



CylanceON-PREM

Administration Guide

2.0.0

Contents

- Overview..... 7**
 - Steps to get Start with CylanceON-PREM.....7

- Requirements: CylanceON-PREM..... 9**
 - Things to consider about CylanceON-PREM.....10

- Configuring the CylanceON-PREM virtual appliance..... 12**
 - Prerequisites..... 12
 - Import the OVA and configure a static IP address..... 12
 - Import the OVA and configure DHCP..... 12
 - Configure CylanceON-PREM..... 13
 - External database overview..... 15

- Configuring the console..... 16**
 - Log in to CylanceON-PREM..... 16
 - Log in using identity provider credentials..... 16
 - Log in using certificate-based authentication..... 16
 - Administrative dashboard..... 16
 - Filter lists..... 18
 - Export lists..... 18
 - Policies..... 18
 - Add a policy..... 18
 - Threat settings..... 19
 - Memory protection..... 20
 - Memory protection violation types..... 21
 - Script control..... 23
 - Device control..... 24
 - Application control..... 25
 - Agent settings..... 25
 - Exclusions..... 25
 - Wildcards in memory violation exclusions..... 27
 - Import a policy..... 29
 - Policy rule sets..... 29

- Setting up the CylancePROTECT agent..... 33**
 - Adding the CA certificate to endpoints..... 33
 - Add a root CA certificate to Windows..... 33
 - Add a root CA certificate to MacOS..... 33
 - Installing the CylancePROTECT Desktop agent for Windows..... 34
 - Windows installation parameters..... 34
 - Installing the CylancePROTECT Desktop agent for macOS..... 35
 - MacOS installation parameters..... 35

Installing the CylancePROTECT Desktop agent for Linux.....	36
Linux OS installation parameters.....	37
Examples for the Linux configuration file.....	37
Upgrading the CylancePROTECT Desktop agents.....	37
Using virtual machines.....	38

Device management.....39

Assign a policy.....	39
Remove a device.....	39
Device details.....	39
Change a policy.....	39
Change a tag.....	40
View events.....	40
Device tags.....	40
Create a device tag.....	40
Assign a tag.....	41
Tag rules.....	41
Remove a device tag.....	43
Set agent logging level.....	44

Threat management.....45

Manage threat events.....	45
Threat event fields.....	45
Cylance score.....	46
Manage script events.....	46
Script event fields.....	47
Manage memory events.....	48
Memory event fields.....	48
Manage device events.....	48
Device event fields.....	49
Manage application events.....	49
Application event fields.....	50

Global lists.....51

Add a global list entry.....	51
Import a global list.....	51
Add files to safelist by certificate.....	52
Import a .csv file that contains a list of certificates that have been added to the global safe list or global quarantine list.....	52

Administration.....53

Managing users.....	53
Create a user.....	53
Create a user with identity provider settings enabled.....	53
Change a user password.....	54
Deactivate a user.....	55
Add administrators who must use certificate-based authentication.....	55
Edit an existing administrator to use certificate-based authentication.....	55
Managing roles.....	56

Create a role.....	56
Role permissions.....	56
Update profile information.....	59
Audit logs.....	59
Managing Certificates.....	60
Add a certificate.....	60
Setting up email notifications.....	61
Set up integration with an SMTP server.....	61
Select which threats to be notified about.....	61
Settings.....	61
Upgrade CylanceON-PREM.....	63
Reboot the virtual appliance.....	64
Configure session timeout.....	64
Update CylanceON-PREM SSL certificate version 1.3.1 and later.....	64
Update CylanceON-PREM SSL certificate version 1.2.2.1 and earlier.....	65
Change the certificate cipher mode.....	65
Enable maintenance mode.....	65
Change network settings.....	65
Check an IP address.....	66
Change the log level.....	66
Download logs.....	66
Configure syslog/SIEM settings.....	66
Update database connection settings.....	67
Configure active directory.....	68
Configure identity provider settings.....	68
Using certificate-based authentication.....	69
Add a banner to the login screen.....	69
Applications.....	69
Add an application.....	70

CylanceON-PREM API..... 71

Application management.....	71
Add an application (API).....	71
Access token.....	71
Generate an access token.....	72
View API documentation (YAML file).....	73
Apply missing header information.....	75
Response codes.....	76

Troubleshooting..... 77

Agent not communicating with CylanceON-PREM.....	77
Web browser reports insecure webpage.....	77
Unable to connect to external database.....	77
Configure static IP using the OVF tool.....	78
Remote server 404 error in log files.....	78
Log in with a local administrator account.....	78
Online Certificate Status Protocol issues.....	78
A user is not receiving email notifications.....	79
Before you contact support.....	79
Enable debug logging.....	79
Download logs.....	79

Legal notice..... 81

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 management 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 management console.

Steps to get Start with CylanceON-PREM

The following steps outline how you can get started with [CylanceON-PREM](#) including pre-deployment steps, deployment steps, [CylanceON-PREM](#) configuration steps, console configuration steps, and Agent installation steps.

Item	Steps
Pre-deployment steps	<ol style="list-style-type: none">1. Verify system requirements:<ul style="list-style-type: none">• Requirements: CylanceON-PREM• Things to consider about CylanceON-PREM2. 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	<ol style="list-style-type: none">1. Import the CylanceON-PREM virtual appliance (OVA file):<ul style="list-style-type: none">• Import the OVA and configure a static IP address• Import the OVA and configure DHCP
CylanceON-PREM configuration steps	<ol style="list-style-type: none">1. Log in to the management console to configure CylanceON-PREM. See Configure CylanceON-PREM for more information.2. Select a certificate option:<ul style="list-style-type: none">• Generate and submit a CSR from CylanceON-PREM• Generate an SSL certificate and private key using a different computer, then upload to CylanceON-PREM3. Select a database option:<ul style="list-style-type: none">• 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	<ol style="list-style-type: none">1. Add or import a policy:<ul style="list-style-type: none">• Add a policy• Import a policy2. Create a device tag (optional).3. Add a tag rule (optional).4. Add a policy rule (optional).

Item	Steps
Agent installation steps	<p>Starting with ON-PREM 1.8.0, Windows XP and Windows 2003 are no longer supported due to a lack of AES support on these operating systems. Agents need to be running on Windows 7 or later or Windows Server 2008 SP2 or later. For more information about supported operating systems, refer to the requirements.</p> <ol style="list-style-type: none"><li data-bbox="493 415 976 443">1. Adding the CA certificate to endpoints<li data-bbox="493 449 846 476">2. Copy the installation token<li data-bbox="493 483 971 510">3. Install agents on devices (endpoints):<ul data-bbox="529 533 1263 632" style="list-style-type: none"><li data-bbox="529 533 1263 560">• Installing the CylancePROTECT Desktop agent for Windows<li data-bbox="529 567 1243 594">• Installing the CylancePROTECT Desktop agent for macOS<li data-bbox="529 600 1222 627">• Installing the CylancePROTECT Desktop agent for Linux

Requirements: CylanceON-PREM

CylanceON-PREM is provided as an OVA (virtual appliance) and supports VMware ESXi 6.5 or later. To get started setting up CylanceON-PREM, review this section and verify that your organization's environment satisfies the requirements of CylanceON-PREM features and components for either use as an all-in-one virtual appliance or as an endpoint management virtual appliance.

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. This option is recommended 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 requirements.

Item	Description
RAM	16 GB
CPU	2.2 GHz quad-core (Intel Xeon processors or later)
Free disk space	1 TB
Web browser support	<ul style="list-style-type: none">• Google Chrome (latest 2 versions)• Mozilla Firefox (latest 2 versions)• Apple Safari (latest 2 versions)• Microsoft Edge (latest version)
CylancePROTECT	For support Agents, see the compatibility matrix .
Root certificate authority (CA) certificate	Root certificate authority (CA) certificate must be 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. If the latter method was used to obtain the certificate, the private key will also need to be installed on CylanceON-PREM.

