafe file to prevent it from executing. On a device, quarantining a file will move the file from its original location to the Cylance Quarantine directory.
	• **For Windows:** C:\ProgramData\Cylance\Desktop\q
	• **For macOS:** /Library/Application Support/Cylance/Desktop/q
	Some malware is designed to drop other files in certain directories. This malware will continue to do so until the file is successfully dropped. To stop the malware from continually dropping the removed file, the Agent will modify the dropped file so it won't execute and leave it in the folder.
	Note: Auto Quarantine Unsafe Files must be selected for Auto Quarantine Abnormal Files to be available.
Background Threat Detection	Use this option to perform a full disk scan to detect and analyze any dormant threats on the disk. The full disk scan is designed to minimize impact to the end-user by using a low amount of system resources.
	The user can choose to run the scan once (upon installation only) or run recurring (which performs a scan every 9 days). A significant upgrade to the Cylance model, like adding new operating systems, will also trigger a full disk scan. Each time a new scan is performed, all files will be rescanned.
	It is recommended that users set Background Threat Detection to Run Once. Due to the predictive nature of the CylancePROTECT technology, periodic scans of the entire disk are not necessary but can be implemented for compliance purposes.

Threat Setting	Description
Copy File Samples	Use this option to allow users to specify a network share where file samples can be copied. This allows you to do your own analysis of files the Agent considers Unsafe or Abnormal. • CIFS/SMB network shares are supported. • Specify one network share location. Using the fully qualified path is recommended.For example: `\\server_name\shared_folder` • All files that meet the criteria will be copied to the network share, including duplicates. No uniqueness test will be performed. • Files are compressed. • Files are password protected. The password is `"infected"`.
File Watcher	Use this option to detect and analyze any new or modified files for dormant threats. You should enable File Watcher. However, if Auto Quarantine is enabled for all Unsafe or Abnormal files, all malicious files will be blocked at execution. Hence, it is not necessary to enable File Watcher with Auto Quarantine mode unless you prefer to quarantine a file as it is added to a disk (File Watcher) but before execution (Auto-Quarantine).
Scan Archive	Use this option to set the maximum archive file size the Agent will scan. This setting applies to Background Threat Detection and File Watcher.

Memory protection

The Agent will scan and monitor running processes to protect devices from malware that attempts to take advantage of software vulnerabilities that exploit running processes or executes from within memory space. It is recommended that you block all types of memory violations.

For descriptions of the different violation, process, and escalation types, see Memory Protection Violation Types.

Note: Enabling memory protection may cause errors if there is another application that also monitors running processes. You should disable the other application's memory protection before you enable it in CylanceON-PREM. If that is not possible, then leave memory protection disabled in your CylanceON-PREM policies.

Memory Protection Setting	Description
Alert	The Agent will record the violation and report the incident to the Console.
Block	If an application attempts to call a memory violation process, the Agent will block the process call. The application that made the call is allowed to continue to run.
Ignore	The Agent will not take any action against identified memory violations.
Terminate	If an application attempts to call a memory violation process, the Agent will block the process call and will also terminate the application that made the call.

Memory protection violation types

Exploitation Violation Types	Applies to
Stack Pivot — The stack for a thread has been replaced with a different stack. Generally the system will only allocate a single stack for a thread. An attacker would use a different stack to control execution in a way that is not blocked by Data Execution Prevention (DEP).	Windows macOS
Stack Protect — The memory protection of a thread's stack has been modified to enable execution permission. Stack memory should not be executable, so usually this means that an attacker is preparing to run malicious code stored in stack memory as part of an exploit, an attempt which would otherwise be blocked by Data Execution Prevention (DEP).	Windows macOS
Overwrite Code — Code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass Data Execution Prevention (DEP).	Windows
RAM Scraping — A process is trying to read valid magnetic stripe track data from another process. This is typically related to point of sale systems (POS).	Windows
Malicious Payload — A generic shellcode and payload detection associated with exploitation has been detected.	Windows
Process Injection Violation Types	Applies to
Remote Allocation of Memory — A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system.	macOS
Remote Mapping of Memory — A process has introduced code and/or data into another process. This may indicate an attempt to begin executing code in another process and thereby reinforce a malicious presence.	Windows
Remote Write To Memory — A process has modified memory in another process. This is usually an attempt to store code or data in previously allocated memory (see OutOfProcessAllocation) but it is possible that an attacker is trying to overwrite existing memory in order to divert execution for a malicious purpose.	Windows macOS
Remote Write PE To Memory — A process has modified memory in another process to contain an executable image. Generally this indicates that an attacker is attempting to execute code without first writing that code to disk.	Windows

Exploitation Violation Types	Applies to
Remote Overwrite Code — A process has modified executable memory in another process. Under normal conditions executable memory will not be modified, especially by another process. This usually indicates an attempt to divert execution in another process.	Windows
Remote Unmap of Memory — A process has removed a Windows executable from the memory of another process. This may indicate an intent to replace the executable image with a modified copy for the purpose of diverting execution.	Windows
Remote Thread Creation — A process has created a new thread in another process. A process's threads are usually only created by that same process. This is generally used by an attacker to activate a malicious presence that has been injected into another process.	Windows macOS
Remote APC Scheduled — A process has diverted the execution of another process's thread. This is generally used by an attacker to activate a malicious presence that has been injected into another process.	Windows
DYLD Injection — An environment variable has been set that will cause a shared library to be injected into a launched process. Attacks can modify the plist of applications like Safari or replace applications with bash scripts, that cause their modules to be loaded automatically when an application starts.	macOS
Escalation Violation Types	Applies to
LSASS Read — Memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords.	Windows
Zero Allocate — A null page has been allocated. The memory region is typically reserved, but in certain circumstances it can be allocated. Attacks can use this to setup privilege escalation by taking advantage of some known null de-reference exploit, typically in the kernel.	Windows macOS

Script control

Script control protects devices by blocking malicious Active Script, PowerShell scripts, and Microsoft Office macros from running.

Script control monitors and protects against scripts running in your environment. The Agent can detect the script and script path before the script is executed. Depending on the policy set for Script Control (alert or block), the Agent will allow or block the execution of the script.

Microsoft Office macros use Visual Basic for Applications (VBA) that allows embedding code inside an Office document (typically Word, Excel, and PowerPoint). The main purpose for macros is to simplify routine actions, like manipulating data in a spreadsheet or formatting text in a document. However, malware creators can use macros to run commands and attack the system. It is assumed that a Microsoft Office macro trying to manipulate the system is a malicious action. The Agent looks for malicious actions originating from a macro that affects things outside the Microsoft Office products.

When you use script control, you should consider the following:

- Starting with Microsoft Office 2013, macros are disabled by default. Most of the time, you do not need to enable macros to view the content of an Office document. You should only enable macros for documents you receive from users you trust, and you have a good reason to enable it. Otherwise, macros should always be disabled.
- If the script launches the PowerShell console, and Script Control is set to block the PowerShell console, the script will fail. It is recommended that users change their scripts to invoke the PowerShell scripts, not the PowerShell console.
- Alert only monitors scripts running in your environment. It is recommended for initial deployment or testing.
- Block only allows scripts to run from specific folders. You should use it after you test in Alert mode.

Script Control Setting	Description
Active Script	Active Script includes VBScript and Jscript.
Macros	Microsoft Office macros use Visual Basic for Applications (VBA) to simplify routine actions, like manipulating data in a spreadsheet.
PowerShell	PowerShell refers to PowerShell commands, including one-liners.
Block PowerShell Console Usage	The PowerShell console is blocked.

Device control

Device control protects devices by controlling USB mass storage devices connecting to devices in your organization. You can allow or block things identified as USB mass storage devices, including USB flash drives, external hard drives, and smartphones. Device control is available for the Windows platform only.

Administrators can enable device control using a device policy, and can choose to allow or block access to USB mass storage devices. This only applies to USB devices that are classified as Mass Storage. USB peripherals, such as a keyboard, are not affected. For example, if an administrator creates a policy to block USB mass storage devices, an end-user can still use a USB mouse, but a USB flash drive would be blocked.

As part of a device control policy, administrators can also define exceptions to the policy. This is done by using the vendor ID, product ID, and serial number to specify the exception. Minimally, the vendor ID must be entered, but the product ID and serial number can also be used for a more specific exception.

When enabled, Device Control will log all USB mass storage devices that are inserted, along with the policy that was applied (Allow or Block). If Desktop Notifications are enabled, end-users will see a pop-up notification only if the policy is set to Block. Device Control events can be found on the Protection page, under the External Devices tab.

Note: An Android device could connect and be identified as Android, Still Image, or Windows portable device. If you want to block Android devices, consider blocking Still Image and Windows portable device as well.

Device Control Setting	Description
Blocked	This device type is blocked from accessing the endpoint it is connected to.

Device Control Setting	Description
Full Access	This device type is allowed to access the endpoint it is connected to.

Application control

If enabled, this feature allows users to lockdown specified systems and restrict any changes on the devices after being locked down. Only the applications that exist on a device before the lockdown occurs can execute on that device. Any new applications, as well as changes to the executables of existing applications, will be denied.

Change window

Use the change window option to temporarily disable application control to allow, edit, and run new applications or perform updates. This includes updating the agent. After performing the necessary changes, turn change window off (Closed).

Agent settings

Agent settings can be applied through a policy.

Agent Setting	Description
Desktop Notifications	Agent notification popups can be configured at the policy-level.
Prevent Service Shutdown	The Cylance service is protected from being shutdown either manually or by another process.

Exclusions

All exclusions related to the policy are created using this feature.

Exclusion Setting	Description
Application Control Exclusion	Adding an application control exclusion allows application changes and additions to the specified folders. For Windows, use an absolute path, including the drive letter.
	Example for Windows: C:\Application

Exclusion Setting	Description
External Device Exclusion List	Adding an external device exclusion allows the USB mass storage device to connect to a device.
	• Vendor ID (required) – Include the vendor ID for the USB mass storage device. One way to find the vendor ID is to connect the USB mass storage device to a test endpoint and view the ID in the CylanceON-PREM console.
	• Product ID – Include the product ID for the USB mass storage device. This is optional but can help make a more specific exception.
	• Serial Number – Include the serial number for the USB mass storage device. This is optional but can help make a more specific exception.
	• Comment – Include a comment about why the USB mass storage device is being allowed or blocked. This is optional.
	• Access (required) – Select this option to allow full access or to block the external device.
Memory Violation Exclusion	Adding a memory violation exclusion allows the specified file to run or be installed on any device assigned to the policy. The memory violation exclusion uses a relative file path.
	Example for Windows: \Application\Subfolder\application.exe
	Example for macOS (without spaces): /Applications/SampleApplication.app/Contents/MacOS/executable
	Example for macOS (with spaces): /Applications/Sample Application.app/Contents/MacOS/executable
	See Wildcards in memory violation exclusions for more information.
Policy Safe List	Adding a policy safe list exclusion means all agents assigned to the policy will treat the file as safe, even if Cylance ranks it as unsafe or abnormal. This lets you allow a file to a group of devices but not for the rest of your organization.
	• SHA256 (required) – Include the SHA256 hash for the file you want to allow.
	• MD5 – Include the MD5 hash of the file. This is optional.
	• File Name – Include the filename of the file. This is optional.
	• Category (required) – Use this to categorize files to identify why it is allowed.
	• Reason (required) – Include a reason for allowing this file.
Script Exclusion	Adding a script exclusion allows scripts to run from the specified folder, including subfolders. Use the relative path to the folder.
	Example for Windows: \Application\Subfolder\
Threat Exclusion	Adding a threat exclusion means the folder is excluded from background threat detection and file watcher. This includes subfolders.
	For Windows, use an absolute path, including the drive letter. For macOS, use a relative path, escaping any spaces in the path.
	Example for Windows: C:\Application
	Example for macOS (without spaces): /Applications/SampleApplication.app
	Example for macOS (with spaces): /Applications/Sample\ Application.app

Wildcards in memory violation exclusions

Memory violation exclusions can include the following special characters (all OS): ^ & ' @ { } [ ] , $ = ! - # ( ) % . + ~ _

In Cylance agent 1560 or later, the following additional special characters are also supported for Windows:

- Asterisk (*)
- Any letter value followed by colon (C:)

Pattern Syntax for * Wildcard on Windows

Characters	Usage	Details
*	Excluding executables and applications	Matches zero or more characters, except the platform-specific path separator ('\' on Windows). **Note:** • At this time, "*" escaping is not supported. For example, you cannot exclude a file that contains an asterisk "*" in the file name. • Wildcard exclusions for Memory Violations apply only to Windows at this time.
**	Excluding drives and directories. This can be used to include child directories.	Matches zero or more layers of a directory (e.g. "**\"). Note that "**" is not just a double "*", it is a special notation. To avoid confusion, review the following rules when using this special character: • "**\" is valid if it is at the beginning of pattern, only for Windows. It will match all directories inside all drives. • "**\" can appear in the pattern string multiple times, there is no limitation. **Note:** Wildcard exclusions for Memory Violations apply only to Windows at this time.

Characters	Usage	Details
Examples	N/A	For the following path:

C:\Application\TestApp\MyApp\program.exe (note that relative paths could also be used)

Examples of Correct Exclusions:

- \Application\TestApp\MyApp\program.exe
  - Relative path exclusion without any wildcards.
- C:\Application**\MyApp\program.exe
  - Would exclude program.exe as long as program.exe is located under "MyApp" child directory in C: drive.
- C:\Application**\MyApp*.exe
  - Would exclude any .exe extension file as long as the executable is located under "MyApp" child directory in C: drive.
- C:\Application**\MyApp*
  - Would exclude any executable as long as the executable is located under "MyApp" child directory in C: drive.
- C:\Application\TestApp**\program.exe
  - Would exclude program.exe as long as program.exe is located under any child directory that belongs to "TestApp" parent directory in C: drive.
- **\Application\TestApp\MyApp\program.exe
  - Would exclude program.exe as long as program.exe is located under \Application\TestApp\MyApp\ for any drive.
- **\Application\TestApp\MyApp*.exe
  - Would exclude any .exe extension file as long as the executable is located under \Application\TestApp\MyApp\ for any drive.
- **\Application\TestApp\MyApp*
  - Would exclude any executable as long as the executable is located under \Application\TestApp\MyApp\ for any drive.

Example of Incorrect Exclusions:

- C:\Application\TestA**.exe
  - "**" is used for directories. Use a single asterisk "*" for executables.
- C:\Application**
  - "**" is used for directories. There is no single asterisk "*" specifying executables to exclude.

Not Recommended Exclusions:

- Correct (but not recommended): C:***
  - Would effectively exclude anything in any directory (including child directories) under the C: drive.
- Correct (but not recommended): ***
  - Would effectively exclude anything in any directory (including child directories) in any drive.

Characters	Usage	Details
Note: In a normal wildcard, three asterisks "***" are valid and equal a single asterisk"*". However, three asterisks are not valid for exclusions because it would hide typos. For example, in the pattern "C:***.exe", users might have wanted to type "c:***.exe" but missed one "\". If "***" were treated as a single "*" it could result in different behavior than was intended.		

