Product: CylanceON-PREM

Document: CylanceON-PREM Administrator Guide. This guide is a succinct resource for analysts, administrators, and customers who are reviewing or evaluating the product.

Document Release Date: 1.7.2 rev2, July 2020

About BlackBerry®: BlackBerry develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees’ home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry protects the endpoint without increasing staff workload or costs.

Copyright: © 2020 BlackBerry Inc. All Rights Reserved.
Table of Contents
Contents

Table of Contents ........................................................................................................ 3
Contents ....................................................................................................................... 4
Overview ...................................................................................................................... 8
High-Level Installation and Configuration Steps ......................................................... 9
  Pre-deployment Steps ................................................................................................. 10
  Deployment Steps ....................................................................................................... 10
  CylanceON-PREM Configuration Steps .................................................................. 10
  Console Configuration Steps ...................................................................................... 11
  Agent Installation Steps ............................................................................................ 11
CylanceON-PREM Virtual Appliance ........................................................................... 12
  CylanceON-PREM OVA Requirements .................................................................... 13
  Hardware Requirements ............................................................................................ 13
    All-in-One Virtual Appliance ................................................................................... 13
    Endpoint Management Virtual Appliance (up to 50,000 Endpoints) ................... 13
    External Database ................................................................................................... 13
  Other Requirements .................................................................................................. 14
  Web Browser Support ................................................................................................ 14
Things to Know About CylanceON-PREM ................................................................. 14
Configure CylanceON-PREM Virtual Appliance ...................................................... 15
  Before Configuring CylanceON-PREM ................................................................... 15
  Import OVA and Configure Static IP Address .......................................................... 16
  Import OVA and Configure DHCP ........................................................................... 17
  Configure CylanceON-PREM .................................................................................... 18
  External Database Overview ...................................................................................... 24
Console Configuration ................................................................................................. 25
Log in to CylanceON-PREM ......................................................................................... 26
  Log In Using IdP Credentials .................................................................................... 26
Administrative Dashboard ............................................................................................ 26
Filter Lists .................................................................................................................... 28
Export Lists .................................................................................................................. 29
Policies .......................................................................................................................... 29
  Add a Policy ............................................................................................................... 30
  Import a Policy ........................................................................................................... 41
Cylance Score ................................................................. 81
Script Events ................................................................. 82
Script Event Field Definitions ........................................ 83
Memory Events ............................................................... 83
Memory Event Field Definitions ........................................ 84
Device Events ............................................................... 85
Device Event Field Definitions .......................................... 85
Application Events ......................................................... 86
Application Event Field Definitions ................................... 87
Global Lists .................................................................. 88
Add a Global List Entry .................................................. 89
Import a Global List ....................................................... 89
Remove a Global List Entry ............................................. 90
Administration ................................................................ 91
Managing Users ............................................................. 92
Create a User ................................................................. 92
Create a User with Identity Provider Settings Enabled .......... 92
Password Requirements ................................................ 93
Change a User Password ............................................... 94
Edit a User .................................................................. 94
Deactivate a User ......................................................... 95
Delete a User ............................................................... 95
Role Management .......................................................... 95
Create a Role ............................................................... 96
Role Permissions ........................................................ 96
Edit a Role .................................................................. 99
Delete a Role ............................................................. 99
My Account .................................................................. 100
Update Profile Information ........................................... 100
Change Your Password ............................................... 100
Audit Logs .................................................................. 100
Certificates .................................................................. 101
Add a Certificate ........................................................... 101
Configuration ............................................................... 103
Overview
CylanceON-PREM offers next generation protection to organizations with networks where Internet access is severely restricted or not allowed (air-gapped environments).

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

This guide covers installing, configuring, and monitoring your CylanceON-PREM virtual appliance. This guide also covers the CylancePROTECT Agent installation parameter required to configure your Agents to communicate with your CylanceON-PREM virtual appliance.