Endpoint management virtual appliance

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 management console and other Cylance components necessary to support an on-premises solution. The following are the minimum, dedicated hardware requirements for an external database if used.

Item	Description
External database requirements	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. Setting up, maintaining, and troubleshooting an external database is not supported. Organizations must have a dedicated database administrator for configuring and maintaining their database.
Ram	16GB
CPU	2.2 GHz quad-core (Intel Xeon processors or later)
Free disk space	500 GB
Database	PostgreSQL version 10.4 or later
CylancePROTECT	CylancePROTECT Agent version 1480 or later must be installed on the endpoints.
Root certificate authority (CA) certificate	Root certificate authority (CA) certificate must be 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. If the latter method was used to obtain the certificate, the private key will also need to be installed on CylanceON-PREM.

Things to consider about CylanceON-PREM

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. 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.
Communication through another CylanceON-PREM virtual appliance	A CylanceON-PREM virtual appliance cannot communicate to or through another CylanceON-PREM virtual appliance.
CylanceOPTICS	CylanceON-PREM currently does not support CylanceOPTICS.

Item	Description
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. Modifying anything on the virtual appliance or gaining access to it is not supported.
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.
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 either an internal database or external database, it cannot be changed.
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 .
CylanceON-PREM system account	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.

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 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. Refer to [Import the OVA and configure DHCP](#) for more information.
 - **Static IP:** If you use a static IP address, use that in the DNS entry. Refer to [Import the OVA and configure a static IP address](#) for more information.
- Have a root CA certificate 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. 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.

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 more 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.

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

Before you begin:

- Refer to [Import the OVA and configure a static IP address](#) if you are using a static IP address.
- Refer to [External database overview](#) if you are using an external database.

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

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, such as <https://login.onprem.com>. For a web browser, use a system that can communicate with the CylanceON-PREM virtual appliance.
3. Fill out the form to generate a CSR from CylanceON-PREM to submit to a CA to use with the CylanceON-PREM virtual appliance and click **Generate CSR**. This creates a `cert_request.csr` file in the downloads folder that can be sent to a Certificate Authority (CA) to receive an SSL certificate. 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. If you are using an SSL certificate and key generated on a computer other than CylanceON-PREM, continue to step 4.

Item	Description
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 <code>onprem.cylance.com</code> .
Subject Alternative Name	Enter any alternative names to use for the virtual appliance, such as <code>onprem-alt.cylance.com</code> . The Common Name will be added automatically as a Subject Alternative Name. Click Add after typing an alternative name to add it.
Organization Name	Enter the legal name of the organization.
Organizational Unit	This could be a department name.
City	Enter the city where the organization is located.
State/ Province	Enter the state of province where the organization is located. Do not use an abbreviation.

Item	Description
Country	Enter the two letter ISO abbreviation for the country.

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 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 CylanceON-PREM, you do not have to upload a private key and skip the remaining steps below and continue to Step 7. If you generated a CSR on a different computer, 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. If your CA provides you a .pfx file (combined site certificate and private key), the CA 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. Setting up, maintaining, and troubleshooting an external database is not supported. Organizations must have a dedicated database administrator (DBA) for configuring and maintaining their database.

Item	Configuration
Database connection settings disabled	No configuration required
Database connection settings are enabled	<ol style="list-style-type: none"> a. Enter the hostname or IP address for the external database (for example, <code>database.com</code> or <code>123.45.67.89</code>) b. Enter the port number for the external database (for example, <code>5432</code>) 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: <ul style="list-style-type: none"> • 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.

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.

1. Install PostgreSQL and PostgreSQL server.
2. Initialize the PostgreSQL database.
3. Start and enable autostart postgres service to start the database when the server starts.
4. Force postgres to listen on all ports in postgresql.conf.
5. Allow postgres port through firewall.
6. Enable the pgcrypto extension.
7. 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. A shared database is not recommended for CylanceON-PREM.
8. Authorize remote postgres authentication in pg_hba.conf file.
9. Generate SSL certificates for postgres server connection.
10. Configure SSL in postgresql.conf file.

When you connect the external database to CylanceON-PREM, consider the following:

- Use the fully qualified domain name (FQDN) of the external database. Using the external database IP address is also 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

After configuring the CylanceON-PREM virtual appliance, you can configure the CylanceON-PREM console. This includes setting up and using the console dashboard, filtering lists, and using policies.

Log in to CylanceON-PREM

You can log in to CylanceON-PREM by using `https://<fqdn>`. Replace `<fqdn>` with the fully qualified domain name (FQDN) of your CylanceON-PREM virtual appliance. For 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.

CylanceON-PREM users can log in to CylanceON-PREM using either identity provider credentials or certificate-based authentication.

Log in using identity provider credentials

You can log into CylanceON-PREM using an external identity provider, such as Okta. To configure CylanceON-PREM to use an external identity provider, 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 displays.
2. Log in to your Identity Provider's website and go through any validation processes, such as two factor authentication. After you are authenticated by your identity provider, your browser will redirect to the CylanceON-PREM Dashboard.

Log in using certificate-based authentication

You can log in to CylanceON-PREM using certificate-based authentication. You must have a common access card (CAC) to do so. For more information about certificate-based authentication, refer to [Using certificate-based authentication](#).

1. Insert your CAC in to the computer that you are going to log in to.
2. Select your certificate.
3. Open the CylanceON-PREM login page and click **Certificate-based Sign in**. The administrator is logged in to the console. If you remove your CAC, you are automatically logged out of the console.

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. It also provides quick links to frequently used features in the product.


Item	Description
Access Management	Clicking this widget opens the User Management > Users page.



Item	Description
Acknowledged	<p>This drop-down list filters event widgets to display events as follows:</p> <ul style="list-style-type: none"> • No - Only displays events that have not been acknowledged by a user. A user acknowledges an event by manually restricting or allowing an event, or by clicking Acknowledged on the Events page. • All - Displays all events, both acknowledged and unacknowledged. <p>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 are overridden.</p>
Application Events	<p>This widget 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 > Applications Events page.</p>
Configuration	<p>Clicking this widget opens the Configuration > Settings page.</p>
Device Events	<p>This widget displays the total number of USB mass storage device events in your organization. Clicking this widget opens the Events > Device Events page.</p>
Devices	<p>This widget displays the total number of devices communicating with this CylanceON-PREM virtual appliance. Clicking this widget opens the Device List page.</p>
Global Lists	<p>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.</p>
Memory Events	<p>This widget displays the total number of malicious memory events in your organization. Clicking this widget opens the Events > Memory Events page.</p>
Policies	<p>Clicking this widget opens the Policies page.</p>
Reported On	<p>This drop-down list 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.</p>
Script Events	<p>This widget displays the total number of malicious script events in your organization. Clicking this widget opens the Events > Script Events page.</p>
Threat Events	<p>This widget displays the total number of malicious file events in your organization. Clicking this widget opens the Events > File Events page.</p>


Filter lists

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


Item	Description
Quick Search fields	Search across all items listed in the hint text of the field.
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  . 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 the list. To remove a selected option, click the X to the right of the selected option.

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

After you finish: To remove a filter from a list, click  on the right side above a list and click the X beside an applied filter.