Import a policy

You can import device policies from the CylancePROTECT console (.xml file) and from other CylanceON-PREM console instances (JSON file) to make it easier to create and manage device policies.

When you import a policy from CylancePROTECT, consider the following:

- The CylancePROTECT policy safe list will not be imported because it is a bloom filter, not a list of hashes.
- If the policy also contains settings for BlackBerry Optics, only the CylancePROTECT policy settings will be imported.

1. Click **Policies**.
2. Click the **Import Policy** icon. The Import Policy window displays.
3. Enter a name for the policy under Policy Name.
4. Click **Browse for a file** and select the policy.xml or policy.json file you exported.
5. Click **Import**. The imported policy displays in the Policy list with the name you specified.

Export a policy

You can export a policy from CylanceON-PREM as a JSON file.

1. Select **Policies** from the menu.
2. Click the Export icon in the Action column beside a policy you want to export. The policy is exported to your browser's download folder as a policy.json file.

Policy rule sets

You can automatically assign a policy to devices using a policy rule. Policy rules are created as part of a rule set. The first policy rule in the set that evaluates to *True* assigns the associated policy to a device. When a policy is assigned to a device, the remainder of the rule set is not evaluated since a device can only have one policy assigned.

Example: You have six policy rules in a rule set. The first two rules evaluate to *False*. The third rule evaluates to *True* and its policy is assigned. The remaining three policy rules are not evaluated since a policy was already assigned, even though rules 4 and 5 would have evaluated to *True* for the device.

You can also manually assign policies to individual devices. For information on manual assignment, see Assign a policy.

Policy rule priority

You can prioritize the priority of a rule by changing its order in the rule set. For example, if you created a number of rules for various policies, and you want the third rule in the set to run first, you can drag the rule to the top of the list. Policy rules evaluate the first rule in the set that runs and evaluates each rule, in order, until it finds a match. As soon as a match is found, the policy associated with that rule is assigned.

Evaluating policy rules

Rules are evaluated in the following scenarios:

- After you edit a rule set and click **Save**. The process of saving the rule set causes all devices to be evaluated against the newly saved rule set.
- Newly added devices will be evaluated when the Agent registers with the CylanceON-PREM Console.
- When the Agent reports updated device attributes to the CylanceON-PREM Console (found under the General Info section on the **Device List >** *select a device* **> Device Details** page). If the device IP or other attribute changes, the rules will be re-evaluated and applied for that device only.
- If a tag is added or removed on a device, the rules will be re-evaluated and applied for that device only.

If no rules match a device, the "Default" rule will be applied along with the Default policy.

Add a policy rule

You can create tags and tag rules first to group the devices. Then create a policy rule that uses the Tag condition to apply a policy to the group of devices. See Add a device tag and Add a tag rule for more information.

Review the following:

- Policies can only be associated with one rule. If the **Add New Rule** button is disabled, it means no policies exist or all policies are assigned to a rule and you will need to create a new policy. See Add a policy for more information.
- Policy rules are not evaluated until the rule set is saved.

1. Add a policy. See Add a policy for more information.
2. Click **Rules > Policy Rules**.
3. Click **Add New Rule**. You can add multiple rules to the rule set at the same time.
4. (Optional) Rules run based on their order in the rule set with the first rule running first, and so on. To reorder the rule, click ⠿ and drag the rule to the correct location in the rule set.
5. Enter a **Rule Name**.
6. (Optional) Enter a Rule Description.
7. Select a policy for **Devices affected will receive the following policy**.
8. Create a rule condition. Rule conditions contain three parts that are used to determine whether a policy rule will be applied: evaluation property, operator, and value. If the rule condition evaluates to *True*, the policy will be applied to a device.
   a) Click an evaluation property from the drop-down list beside **Device Name**.
   b) Click an operator from the drop-down list beside **Starts With**. See Policy rule operators for a description of all available operators.
   c) Enter or select a value for the conditions. This varies depending on the other conditions selected. For example, selecting Device Name will require entering some device name information; selecting Operating System will require selecting a target OS from a list.
9. To add another condition to the rule, click **Add "And" condition** or **Add "OR" condition block**, then enter the condition information.
10. Click **Save**.

Policy rule operators

Review the following table for a list of operators available for policy rules.

Operators	Description
Device Name	This operator uses the information provided to see if the device name matches the condition. • **Contains:** The device name must contain the provided information, but it can be anywhere within the name. • **Does Not Contain:** The device name must not contain the provided information. • **Does Not End With:** The device name must not end with the provided information. • **Does Not Start With:** The device name must not start with the provided information. • **Ends With:** The device name must end with the provided information. • **Starts With:** The device name must start with the provided information. The Device Name value is case sensitive.
Distinguished Name (LDAP)	This operator uses the information provided to see if the distinguished name matches the condition. • **Contains:** The distinguished name must contain the provided information, but it can be anywhere within the name. • **Does Not Contain:** The distinguished name must not contain the provided information. • **Does Not End With:** The distinguished name must not end with the provided information. • **Does Not Start With:** The distinguished name must not start with the provided information. • **Ends With:** The distinguished name must end with the provided information. • **Starts With:** The distinguished name must start with the provided information.
Domain name	This operator uses the information provided to see if the domain name matches the condition. • **Contains:** The domain name must contain the provided information, but it can be anywhere within the name. • **Does Not Contain:** The domain name must not contain the provided information. • **Does Not End With:** The domain name must not end with the provided information. • **Does Not Start With:** The domain name must not start with the provided information. • **Ends With:** The domain name must end with the provided information. • **Starts With:** The domain name must start with the provided information.
IPv4 Address in Range	Provide an IPv4 address range. Any device with an IP address within the given range meets this condition.

Operators	Description
Member of (LDAP)	This operator uses the information provided to see if the device's group membership matches the condition. • **Contains:** The Member Of must contain the provided information, but it can be anywhere within the member information. • **Does Not Contain:** The Member Of must not contain the provided information. • **Is:** The Member Of must match the provided information. • **Is Not:** The Member Of must not match the provided information.
Operating System	This operator uses the information provided to see if the device's operating system matches the condition. • **Is:** The device operating system must match the selected OS. • **Is Not:** The device operating system must not match the selected OS.
Tag	This operator uses the information provided to see if the device has any tags that match the condition. • **Is Any Of:** The device must match one or more of the tags in this condition. You can add multiple tags to this condition.

Agent installation

Devices are added to your organization by installing the CylancePROTECT agent on each system. When they are connected to the CylanceON-PREM console, you can apply policies (to manage identified threats) and organize your devices based on your needs.

The agent is designed to use a minimal amount of system resources. The agent treats files or processes that execute as a priority because these events could be malicious. Files that are simply on disk (in storage but not executing) take a lower priority because while these could be malicious, these do not pose an immediate threat.

Note: CylanceON-PREM requires CylancePROTECT Agent version 1480 or higher to be installed on the endpoints. The agent also requires an installation parameter to configure the agent to communicate with your CylanceON-PREM virtual appliance.

Important note about initial deployment

You must limit the installation of agents to batches of 1,000 endpoints at a time to avoid issues with horizontal scaling during initial endpoint activity.

Add the root CA certificate to every endpoint

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

Add a root CA certificate to Windows

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

Add a root 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`. Click the Terminal icon.
3. In Terminal, type `cd ./Downloads` and press **Return**.

4. 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 change it in the command before running it.
5. Type your password and press **Return**.

Copy installation token

An Installation Token is required when installing the CylancePROTECT Agent.

Note: Do not use the Installation Token from the Cylance Console.

1. Using a web browser, log in to CylanceON-PREM.
2. Click **Settings**.
3. Copy the Installation Token.

Install the Windows agent

This section includes information about Windows system requirements, hardware requirements, and installation parameters.

Windows system requirements

BlackBerry recommends that your device meet the following system requirements.

Supported Windows operating systems

The device can be a physical or virtual machine.

OS	32-Bit	64-Bit	Notes
Windows XP SP3	X	X	KB 968730* and KB 2868626 hotfix must be installed.** ***
			The trusted root certificates listed in KB 293781 must be installed.
Windows Vista	X	X	The trusted root certificates listed in KB 293781 must be installed.
Windows 7	X	X	KB4054518 must be installed on Windows 7 (32-bit and 64-bit) and Windows 7 Embedded (32-bit and 64-bit) systems that use agent 1494 or agent 1550 and later. For more information, read the KB article here. ***
			The trusted root certificates listed in KB 293781 must be installed.
			Support includes Windows Embedded Standard 7 and Embedded POSReady 7.
			Windows POSReady 7 requires agent 1450 or later.

OS	32-Bit	64-Bit	Notes
Windows 8 and 8.1	X		Windows 8 Embedded requires agent 1480 or later. Windows RT is not supported.
Windows 10	X	X	Supports Enterprise, Pro, and Home editions require agent 1310 or later. **Note:** This is for Windows 10 versions prior to the Anniversary update.
Windows 10 Anniversary Update (v1607)	X	X	Windows 10 Anniversary Update (v1607) - requires agent 1400 or later. • Microsoft Windows 10 Device Guard and Credential Guard are supported with agent version 1410 or later. • Microsoft has also introduced a version of Windows Subsystem for Linux (WSL) in the Windows 10 Anniversary Update. WSL lets users run a bash shell on Ubuntu on Windows and has been received very positively by the developer community. WSL is disabled by default and Microsoft is likely to introduce more features before it becomes generally available. Cylance is following these updates and will introduce necessary controls for WSL when it becomes mainstream. Until then, Cylance recommends disabling this feature.
Windows 10 Creators Update (v1703)	X	X	Windows 10 Creators Update (v1703) - requires agent 1440 or later. • **Note:** Windows 10 Creators Update has the same known issues as the Windows 10 Anniversary Update.
Windows 10 Fall Creators Update (v1709 - Redstone 3)	X	X	Windows 10 Fall Creators Update (v1709 - Redstone 3) - requires agent 1440 or later. • agent 1480 added the detection of Microsoft OneDrive files. **Note:** There is one known issue with OneDrive files changing status from "Onlineonly file" to "Locally available file." • Enabling Windows Defender Device Guard Code Integrity will cause Modern Apps to fail with error 0xC000047E when Memory Protection or Script Control is enabled. This issue was resolved with the release of agent 1480. Please read: Memory Protection: Conflict with Modern Apps and Device Guard Code Integrity. • **Note:** Windows 10 Fall Creators Update has the same known issues as the Windows 10 Anniversary Update.
Windows 10 Enterprise 2016 LTSB (Long Term Servicing Branch)	X	X	Windows 10 Enterprise 2016 LTSB (Long Term Servicing Branch) - requires agent 1460 or later.

OS	32-Bit	64-Bit	Notes
Windows 10 April 2018 Update (v1803)	X	X	Windows 10 April 2018 Update (v1803) - requires agent 1490 or later.
Windows 10 "Redstone 5" October 2018 Update (v1809)	X	X	Windows 10 "Redstone 5" October 2018 Update (v1809) - requires agent 1510 or later. • Case sensitive directories are not supported. • **Note:** Unified Write Filter (UWF) is not supported for Windows 10 at this time. The UWF is an optional feature within Windows OS. To ensure you do not experience a conflict, make sure that the UWF is disabled before installing the agent.
Windows 10 Enterprise 2019 LTSC	X	X	Windows 10 Enterprise 2019 LTSC - requires agent 1510 or later.
Windows 10 "Redstone 6" May 2019 Update (v1903)	X	X	Windows 10 "Redstone 6" May 2019 Update (v1903) - requires agent 1530 or later. • Case sensitive file systems are not supported.
Windows 10 "19H2" November 2019 Update (v1909)	X	X	Windows 10 "19H2" November 2019 Update (v1909) - requires agent 1540 or later. • Case sensitive file systems are not supported.
Windows 10 2004 "20H1" May 2020 update	X	X	Windows 10 2004 "20H1" May 2020 update - requires agent 1560 or later. • Case sensitive file systems are not supported.
Windows 10 IoT Enterprise	X	X	Limited support is available in agent 1510. • Windows 10 IoT Core and Windows 10 IoT Core Services are not supported. • ARM is not supported. • The agent does not support the Unified Write Filter (UWF) on Windows 10 IoT. The UWF is an optional feature within Windows OS. To ensure you do not experience a conflict, make sure that the UWF is disabled before installing the agent.
Windows Server 2003 SP2 and 2003 R2	X	X	KB 968730* and KB 2868626 hotfix must be installed.** *** The trusted root certificates listed in KB 293781 must be installed on Windows Server 2003 SP2.

OS	32-Bit	64-Bit	Notes
Windows Server 2008 and 2008 R2	X (2008 Only)	X	KB 3004394 hotfix must be installed on Windows Server 2008 R2 (64-bit) systems.** *** The trusted root certificates listed in KB 293781 must be installed. KB4054518 must be installed on Windows Server 2008 R2 (64-bit) systems that use agent 1494 or agent 1550 and later. For more information, read the KB article here. *** Windows Server 2008 and 2008 R2 Foundation editions require agent 1540 or later. Windows Server 2008 Server Core and 2008 R2 Server Core are not supported.
Windows Server 2012 and 2012 R2	-	X	Agent 1450 or later is required. Supports Standard, Data Center, Essentials, Server Core, Embedded, and Foundation editions. • Windows Server 2012 and 2012 R2 - Embedded edition requires agent 1480 or later. • Windows Server 2012 and 2012 R2 Foundation editions require agent 1540 or later. • Windows Server 2012 and 2012 R2 - Minimal Server Interface is not supported. • Windows Storage Server 2012 is not supported.
Windows Server 2016	-	X	Agent 1410 or later is required. Supports Standard, Data Center, Essentials, and Server Core editions. • Windows Server Core 2016 requires agent 1450 or later • Windows 2016 Nano Server is not supported. • Windows Storage Server 2016 is not supported.

OS	32-Bit	64-Bit	Notes
Windows Server 2019	-	X	Agent 1510 or later is required. Supports Standard, Data Center, and Core editions. • Windows Storage Server 2019 is not supported. • Windows Server 2019 Data Center edition is supported on agent 1530 or later. • Windows Server 2019 Core edition is supported on agent 1560 or later. **Note:** Windows Server 2019 Data Center **does not** support the following features: • Hyper-V Server Role is not supported with Shielded Virtual Machines • Host Guardian Hyper-V Support • Software-defined Networking • Storage Spaces Direct

* For Windows XP and Windows Server 2003, the hotfix in Microsoft's KB 968730 resolves a communication issue with the Console. These older operating systems can have issues obtaining a certificate if the certificate authority (CA) uses SHA256 encryption or later. Cylance is required to use this level of encryption to meet Microsoft security requirements.

** For additional information about errors when accessing secure Cylance hosts, visit support.blackberry.com to read article 66475.

*** Cylance Support does not provide assistance in searching and implementation of any Microsoft related KB's or other third-party patches. For any issues with finding or implementing Microsoft related KB's, please reach out to Microsoft for assistance.