**High-Level Installation and Configuration Steps**

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

1. Verify System Requirements:
   - "CylanceON-PREM OVA Requirements" on page 13
   - "Hardware Requirements" on page 13
   - "Other Requirements" on page 14
   - "Web Browser Support" on page 14
   - "Things to Know About CylanceON-PREM" on page 14

2. Create a DNS Entry on the Network. See "Before Configuring CylanceON-PREM" on page 15 for more information.

3. Locate root CA certificate. See "Before Configuring CylanceON-PREM" on page 15 for more information.

Deployment Steps

4. Import CylanceON-PREM Virtual Appliance (OVA file):
   - "Import OVA and Configure Static IP Address" on page 16
   - "Import OVA and Configure DHCP" on page 17

CylanceON-PREM Configuration Steps

5. Log into the Console to configure CylanceON-PREM. See "Configure CylanceON-PREM" on page 18 for more information.

6. Select a Certificate option:
   - Generate and submit a CSR from CylanceON-PREM.
   - Generate an SSL certificate and private key using a different computer, then upload to CylanceON-PREM.

7. Select a database option:
   - If using an external database, see "External Database Overview" on page 24 before continuing.
   - Configure database options. See "Choose a database option." on page 22 for more information.
Console Configuration Steps

8. Add or import a policy:
   - "Add a Policy" on page 30
   - "Import a Policy" on page 41

9. (Optional) "Add a Device Tag" on page 73.

10. (Optional) "Add a Tag Rule" on page 74.

11. (Optional) "Add a Policy Rule " on page 43.

Agent Installation Steps

12. "Add Root CA Certificate to Every Endpoint" on page 47.


14. Install agents on devices (endpoints):
   - "Windows Agent" on page 49
   - "macOS Agent" on page 55
   - "Linux Agent" on page 58
CylanceON-PREM Virtual Appliance
CylanceON-PREM OVA Requirements

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

Hardware Requirements

All-in-One Virtual Appliance

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

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

- RAM: 16GB
- CPU: 2.2 GHz quad-core (Intel Xeon processors or later)
- Free Disk Space: 1TB

Endpoint Management Virtual Appliance (up to 50,000 Endpoints)

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

- RAM: 16GB
- CPU: 2.2 GHz 20-core (Intel Xeon processors or later)
- Free Disk Space: 1TB

External Database

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

- RAM: 16GB
- CPU: 2.2 GHz quad-core (Intel Xeon processors or later)
- Free Disk Space: 500GB
- Database: PostgreSQL version 10.4 (or higher)

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

**Note:** When connecting the Endpoint Management Virtual Appliance with the External Database for the first time, CylanceON-PREM will create the necessary tables in the database.

### Other Requirements
- CylancePROTECT Agent version 1480 or higher installed on the endpoints
- Root Certificate Authority (CA) certificate, installed (trusted) on each endpoint
- Obtain a server certificate by submitting a Certificate Signing Request generated by CylanceON-PREM or on another server to your Certificate Authority of choice. The server certificate must be installed on CylanceON-PREM, and if the latter method was used to obtain the certificate, the private key will also need to be installed on CylanceON-PREM.

### Web Browser Support
The CylanceON-PREM web portal currently supports:
- Google Chrome (latest 2 versions)
- Mozilla Firefox (latest 2 versions)
- Apple Safari (latest 2 versions)
- Microsoft Edge (latest version)
- Microsoft Internet Explorer 11 (with latest updates)

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

**WARNING:** Administrators should generate a random password when changing or resetting a user's password. Do not use a generic password because the password may already be in the user's history (last 10 passwords) so it will be prohibited.
- A CylanceON-PREM virtual appliance cannot communicate to or through another CylanceON-PREM virtual appliance.
- CylanceON-PREM currently does not support CylanceOPTICS.
- 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 since it is a proprietary system. Cylance does not support modifying anything on the virtual appliance or gaining access to it.
- Devices configured to communicate with CylanceON-PREM must be able to communicate with the DNS hostname you created for CylanceON-PREM. Removing a device from that network results in the device being Offline. In Offline mode, Agents will continue to function as designed, using the last policy update received while the device was Online.
- There are currently no migration options to go from an All-in-One virtual appliance to an Endpoint Management Virtual Console with an external database (PostgreSQL), or vice versa. This includes upgrading the virtual appliance. Once a virtual appliance is deployed, with an internal database or an external database, it cannot be changed to the other.
- It is recommended to utilize the VMware vSphere High Availability feature to provide failure protection against hardware and operating system outages for your CylanceON-PREM environment. For more information, see VMware’s article here.