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  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, such as to automatically quarantine the threat, ignore it 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. For descriptions for each policy option, refer to [Threat settings](#).
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.
Auto Delete Quarantine	<p>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.</p> <p>The number of days starts when the file was first quarantined. This action is included in the Agent log file for verification.</p> <p>If this feature is not enabled, the quarantined files will remain on the device until the quarantined files are manually deleted.</p>
Auto Quarantine Abnormal Files	<p>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.</p> <ul style="list-style-type: none"> • For Windows: C:\ProgramData\Cylance\Desktop\q • For macOS: /Library/Application Support/Cylance/Desktop/q <p>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.</p> <p>Note: Auto Quarantine Unsafe Files must be selected for Auto Quarantine Abnormal Files to be available.</p>
Auto Quarantine Unsafe Files	<p>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.</p> <ul style="list-style-type: none"> • For Windows: C:\ProgramData\Cylance\Desktop\q • For macOS: /Library/Application Support/Cylance/Desktop/q <p>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.</p> <p>Note: Auto Quarantine Unsafe Files must be selected for Auto Quarantine Abnormal Files to be available.</p>

Threat Setting	Description
Background Threat Detection	<p>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.</p> <p>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.</p> <p>It is recommended that users set Background Threat Detection to Run Once. Due to the predictive nature of the CylancePROTECT Desktop technology, periodic scans of the entire disk are not necessary but can be implemented for compliance purposes.</p>
Copy File Samples	<p>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.</p> <ul style="list-style-type: none"> • CIFS/SMB network shares are supported. • Specify one network share location. Using the fully qualified path is recommended. For example: <code>\\server_name\shared_folder</code> • 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	<p>Use this option to detect and analyze any new or modified files for dormant threats.</p> <p>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).</p>
Scan Archive	<p>Use this option to set the maximum archive file size the Agent will scan. This setting applies to Background Threat Detection and File Watcher.</p>

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	Violation
Windows macOS	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	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.

Process Injection Violation Types

Applies to	Violation
macOS	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.
Windows	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 macOS	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	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	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 macOS	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	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.
macOS	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.

Escalation Violation Types

Applies to	Violation
Windows	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 macOS	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.

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 the organization. When you enable device control, you can allow full access, read-only, or block USB mass storage devices, such as USB flash drives, external hard drives, and smartphones. As part of the policy, you can also use exclusions to define the access level for specific mass storage devices using the vendor ID, product ID, and serial number. For example, you can block all USB mass storage devices, but create exclusions to allow full access to some authorized devices only. Device control is available for the Windows platform only.

Device control does not affect USB peripherals such as a mouse or keyboard. For example, when you create a policy to block all USB mass storage device types, a user can still use a USB keyboard.

Device control is available for the Windows platform only.

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 device control is enabled, all USB mass storage devices that are inserted are logged, along with the policy action that was applied (full access, read-only, or block). If the policy action is set to read-only or block, and desktop notifications are enabled on the device, a pop-up notification appears on the device when a USB mass storage device is connected. You can find the log of device control events on the Protection > External Devices screen in the console.

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.
Full Access	This device type is allowed to access the endpoint it is connected to.
Read-Only	<p>This device type is allowed to connect to the endpoint and view contents, without the ability to write or copy to it. Available for Windows-based devices only.</p> <p>The following USB device types can be configured for read-only access:</p> <ul style="list-style-type: none">• Still image• USB CD/DVD RW• USB drive• VMWare USB passthrough• Windows portable device

Supported device types for device control

Device type	Description
Android	<p>This is a portable device running Android OS, like a smartphone or a tablet. This type of device does not support read-only.</p> <p>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.</p>

Device type	Description
iOS	This is an Apple portable device running iOS, like an iPhone or an iPad. This type of device does not support read-only. Note: Some iOS devices will not charge when device control is enabled and set to block unless the device is powered off. Apple includes their charging capability within functions of the device that are required for our iOS device blocking capability. Non-Apple devices do not bundle their charging capability in this manner and are not impacted.
Still Image	This device class includes scanners, digital cameras, multi-mode video cameras with frame capture, and frame grabbers. The agent sees Canon cameras as a Windows Portable Device, not as a Still Image device.
USB CD DVD RW	This is a USB optical drive.
USB Drive	This is a USB hard drive or USB flash drive.
VMware USB Passthrough	This is a VMware virtual machine client that has USB devices connected to the host.
Windows Portable Device	These are portable devices that use the Microsoft Windows Portable Device (WPD) driver technology, such as mobile phones, digital cameras, and portable media players.

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 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	<p>Adding an application control exclusion allows application changes and additions to the specified folders. For Windows, use an absolute path, including the drive letter.</p> <p>Example for Windows: C:\Application</p>
External Device Exclusion List	<p>Adding an external device exclusion allows the USB mass storage device to connect to a device.</p> <ul style="list-style-type: none"> • 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, read-only permissions, or to block the external device.
Memory Violation Exclusion	<p>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.</p> <p>Example for Windows: \Application\Subfolder\application.exe</p> <p>Example for macOS (without spaces): /Applications/SampleApplication.app/Contents/MacOS/executable</p> <p>Example for macOS (with spaces): /Applications/Sample Application.app/Contents/MacOS/executable</p> <p>See Wildcards in memory violation exclusions for more information.</p>
Policy Safe List	<p>Adding a policy safe list exclusion means all agents assigned to the policy will treat the file as safe, even if BlackBerry 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.</p> <ul style="list-style-type: none"> • 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	<p>Adding a script exclusion allows scripts to run from the specified folder, including subfolders. Use the relative path to the folder.</p> <p>Example for Windows: \Application\Subfolder\</p>

Exclusion Setting	Description
Threat Exclusion	<p>Adding a threat exclusion means the folder is excluded from background threat detection and file watcher. This includes subfolders.</p> <p>For Windows, use an absolute path, including the drive letter. For macOS, use a relative path, escaping any spaces in the path.</p> <p>Example for Windows: C:\Application</p> <p>Example for macOS (without spaces): /Applications/SampleApplication.app</p> <p>Example for macOS (with spaces): /Applications/Sample\ Application.app</p>

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:)

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.

Pattern Syntax for * Wildcard on Windows

Characters	Usage	Details
*	Excluding executables and applications	<p>Matches zero or more characters, except the platform-specific path separator ('\ on Windows).</p> <p>Note:</p> <ul style="list-style-type: none"> • 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.	<p>Matches zero or more layers of a directory (e.g. "**\").</p> <p>Note that "**" is not just a double "*", it is a special notation. To avoid confusion, review the following rules when using this special character:</p> <ul style="list-style-type: none"> • "**\" 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. <p>Note: Wildcard exclusions for Memory Violations apply only to Windows at this time.</p>

The following are examples based on the following path. Relative paths can also be used.

C:\Application\TestApp\MyApp\program.exe

Example	Description
Correct Exclusions	<p>The following is an example of a correct relative path exclusion without any wildcards:</p> <ul style="list-style-type: none">• \Application\TestApp\MyApp\program.exe <p>The following would exclude program.exe as long as program.exe is located under "MyApp" child directory in C: drive:</p> <ul style="list-style-type: none">• C:\Application**\MyApp\program.exe <p>The following would exclude any .exe extension file as long as the executable is located under "MyApp" child directory in C: drive:</p> <ul style="list-style-type: none">• C:\Application**\MyApp*.exe <p>The following would exclude any executable as long as the executable is located under "MyApp" child directory in C: drive:</p> <ul style="list-style-type: none">• C:\Application**\MyApp* <p>The following would exclude program.exe as long as program.exe is located under any child directory that belongs to "TestApp" parent directory in C: drive:</p> <ul style="list-style-type: none">• C:\Application\TestApp**\program.exe <p>The following would exclude program.exe as long as program.exe is located under \Application\TestApp\MyApp\ for any drive:</p> <ul style="list-style-type: none">• **\Application\TestApp\MyApp\program.exe <p>The following would exclude any .exe extension file as long as the executable is located under \Application\TestApp\MyApp\ for any drive:</p> <ul style="list-style-type: none">• **\Application\TestApp\MyApp*.exe <p>The following would exclude any executable as long as the executable is located under \Application\TestApp\MyApp\ for any drive.</p> <ul style="list-style-type: none">• **\Application\TestApp\MyApp*
Incorrect Exclusions	<p>The following example is incorrect because "*" is used for directories. Use a single asterisk "*" for executables:</p> <ul style="list-style-type: none">• C:\Application\TestA**.exe <p>The following example is incorrect because "*" is used for directories. There is no single asterisk "*" specifying executables to exclude:</p> <ul style="list-style-type: none">• C:\Application**

Example	Description
Not Recommended Exclusions	<p>The following is correct, but not recommended. It would effectively exclude anything in any directory (including child directories) under the C: drive:</p> <ul style="list-style-type: none"> • C:*** <p>The following is correct, but not recommended. It would effectively exclude anything in any directory (including child directories) in any drive:</p> <ul style="list-style-type: none"> • ***

Import a policy

You can import device policies from the CylancePROTECT Desktop 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 Desktop, consider the following:

- The CylancePROTECT Desktop 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 CylanceOPTICS, only the CylancePROTECT Desktop policy settings will be imported.
1. In the console, on the menu bar, 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.