Note: CylancePROTECT does not support scanning unhydrated files from Microsoft OneDrive.

Additional Windows requirements

Requirement	Description
Processor	• Requires at a minimum a two core processor. • Supports the SSE2 Instruction set. • Supports the x86_64 instruction set. • Does not support the ARM instruction set.
RAM	• 2 GB
Available Hard Drive Space	• 600 MB **Note:** Disk space usage can increase depending on features enabled, like setting the log level to Verbose.)

Requirement	Description

Additional Software/ Requirement	• .NET Framework 4.6.2 or higher is required starting with Agent 1570. **Note:** A fully functioning installation of .NET Framework that meets the above specifications is a requirement for the agent to be installed and function as expected.
	• Internet Browser
	• Internet access to login, access the installer, and register the product
	• Local administrator rights to install the software
	• Root Certificates:
	    • VeriSign Class 3 Public Primary Certification Authority - G5
	    • GeoTrust Global CA
	    • thawte Primary Root CA
	    • DigiCert Global Root C
	
	Note: Devices missing any of the above root certificates may experience issues with the Cylance service not starting or the device being unable to communicate with the Console. Please see this article for more details about missing root certificates.

Other	• TLS 1.2 is supported and requires .NET Framework 4.5.2 or higher

Windows installation parameters

The agent must be installed through GPO, SCCM, MSIEXEC, or a similar method. The following parameters are built in to the MSI installer. If an installation parameter is not defined, the default setting is used (if available).

Property	Value	Description
PIDKEY	Installation Token	This is the installation token from your CylanceON-PREM Console.
LAUNCHAPP	0 or 1	0: The system tray icon and the start menu folder are hidden at run-time. 1: The system tray icon and the start menu folder are visible at run-time. This is the default setting.
SELFPROTECTIONLEVEL	1 or 2	1: Only local administrators can make changes to the registry and services. 2: Only the system administrator can make changes to the registry and services. This is the default setting.
APPFOLDER	Target Installation Folder	This specifies the agent installation directory. The default location is: C:\Program Files\Cylance\Desktop.

Property	Value	Description
REGWSC	0 or 1	0: The agent is not registered with Windows as an anti-virus program. This allows CylancePROTECT and Windows Defender to run at the same time on the endpoint.
		1: The agent is registered with Windows as an anti-virus program. This is the default setting.
InstallRegistrationURL	CylanceON-PREM URL	This is the URL for your CylanceON-PREM console.
		Example of third-level domain name: https://login.onprem.com
		Example of second-level domain name: https://onprem.com
InstallTrustedSuffix	CylanceON-PREM URL suffix	This is the URL suffix for your CylanceON-PREM console.
		Example: example.com
InstallInfinityURL	CylanceON-PREM URL	This is the URL for your CylanceON-PREM console.
		Note: You must set the Infinity URL to point to the CylanceON-PREM server URL, which prevents the Agent from attempting to communicate with Cylance Infinity cloud.
		Example of third-level domain name: https://login.onprem.com
		Example of second-level domain name: https://onprem.com

MSI example

```
msiexec /i CylanceProtect_x64.msi /qn PIDKEY=YourInstallationToken
  LAUNCHAPP=1 InstallRegistrationURL=https://onprem.example.com
  InstallTrustedSuffix=example.com InstallInfinityURL=https://onprem.example.com
```

EXE example

```
CylanceProtectSetup.exe /s PIDKEY=YourInstallationToken
  LAUNCHAPP=1 InstallRegistrationURL=https://onprem.example.com
  InstallTrustedSuffix=example.com InstallInfinityURL=https://onprem.example.com
```

Install the macOS agent

This section includes information about macOS system requirements, hardware requirements, and installation parameters.

Supported MacOS operating systems

(Optional) Use the following table to list items and descriptions. If necessary, include an introductory phrase. To create a comparison table, add columns as needed.

OS	Notes
Mac OS X 10.9	Agent 1300 or later
Mac OS X 10.10	Agent 1300 or later
Mac OS X 10.11	Agent 1310 or later
macOS Sierra (10.12)	Agent 1410 or later
macOS High Sierra (10.13)	Agent 1450 or later* **
macOS Mojave (10.14)	Agent 1510 or later* ** ***
macOS Catalina (10.15)	Agent 1550 or later* ***

*macOS High Sierra 10.13 or later includes a new security feature that requires users to approve new third-party kernel extensions. Read this Agent Installation - macOS High Sierra - Secure Kernel Extension Loading article for more information.

**Prior to CylancePROTECT Agent version 1510, the CylancePROTECT Agent was a 32-bit binary for macOS. With the release of 1510, the CylancePROTECT Agent for macOS is a 64-bit binary. With the advent of macOS High Sierra (10.13.4), Apple began to notify users that 32-bit based applications are not optimized to be used on a macOS based machine. This requires additional steps for Agent 1500 or earlier installations, and displays a notification for macOS High Sierra 10.13.4 once; or every 30 days for macOS Mojave 10.14. Read the macOS and 32- bit compatibility article for more information.

***macOS Mojave introduced a security feature that allows third-party applications to access protected user data.

- macOS Mojave version 10.14.x (recommended) - If you are running macOS Mojave and have installed CylancePROTECT, it is recommended that you enable Full Disk Access on your macOS system. If Full Disk Access is not enabled, CylancePROTECT cannot process files secured by user data protection.
- macOS Catalina version 10.15.x or higher (required) - If you are running macOS Catalina or higher and have installed CylancePROTECT, it is required that you enable Full Disk Access on your macOS system. If Full Disk Access is not enabled, Cylance products will be unable to process files secured by user data protection. Starting with macOS Catalina (10.15.x), this now includes the user's Desktop, Downloads, and Documents folders.

Read the macOS - Full Disk Access Requirements article for more information.

Note:

- Case Sensitive volume formats are not supported on Mac OS X or macOS at this time.
- Support for macOS 64-bit is available in Agent 1510 or higher.

Additional MacOS requirements

Requirement	Description
Processor	• Requires at a minimum a two core processor • Supports the SSE2 instruction set • Supports x86_64 instruction set
RAM	• 2 GB
Available Hard Drive Space	• 600 MB **Note:** Disk space usage can increase depending on features enabled, like setting the log level to Verbose.

Additional Requirements	• Internet Browser
	• Internet access to login, access the installer, and register the product
	• Local administrator rights to install the software
	• Root Certificates:
	  • VeriSign Class 3 Public Primary Certification Authority - G5
	  • GeoTrust Global CA
	  • thawte Primary Root CA
	  • DigiCert Global Root
	
	Note: Devices missing any of the above root certificates may experiences issues with the Cylance service not starting or the device being unable to communicate with the Console. Please see this article for more details about missing root certificates.

Other	• TLS 1.2 is supported

Installation parameters – MacOS

The Agent must be installed using the command line options in Terminal. The following parameters are built into the .pkg installer. If an installation parameter is not defined, the default setting is used (if available).

Property	Value	Description
YOURINSTALLTOKEN	Installation Token	This is the installation token from your CylanceON-PREM console.
NoCylanceUI		The agent icon should not appear on startup. The default setting is the icon is visible.
SelfProtectionLevel	1 or 2	1: Only local administrators can make changes to the registry and services. 2: Only the system administrator can make changes to the registry and services. This is the default setting.

Property	Value	Description
LogLevel	0, 1, 2, or 3	0: Error — Only error messages are logged.
		1: Warning — Error and warning messages are logged.
		2: Information (default) — Error, warning, and information messages are logged. This may provide some details during troubleshooting.
		3: Verbose — All messages are logged. When troubleshooting, this is the recommended log level. However, verbose log file sizes can grow very large. It is recommended to turn Verbose on during troubleshooting and then change it back to Information when troubleshooting is complete.
InstallRegistrationURL	CylanceON-PREM URL	This is the URL for your CylanceON-PREM console.
		Example of third-level domain name: https://login.onprem.com
		Example of second-level domain name: https://onprem.com
InstallTrustedSuffix	CylanceON-PREM URL suffix	This is the URL suffix for your CylanceON-PREM console.
		Example: example.com
InstallInfinityURL	CylanceON-PREM URL	This is the URL for your CylanceON-PREM console.
		Example of third-level domain name: https://login.onprem.com
		Example of second-level domain name: https://onprem.com

```
echo YourInstallationToken > cyagent_install_token
echo InstallRegistrationURL=https://onprem.example.com >> cyagent_install_token
echo InstallTrustedSuffix=example.com >> cyagent_install_token
echo InstallInfinityURL=https://onprem.example.com >> cyagent_install_token
sudo installer-pkg CylancePROTECT.pkg -target /
```

Install the Linux agent

This section includes information about Linux system requirements, hardware requirements, and installation steps.

Linux system requirements

BlackBerry recommends that your device meet the following system requirements.

Supported Linux operating systems

OS	32-bit	64-bit	Notes
RHEL/CentOS 6.6	X	X	Requires agent 1480 or later **
RHEL/CentOS 6.7	X	X	Requires agent 1480 or later **
RHEL/CentOS 6.8	X	X	Requires agent 1480 or later **
RHEL/CentOS 6.9	X	X	Requires agent 1480 or later **
RHEL/CentOS 6.10	X	X	Requires agent 1500 or later **
RHEL/CentOS 7.0	X	X	Requires agent 1480 or later **
RHEL/CentOS 7.1		X	Requires agent 1480 or later **
RHEL/CentOS 7.2		X	Requires agent 1480 or later **
RHEL/CentOS 7.3		X	Requires agent 1480 or later **
RHEL/CentOS 7.4		X	Requires agent 1480 or later **
RHEL/CentOS 7.5		X	Requires agent 1490 or later **
RHEL/CentOS 7.6		X	Requires agent 1510 or later **
RHEL/CentOS 7.7		X	Requires agent 1550 or later **
RHEL/CentOS 8.0		X	Requires agent 1574 or later **
RHEL/CentOS 8.1		X	Requires agent 1574 or later **
RHEL/CentOS 8.2		X	Requires agent 1574 or later **
Ubuntu LTS/Xubuntu 14.04	X	X	Requires agent 1574 or later **

OS	32-bit	64-bit	Notes
Ubuntu LTS/Xubuntu 16.04	X	X	Requires agent 1480 or later
Ubuntu LTS/Xubuntu 18.04		X	Requires agent 1510 or later
Amazon Linux 1		X	Requires agent 1574 or later
Amazon Linux 2		X	Requires agent 1574 or later
SUSE (SLES) 11.4		X	Requires agent 1574 or later
SUSE (SLES) 12 SP1, SP2, SP3, SP4		X	Requires agent 1574 or later

**FIPS support:

- For RHEL\CentOS 6.x and 7.x, FIPS support is available in Agent 1560 or higher. To enable FIPs, see FEDERAL INFORMATION PROCESSING STANDARD (FIPS) and How RHEL 8 is designed for FIPS 140-2 requirements.
- For RHEL\CentOS 8.x, FIPS support is available in agent 1574 or higher. To enable FIPS, see How RHEL 8 is designed for FIPS 140-2 requirements for more information.

Additional Linux requirements

Requirement	Description
Processor	• Requires at a minimum a two core processor • Supports the SSE2 instruction set • Supports x86_64 instruction set
RAM	• 2 GB
Available Hard Drive Space	• 600 MB

Other	• TLS 1.2 is supported.
	• Required packages:
	  • glibc.i686
	  • dbus-libs.i686
	    • dbus version 1.10.x or higher
	  • openssl-libs.i686
	  • libgcc.i686
	  • sqlite.i686

Configure Linux agents

Convert and distribute certificates

Agents must trust the certificate that the 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 Linux Agent endpoint.

Mono for Linux steps

The following steps use a CentOS 7.6 virtual machine and 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 CylanceON-PREM virtual appliance.
3. After changing directories, enter the cert-sync command:

   `cert-sync <YOURCERTIFICATE>`

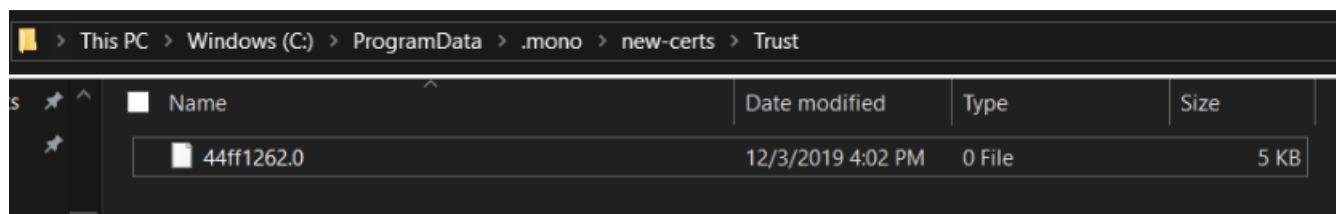   where <YOURCERTIFICATE> should be replaced with your certificate.

   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 installing 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 get around this, 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.

   The following command prompt window appears:

```
Administrator: Open Mono x64 Command Prompt                    —    □

Mono version 6.4.0.198
Prepending 'C:\Program Files\Mono\bin\' to PATH

C:\windows\system32>_
```

3. Change directories to the location where your certificate is stored.

   Note: The certificate needs to be in PEM format.

   Note: IMPORTANT: The certificate required is the one used to sign the certificate and key for your CylanceON-PREM virtual appliance.