Configure CylanceON-PREM Virtual Appliance

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

Before Configuring CylanceON-PREM

- Create a DNS entry on your network (work with your IT department, if necessary).
  - Create a fully qualified domain name (FQDN) for the virtual appliance. For example, a fully qualified domain name could be login.onprem.com or onprem.com.
  - The DNS entry will also need the IP address of the OVA operating system.
  - **DHCP:** If you use DHCP, the IP address for CylanceON-PREM can be seen on the login screen of the virtual appliance.
  - **Static IP:** If you use a static IP address, use that in the DNS entry. Also follow the Import OVA and Configure Static IP Address task.
- Have a root CA certificate. This is installed (trusted) on every endpoint.
- Obtain a server certificate by submitting a Certificate Signing Request generated by CylanceON-PREM or on another server to your Certificate Authority of choice. The server certificate must be installed on CylanceON-PREM, and if the latter method was used to obtain the certificate, the private key will also need to be installed on CylanceON-PREM.

**Import OVA and Configure Static IP Address**

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

**IMPORTANT:** 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 does not display so you will need to use the VMware OVF Tool to import the OVA and configure a static IP address. For information about using the VMware OVF Tool, see "Configure Static IP using the OVF Tool" on page 137.

**Note:** If DHCP is used, go to the “Import OVA and Configure DHCP” on the next page task.

**To Import the OVA and Configure a Static IP Address**

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

10. Click **Finish**.

**Import OVA and Configure DHCP**

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

**Note:** If a static IP address is used, go to the "Import OVA and Configure Static IP Address" on the previous page task.

1. In VMware vSphere, select **Actions > Deploy OVF Template**. The Deploy OVF Template window displays.

2. Select the OVA file, then click **Next**.

3. Type a name for the virtual machine, select a location, then click **Next**.

4. Select a computer resource, then click **Next**.

5. Review the details, then click **Next**.
6. Select storage and other settings, then click Next.

7. Select a network, then click Next.

8. Click Next. Leaving the Customize Template field blank will enable DHCP on the virtual appliance.

9. Click Next. Review the settings.

10. Click Finish.

Configure CylanceON-PREM

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

Notes:

- If you are using a static IP address, do the "Import OVA and Configure Static IP Address" on page 16 task first.

- If you are using an external database, read " External Database Overview" on page 24 for an overview of the setup.

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

2. Open a web browser and go to https://<fqdn>.
   - Replace <fqdn> with the fully qualified domain name (FQDN) from the DNS entry.
   - For a web browser, use a system that can communicate with the CylanceON-PREM virtual appliance.

   Note: A warning message might appear, stating that your CylanceON-PREM site is not secure. This is because the SSL certificate and key have not been added to your CylanceON-PREM virtual appliance. After the SSL certificate and key have been added, the warning might still appear next to the URL. Once configuration is complete, the warning message will go away after closing and then reopening the web browser.

3. To generate a certificate signing request (CSR) from CylanceON-PREM that will be submitted to a Certificate Authority (CA) to use with the CylanceON-PREM virtual appliance:

   Note: To use an SSL certificate and key generated on a computer other than CylanceON-PREM, go to step 4.
• Fill out the form.

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

  b. **Subject Alternative Name:** Any alternative names to use for the virtual appliance, such as `onprem-alt.cylance.com`. Please note that the Common Name will be added automatically as a Subject Alternative Name. Click **Add** after typing an alternative name to add it.

c. **Organization Name:** The legal name of the organization.

d. **Organizational Unit:** This could be a department name.

e. **City:** The city where the organization is located.

f. **State / Province:** The state or province where the organization is located. Do not use an abbreviation.

g. **Country:** The two letter ISO abbreviation for the country.
Click **Generate CSR**. This creates a `cert_request.csr` file in the Downloads folder. Send this to your Certificate Authority who should then send back an SSL certificate.