After you finish: To export the policy as a JSON file, click the export icon in the Action column.

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 prioritize a rule by changing its order within the rule set. Policy rules evaluate the first rule set in order and evaluates each rule in order until it find one that is true, which is then applied to the device.

When assigning policy rules, consider the following:


- After you edit a rule set and click **Save**, the newly saved rule set will be evaluated against all devices.
- Newly added devices will be evaluated when the Agent registers with the CylanceON-PREM Console.
- When the Agent reports updated attributes to the CylanceON-PREM Console, the rule set will be re-evaluated and applied to a device that has had an attribute changed. Attributes for a device can be found on the Device Details page of a device.
- 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.

You can also manually assign policies to individual devices. See [Assign a policy](#) for more information.

Add a policy rule

You can create tags and tag rules to group devices within CylanceON-PREM. After this, you can 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.

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. In the console, on the menu bar, click **Rules > Policy Rules**.
2. Click **Add New Rule**. You can add multiple rules to the rule set at the same time. Rules run based on their order in the rule set. You can reorder the rule by clicking  and dragging the rule to the correct location in the rule set.
3. Enter a **Rule Name**.
4. Optionally, you can enter a Rule Description.
5. Select a policy for **Devices affected will receive the following policy**.
6. 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.
7. Click **Add "And" condition** or **Add "OR" condition block** to add another condition to the rule, then enter the condition information.
8. Click **Save**.

Policy rule operators

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

Operators	Description
Device Name	<p>This operator uses the information provided to see if the device name matches the condition. The Device Name value is case sensitive.</p> <ul style="list-style-type: none">• 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.

Operators	Description
Distinguished Name (LDAP)	<p>This operator uses the information provided to see if the distinguished name matches the condition.</p> <ul style="list-style-type: none"> • 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	<p>This operator uses the information provided to see if the domain name matches the condition.</p> <ul style="list-style-type: none"> • 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	<p>Provide an IPv4 address range. Any device with an IP address within the given range meets this condition.</p>
Member of (LDAP)	<p>This operator uses the information provided to see if the device's group membership matches the condition.</p> <ul style="list-style-type: none"> • 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	<p>This operator uses the information provided to see if the device's operating system matches the condition.</p> <ul style="list-style-type: none"> • Is: The device operating system must match the selected OS. • Is Not: The device operating system must not match the selected OS.

Operators	Description
Tag	<p>This operator uses the information provided to see if the device has any tags that match the condition.</p> <ul style="list-style-type: none">• Is Any Of: The device must match one or more of the tags in this condition. You can add multiple tags to this condition.

Setting up the CylancePROTECT agent

Devices are added to your organization by installing the CylancePROTECT Desktop 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, they do not pose an immediate threat. CylanceON-PREM requires CylancePROTECT Desktop 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

An installation token is required when installing the CylancePROTECT Desktop agent. The installation token is found in the management console. Using a web browser, log in to CylanceON-PREM and copy the installation token found on the **Settings** page. When initially deploying, 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.

Adding the CA certificate to endpoints

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** and 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**.

Installing the CylancePROTECT Desktop agent for Windows

For information about the CylancePROTECT Desktop agent for Windows, including system requirements, hardware requirements, and installation, see [Requirements: CylancePROTECT Desktop](#) and [Install the Windows agent](#). The following section provides instructions specific to installing the CylancePROTECT Desktop Windows agent with CylanceON-PREM.

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: <code>C:\Program Files\Cylance\Desktop</code> .
REGWSC	0 or 1	0: The agent is not registered with Windows as an anti-virus program. This allows CylancePROTECT Desktop 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: <code>https://login.onprem.com</code> Example of second-level domain name: <code>https://onprem.com</code>

Property	Value	Description
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. 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
```

Installing the CylancePROTECT Desktop agent for macOS

For information about the CylancePROTECT Desktop agent for macOS, including system requirements, hardware requirements, and installation, see [Requirements: CylancePROTECT Desktop](#) and [Install the macOS agent](#). The following section provides instructions specific to installing the CylancePROTECT Desktop macOS agent with CylanceON-PREM.

MacOS installation parameters

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.

Property	Value	Description
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.
LogLevel	0, 1, 2, or 3	0: Error - Only error messages are logged. 1: Warning - Error and warning messages are logged. 2: Information - Error, warning, and information messages are logged. This may provide some details during troubleshooting. This is the default setting. 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: onprem.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 /
```

Installing the CylancePROTECT Desktop agent for Linux

For information about the CylancePROTECT Desktop agent forLinux, including system requirements, hardware requirements, and installation, see [Requirements: CylancePROTECT Desktop](#) and [Install the Linux agent](#). The

following section provides instructions specific to installing the CylancePROTECT Desktop Linux agent with CylanceON-PREM.

Linux OS installation parameters

For information on Linux OS installation parameters, see [Create a configuration file](#).