4. 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

```
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:

```
      >  This PC  >  Windows (C:)  >  ProgramData  >  .mono  >  new-certs  >  Trust

s  📌  ^      ■  Name               ^          Date modified      Type       Size
   📌             44ff1262.0                   12/3/2019 4:02 PM  0 File          5 KB
```

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

The following installation uses a CentOS 7.4 virtual machine and the user is logged in as the root user.

1. Download the CylancePROTECT Linux agent for CylanceON-PREM. See the How to request access to CylanceON-PREM downloads KB article for more information.

   Note: Do not download the CylancePROTECT Linux agent for CylanceON-PREM from the Cylance console.
2. Copy synced certificates to the proper directory for all target Linux machines. For more information, see Convert and distribute certificates.
3. Create the config_defaults.txt file and include the installation parameters.

   - Enter `mkdir /opt/cylance`, then press **Enter**. This creates the 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 Console.
   - Enter `echo InstallRegistrationURL=<onpremurl> >> config_defaults.txt`, then press **Enter**. Replace <onpremurl> with the fully-qualified domain name for the server. Example: https://onprem.example.com. See more examples in the next section.
   - Enter `echo InstallTrustedSuffix=<onpremsuffix> >> config_defaults.txt`, then press **Enter**. Replayce <onpremsuffix> with the URL suffix for the server. Example: example.com. See more examples in the next section.
   - Enter `echo InstallInfinityURL=<onpremurl> >> config_defaults.txt`, then press **Enter**. Replace <onpremurl> with the fully-qualified domain name for the server. Example: https://onprem.example.com. See more examples in the next section.
4. Navigate to the folder with the 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**.
5. Type `rpm -ivh CylancePROTECT.el7.rpm`, then press **Enter**. This installs the Linux Agent. This example installs the Linux Agent for RHEL 7 / CentOS 7 (el7). Change the RPM file name as needed during installation.
6. Optionally, type `rpm -ivh CylancePROTECTUI.el7.rpm`, then press **Enter**. This installs the UI for the Linux Agent. The UI is not required to run the Agent. 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 CylanceON-PREM. Use the DNS for your virtual appliance.

Example of third-level domain name (onprem.example.com):

```
InstallRegistrationURL=<onpremurl> Example: https://onprem.example.com
InstallTrustedSuffix=<onpremurlsuffix> Example: example.com
InstallInfinityURL=<onpremurl> Example: https://onprem.example.com
Example of second-level domain name (example.com):
```

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

```
InstallRegistrationURL=<onpremurl> Example: https://example.com
InstallTrustedSuffix=<onpremurlsuffix> Example: example.com
InstallInfinityURL=<onpremurl> Example: https://example.com
```

Example:

```
echo InstallToken=YourInstallationToken > config_defaults.txt
echo InstallRegistrationURL=<onpremurl> >> config_defaults.txt
echo InstallTrustedSuffix=<onpremurlsuffix> >> config_defaults.txt
echo InstallInfinityURL=<onpremurl> >> config_defaults.txt
```

Upgrade agents

To upgrade CylancePROTECT Agents that communicate with your CylanceON-PREM virtual appliance:

1. Download the latest Agent upgrade package for your operating system. See FAQ – Where can I download the latest upgrade package for CylancePROTECT for more information.
2. Use a third-party deployment tool to deploy the Agent upgrade package.

Virtual machines

Below are some recommendations for using the CylancePROTECTAgent on a virtual machine image. For best practices, see the virtual desktop infrastructure (VDI) best practices section in the CylancePROTECT Administrator Guide.

- For non-persistent VDI environments, you can use Agent 1490 (or higher) and an installation parameter to instruct the Agent during installation that will be running in a pool of cloned images. This will enable the Agent to recognize each clone as a unique endpoint and persist their identification when they refresh. See the virtual desktop infrastructure (VDI) best practices guide section for more information.
- Some virtual machine software has security settings that conflict with CylancePROTECT's Memory Protection feature. This conflict may result in an unresponsive virtual machine. If this happens, you should either disable the Memory Protection feature or use different virtual machine software.

Device management

The Device List page displays a list of all devices (endpoints with Agents installed) in your organization. The agent must be configured to communicate with your CylanceON-PREM virtual appliance.

Note:

- To filter entries in this list to find information faster, click ☰. See Filter Lists for more information
- To use entries in this list in other applications, click ⊡. See Export Lists for more information.

Assign a policy

You can assign policies manually using this procedure or automatically using policy rules. When assigning policies manually, you can select one or more devices and manually assign them to a policy. For more information about automatically assigning policies, see Policy rule sets.

1. Select **Devices > Device List**.
2. Select one or more devices from the list.
3. Click **Assign Policy**.
4. Click the policy list, then select a policy.
5. Click **Assign Policy to Selected Devices**.

Remove a device

You can also select one or more devices and remove them from your CylanceON-PREM console.

1. Select **Devices > Device List**.
2. Select one or more devices from the list.
3. Click **Remove**. A confirmation message is displayed.
4. Click **Remove Device**.

   Note:

   - Uninstalling the Agent from an endpoint does not remove the device from your CylanceON-PREM console. You must manually remove the device from the console.
   - If you remove a device from your CylanceON-PREM console that still has the agent installed, the agent will ask the user to input the installation token. Either input the installation token or uninstall the Agent from the endpoint.

Device details

Clicking on a device in the Devices List opens the Device Details page. This page contains information related to the selected device, including hostname, policy assigned, device tags, and events found on the endpoint.

Change a policy

A device can only be assigned to one policy.

Note: If a policy is associated with a policy rule, it cannot be manually assigned and does not appear in the list.

1. Select **Devices > Device List**. Select a device.
2. Select a policy from the **Policy** list.
3. Click **Save**.

Change a tag

Multiple tags can be applied to a device. Tags can help you organize and manage your devices.

Note: If a tag is associated with a tag rule, it cannot be manually assigned and does not appear in the list.

1. Select **Devices > Device List**. Select a device.
2. Select one or more tags from the **Tags** list.
3. Click **Save**.

View events

Events are malicious activities found on a device. This can be related to files (threats), scripts, memory, devices, or applications. Each event widget displays the number of events found on that device. Click an events widget to view that events page.

These events pages display the same information as the global events pages (accessed from the Events menu) filtered for the selected device except for the Script Events page. For more information about the global events, see the relevant sections under Threat management. For information about the Script Events page, see the section below.

Device tags

Tags allow you to create common groupings for devices based on physical location, priority, operating system version, business unit, etc. Using these common groupings, you can quickly locate devices or evaluate threats. For example, if you create tags based on operating system version and learn that a vulnerability is targeting a specific operating system, you can use the Device Tags list to quickly find all devices with that operating system across your organization.

After you create tags, you can assign them to a device manually or automatically, but not both. For information about manually assigning tags to devices, see Assign a tag or Change a tag . For information about automatically assigning tags to devices, see Add a tag rule .

Add a device tag

You can manually add a tag to a device

1. Click **Devices > Device Tags**.
2. Click **Add New Device Tag**.

3. Type a name for the tag.
4. Click **Add New Tag**.

Assign a tag

Tags can be assigned manually using this procedure or automatically using tag rules. When you assign tags manually, you can select multiple devices at a time and assign them to a tag. For more information about automatically assigning tags, see Tag rules.

Note: If a tag is associated with a tag rule, it cannot be manually assigned and does not appear in the Assign Tag dialog.

1. Select **Devices > Device List**.
2. Select one or more devices from the list.
3. Click **Assign Tag**.
4. Click the drop-down list and select a tag from the list.
5. Click **Assign Tags**.

Tag rules

Tag rules automatically assign or remove tags from devices. This helps you to automatically organize and manage tags on your devices. If a tag is assigned to a device using a tag rule, and the device later evaluates to *false*, the tag will be automatically removed from the device.

You can also manually assign tags to individual devices. For information on manual assignment, see Assign a tag.

Example: If a device is located in the Portland office and the user transfers to the Austin office, if you manually assigned tags, you will need to remove the Portland tag from the device and then assign the Austin tag. If you use tag rules to assign tags, when the user transfers to Austin, the tag rule for Portland will evaluate to *false* and automatically remove the Portland tag. When the tag rule for the Austin office evaluates to *True*, the Austin tag will be assigned to the device.

Tag rules are independent of each other and there are no priorities like those used in policy rule sets.

Multiple tags can be assigned to a device using tag rules. As long as each tag rule evaluates to *True*, the tag will be assigned. For example, a device can have both an Austin office tag and an Engineering tag assigned to it.

Tag rules are deterministic

The same tag cannot be applied both manually and automatically. The reasons behind this are as follows:

- For automatic tagging to be useful, you want the tags to reflect a device's current state and not the device's past state. This means tags are both automatically assigned and removed from devices. In the example above, a device originally sat in the Portland office. When the user transferred to Austin, it would have both Portland and Austin tags assigned unless Portland was removed.
- If you can manually remove a tag that was assigned by a tag rule, it is no longer deterministic. For example, if you have 10 devices that should have the same tag assigned, but the tag could be manually removed from one device, you wouldn't have any way to know why the tag wasn't applied to that device and might wonder if there was an issue with the rule.

Evaluating tag rules

Tag rules are evaluated in the following scenarios:

- Newly created tag rules will evaluate against all devices.
- Edited tag rules will evaluate against all devices.
- A report of updated device attributes will evaluate all tag rules against that device.

Add a tag rule

A tag can only be associated with one tag rule. However, you can add multiple AND/OR conditions to evaluate additional properties of a tag rule.

1. Add a device tag. See Add a device tag for more information.
2. Click **Rules > Tag Rules**.
3. Click **Add New Tag Rule**.
4. Enter a **Tag Rule Name**.
5. (Optional) Enter a rule description.
6. Select a tag for **Devices affected will receive the following tag**.
7. Create a rule condition. Rule conditions contain three parts that are used to determine whether a tag rule will be applied: evaluation property, operator, and value. If the rule condition evaluates to *True*, the tag will be applied to a device.
   a) Click an evaluation property from the drop-down list beside **Device Name**.
   b) Click an operator from the drop-down list beside **Starts With**. See Tag rule operators for a detailed description of all available operators.
   c) Enter or select a value for the conditions. This varies depending on the other conditions selected. For example, if you select Device Name, you must enter some device name information; if you select Operating System, you must select a target OS from a list.
8. To add another condition to the rule, click **Add "And" condition** or **Add "OR" condition block**, then enter the rule condition information.
9. Click **Add New Tag Rule**.

   Note: To remove a tag rule, select a rule and click **Remove**. If you remove a tag rule, it will also remove the tag from all devices.

Best practice: exclude a device from a rule

When you use tag rules, you may need to create an exception to a tag rule to exclude a device that would otherwise evaluate to *True* and have the tag assigned. For example, you have a tag rule with the following condition:

- Evaluation Property = Device Name
- Operator = Starts With
- Value = Sal

There are 20 devices that match this criteria and will have the tag assigned. However, you want to exclude one of the devices from the tag assignment. In the tag rule, you can add an "AND " condition and set the rule condition to:

- Evaluation property = Device
- Operator = Is Not
- Value = *Sal123East*

Tag rule operators

Review the following table for a list of operators available for tag rules.

Operator	Description
Device Name	This operator uses the information provided to see if the device name matches the condition. • **Contains:** The device name must contain the provided information, but it can be anywhere within the name. • **Does Not Contain:** The device name must not contain the provided information. • **Does Not End With:** The device name must not end with the provided information. • **Does Not Start With:** The device name must not start with the provided information. • **Ends With:** The device name must end with the provided information. • **Starts With:** The device name must start with the provided information. The Device Name field is case sensitive.
Device	This operator uses the information provided to see if the selected device matches the condition. • **Is Not:** The device name must not match the provided information.
Distinguished Name (LDAP)	This operator uses the information provided to see if the distinguished name matches the condition. • **Contains:** The distinguished name must contain the provided information, but it can be anywhere within the name. • **Does Not Contain:** The distinguished name must not contain the provided information. • **Does Not End With:** The distinguished name must not end with the provided information. • **Does Not Start With:** The distinguished name must not start with the provided information. • **Ends With:** The distinguished name must end with the provided information. • **Starts With:** The distinguished name must start with the provided information.

Operator	Description
Domain name	This operator uses the information provided to see if the domain name matches the condition. • **Contains:** The domain name must contain the provided information, but it can be anywhere within the name. • **Does Not Contain:** The domain name must not contain the provided information. • **Does Not End With:** The domain name must not end with the provided information. • **Does Not Start With:** The domain name must not start with the provided information. • **Ends With:** The domain name must end with the provided information. • **Starts With:** The domain name must start with the provided information.
IPv4 Address in Range	This operator uses an IP address range that you specify. Any device with an IP address within the given range meets this condition.
Member of (LDAP)	This operator uses the information provided to see if the device's group membership matches the condition. • **Contains:** The Member Of must contain the provided information, but it can be anywhere within the member information. • **Does Not Contain:** The Member Of must not contain the provided information. • **Is:** The Member Of must match the provided information. • **Is Not:** The Member Of must not match the provided information.
Operating System	This operator uses the information provided to see if the device's operating system matches the condition. • **Is:** The device operating system must match the selected OS. • **Is Not:** The device operating system must not match the selected OS.

Edit a tag name

You can edit the name of a tag that is manually or automatically applied to devices and the new name will be applied to the devices. If the tag is used in a tag rule, the tag will be updated in the rule and applied to the devices.

1. Click **Devices > Device Tags**.
2. Click 🖉 in the Action column beside the tag.
3. Rename the tag.
4. Click **Update Tag**.

Remove a tag from a device

You can use this feature to manually remove a tag. If a tag has been automatically assigned to a device using a Tag Rule, it cannot be manually removed from a device. Instead, you will need to modify the Tag rule so it will be unassigned.

1. Click **Devices > Device Tags**.
2. Click on a tag. A list of devices assigned to the tag displays.
3. Select the checkboxes for the devices for which you want to remove the tag.
4. Click **Remove Tag From Device**.

Remove a tag from the CylanceON-PREM console

In addition to removing a tag from a device, you can also remove it from the CylanceON-PREM Console. When you remove a tag from the Console, the tag will also be removed from devices.

1. Click **Devices > Device Tags**.
2. Select the checkbox beside the tag you want to remove.
3. Click **Remove**.

Set agent logging level

Agent logs provide details about agent activity, including errors and warnings. There are four levels of logging available:

- Errors - Records errors only
- Warnings - Records errors and warnings
- Information - Gives a baseline of activity by the program that includes information, errors, and warnings. This is the default agent setting.
- Verbose - Detailed information of program activity; useful for troubleshooting.

  Note: Verbose logging can use a lot of disc space due to the amount of information recorded. It is recommended to only enable verbose logging while troubleshooting issues. When troubleshooting is complete, set the agent logging level to information.

1. Click **Devices > Device List**.
2. Click on a device. The device details page displays.
3. For **Agent Logging Level**, select a logging level.
4. Click **Save**.

Threat management

This section includes information about acting on and acknowledging threat events.

Act on threat events

The Threat Events page displays a list of files that are considered threats, that were found on devices in your organization. You can select a threat, or multiple threats, and add them to the Global Quarantine list or the Global Safelist.

On the Threat Events page, you can add a threat event to a global list (quarantine or safe), or acknowledge that the event has been reviewed (but no action was taken).

1. In the console, select **Events > Threat Events**. Or click the Threat Events widget on the Dashboard.
2. (Optional) Click **<number> Removed Threats** above the right side of the list to view the total number of threat events automatically removed by the Agent. If your policy has **Auto Delete Quarantine** enabled for a specified number of days in Threat Settings, files automatically quarantined by the Agent will be deleted after a specified number of days and will be removed from the Threat Events page. This button allows you to view all removed threats that were automatically deleted by the Agent since the beginning of time.
3. Click the check box for one or more events and select an action:

    *   **Globally Quarantine** – Click to add events to the Global Quarantine list and set the event status to Acknowledged. These events are automatically quarantined on all devices in your organization.
    *   **Globally Safelist** – Click to add events to the Global Safelist and set the event status to Acknowledged. These events are allowed on all devices in your organization.
    *   **Acknowledge** – Click to change the event status from *No* to *Acknowledged* (Yes). Acknowledged means that a user has manually acknowledged an event by either clicking on this button or by manually adding the event to the Global Quarantine or Safe List. If you do not want to take any other action on an event (like adding it to the Quarantine or Safe List), and know the event isn't a threat, the Acknowledge button is an easy way to lower the threat in the list so you can focus on events that do require attention. By default, the events list displays events that have not been acknowledged first.

    Note:

    *   To filter entries in this list to find information faster, click ▼. See Filter Lists for more information
    *   To use entries in this list in other applications, click ⊡. See Export Lists for more information.

Threat event field definitions

The following information displays in the Events List:

File Event	Description
Acknowledged	Acknowledging an event means it has been reviewed.
Detected By	This is the name of the CylancePROTECT feature that detected the event.
Device Name	This is the name of the device.
File Owner	This is the owner of the file that is considered to be a threat.
File Path	This is the path where the threat was found.

File Event	Description
File Status	This is the status of the file on the device (Unsafe, Quarantined, Waived, or Abnormal).
Global List	This indicates whether an event has been added to the Global List (Quarantine or Safe) or blank if the event is new.
Hash	This is the is the SHA256 hash for the file.
Reported On	This is the date and time the event was first discovered in your organization.
Score	This is the Cylance Score for the event. The range is -1 to -1,000. See Cylance score for more information.

Cylance score

When you view threat information in the CylanceON-PREM console, a Cylance Score is assigned to a file that is a potential threat to your devices. The score represents the confidence level that the file poses a real danger to your environment. The higher the score, the greater the confidence level that the file can be used for malicious purposes. Based on the score, threats are considered either unsafe or abnormal.

- **Unsafe:** A file with a score ranging from -600 to -1000. An unsafe file is a suspicious file that can be used to negatively impact your devices.
- **Abnormal:** A file with a score ranging from -1 to -599. An abnormal file might pose a threat to your devices.

Files with a score of 0 to 1,000 are considered safe and do not appear in the Console.

Note: When calculating the score, CylanceON-PREM uses the local model when analyzing files and does not require an Internet connection to gather threat information.

Act on script events

The script events page displays a list of scripts that are considered threats, that were found on devices in your organization. You can select a script, or multiple scripts, and add them to the Global Safelist.

Note: This page aggregates the same event for all devices to help "keep the noise down". A separate Script Events page is available that provides more information on the Device List > *select a device* > Script Events widget. For more information, see View events .

On the Scripts Events page, you can add a script event to the global safelist or acknowledge that the event has been reviewed (but no action was taken).

1. In the console, select **Events > Script Events**. Or click the Script Events widget on the dashboard.
2. Click the check box for one or more events and select an action:
3. Click an action.

- **Globally Safelist** – Adds events to the Global Safelist. These events are allowed on all devices in your organization.
- **Acknowledge** – Click to change the event status from *No* to *Acknowledged* (Yes). Acknowledged means that a user has manually acknowledged an event by either clicking on this button or by manually adding the event to the Global Quarantine or Safe List. If you do not want to take any other action on an event (like adding it to the Quarantine or Safe List), and know the event isn't a threat, the Acknowledge button is an

easy way to lower the threat in the list so you can focus on events that do require attention. By default, the events list displays events that have not been acknowledged first.

Note:

- To filter entries in this list to find information faster, click ≂. See Filter Lists for more information
- To use entries in this list in other applications, click ⊡. See Export Lists for more information.

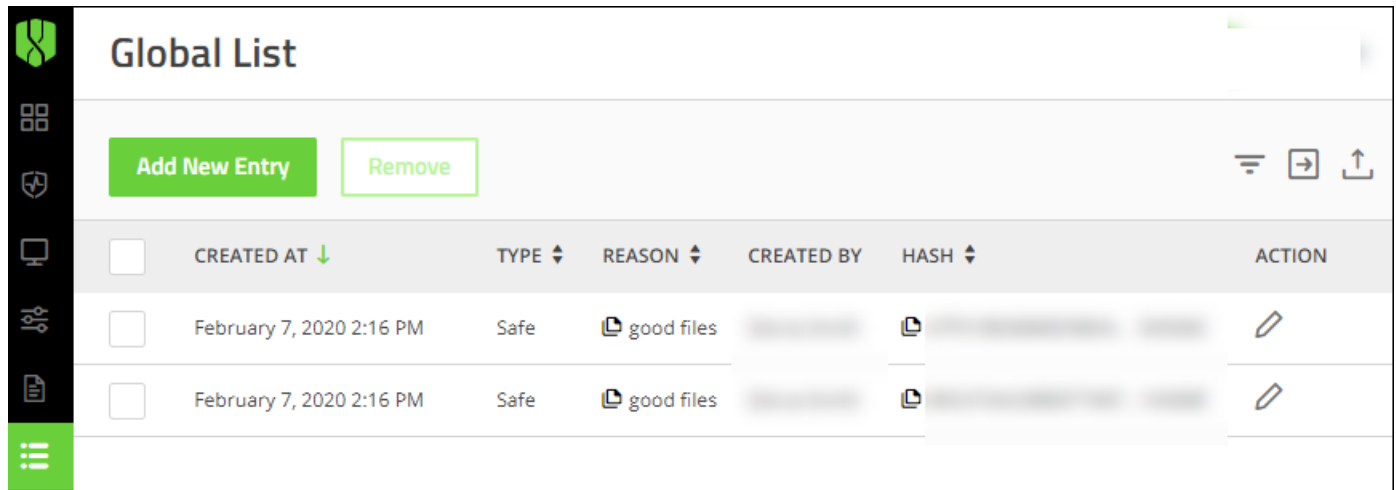## Script event field definitions

The following information displays in the Events List:

Script Event	Description
# Devices	This is the number of devices affected by this script.
Acknowledged	Acknowledging an event means it has been reviewed.
Alerts	This is the number of alerts triggered by this script.
Blocks	This is the number of times the script was discovered and was blocked.
Drive Type	This is the drive or storage type the script was discovered on. **Example:** Internal Hard Drive or Network Drive.
File Path	This is the path where the script was found.
Interpreter	This is the script interpreter that is responsible for executing the script. This could be PowerShell, Active Script, or Microsoft Office Macros.
Last Reported	This is the date and time the script was last discovered on devices in your organization.
Hash	This is the SHA256 hash for the script file.
Safe	This is the current status of the event.

Acknowledge memory events

The Memory Events page displays a list of memory-related events that are considered threats, that were found on devices in your organization.

On the Memory Events page, you can acknowledge that the event has been reviewed.

1. In the console, select **Events > Memory Events**. Or click the Memory Events widget on the dashboard.
2. Click the checkbox for one or more events and select an action:

   Acknowledge – Click to change the event status from *No* to *Acknowledged* (Yes). Acknowledged means that a user has manually acknowledged an event by either clicking on this button or by manually adding the event to the Global Quarantine or Safe List. If you do not want to take any other action on an event (like adding it to the Quarantine or Safe List), and know the event isn't a threat, the Acknowledge button is an easy way to lower the threat in the list so you can focus on events that do require attention. By default, the events list displays events that have not been acknowledged first.