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=<onpremsuffix> 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=<onpremsuffix> Example: example.com
InstallInfinityURL=<onpremurl> Example: https://example.com
```

Example:

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

Upgrading the CylancePROTECT Desktop agents

You can upgrade CylancePROTECT Desktop Agents that communicate with your CylanceON-PREM virtual appliance.

1. Download the latest Agent upgrade package for your operating system.

Task	Steps
For Windows and macOS:	See FAQ – Where can I download the latest upgrade package for CylancePROTECT Desktop for more information.
For Linux:	See How to request access to CylanceON-PREM downloads for more information.

2. Use a third-party deployment tool to deploy the Agent upgrade package.

Using virtual machines

Below are some recommendations for using the CylancePROTECT Desktop Agent on a virtual machine image. For best practices, see [Best practices for deploying CylancePROTECT Desktop on Windows virtual machines](#).

- 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.
- Some virtual machine software has security settings that conflict with CylancePROTECT Desktop'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. For more information on configuring agents, see [Setting up the CylancePROTECT agent](#).

Assign a policy

You can assign policies manually on the Device List page or automatically by using policy rules. When assigning policies manually, you can select multiple devices and assign them to a policy. For more information about automatically assigning policies, see [Policy rule sets](#).

1. In the console, on the menu bar, click **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 select one or more devices and remove them from your CylanceON-PREM console.

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.

1. In the console, on the menu bar, click **Devices > Device List**.
2. Select one or more devices from the list.
3. Click **Remove**. A confirmation message is displayed.
4. Click **Remove Device**.

Device details

You can view the Device Details page by clicking on a device in the Devices List. The Device Details page contains information related to the selected device, including hostname, policy assigned, and events found on the endpoint.

Change a policy

You can change the policy assigned to a device from the Device List page. A device can only be assigned to one policy. If a policy is associated with a policy rule, it cannot be manually assigned to devices and does not appear as an option on the list.

1. In the console, on the menu bar, click **Devices > Device List**.
2. Select a device from the list to open the device details.
3. Select a policy from the **Policy** list.
4. Click **Save**.

Change a tag

You can apply multiple tags to a device from the Device Details page. Tags can help you organize and manage your devices. If a tag is associated with a tag rule, it cannot be manually assigned to devices and does not appear as an option on the list.

1. In the console, on the menu bar, click **Devices > Device List**.
2. Select a device from the list to open the device details page.
3. Select one or more tags from the **Tags** list.
4. Click **Save**.

View events

You can view events that have been found on devices within CylanceON-PREM on the Events page. Events are malicious activities found on a device that can be related to files (threats), scripts, memory, devices, or applications. Each event page displays the number of events found on that device. Events can also be seen from the threat widgets found on the Dashboard.

1. In the console, on the menu bar, click **Events**.
2. Click on the page for the type of events you want to review. You can select:
 - Threat events
 - Script events
 - Memory events
 - Device events
 - Application events
3. Click an event to view more details.

Device tags


You can create common groupings for devices based on physical location, priority, operating system version, business unit, etc. by using tags in CylanceON-PREM. 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 either manually or automatically, but not both. For information about manually assigning tags to devices, see [Assign a tag](#) . For information about automatically assigning tags to devices, see [Add a tag rule](#).

Create a device tag

You can create a device tag from the Device Tags page.

1. From the console, on the menu bar, click **Devices > Device Tags**.
2. Click **Add New Device Tag**.
3. Type a name for the tag.
4. Click **Add New Tag**.

After you finish: You can edit a tag name by clicking  beside the tag.

Assign a tag

You can assign tags manually on the Device List page or automatically by using tag rules. When assigning tags manually, you can select multiple devices and assign them to a tag. If a tag is associated with a tag rule, it cannot be manually assigned to a device and does not appear in the Assign Tag dialog. For more information about automatically assigning tags, see [Tag rules](#).

1. In the console, on the menu bar, click **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 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 more information, see [Assign a tag](#).

Example: If a device you manually assigned tags to is located in the Portland office and the user transfers to the Austin office, 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 and 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, not the device's past state. This means tags have to be able to be assigned and removed from devices automatically to reflect their current state. 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 the Portland tag 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 can be manually removed from one device, you wouldn't have any way of knowing why the tag wasn't applied to that device. You 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 for a tag rule.

Before you begin: Add a device tag to a device. See [Add a device tag](#) for more information.

1. In the console, on the menu bar, click **Rules > Tag Rules**.
2. Click **Add New Tag Rule**.
3. Enter a **Tag Rule Name**. Optionally, you can enter a description for the tag rule.
4. Select a tag from the **Devices affected will receive the following tag** drop-down for the rule.
5. 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 device name information; if you select Operating System, you must select a target OS from a list.
6. To add another condition to the rule, click **Add "And" condition** or **Add "OR" condition block**, then enter the rule condition information.
7. Click **Add New Tag Rule**.

After you finish:

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

To exclude a device from a tag rule, you can add an AND condition to exclude the specific device. You would set the Evaluation property to device, Operator value to Is Not, and Value to the specific device.

Tag rule operators

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

Operator	Description
Device Name	<p>This operator uses the information provided to see if the device name matches the condition. The Device Name field is case sensitive.</p> <ul style="list-style-type: none"> • 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.
Device	<p>This operator uses the information provided to see if the selected device matches the condition.</p> <ul style="list-style-type: none"> • Is Not: The device name must not match the provided information.

Operator	Description
Distinguished Name (LDAP)	<p>This operator uses the information provided to see if the distinguished name matches the condition.</p> <ul style="list-style-type: none"> • 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	<p>This operator uses the information provided to see if the domain name matches the condition.</p> <ul style="list-style-type: none"> • 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	<p>This operator uses an IP address range that you specify. Any device with an IP address within the given range meets this condition.</p>
Member of (LDAP)	<p>This operator uses the information provided to see if the device's group membership matches the condition.</p> <ul style="list-style-type: none"> • 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	<p>This operator uses the information provided to see if the device's operating system matches the condition.</p> <ul style="list-style-type: none"> • Is: The device operating system must match the selected OS. • Is Not: The device operating system must not match the selected OS.

Remove a device tag

You can manually remove a tag from a device from the Device Tags page. 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 the device will be unassigned from the rule. For more information on tag rules, see [Tag rules](#).

1. In the console, on the menu bar, click **Devices > Device Tags**.
2. Select a tag from the list. 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**.

After you finish: To remove a tag from the CylanceON-PREM console, select the checkbox beside the tag you want to remove on the Device Tags page and 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. In the console, on the menu bar, click **Devices > Device List**.
2. Click on a device to view the device details page.
3. For **Agent Logging Level**, select a logging level.
4. Click **Save**.

Threat management

You can view and manage threats found on devices in your organization using the Threat Events page in the CylanceON-PREM console. You can select a threat, or multiple threats, and add them to the Global Quarantine list or the Global Safelist. You can also acknowledge that an event has been reviewed and no action taken, such as if you found the event to be safe.

Manage threat events


You can manage threats found on devices in your organization on the Threat Events page.

1. In the console, on the menu bar, click **Events > Threat Events**. Optionally, you can also click the Threat Events widget on the Dashboard.
2. Do any of the following:

Task	Steps
View removed threats.	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.
Add a threat to the Global Quarantine list.	<ol style="list-style-type: none">a. Select one or more events from the list.b. Click Globally Quarantine. These events are automatically quarantined on all devices in your organization. The event status is also set to Acknowledged.
Add a threat to the Global Safelist.	<ol style="list-style-type: none">a. Select one or more events from the list.b. Click Globally Safelist. These events are allowed on all devices in your organization. The event status is also set to Acknowledged.
Acknowledge a threat.	<ol style="list-style-type: none">a. Select one or more events from the list.b. Click Acknowledge. This changes the event status from <i>No</i> to <i>Acknowledged</i>. This means that a user has manually acknowledged an event and lowers the threat in the list, allowing you to focus on events that require more attention. By default, the events list displays events that have not been acknowledged first.

After you finish:

To filter entries in this list to find information faster, click .

To export the entries in this list to be used in other applications, click .

Threat event fields

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 Desktop 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 Status	This is the status of the file on the device. The status can be Unsafe, Quarantined, Waived, or Abnormal.
Global List	This indicates whether an event has been added to the Global Quarantine list or Global Safelist. If the event is new, the field will be blank.
Hash	This 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. When calculating the score, CylanceON-PREM uses the local model when analyzing files and does not require an internet connection to gather threat information.

Manage script events


You can manage script events found on devices in your organization on the Script Events page. The Script Events page displays a list of scripts that are considered threats. You can select one or more scripts and add them to the Global Safelist or acknowledge them. The Script Events page aggregates the same event for all devices to help "keep the noise down." You can view more details on a script event by selecting **Script Events** on the details page of a device. For more information on viewing events, see [View events](#).


1. In the console, on the menu bar, select **Events > Script Events**. Optionally, you can click the Script Events widget on the dashboard.

2. Do any of the following:

Action	Steps
Add an event to the Global Safelist.	<ol style="list-style-type: none"> Select one or more events from the list. Click Globally Quarantine. These events are automatically quarantined on all devices in your organization. The event status is also set to Acknowledged.
Acknowledge a threat.	<ol style="list-style-type: none"> Select one or more events from the list. Click Acknowledge. This changes the event status from <i>No</i> to <i>Acknowledged</i>. This means that a user has manually acknowledged an event and lowers the threat in the list, allowing you to focus on events that require more attention. By default, the events list displays events that have not been acknowledged first.

After you finish:

To filter entries in this list to find information faster, click .

To export the entries in this list to use in other applications, click .

Script event fields

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. For example, it might list 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.


Manage memory events

You can manage Memory events found on devices in your organization on the Memory Events page. The Memory Events page displays a list of memory-related events that are considered threats. On the Memory Events page, you can acknowledge that a memory event has been reviewed.

1. In the console, on the menu bar, click **Events > Memory Events**. Optionally, you can click the Memory Events widget on the dashboard.
2. Select one or multiple events on the list and click **Acknowledge**. This changes the event status from *No* to *Acknowledged*. This means that a user has manually acknowledged an event and lowers the threat in the list, allowing you to focus on events that require more attention. By default, the events list displays events that have not been acknowledged first.

After you finish:

To filter entries in this list to find information faster, click .

To export entries in this list to use in other applications, click .

Memory event fields

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.

Manage device events


You can manage device events found on devices in your organization from the Device Events page. The Device Events page displays a list of USB mass storage device events that are considered threats. On the Device Events page, you can acknowledge that an event has been reviewed.

1. In the console, on the menu bar, click **Events > Device Events**. Optionally, you can click the Device Events widget on the dashboard.

2. Select one or more events from the list and click **Acknowledge**. This changes the event status from *No* to *Acknowledged*. This means that a user has manually acknowledged an event and lowers the threat in the list, allowing you to focus on events that require more attention. By default, the events list displays events that have not been acknowledged first.

After you finish:

To filter entries in this list to find information faster, click .

To export entries in this list to use in other applications, click .

Device event fields

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.


Manage application events

You can manage application events found on devices in your organization on the Application Events page. The Application Events page displays a list of application events that are considered threats. You can review and acknowledge application events on the Application Events page.

1. In the console, on the menu bar, click **Events > Application Events**. Optionally, you can click the Application Events widget on the dashboard.
2. Select one or more events on the list and click **Acknowledge**. This changes the status from *No* to *Acknowledged*. This means that a user has manually acknowledged an event and lowers the threat in the list, allowing you to focus on events that require more attention. By default, the events list displays events that have not been acknowledged first.

After you finish:

To filter entries in this list to find information faster, click .

To export entries in this list to use in other applications, click .

Application event fields

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 view and manage events that have been quarantined or added to the safe list for your organization using the Global Lists page.

Add a global list entry

1. In the console, on the menu bar, click **Global Lists**. Optionally, you can click the Global Lists widget on the dashboard.
2. Click **Add New Entry**.
3. On the **Add Global List Entry**, select an entry type from the drop down:

Item	Description
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**.

After you finish: To remove a global list entry, select one or more entries from the list and click **Remove**. A confirmation message displays. Click **Remove Global List Entry**.


Import a global list

You can import a Global List from CylancePROTECT Desktop 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.

Add files to safelist by certificate

You can add files to your CylanceON-PREM console safelist by certificate, allowing custom software that is properly signed to run without being quarantined by the agent. The timestamp, subject, issuer, and thumbprint information from the certificate is extracted by the console and allows administrators to establish a safelist by signed certificate, as represented by the SHA1 thumbprint. CylanceON-PREM does not check if the certificate is expired and does not save or upload the certificate to the console. The certificate timestamp is used to represent when the certificate was created. If the certificate changes, such as it is renewed or replaced, it should be added to the safe list in the management console. The safe list by certificate feature works with PowerShell, ActiveScript, and Office macros.


This feature currently works with Windows and macOS agents only

1. In the console, on the menu bar, click **Global Lists > Certificates**.
2. Click **Add New Entry**. The **Add Global List Entry** modal displays.
3. Drag and drop the certificate to the modal. Optionally, you can browse for the certificate.
4. Select whether the certificate applies to executables or scripts. This allows you to add an executable or script by certificate instead of by folder location. Optionally, you can provide a reason for adding the certificate to the safe list.
5. Click **Create**. The Issuer, Subject, Thumbprint, and Notes are added to the repository.

Import a .csv file that contains a list of certificates that have been added to the global safe list or global quarantine list

You can import a .csv file that contains a list of certificates that have been added to the global safe list or global quarantine list.

Before you begin: You must have exported a csv file of certificates from Cylance Endpoint Security or ON-PREM.

1. In the console, on the menu bar, click **Global Lists > Certificates**.
2. Click .
3. Select the type of list you are importing.
4. Do one of the following:
 - Browse for a .csv file.
 - Drag-and-drop a .csv file onto the screen.
5. Click **Import**. After the file is 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.

Administration

The CylanceON-PREM console offers many ways to manage your users and devices.

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.

CylanceON-PREM has two pre-defined roles: Administrator and Read-Only. You can create custom roles and assign them to users. For more information about custom roles, see [Managing roles](#).

When you deploy CylanceON-PREM for the first time, the console 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. For more information on custom roles, see [Managing roles](#).

1. In the console, on the menu bar, click **Access Management > User Management**. Optionally, you can 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. Optionally, if you are assigning a Read-Only role to a user with a local user account, you can enable the **No password expiration for read-only accounts** option.
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. CylanceON-PREM does not provide any email notifications.

After you finish:

To edit a user, click  in the Action column beside the entry.

To delete a user, click  besides the user you want to delete and click **Delete**. A message displays prompting you to confirm the deletion. Click **Remove 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 need to reactivate them in the future.

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. For more information on configuring IDP settings, see [Configure identity provider settings](#).

1. In the console, on the menu bar, click **Access Management > User Management**. Optionally, you can 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. CylanceON-PREMDoes not provide any email notifications.

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

Change a user password

Administrators can change a user's password from the User Management screen. 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, such as through the IDP's website.

You should generate a random password when you change or reset a user's password. Do not use a generic password because the password might be in the user's password history and therefore will be prohibited. CylanceON-PREM saves a minimum of ten generations when it comes to a user's password.

1. In the console, on the menu bar, 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**.

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.
- Users will be locked out for five minutes after three failed attempts to enter their password.
- Passwords expire after 180 days.
 - If the user has a Read-Only role assigned and has a local user account, you can enable the no password expiration option. Password expiration is enabled by default.


Only Administrators can change or reset a user's password. You should generate a random password when you change or reset a user's password. Do not use a generic password because the password might be in the user's password history and therefore will be prohibited. CylanceON-PREM saves a minimum of ten generations when it comes to a user's password.

For Read-Only users who have a local user account, you can enable the option for **No password expiration for read-only accounts** when creating or editing a user. This option exempts Read-Only users from having to update


their password every 180 days. LDAP and SSO user accounts do not have this option. For more information on creating a user, see [Create a user](#).

Deactivate a user


You can deactivate a user from the CylanceON-PREM console. After deactivating a user, the user cannot log in to your CylanceON-PREM console. You can still perform actions on deactivated users, such as edit or view the user's information.

1. In the console, on the menu bar, click **Access Management > User Management**.
2. Click  for the user you want to deactivate.
3. Click **Deactivate**. A message appears asking if you are sure you want to deactivate the user.
4. Click **Deactivate User**.

After you finish:

To delete a user, click  beside the user you want to delete and click **Delete**. A message displays prompting you to confirm the deletion. Click **Remove 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 need to reactivate them in the future.


Activate a deactivated user

1. Click **Access Management > User Management**.
2. Click  beside the user you want to activate.
3. Click **Activate**.

Add administrators who must use certificate-based authentication

1. In the console, on the menu bar, 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 console, on the menu bar, click **Access Management > User Management**.
2. Click  beside the administrator that you want to configure to use certificate-based authentication.
3. In the Account Type section, click **Certificate**.
4. Type the UPN for the administrator.
5. Click **Update**.

Managing roles


You can control access to your CylanceON-PREM console by using roles. 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. In the console, on the menu bar, 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. A role must have View permission to create, edit, or delete and entry. For more information on role permissions, see [Role permissions](#).
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, the 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. <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• 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	<p>Devices are your endpoints with Agents. Agents must be configured to communicate with your CylanceON-PREM Console.</p> <ul style="list-style-type: none"> • 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	<p>Exclusions define what is on the Safe List or the Quarantine list.</p> <ul style="list-style-type: none"> • 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	<p>Installation tokens are a randomly generated string of characters that enables the agent to report to its assigned account on the CylanceON-PREM console.</p> <p>Note: View System Settings must also be enabled for users to view the installation token.</p> <ul style="list-style-type: none"> • 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	<p>Network Settings define the IP Address for the CylanceON-PREM appliance as well as other configuration options.</p> <p>Note: View System Settings must also be enabled for users to view the installation token.</p> <ul style="list-style-type: none"> • Update allows users to edit the fields in Network Settings.
Policies	<p>Policies define what the Agent will do with threats.</p> <ul style="list-style-type: none"> • 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.
Roles	<p>Roles define what a user can do in the CylanceON-PREM Console.</p> <ul style="list-style-type: none"> • 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.

Role Permission Type	Description