Note:

- To filter entries in this list to find information faster, click ⬇. See Filter Lists for more information
- To use entries in this list in other applications, click ➡. See Export Lists for more information.

Memory event field definitions

The following information displays in the Events List:

Memory Event	Description
Acknowledged	Acknowledging an event means it has been reviewed.
Action	This is the action taken on the event.
Device Name	This is the name of the device.
File Path	This is the path to the file that triggered the memory event.
Hash	This is the SHA256 hash information for the event.
Reported On	This is the date and time the event was first discovered in your organization.
Process ID	This is the ID of the process that caused the memory event.
Type	This is the exploit type.
Username	This is the user that was logged in to the device when the memory event occurred.

Acknowledge device events

The Device Events page displays a list of USB mass storage device events that occurred on devices in your organization.

On the Device Events page, you can acknowledge that the event has been reviewed.

1. In the console, select **Events > Device Events**. Or click the Device Events widget on the dashboard.
2. Click the checkbox for one or more events and select an action:

   Acknowledge – Click to change the event status from *No* to *Acknowledged* (Yes). Acknowledged means that a user has manually acknowledged an event by either clicking on this button or by manually adding the event to the Global Quarantine or Safe List. If you do not want to take any other action on an event (like adding it to the Quarantine or Safe List), and know the event isn't a threat, the Acknowledge button is an easy way to lower the threat in the list so you can focus on events that do require attention. By default, the events list displays events that have not been acknowledged first.

   Note:

   - To filter entries in this list to find information faster, click ⬇. See Filter Lists for more information
   - To use entries in this list in other applications, click ➡. See Export Lists for more information.

Device event field definitions

The following information displays in the Events List:

Device Event	Description
Acknowledged	Acknowledging an event means it has been reviewed.
Action	This is the action taken on the event. This could be Block or Allow.
Device Name	This is the name of the device.
Device Type	This is the type of USB mass storage device.
Last Detected	This is the date and time the device event last occurred.
Last Reported User	This is the last user that logged into the device.
Name	This is the name of the USB mass storage device.
Product ID	This is the product identifier for the USB mass storage device.
Serial Number	This is the serial number for the USB mass storage device.
Vendor ID	This is the vendor identifier for the USB mass storage device.

Acknowledge application events

The Application Events page displays a list of application events that are considered threats, that were found on devices in your organization.

On the Application Events page, you can acknowledge that the event has been reviewed.

1. In the console, select **Events > Application Events**. Or click the Application Events widget on the dashboard.
2. Click the checkbox for one or more events and select an action:

    Acknowledge – Click to change the event status from *No* to *Acknowledged* (Yes). Acknowledged means that a user has manually acknowledged an event by either clicking on this button or by manually adding the event to the Global Quarantine or Safe List. If you do not want to take any other action on an event (like adding it to the Quarantine or Safe List), and know the event isn't a threat, the Acknowledge button is an easy way to lower the threat in the list so you can focus on events that do require attention. By default, the events list displays events that have not been acknowledged first.

    Note:

    *   To filter entries in this list to find information faster, click ☰. See Filter Lists for more information
    *   To use entries in this list in other applications, click ⤷. See Export Lists for more information.

Application event field definitions

The following information displays in the Events List:

Application Event	Description
Acknowledged	Acknowledging an event means it has been reviewed.
Action	This is the action taken on the event.
Device Name	This is the name of the device.
File Path	This is the path to the file that triggered the memory event.
Hash	This is the hash (SHA256) or other identifier for the application event.
Last Reported User	This is the last user that logged into the device.
Reported On	This is the date and time the event was first discovered in your organization.
Type	This is the exploit type.

Global lists

You can use this page to view a list of all events (file, script, memory, etc.) that have been quarantined or added to the safe list on devices in your organization.

Add a global list entry

1. In the console, click **Global Lists** or click the Global Lists widget on the dashboard.
2. Click **Add New Entry**.
3. Select an action from the list:
   - **Quarantine:** The entry is added to the Global Quarantine list. This entry will be quarantined on all devices in your organization.
   - **Safe:** The entry is added to the Global Safelist. This entry will be allowed on all devices in your organization.
   - **Script:** The entry is added to the Safe Script list. This script will be allowed on all devices in your organization.
4. Type in the SHA256 hash for the entry.
5. Type a reason for adding this entry.
6. Click **Create**.

Import a global list

You can import a Global List from CylancePROTECT or CylanceON-PREM so that you don't have to manually add hashes to the Global List.

Note: Importing a CylanceON-PREM Global List that was exported from CylanceON-PREM is available in CylanceON-PREM v1.7.1 or higher.

1. Click **Global Lists**. Or click the Global Lists widget on the dashboard.
2. Click [↑]. The Import Global List window displays.
3. Select the type of list you are importing.

4. Browse for a .csv file or drag and drop one in the box.
5. Click **Import**. Once imported a dialog displays the results:

   - **Imported** - This is the number of entries that were imported.
   - **Skipped** - This is the number of entries were not imported because they already exist in the Global List.
   - **Conflicts** - This is the number of entries that were in conflict because they were the wrong type. For example, you imported quarantined entries but the .csv file also contained three safelist entries so the three safelist entries would be listed as conflicts.

     Note: You can export entries in this list for use in other applications by clicking [→]. See Export Lists for more information.

Remove a global list entry

1. Click **Global Lists**. Or click the Global Lists widget on the dashboard.
2. Click the checkbox for one or more entries.
3. Click **Remove**. A confirmation message displays.
4. Click **Remove Global List Entry**.
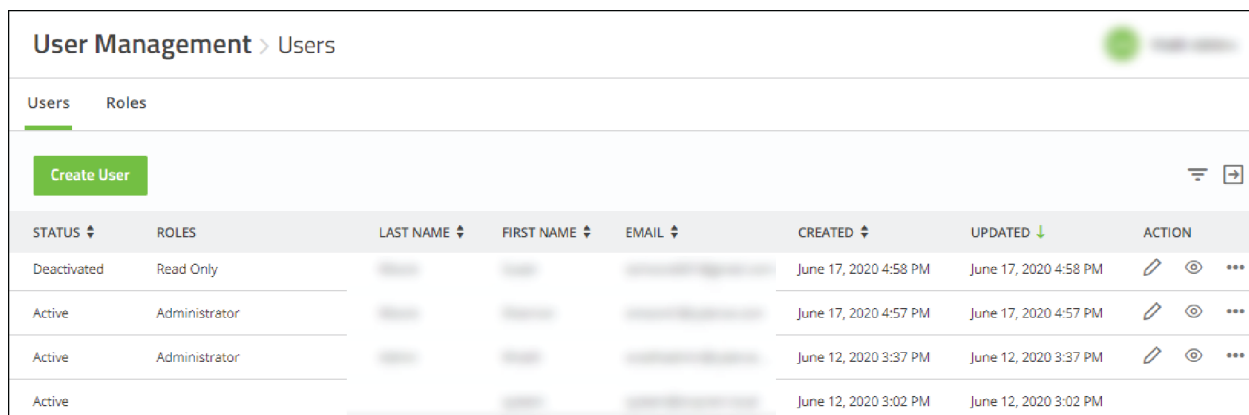
Administration

This section includes information about managing users, managing roles, the audit log, and applications.

Managing users

You can manage users who have access to your CylanceON-PREM console, and what those users can do based on the role assigned to them.

Note: When you deploy CylanceON-PREM for the first time, it creates a system account (First Name=system and Email=system@onprem.local) that is used in Audit Logs to identify actions taken by the system versus actions taken by a CylanceON-PREM user. For example, the system account is used when the system applies a policy to a device as a result of a policy rules match.

Create a user

CylanceON-PREM has two pre-defined roles: Administrator and Read-Only. You can create custom roles and assign them to users. See Managing roles for more information.

1. Click **Access Management > User Management**. Or click the User Management widget on the Dashboard.
2. Click **Create User**.
3. Type in the user information – First Name, Last Name, and email address. The email address must be unique to your console. The user's email address is their username.
4. Type and confirm a password for the user. See Password requirements for important information about setting passwords.
5. Select an **Associated Role** for the user.
6. Click **Create**. You must communicate the username and password to the appropriate user. It is highly recommended the user change the password the first time they log in.

   Note: CylanceON-PREM does not provide any email notifications.

After you finish: To edit a user, click ✎ in the Action column beside the entry to edit.

Create a user with identity provider settings enabled

With CylanceON-PREM version 1.5.4.1 or higher, administrators can enable Identity Provider Settings for Single Sign-On access to the console. Read Configure identity provider settings for settings information.

1. Click **Access Management > User Management**. Or click the User Management widget on the Dashboard.

2. Click **Create User**.

3. Type in the user information – First Name, Last Name, and email address. The email address must be unique to your console. The user's email address is their username.

4. Select **SSO** for Account Type. A password is not required because authentication is done through the identity provider.

5. Select an **Associated Role** for the user.

6. Click **Create**. You must communicate the username and password to the appropriate user. It is highly recommended the user change the password the first time they log in.

   Note: CylanceON-PREM does not provide any email notifications.

Password requirements

Passwords in CylanceON-PREM have the following requirements:

- Passwords must be a minimum of 14 characters and include all of the following:
  - At least one upper-case letter (A through Z)
  - At least one lower-case letter (a through z)
  - At least one numeric (0 through 9)
  - At least one special character (for example, ~!@#$%^&*()_ + = ' [ ] / ? > <)
  - Passwords cannot contain personally identifiable information
- Passwords cannot be the same as the last ten passwords.
- Passwords expire after 180 days.
- Users will be locked out for five minutes after three failed attempts to enter their password.

Note: Administrators should generate a random password when changing or resetting a user's password. Do not use a generic password because the password may already be in the user's history (last ten passwords) so it will be prohibited.

Change a user password

For users configured with an identity provider, the password is not changed in the CylanceON-PREM Console. The password must be changed through the identity provider (like the IdP's website).

Only administrators can change a user's password.

Note: You should generate a random password when you change or reset a user's password. Do not use a generic password because the password will already be in the user's history (saved for minimum of ten generations) so it will be prohibited.

1. Click **Access Management > User Management**.

2. Click [•••] beside the user whose password you want to change.

3. Click **Change Password**.

4. Type and confirm the new password. See Password requirements for important information about setting passwords.

5. Click **Update**.

Deactivate a user

After deactivating a user, the user cannot log in to your CylanceON-PREM console. You can still perform actions on deactivated users (edit and view).

1. Click **Access Management > User Management**.

2. Click [▪▪▪] for the user you want to deactivate.

3. Click **Deactivate**.

Activate a deactivated user

1. Click **Access Management > User Management**.

2. Click [▪▪▪] beside the user you want to activate.

3. Click **Activate**.

Delete a user

Deleted users are permanently removed from the system and cannot be recovered. You should Deactivate a user if you want to keep a record of the user in the system or if you need to reactivate them in the future.

1. Click **Access Management > User Management**.

2. Click [▪▪▪] beside the user you want to delete.

3. Click **Delete**. A message displays prompting you to confirm the deletion.

4. Click **Remove User**.

Add administrators who must use certificate-based authentication

1. In the CylanceON-PREM console, click **Access Management > User Management**.

2. Click **Create User**.

3. Type the administrator's information.

4. For Account Type, select **Certificate**.

5. Type the UPN for the administrator.

6. Select any of the Associated Roles.

7. Click **Create**.

Edit an existing administrator to use certificate-based authentication

1. In the CylanceON-PREM console, click **Access Management > User Management**.

2. Click ✐ beside the administrator that must use certificate-based authentication.

3. In the Account Type section, click **Certificate**.

4. Type the UPN for the administrator.

5. Click **Update**.

Managing roles

Roles allow or restrict access to your CylanceON-PREM console. CylanceON-PREM has two default roles: administrator and read-only. Administrators can create custom roles and assign these to users. Custom roles display as check boxes below the default roles.

- **Administrators** have global permissions and can add or remove users, assign tags, manage devices, and manage policies.

- **Read-Only** users can view information in your CylanceON-PREM console. Read-only users cannot make any changes.

Create a role

1. Click **Access Management > Role Management**.
2. Click **Create Role**.
3. Type in a name for the new role. The role name must be unique.
4. Select the permissions granted to the role. See Role permissions for more information. A role must have View permission to create, edit, or delete an entry.
5. Click **Create**.

After you finish:

- To edit a role, click ✎ beside the role you want to edit.
- To delete a role, click 🗑 beside the role you want to delete.
  If a role is assigned to one or more users, that role cannot be deleted. Reassign these users to another role, then delete the role.

Role permissions

The following table describes the available permissions:

Role Permission Type	Description
Application	Applications allow access to the CylanceON-PREM API. • View allows users to view the Application Settings and the Application ID, but users cannot view the Application Secret. • Create allows users to add a new application. • Update allows users to edit and update an application. • Delete allows users to delete an application.
Audit Logs	Audit Logs record all user interactions with your CylanceON-PREM Console. This includes creating, updating, and deleting things. • View allows users to view the Audit Logs page. Users can also download the Audit Logs as a CSV file.
Detection Events	Detection Events are threat events discovered on your devices. • View allows users to view all Events pages, including File Events, Script Events, Memory Events, Device Events, and Application Events.

Role Permission Type	Description
Devices	Devices are your endpoints with Agents. Agents must be configured to communicate with your CylanceON-PREM Console. • View allows users to view the Device List page. This option must be selected for users to create, update, or delete tags. • Create allows users to add a new device using the installation token. • Update allows users to edit and update device information. • Delete allows users to delete devices from the CylanceON-PREM Console.
Exclusions	Exclusions define what is on the Safe List or the Quarantine list. • View allows users to view the Safe/Quarantine page. This option must be selected for users to create, update, or delete tags. • Create allows users to create a new Exclusion. • Update allows users to edit existing Exclusions. • Delete allows users to delete existing Exclusions.
Installation Token	Installation tokens are a randomly generated string of characters that enables the agent to report to its assigned account on the CylanceON-PREM console. **Note:** View System Settings must also be enabled for users to view the installation token. • Regenerate allows users to generate a new installation token. Regenerating the installation token should only be used to prevent installation of new agents with the existing token. All agents installed using the token prior to regenerating it will continue to communicate with the console.
Network Configuration	Network Settings define the IP Address for the CylanceON-PREM appliance as well as other configuration options. **Note:** View System Settings must also be enabled for users to view the installation token. • Update allows users to edit the fields in Network Settings.
Policies	Policies define what the Agent will do with threats. • View allows users to view the Policies page. This option must be selected for users to create, update, or delete tags. • Create allows users to create new Policies. • Update allows users to edit existing Policies. • Delete allows users to delete existing Policies.

Role Permission Type	Description
Roles	Roles define what a user can do in the CylanceON-PREM Console. • View allows users to view the Role Management page. This option must be selected for users to create, update, or delete tags. • Create allows users to create new Roles. • Update allows users to edit existing Roles. • Delete allows users to delete existing Roles.
Rules	Rules can automatically assign a policy to a device, based on the selected conditions (like Device Name, IPv4 Address, or Operating System). • View allows users to view the Rules page. • Create allows users to create a rule. • Update allows users to edit existing rules. • Delete allows users to delete rules.
SSL Certificates	CylanceON-PREM requires a certificate to ensure secure communication between the server and the endpoints. • View allows users to view the Certificates page. • Install allows users to add a certificate. • Update allows users to update a certificate. • Delete allows users to delete a certificate.
System Logging Settings	System Logging Settings sets the level of information captured in the log file. **Note:** View System Settings must also be enabled for users to view system logging settings. • Update allows users to change the logging level for the CylanceON-PREM virtual appliance.
System Logs	System logs are the log files for the CylanceON-PREM virtual appliance. System logs can help when troubleshooting issues with the virtual appliance. **Note:** View system settings must also be enabled for users to view system version. • Downloads allows users to download System Logs.
System Settings	System Settings displays the installation token (used when installing the agent) and system settings (version, hostname, IP address, log level, and console language). • View allows users to view the System Settings page.

Role Permission Type	Description
System Version	System Version provides a way to update the CylanceON-PREM virtual appliance. **Note:** View system settings must also be enabled for users to view system version. • Update allows users to update the CylanceON-PREM virtual appliance.
Tags	Device Tags allow you to group your devices based on your criteria. • View allows users to view the Device Tagging page. This option must be selected for users to create, update, or delete tags. • Create allows users to create a Device Tag. • Update allows users to update a Device Tag. • Delete allows users to delete a Device Tag.
Users	Users have access to the CylanceON-PREM Console. Use roles to grant or restrict access to the CylanceON-PREM console. • View allows users to view the User Management page. This option must be selected for users to create, update, or delete tags. • Create allows users to create a User. • Update allows users to update a User. • Delete allows users to delete a User.

Update profile information

1. Hover over your account name. Click **My Account**.
2. Under Update Information, change your profile information. You can change your first and last Name only.
3. Click **Update**.

Change your password

1. Hover over your account name. Click **My Account**.
2. Under Change Password, type in your old password, then type in and confirm your new password. See Create a user for more information.
3. Click **Update**.

Audit logs

The audit logs contain information pertaining to the following actions performed from the CylanceON-PREM console.

Note: When you deploy CylanceON-PREM for the first time, it creates a system account (First Name=system and Email=system@onprem.local) that is used in Audit Logs to identify actions taken by the system versus actions taken by a CylanceON-PREM user. For example, the system account is used when the system applies a policy to a device as a result of a policy rules match.

Event	Actions
Agent Update	Edit
Device	Edit, delete
Global List	Create, delete
Login	Success, failure
Logout	Success, failure
Policy	Create, edit, delete
Policy Rule	Create, edit, delete, auto policy applied The Audit Log will have one entry per device when a rule is automatically applied because conditions were met.
Role	Create, update, delete
Tag	Create, update, delete, assigned
Tag Rule	Create, update, delete, auto tag applied The Audit Log will have one entry per device when a rule is automatically applied because conditions were met.
Threat	Quarantine, waive, global quarantine, safe list
User	Create, edit, delete, assigned
Virtual Appliance Update	Enable or disable maintenance mode

Note:

- To filter entries in this list to find information faster, click ☰. See Filter Lists for more information
- To use entries in this list in other applications, click ⬆. See Export Lists for more information.

Certificates

You can view and manage certificates used by the following features from this page:

- Syslog/SIEM
- LDAP
- External database

The certificate can be added before or after configuring these features.

Note:

- You cannot manage the CylanceON-PREM SSL certificate from this page. See Update the SSL certificate version 1.2.2.1 and earlier for more information.
- The certificate is only needed if TLS/SSL is enabled.

Add a certificate

1. Select **Configuration > Certificates**.
2. Click **Add Certificate**.
3. Type in the name for this certificate, such as postgres.crt.
4. Drag the certificate to the **Install certificate** box or click **Browse for a file** and select the certificate.
5. Click **Install Certificate**. The certificate should be displayed on the page.

After you finish:

- To remove a certificate, click 🗑.
- To change or update a certificate, click ✏ and install the new certificate.

Settings

The Settings page displays information related to your CylanceON-PREM system, like the installation token, the CylanceON-PREM version you are using, and the ability to update the CylanceON-PREM appliance.

CylanceON-PREM Info	Description
Installation Token	This setting shows the installation token used when installing the CylancePROTECT Agent. This is unique for each virtual appliance. See Regenerate an installation token for more information.
Version	This setting shows the version for CylanceON-PREM. See Upgrade for more information.
Hostname	This setting shows the fully qualified domain name (FQDN) for the virtual appliance. See Reboot the virtual appliance for more information.
Console Language	This setting shows the language selected when the virtual appliance was initially configured.
Session Timeout	This setting specifies how long a user can be inactive (no keyboard or mouse movement) before being automatically logged out of the console. The time range is 5 minutes to 8 hours and can be set in 5 minute increments. The default timeout is 10 minutes.

CylanceON-PREM Info	Description
Certificate Expiration	This setting shows the date and time the CylanceON-PREM SSL certificate expires. See Update the SSL certificate version 1.2.2.1 and earlier for more information.
Certificate Ciphers	This setting shows whether the certificate is running using strict mode of TLS 1.1 or higher (default) or the legacy TLS 1.0 mode. See Change the certificate cipher mode for more information.
Certificate Signing Request	This setting shows whether a CSR is being used for this appliance and allows you to generate a new CSR, if needed. See Generate a CSR in the configuration steps for more information.
Maintence Mode	**Description**
Maintenance Mode	This setting shows the status of Maintenance Mode. When enabled, this pauses activity between CylanceON-PREM and CylancePROTECT devices to allow making changes to the virtual appliance without interruption.
Network Settings	**Description**
IP Assignment	This setting shows how the IP address is assigned to the virtual appliance, whether it is DHCP or Static.
IP Address	This setting shows the IP address for the virtual appliance.
Subnet Mask	This setting shows the subnet mask.
Default Gateway	This setting shows the IP address for the default gateway with which CylanceON-PREM is communicating. Click Ping to test the connection between CylanceON-PREM and the default gateway.
DNS Servers	This setting shows the IP addresses for the DNS servers with which CylanceON-PREM is communicating.
Check an IP Address	This setting allows you to ping an IP address to test the connection between CylanceON-PREM and the endpoint.
Debug Logs	**Description**
Log Level	This setting shows the log level for the virtual appliance. This setting shows logging can consume a high amount of disk space. Debug logging should only be used when troubleshooting server issues. Otherwise, the level should be set to Information (INFO).
On or After	This setting shows the start date to include when downloading the log files for the virtual appliance.
Database Connection Settings	**Description**

CylanceON-PREM Info	Description
Database Connection Settings	This setting shows the connection information for the external database if it is configured.
Syslog/SIEM	**Description**
Syslog/SIEM	This setting shows the status of messaging being forwarded to a Syslog server. See Configure syslog/SIEM settings for more information.
LDAP	**Description**
LDAP	This setting shows the status of LDAP/Active Directory integration. See Configure active directory for more information.
Identity Provider Settings	**Description**
Identity Provider Settings.	This setting shows the external identity provider (IdP) settings. See Configure identity provider settings for more information.

Regenerate an installation token

Regenerating an installation token provides a unique token for new installation of the CylancePROTECT Agent. Agents installed using the old token will continue to communicate with your CylanceON-PREM virtual appliance. Regenerating your installation token is helpful as a security measure or if your current token has been compromised.

1. Click **Configuration > Settings**.
2. Under CylanceON-PREM Info, click **Regenerate**. This creates a new, unique installation token.

Upgrade CylanceON-PREM

Administrators can apply the latest CylanceON-PREM upgrade package to the virtual appliance. The upgrade path for CylanceON-PREM is sequential. For example, if you have version 1.4.3 installed, you must upgrade to 1.4.5, then 1.5.4.1, then 1.6, and so on until you upgrade to the latest release.

Note:

• It is recommended to enable maintenance mode and take a snapshot of the virtual appliance before upgrading.
• When you update the CylanceON-PREM virtual appliance, there is no way to change from an internal database to an external database, or vice versa.

When updating the CylanceON-PREM virtual appliance, there is no way to change from an internal database to an external database, or vice versa.

1. Obtain the latest CylanceON-PREM file.
2. Log in to your CylanceON-PREM Console.
3. Click **Configuration > Settings**.
4. Click **Maintenance Mode**. This pauses site activity, including communication between the virtual appliance and the Agents, to ensure you can take a complete VM snapshot.
5. Take a snapshot of the CylanceON-PREM virtual appliance.
6. Under CylanceON-PREM Info, click **Upgrade**.
7. Select the **I have taken a VM snapshot** check box. Click **Proceed with Upgrading**.

8. Click **Browse for a file**, select the CylanceON-PREM file you want to use for this update. Click **Open**. You could drag and drop the file to select it.

9. Click **Start Upgrade**. During the upgrade, there are two things to look for: the update is in progress message and a successful update notification. After the Update Success modal displays, the virtual appliance will restart. While restarting, the CylanceON-PREM Console will be unavailable. If the entire upgrade process, including the restart, takes longer than 10 minutes, you must re-log in to the CylanceON-PREM Console.

10. After the upgrade is complete, click **Maintenance Mode** and disable it. Site activity resumes.

   Note: If you refresh the Settings page after the upgrade completes and the web browser displays a blank page, clear the browsing data.

Reboot the virtual appliance

From the Settings page, you can reboot the CylanceON-PREM virtual appliance and restart services. This is useful if you don't have direct access to the virtual machine. This action will take the virtual appliance offline for a period of time until it and the related services restart.

1. In the console, click **Configuration > Settings**.
2. Under CylanceON-PREM Info, click **Reboot** beside the Hostname. A message displays warning you that the virtual appliance will go offline for a brief period of time as it reboots and services restart.
3. Click **Reboot**.

Configure session timeout

Administrators can set how long a user can be inactive before being logged out of the CylanceON-PREM console. The time range is from 5 minutes, up to 8 hours. The default setting is 10 minutes.

1. In the console, click **Configuration > Settings**.
2. Click 🖉 beside Session Timeout.
3. Use the slider to adjust the amount of time.
4. Click **Apply**.

Update CylanceON-PREM SSL certificate version 1.3.1 and later

For more information on certificate guidelines, refer to the Certificate Guidelines.

1. In the console, click **Configuration > Settings**.
2. Under CylanceON-PREM Info, click **Update** beside Certificate Expiration.
3. Type in the FQDN (Common Name) or Subject Alternative Name for the virtual appliance in the Hostname field. The FQDN must match the DNS entry.
4. Drag the SSL certificate to the **Upload certificate** box or click **Browse for a file** and select the certificate.
   - If you generated the Certificate Signing Request using CylanceON-PREM, you do not have to upload a private key.
   - If you generated the Certificate Signing Request on another computer, drag the private key to the **Upload Key** box or click **Browse for a file** and select the private key.
5. Click **Save**.

Update CylanceON-PREM SSL certificate version 1.2.2.1 and earlier

To update the CylanceON-PREM SSL certificate, go through the configuration process again, using the updated SSL certificate and key. For more information on certificate guidelines, refer to the Certificate Guidelines.

1. Open a web browser and go to `https://<fqdn>/config`. The CylanceON-PREM configuration page displays.
2. Click **+SSL Certificate**, select the new SSL certificate, then click **Open**.
3. Click **+SSL Key**, select the new SSL key, then click **Open**.
4. Click **Submit**.

Change the certificate cipher mode

CylanceON-PREM defaults to using TLS 1.1 + (Strict Mode) to secure its communications over computer networks. If you need to support legacy operating systems that require TLS 1.0, such as Windows XP, you can revert to TLS 1.0 (Legacy Mode).

1. In the console, click **Configuration > Settings**.
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 enable legacy mode, a message displays informing you that you will need to close the current browser window and open a new one to see your change.
4. If you want to change back to strict mode, click **Change** beside certificate ciphers again. You will be prompted to close the current browser window and open a new one to update the settings.

Enable maintenance mode

Maintenance mode pauses all communication between CylanceON-PREM and the endpoints. This allows you to take a complete snapshot of the virtual appliance. Maintenance mode should be enabled when upgrading the appliance or changing the network settings.

1. In the console, click **Configuration > Settings**.
2. Click the toggle button beside **Maintenance Mode**. When you finish your changes, disable Maintenance Mode.

Change network settings

Before changing network settings, take a snapshot of the virtual appliance so you can revert, if necessary.

1. In the console, click **Configuration > Settings**.
2. Click **Maintenance Mode** to enable it. You must enable maintenance mode before editing the network settings.
3. For network settings, click ✎. A warning message displays, reminding you to take a snapshot of your virtual appliance. You must acknowledge the message before you can continue.
4. Click **I have taken a VM snapshot**, then click **Proceed to Edit Network Settings**.
5. Change the network settings. For DHCP, the network settings are provided by your DHCP server. For Static IP Addresses:
   - Type in the IP address, subnet mask, default gateway, and DNS servers.
6. Click ✅.
7. Click **Maintenance Mode** and confirm disabling it. Site activity resumes.

Check an IP address

The network settings allow you to enter an IP address and check if the CylanceON-PREM virtual appliance can communicate with the endpoint.

1. In the console, click **Configuration > Settings**.
2. Under Network Settings, type the IP address in the **Enter a Custom IP Address** field.
3. Click **Ping**. If the ping is successful, a message is displayed.

Change the log level

1. In the console, click **Configuration > Settings**.
2. Under System Settings, click 🖉 beside Log Level.
3. Select a logging level from the list.
4. Click ✅.

Note: Debug logging can consume a high amount of disk space. Debug logging should only be used when troubleshooting server issues. Otherwise, the level should be set to Information (INFO).

Download logs

1. In the console, click **Configuration > Settings**.
2. For Download Logs, select a date for **On or After**.
3. Click **Download**, then click **OK** to save the file.

Configure syslog/SIEM settings

CylanceON-PREM supports forwarding events to a Syslog server. The context of each event is Unicode plain text consisting of key-value pairs, separated by commas. Due to a size limitation of most Syslog servers, the details of each message (Cylance-specific payload) is limited to 2048 characters.

Note: The syslog feature requires CylanceON-PREM version 1.1.0 or higher.

1. Click **Configuration > Settings**.
2. Click 🖉 beside Syslog/SIEM. This expands the Syslog settings.
3. Click the Syslog/SIEM toggle to enable the feature. Use this toggle to enable or disable the feature without losing any settings.
4. Configure the Syslog settings. Read the *CylancePROTECT Syslog Guide* for details about each setting.

   - With TLS/SSL enabled, administrators can add an SSL certificate instead of pasting in the certificate information. The certificate can be added after configuring Syslog settings. Make sure you save any changes to this section before navigating to the Certificates page (Configuration > Certificates) to ensure your changes are not lost.

     Note: With **Verify Peer Mode** disabled, the SSL certificate is not required. The connection is encrypted, but CylanceON-PREM will not validate the peer certificate.

     ⚠️ **CAUTION:** UDP does not support notifications when the Syslog server shuts down.

5. Click ✅.
6. To upload an SSL certificate, go to the Certificates page (**Configuration > Certificates**), and add the certificate.

   Note:

   - The Threat Classifications event type is not available for CylanceON-PREM because the virtual appliance does not communicate with the CylancePROTECT Console.
   - To remove a Syslog server shut down notification, re-enable Syslog. If you no longer want to use Syslog, re-enable Syslog and then disable Syslog.

Syslog message failures

If there is a connection issue between CylanceON-PREM and your Syslog server, CylanceON-PREM will create an error message in the Audit Logs. If there are a lot of consecutive failures, CylanceON-PREM will disable Syslog to prevent too many messages from entering the queue.

- 30 connection failures: A warning message is sent to the Audit Log.
- 100 connection failures: An error message is sent to the Audit Log and Syslog is disabled.

Update database connection settings
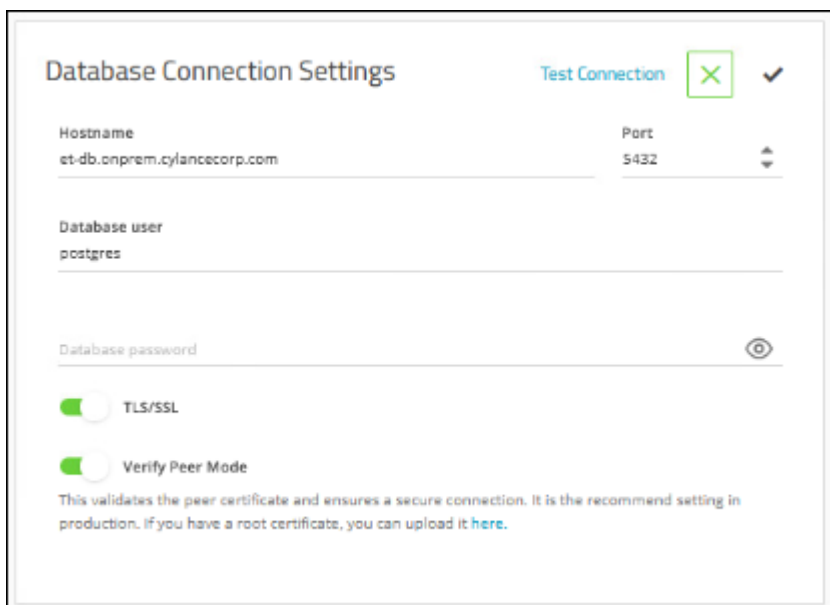
Allows users to change the external database information. This section is not displayed when you use the database shipped with CylanceON-PREM.

Note: The web browser might auto-populate the database password with the user password stored in cache. It is recommended to click the "eye" icon to make sure the correct password is entered. This appears to affect the Chrome web browser only.

1. Click **Configuration > Settings**.
2. Click 🖉 beside Database Connection Settings.
3. Update the PostgreSQL database information.

    - Hostname
    - Port
    - Database User
    - Database Password
    - TLS/SSL
    - Verify Peer Mode

        With **Verify Peer Mode** disabled, the SSL certificate is not required. The connection is encrypted, but CylanceON-PREM will not validate the peer certificate.

        You can add the certificate after you configure the syslog settings. Make sure you save any changes to this section before navigating to the Certificates page (Configuration > Certificates) to ensure your changes are not lost.

4. Click **Test Connection**. This tests to ensure that CylanceON-PREM can communicate with the database.

5. Click ✅.

6. To upload the external database certificate for SSL connection, go to the Certificates page (**Configuration > Certificates**), and add the certificate.

Configure active directory

If the LDAP Server is configured, CylanceON-PREM user logins are authenticated and authorized using the corporate LDAP server, including Microsoft's Active Directory.

Note: IMPORTANT: If active directory is enabled, the username for the CylanceON-PREM local user account must have have ".\" before the username when logging into the Console. For example, jsmith@cylance.com will need to be entered as ".\jsmith@cylance.com" to log into the CylanceON-PREM Console.

1. Add the SSL certificate for the LDAP Server. See Certificates for more information.

2. Click **Configuration > Settings**.

3. Click 🖊 beside LDAP. This expands the LDAP configuration settings.

4. Enable the LDAP toggle.

5. Enter your LDAP/Active Directory information:
   - **Base Distinguished Name:** This is the base distinguished name (DN) used as a base for the LDAP search to look for the user DN.
   - **Group Distinguished Name:** This is the group distinguished name (DN) used to perform an LDAP search to check if the user is a member of the group DN.
   - **LDAP FQDN:** This modifies the FQDN to the LDAP server's fully qualified domain name (FQDN).The FQDN must be configured on the Domain Server.
   - **Port:** This is the port number of the LDAP server.
   - **TLS/SSL:** This ensures the confidentiality of the user credentials, an encrypted LDAP connection should be used between the CylanceON-PREM server and LDAP server. There are two encryption methods you can choose from, startTLS and LDAPS.

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

7. Enter the username and password for the LDAP server, then click **Test**. A message displays indicating whether the test connection was successful.

   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)

8. Click ✅.

Configure identity provider settings

Configure CylanceON-PREM to accept authentication from an external identity provider, like Okta.

1. Click **Configuration > Settings**.

2. Click 🖊 beside Identity Provider Settings.

3. Enable the Identity Provider toggle.

4. Enter the identity provider information.
   - **Single Sign-On**: This is the single sign-on or SAML response URL that is provided by the identity provider.
   - **Entity ID**: This is the entity ID, issuer, or application name that is provided by the identity provider.
   - **x.509 Certificate**: This is provided by the identity provider.

5. Click ✅. CylanceON-PREM will generate a **Service Provider Entity ID** that the identity provider will need to complete the single sign-on configuration.

Using certificate-based authentication

The CylanceON-PREM console now supports certificate-based authentication when an administrator logs in. You can create other administrators that must use certificate-based authentication and add or remove certificates from the CylanceON-PREM server. The CA certificates uploaded to the CylanceON-PREM server specify which client certificates are trusted for access to the console. If the client certificate is trusted by the Certificate Authority, then the user is authenticated and can access the console. During authentication, the server checks for revoked certificates to ensure the certificate has not been revoked. If the certificate has been revoked, the administrator will not be allowed to log in to the console. As a failsafe, the console will not allow you to delete or deactivate all of the local administrator accounts.

Enable certificate-based authentication and import certificates

Before you begin: Ensure that you have saved copies of the CA certificates that you'll be using in .pem, .crt, or .der format.

1. In the CylanceON-PREM console, click **Configuration > Settings**.
2. Click 🖉 beside **Certificate Based Authentication**.
3. Turn on the **Certificate-Based Authentication** setting.
4. Click **Add Certificate**.
5. Browse for the file or drag and drop the file to upload it.
6. Click **Upload Certificate**.
7. Click ✅.
   Uploading a certificate replaces the previously uploaded certificate. To upload multiple CA certificates, concatenate them into one file.

Add a banner to the login screen

You can create a custom banner with custom text that displays on the Login screen. For example, a consent banner so that the user provides consent (e.g. consent for monitoring) before the user logs in.

1. Click **Configuration > Settings**.
2. Click 🖉 beside the Login Screen Banner.
3. Enable the Login Screen Banner toggle.
4. Enter a **Title** for the banner.
5. Enter a **Message** that you want to display to users. The Message field only accepts plain text and can be a maximum of 1500 characters, Any HTML, JavaScript, etc. entered in this field will be escaped.
6. Click ✅.

Applications

The Console Applications page provides integration with the CylanceON-PREM API. Administrators can manage multiple API applications, including the access privileges to your CylanceON-PREM data. An application has a unique application ID and application secret for generating an access token, which is used to access the API. Administrators create the applications, then give API users the application ID and application secret.

Note: If necessary, administrators can regenerate the application secret and provide API users with the new information.

Add an application

CylanceON-PREM can have up to ten custom applications.

1. In the console, click **Configuration > Applications**.
2. Click **Add Application**. The Add Application dialog displays.
3. Type the name of the application. Click **Next Step**. The console does not enforce a unique name for Applications. It is recommended to create Applications with unique names for easy identification.
4. Set permissions for the application. Click **Save Application**.
5. You will need to copy the application ID and application secret to use when generating an access token. To copy this information to use at a later time, click the down arrow to the right of the application name and copy it.
6. Click **OK, got it** to close the dialog.

   Note:

   - To edit an application, click ✎ , then update the application name or permissions.

- To remove an application, click 🗑.
- To view the YAML file, click the **API Documentation** link. Once displayed, you can right-click in the browser and select **Save as** to download the *api-docs.yaml* file. See View API documentation (YAML file) for more information.

CylanceON-PREM API

The CylanceON-PREM API is a set of RESTful APIs that allows administrators to use API requests to manage their CylanceON-PREM virtual appliance instead of using the CylanceON-PREM Console.

Note: The CylanceON-PREM API is different from the Cylance User API.

The following high-level steps are required to configure and use the CylanceON-PREM API:

1. Add an application in the CylanceON-PREM console. See Applications for more information.
2. Generate an access token. See Access token for more information.
3. View API documentation to generate the curl commands or URL requests with your selected parameters. See View API documentation (YAML file) for more information.
4. Execute the generated commands or requests against the CylanceON-PREM appliance. Currently the curl commands and URL requests generated by the YAML file do not include the access token and other header information required for an API request. See Apply missing header information for an example of the missing header information.

   Note: The execution of API requests is beyond the scope of this document.

Application management

CylanceON-PREM administrators can manage multiple API applications, including the access privileges to your CylanceON-PREM data. An application has a unique application ID and application secret for generating an access token to use the API. Administrators create the applications, then give users the application ID and application secret.

Note: If necessary, administrators can regenerate the application credentials and provide users the new credentials.

Add an application (API)

A CylanceON-PREM instance can have up to 10 custom applications

1. Select **Configuration > Applications**.
2. Click **Add Application**.
3. Type a name for the application, then click **Next Step**.

   Note: The console does not enforce a unique name for applications. It is recommended to create applications with unique names for easy identification.
4. Select which console features and the permission level accessible by the application.
5. Click **Save Application**. A success message is displayed, including the application ID and application secret. To view the application secret, click the eye icon.
6. Click **OK, got it** to close the message.

Access token

The access token represents a grant to access Cylance resources. It contains information about the identity of the caller (application) as well as control information from the token itself, for instance, the date it was issued and expiration.

Note: Before generating an access token you will need to add an application in the CylanceON-PREM console (**Configuration > Applications**) and copy the application ID and application secret. See Applications for more information.

Generate an access token

The access token can be generated using Python. You can use the Python example below, adding the required token claims that you need.

> ⚠️ **CAUTION:** The following requirements and script are just an example. This may change based on end-user requirements (example: using a different version of Python).

Software requirements

- Python 3.7 or higher (available from https://www.python.org/downloads/). Make sure to set the following options during installation:
  - Check the **Add Python <version> to PATH** checkbox at the beginning of the Python installation.
  - Click **Disable path length limit** to remove the 260 character MAX_PATH limitation at the end of the installation.
- Python Requests Library 2.22.0 or higher:
  - Open a command prompt on the machine where Python is installed, then run the following command to install the latest Requests library:

```
python -m pip install requests
```

> ⚠️ **CAUTION:** You will need to use the access token to execute the API requests.

Example Script

The following example code can be used to get an access token using Python.

```python
import requests # requests version 2.22.0 as of the time of authoring

# Set the base url. Example: https://login.onprem-cylance.com. This url
# will be specific to your installation of CylanceON-PREM.
onprem_base_url = "<your_base_url>"
# Set the Application ID
appID = "<your_app_id>"
# Set the Application Secret
appSecret = "<your_app_secret>"

# Make a POST request to get the application token.
token_headers = {
    "Content-Type": "application/json",
    "Accept": "application/json",
}
token_request_body = {
    "clientId": appID,
    "clientSecret": appSecret,
    "scope": "*"
}
token_url = f"{onprem_base_url}/cyapi/v1/application/token"

token_result = requests.post(token_url, json=token_request_body,
 headers=token_headers,verify=False)

token_url_json_results = token_result.json()
print("Got result from token request:")
print(token_url_json_results)
```

Token lifecycle

An access token should be used only once per request. This means the same token should not be usable for more than one request to prevent impersonation attempts. The jti attribute uniquely identifies the token. It can be used to keep track of all the tokens and prevent them from being reused. To ensure that the access token can be used only once, an expiration is enforced on the token. This means the token is usable within a ten minutes or less.

View API documentation (YAML file)

This example uses the Swagger UI editor to view the CylanceON-PREM YAML file.

⚠️ **CAUTION:** The purpose of the YAML file is to generate the Curl command or Request URL with your selected parameters. The file does not include logic required to test the API in Swagger.

1. Download the CylanceON-PREM YAML file:
   a) Log in to your CylanceON-PREM Console.
   b) Select **Configuration > Applications**.
   c) Click the **API Documentation** link. The API documentation opens in a new browser window.
   d) Right-click on the documentation and select **Save as** to download the *api-docs.yaml* file.
2. Open the *api-docs.yaml* file in an editor, such as Notepad ++. Add your CylanceON-PREM fully qualified domain name (FQDN) to the URLs under `servers`. The image below uses `login.onprem-cylance.com` as the hostname.

```
 1    openapi: 3.0.0
 2   ⊟info:
 3      title: 'CylanceON-PREM API'
 4      description: "\nWhen creating requests, replace `your.FQDN` in each server with
             the fully qualified domain name (FQDN)\nfor your virtual appliance. The curl
             reqests output by the documentation will include the proper Content-Type\nheader
             based on the request body type, and the proper Accept header based on the media
             type selected for the\nsuccess response. The Authorization header will have to be
             added to the curl request based on the token\nreceived from the API Access
             endpoint."
 5      version: 1.0.0
 6   ⊟servers:
 7     -
 8        url: https://login.onprem-cylance.com/cyapi/v1
 9        description: 'API Access server. Use this server for the POST
             /application/token endpoint.'
10     -
11        url: https://login.onprem-cylance.com/cyapi/v1/client
12        description: 'Client API server. Use this server for all other endpoints.'
13   ⊟paths:
14      /audits:
15        get:
16          tags:
17            - 'Audit Logs'
18          summary: 'Search Audit Logs'
19          operationId: 'App\Http\Controllers\Api\AuditController::getAudit'
20          parameters:
21            -
```

3. Save the api-docs.yml file.
4. Open a web browser and type in http://editor.swagger.io. The Swagger Editor displays.
5. Select **File > Import file**, select the api-docs.yml file, then click **Open**. Your updated YAML file is displayed in the Swagger Editor.

6. To view the API documentation click an API, such as Get Devices to view its parameters and responses.
7. (Optional) To generate the web service endpoint with your selected parameters:
   a) Under Servers, select `/cyapi/v1` for the OAuth Access Token API, or select `/cyapi/v1/client` for all other API requests.
   b) Click on **Try it out** to enable adding any parameter updates you want to include in the request.
   c) Update or add any parameters by selecting options.
   d) Update the request body with your values for POST and PATCH requests.
   e) Scroll to the end of the parameters, then click **Execute**. The Curl command and Request URL display:

CAUTION: The Server Response will return Failed to Fetch. The purpose of the YAML file is to generate the Curl command or Request URL. The file does not include logic required to test the API in Swagger.

8. You can now use these commands to update your CylanceON-PREM appliance from the API.

Apply missing header information

The YAML file does not include the access token required to make an API request. You will need to include additional header information in the request.

Curl requests

For example, for the GET Devices call, if you use the YAML File in Swagger with the default options selected and https://login.onprem-cylance.com/cyapi/v1/client is set as the server, the following Curl command is generated:

```
curl -X GET "https://login.onprem-cylance.com/cyapi/v1/client/devices?
page=1&pageSize=50&includeMeta=true" -H "accept: application/json"
```

However, for this command to work, you must include the access token:

```
curl -X GET "https://login.onprem-cylance.com/cyapi/v1/client/devices?
page=1&pageSize=50&includeMeta=true" -H "accept: application/json" -H
 "authorization: Bearer {{access-token}}"
```

```
curl -X GET "https://login.onpremcylance.com/cyapi/v1/client/devices?
page=1&pageSize=50&includeMeta=true"
 -H "accept: application/json"
```

```
-H "authorization: Bearer {{accesstoken}}"
```

Note: Replace {{access-token}} with the access token you generated using your application ID and application secret. See Access token .

Request URL

For example, for the GET Devices call, if you use the YAML file in Swagger with the default options selected and https://login.onprem-cylance.com/cyapi/v1/client is set as the server, the following URL command is generated:

https://login.onprem-cylance.com/cyapi/v1/client/devices?page=1&pageSize=100

However, for the command to work, it will require the following Headers:

- Accept: application/json
- Authorization: Bearer {{access-token}}

Note: Replace {{access-token}} with the access token you generated using your application ID and application secret. See Access token .

Response codes

Each API request will receive a response with a JSON payload and a standard HTTP status code.

Note: Some API request sections include additional response status descriptions (specific to that request) to help you troubleshoot issues.

Status Code	Description
200 - OK	This indicates a successful call and operation. The response payload will be JSON, structured according to the nature of the request.
400 - Bad Request	There was a problem with the structure of the request or the payload. If determinable, the response payload will identify the failure in the request. A common case of this type of error is malformed JSON in the request body. A JSON validator can be used to troubleshoot these issues.
401 - Unauthorized	This indicates invalid credentials were passed or some other failure in authentication.
403 - Forbidden	The request has been successfully authenticated, but authorization to access the requested resource was not granted.
404 - Not Found	A request was made for a resource that doesn't exist. Common causes are either an improperly formed URL or an invalid API key.
409 - Conflict	A request was made to create or update an aspect of the resource that conflicts with another. The most common reason for this code is a Tenant name or User email that is already in use.
500 - Internal Server Error	A catch-all code response for any unhandled error that has occurred on the server. Contact Cylance Support for help with this issue.
501 - Not Implemented	A request was made against a resource with an operation that has yet to be implemented. Such operations should be identified accordinly in documentation.
Other	Contact Cylance Support if you encounter any status codes that are not on this list.

Troubleshooting

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

Agent not communicating with CylanceON-PREM

- Make sure the Agent (version 1480 or higher) is installed on the endpoint. For example, you can check for the Cylance icon in the system tray or check the list of apps installed on the endpoint.
- Ensure the root CA certificate is installed on the endpoint in the Local Machine Certificate Store. This root CA certificate is the one that signed the certificate and key used to configure CylanceON-PREM.

Web browser reports insecure webpage

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

- Install the root CA certificate used to configure your CylanceON-PREM virtual appliance on the endpoint in the Local Machine Certificate Store.

Unable to connect to external database

If CylanceON-PREM is unable to connect to the external database (for example, the database is powered off), you will receive an error message. The error message displayed depends on the page in the CylanceON-PREM console.

The following CylanceON-PREM console pages are still accessible when the external database is not available: Rules, User Management, Role Management, Audit Logs, and Settings.
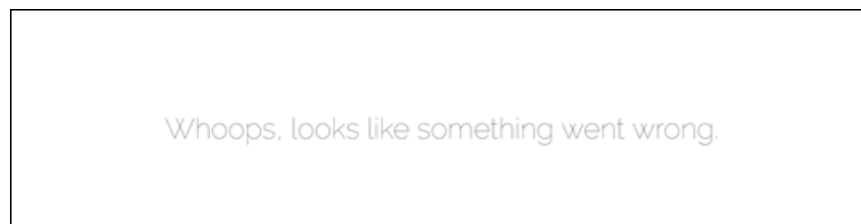
Error message for Database Connection Settings when external database is not available:
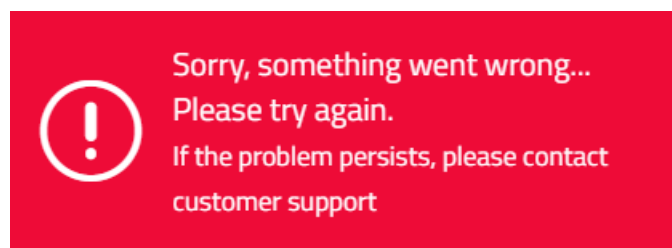
Error message for all other console pages when external database is not available:

Database connection failure. Please check your connection properties. ✕

Configure static IP using the OVF tool

The CylanceON-PREM 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 CylanceON-PREM OVA file.
4. Type the following:`ovftool -ds=datastore1 -n=CylanceONPREM1.0.1 --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 CylanceONPREM_1.0.1.ova vi://test_user@10.60.41.80`
5. Press **Enter**. The OVA file is imported into vSphere.

Remote server 404 error in log files

When you are logging files in verbose mode, a "The remote server returned an error: (404) Not Found" error will be logged. This informational message is logged periodically when the agent attempts to communicate with the Cloud Infinity server URL which is not supported when using Cylance ON-PREM.

Log in with a local administrator account

If an administrator cannot log in to the console using certificate-based authentication, you can log in using a local administrator account to troubleshoot the issue.

Note: As a failsafe, the CylanceON-PREM console will not allow you to delete or deactivate all of the local administrator accounts.

1. Log in using your local administrator account.
2. Troubleshoot and fix problems with certificate-based authentication for the affected administrator account.

Online Certificate Status Protocol issues

During authentication, CylanceON-PREM checks for revoked certificates with an Online Certificate Status Protocol (OCSP) server. Here are some tasks you can perform if you encounter an issue with the OCSP certificate check.

• Check that the correct OCSP is configured in the Authority Information Access field of the certificate.
• Check that there is connectivity to the OCSP.
• Ensure the OCSP is running.

Before you contact support

If the above troubleshooting suggestions do not resolve your issue, before contacting Cylance Support, enable Debug logging on the CylanceON-PREM System page, wait for at least 20 minutes, then download the log file and submit it to Cylance Support.

Enable debug logging

1. Click **Configuration > System**.
2. Under System Settings, click ✎ beside Log Level.
3. Select **Debug**.
4. Click ✅.

Download logs

1. Click **Configuration > System**.
2. For Download Logs, select a date for **On or After**.
3. Click **Download**, then click **OK** to save the file.

Debug Logs	✎
Log Level	WARNING
On or After 08/06/2018 📅	Download
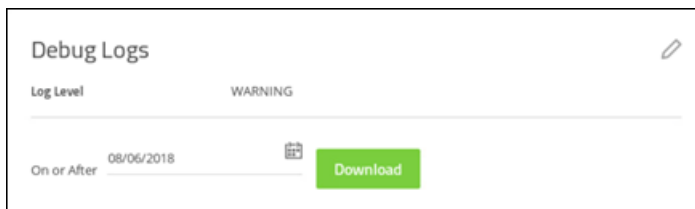
4. Create a BlackBerry Support ticket and include the CylanceON-PREM log file.
   a) Log in to myAccount (https://myaccount.blackberry.com).
   b) Navigate to the Support Community menu, then select **Create Case**.
   c) Select **BlackBerry Protect**.
   d) Select **ON-PREM**.
   e) Click **Next**.
5. In the Search Issue Summary box, complete the following steps:
   a) Type **Download ON-PREM link**, then check the box.
   b) Click **Next**.
   c) In the detailed description box, enter the request for the required links.
   d) Click **Submit Case**.

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