Rules	<p>Rules can automatically assign a policy to a device, based on the selected conditions (like Device Name, IPv4 Address, or Operating System).</p> <ul style="list-style-type: none"> • 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	<p>CylanceON-PREM requires a certificate to ensure secure communication between the server and the endpoints.</p> <ul style="list-style-type: none"> • 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	<p>System Logging Settings sets the level of information captured in the log file.</p> <p>Note: View System Settings must also be enabled for users to view system logging settings.</p> <ul style="list-style-type: none"> • Update allows users to change the logging level for the CylanceON-PREM virtual appliance.
System Logs	<p>System logs are the log files for the CylanceON-PREM virtual appliance. System logs can help when troubleshooting issues with the virtual appliance.</p> <p>Note: View system settings must also be enabled for users to view system version.</p> <ul style="list-style-type: none"> • Downloads allows users to download System Logs.
System Settings	<p>System Settings displays the installation token (used when installing the agent) and system settings (version, hostname, IP address, log level, and console language).</p> <ul style="list-style-type: none"> • View allows users to view the System Settings page.
System Version	<p>System Version provides a way to update the CylanceON-PREM virtual appliance.</p> <p>Note: View system settings must also be enabled for users to view system version.</p> <ul style="list-style-type: none"> • Update allows users to update the CylanceON-PREM virtual appliance.
Tags	<p>Device Tags allow you to group your devices based on your criteria.</p> <ul style="list-style-type: none"> • 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.

Role Permission Type	Description
Users	<p>Users have access to the CylanceON-PREM Console. Use roles to grant or restrict access to the CylanceON-PREM console.</p> <ul style="list-style-type: none"> View allows users to view the User Management page. This option must be selected for users to create, update, or delete tags. <p>This option must be selected for users to create, update, or delete tags.</p> <ul style="list-style-type: none"> Create allows users to create a User. Update allows users to update a User. Delete allows users to delete a User.

Update profile information

You can update your profile information in the CylanceON-PREM console on the **My Account** page.

1. In the console, click 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**.

After you finish: To change your password, type in your old password and type in and confirm your new password in the Change Password section. For more information on password, see [Password requirements](#).

Audit logs


You can review the audit log for information on various actions performed from the CylanceON-PREM console. You can view audit logs by clicking **Audit Logs** on the menu bar of the console.

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

Event	Actions
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

To filter entries in this list to find information faster, click .

To export entries in this list to use in other applications, click .

Managing 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. The certificate is only needed if TLS?SSL is enabled. You cannot manage the CylanceON-PREM SSL certificate from this page. For more information on managing your SSL certificate, see [Update the SSL certificate version 1.2.2.1 and earlier](#).

Add a certificate

You can add a certificate from the **Configuration > Certificates** screen.

1. In the console, on the menu bar, click **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. Optionally, you can 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 change or update a certificate, click  and install the new certificate.



To remove a certificate, click .

Setting up email notifications

You can enable email notifications to alert administrators when a threat is detected.

Note that there is no column in the email notification to display the number of Waived threats. However, the number displayed in the "New" column includes any Waived threats that were found.

Set up integration with an SMTP server

1. In the console, on the menu bar, click **Configuration > Settings > SMTP**.
2. Click .
3. Fill in the fields. Note that you must enter the same email address in the **Sender Address** and **Username** fields.
4. Click .

Select which threats to be notified about

1. In the console, click **<your account name> My Account**.
2. Select which threats that you want to be notified about.
3. Click **Update**.

Settings

The Settings page displays information related to your CylanceON-PREM system, like the installation token, the CylanceON-PREM version you are using, or the hostname. You can also update the CylanceON-PREM appliance from the Settings page.

CylanceON-PREM Info

Info	Description
Installation Token	This setting shows the installation token used when installing the CylancePROTECT Desktop Agent. This is unique for each virtual appliance. Regenerating an installation token provides a unique token for new installation of the CylancePROTECT Desktop. 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.
Version	This setting shows the version for CylanceON-PREM. See Upgrade CylanceON-PREM 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.

Info	Description
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.
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.

Maintenance Mode

Info	Description
Maintenance Mode	This setting shows the status of Maintenance Mode. When enabled, this pauses activity between CylanceON-PREM and CylancePROTECT Desktop devices to allow making changes to the virtual appliance without interruption.

Network Settings

Info	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.
Debug Logs	This setting allows you to ping an IP address to test the connection between CylanceON-PREM and the endpoint.

Info	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

Info	Description
Database Connection Settings	This setting shows the connection information for the external database if it is configured.

Syslog/SIEM

Info	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

Info	Description
LDAP	This setting shows the status of LDAP/Active Directory integration. See Configure active directory for more information.

Identity Provider Settings

Info	Description
Identity Provider Settings.	This setting shows the external identity provider (IdP) settings. See Configure identity provider settings for more information.

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.

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 and external database, or vice versa.

1. Obtain the latest CylanceON-PREM file.
2. In the console, on the menu bar, click **Configuration > Settings**.
3. 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.
4. Take a snapshot of the CylanceON-PREM virtual appliance.
5. Under CylanceON-PREM Info, click **Upgrade**.
6. Select the **I have taken a VM snapshot** check box. Click **Proceed with Upgrading**.
7. Click **Browse for a file**, select the CylanceON-PREM file you want to use for this update. Click **Open**. Optionally, you can drag and drop the file to select it.
8. 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.
9. 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

You can reboot the CylanceON-PREM virtual appliance from the Settings page 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, on the menu bar, 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, on the menu bar, click **Configuration > Settings**.
2. Click **Edit** 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

You can update CylanceON-PREM SSL certificate from the **Configuration > Settings** screen in the console for CylanceON-PREM version 1.3.1 and later. For more information on certificate guidelines, refer to the [Certificate Guidelines](#).

1. In the console, on the menu bar, 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. Optionally, you can 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

You can update the CylanceON-PREM SSL certificate for CylanceON-PREM version 1.2.2.1 and older by repeating the configuration process and 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`. Replace `<fqdn>` with the fully qualified domain name (FQDN) from the DNS entry. 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, you can revert to TLS 1.0 (Legacy Mode).

1. In the management console, on the menu bar, 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


You can enable maintenance mode in order to take a complete snapshot of the CylanceON-PREM virtual appliance. Maintenance mode pauses all communication between CylanceON-PREM and the endpoints. Maintenance mode should be enabled when upgrading the appliance or changing the network settings.

1. In the console, on the menu bar, click **Configuration > Settings**.
2. Click the toggle button beside **Maintenance Mode**.
3. Disable Maintenance Mode after you finish your changes.

Change network settings

You can change the network settings for your CylanceON-PREM virtual appliance from the **Configuration > Settings** screen. Before changing network settings, take a snapshot of the virtual appliance so you can revert if necessary.

1. In the console, on the menu bar, 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 information.
6. Click .
7. Click **Maintenance Mode** and confirm disabling it. Site activity resumes.



Check an IP address

You can enter an IP address from the Settings screen and check if the CylanceON-PREM virtual appliance can communicate with the endpoint.

1. In the console, on the menu bar, 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

You can change the log level for the CylanceON-PREM virtual appliance from the Settings screen. You can set the log level to Critical, Error, Warning, Info, or Debug. Setting the log level to Debug can consume a high amount of disc space. Debug logging should only be used when troubleshooting server issues. Otherwise, the level should be set Info.

1. In the console, on the menu bar, click **Configuration > Settings**.
2. Under Settings, click  beside Debug Log.
3. Select a logging level from the list.
4. Click .


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

Administrators can figure CylanceON-PREM version 1.1.0 or higher to forward events from their CylanceON-PREM virtual appliance 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.

The Threat Classifications event type is not available for CylanceON-PREM because the virtual appliance does not communicate with the CylancePROTECT Desktop console.

1. In the console, on the menu bar, 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. For more information on syslog settings, see the [Cylance Syslog Guide](#).

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

Note: UDP does not support notifications when the Syslog server shuts down.

5. Click .

After you finish:

To upload an SSL certificate, go to the **Configuration > Certificates** page and add the certificate. See [Add a certificate](#) for more information.

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 many 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

You can update your database connection settings if you configured an external database when setting up CylanceON-PREM. This section is not displayed when you use the database shipped with CylanceON-PREM. When updating the database connection settings, 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. In the console, on the menu bar, 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 .


After you finish:

To upload the external database certificate for SSL connection, go to the **Configuration > Certificates** page and add the certificate. See [Add a certificate](#) for more information.

Configure active directory


You can enable active directory from the **Configuration > Settings** screen. 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: If active directory is enabled, the username for the CylanceON-PREM local user account must 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 [Managing 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

You can 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 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 console, on the menu bar, 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.

After you finish:

To upload multiple CA certificates, concatenate the certificates into a single 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, you can create a consent banner so that the user provides consent (e.g. consent for monitoring) before the user logs in.

1. In the console, on the menu bar, click **Configuration > Settings**.
2. Click  beside 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.

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

Add an application

You can have up to ten custom applications in CylanceON-PREM.

1. In the console, on the menu bar, 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.

After you finish:

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 BlackBerry 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.

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

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.

The screenshot displays the Swagger Editor interface. On the left, the OpenAPI specification is shown in a dark-themed editor. The code includes the following details:

```

1 openapi: 3.0.0
2 info:
3   title: 'CylanceON-PREM API'
4   description: 'CylanceON-PREM API documentation.'
5   version: 1.0.0
6 servers:
7   -
8     url: 'https://cylance.onprem/cyapi/v1/client'
9 paths:
10  /tags:
11    post:
12      tags:
13      - 'Device Tags'
14      summary: 'Create a new tag'
15      operationId:
16      'App\Http\Controllers\Api\DeviceTaggingController
17      ::createTag'
18      requestBody:
19      required: true
20      content:
21      application/json:
22      schema:
23      required:
24      - name
25      properties:
26      name:
27      type: string
28      maxLength: 50
29      type: object
30 responses:
31  201:
32  description: Created
33  content:
34  application/json:
35  schema:
36  properties:
37  id:
38  description: 'The ID of the tag that was
39  created'
40  type: integer
41  type: object
42  400:
43  $ref: '#/components/responses/ValidationError'
44  401:
45  $ref: '#/components/responses/Unauthorized'
46  403:

```

The right pane shows the rendered API documentation for 'CylanceON-PREM API' (version 1.0.0, OAS3). It features a 'Servers' dropdown menu set to 'https://cylance.onprem/cyapi/v1/client'. Below this, there are two sections: 'Device Tags' (CRUD operations on device tags) and 'Devices' (RUD operations on devices). The 'Device Tags' section includes three endpoints: a POST endpoint for creating a new tag, a DELETE endpoint for deleting a tag, and a PATCH endpoint for adding devices to a tag. The 'Devices' section includes two GET endpoints: one for device search and another for getting a device by ID.

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:

policyId
array[integer]
(query) Filter by policy id. Can include one to many policyIds.

tagId
array[integer]
(query) Filter by tag Id. Can include one to many tagIds.

Responses

Curl

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

Request URL

```
https://cylance.onprem/cyapi/v1/client/devices?page=1&pageSize=50&includeMeta=true
```

Server response

Code	Details
Undocumented	TypeError: Failed to fetch



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 BlackBerry 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 accordingly in documentation.
Other	Contact BlackBerry 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 BlackBerry 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

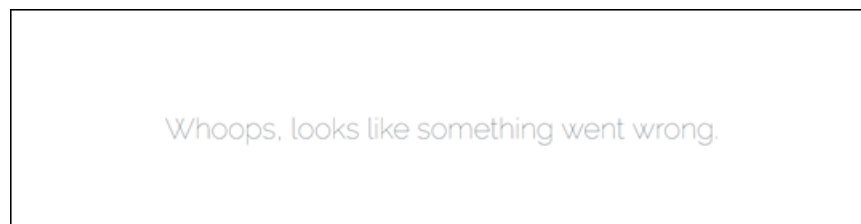
When attempting to log in to the CylanceON-PREM console, the web browser displays an error, reporting an insecure webpage.

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

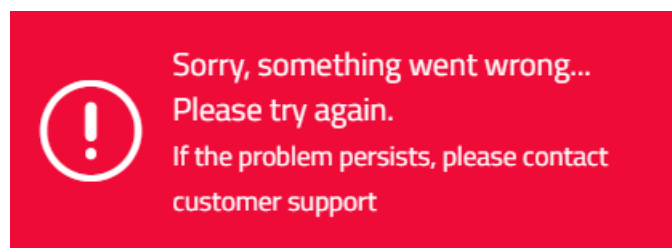
Unable to connect to external database

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 CylanceON-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. You can perform the following tasks 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 the connectivity to the OCSP.
- Ensure the OCSP is running.



A user is not receiving email notifications

- Check to see if there are any new threats in the management console that have a 'Reported On' time within the previous hour.
- Check to see if the SMTP feature is enabled.
- Perform an SMTP test connection.
- Check to see if the user is assigned the administrator role.
- Check to see if the user is subscribed to email notifications.
- Check the audit logs for a 'Send Email' error.

Before you contact support

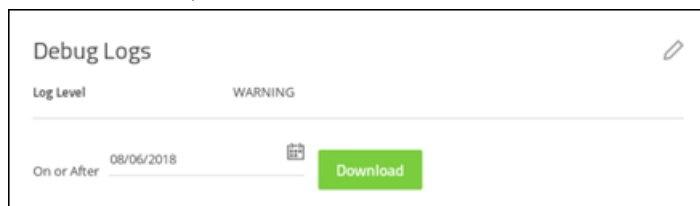
If the above troubleshooting suggestions do not resolve your issue, before contacting BlackBerry Support, enable Debug logging on the CylanceON-PREM System page, wait for at least 20 minutes, then download the log file and submit it to BlackBerry Support.

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.



4. Create a BlackBerry Support ticket and include the CylanceON-PREM log file.
 - a) Log in to myAccount (<https://myaccount.blackberry.com>).
 - b) Select **My Service Requests**, then select **Create Case**. Or select the Support Community dropdown list from the top menu, then select Create Case.
 - c) Under Step 1, select **CylancePROTECT**.
 - d) Under Step 2, select **ON-PREM**.
 - e) Click **Next**.
5. In the Search Issue Summary box, complete the following steps:
 - a) Type **Submit ON-PREM logs**, then check the box.
 - b) Click **Next**.
 - c) In the detailed description box, state that you are submitting CylanceON-PREM logs.

- d) Click **Submit Case**.
- 6. Attach your CylanceON-PREM log file to the support ticket.
 - a) Select **My Service Requests**, then select **View Cases**. Or select the Support Community dropdown list from the top menu, then select View Cases.
 - b) Open the case you just created.
 - c) Click **Attachments**.
 - d) Click the plus sign.
 - e) Enter a description.
 - f) Drag and drop your CylanceON-PREM log file or click Upload Files and add your file. The maximum file size is 2GB.

Legal notice

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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

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

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

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

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

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

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

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

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

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

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

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

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

Published in Canada