**Example**: `onprem.cylance.crt`.

**Note**: If you click **Generate CSR** again, a new private key will be generated, and you will need to provide the latest CSR to the Certificate Authority.

4. Click **Upload Cert and Key**. The Webserver Configuration page displays.
5. 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.

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. Skip the remaining steps below and continue to Step 7.

If you generated a Certificate Signing Request on a different computer than CylanceON-PREM, upload a Private Key:

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

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

**Note:** If your Certificate Authority provides you a PFX file (combined site certificate and private key), they will need to separate it into two separate files. In addition, the private key file cannot be password protected.
7. Click **Save and Continue**. SSL is configured on the virtual appliance.

8. Choose a database option.

   - **Database Connection Settings are Disabled**
     - This is the All-in-One solution
     - This uses the database included with the CylanceON-PREM virtual appliance
     - This supports up to 10,000 endpoints

   - **Database Connection Settings are Enabled**
     - This allows connecting an external database
     - The CylanceON-PREM Endpoint Management virtual appliance is used as the Console and for other Cylance components
     - This supports up to 50,000 endpoints
     - Enter the hostname or IP address for the external database (for example, `database.com` or `123.45.67.89`)
     - Enter the port number for the external database (for example, `5432`)
     - Enter the database user name and password (this database user must be able to add tables to the database)
     - Enable TLS/SSL to use an SSL connection to the external database. If TLS/SSL is enabled, you can also specify the following:
       - Enable Verify Peer Mode to authenticate the external Postgres DB server certificate, and the communications channel is encrypted. Verify Peer Mode=disabled means CylanceON-PREM will not authenticate the external Postgres DB server certificate but the communications is still encrypted.
         - Click **Install Postgres SSL Certificate**, then drag the certificate file to the Install Postgres SSL Certificate dialog box or click **Browse for a file** and select the certificate.
         - Click **Install Certificate**.
     - Click **Test Connection** to ensure the virtual appliance can communicate with the database
• Click **Save and Continue**.

![Database Connection Settings](image_url)

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

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

![Login Screen](image_url)
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 the user's environment. This list is simply provided as guidance and could help if connecting the external database to the virtual appliance is not working.

- Install PostgreSQL and PostgreSQL server
- Initialize the PostgreSQL database
- Start and enable autostart postgres service to start the database when the server starts
- Force postgres to listen on all ports in postgresql.conf
- Allow postgres port through firewall
- Enable the pgcrypto extension
- Create a postgres user
  - If the database is dedicated to CylanceON-PREM, using the default postgres user is an option
  - If the database is shared, then you should create a new postgres user for the CylanceON-PREM database

  **Note:** A shared database is not recommended for CylanceON-PREM

- Authorize remote postgres authentication in pg_hba.conf file
- Generate SSL certificates for postgres server connection
- Configure SSL in postgresql.conf file

When connecting the external database to CylanceON-PREM:

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


For security, CylanceON-PREM will require a user to re-login after 10 minutes of non-activity.

Log In Using IdP Credentials

To configure CylanceON-PREM to use an external identity provider (IdP), like Okta. see "Configure Identity Provider Settings" on page 118.

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 IdP, the CylanceON-PREM Dashboard should display.

2. Log in to your Identity Provider's website and go through any validation processes (like two factor authentication). If you are authenticated by your identity provider, your browser will redirect to the CylanceON-PREM Dashboard.

Administrative Dashboard

The CylanceON-PREM Administrative Dashboard displays when you first log into the Console. This page provides an overview of threat events on devices and quick links to frequently used features in the product.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Management</td>
<td>Clicking this widget opens the <strong>User Management &gt; Users</strong> page.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Filters the event widgets to display events as follows:&lt;br&gt;  - No - Only displays events that have not been acknowledged by a user (manually quarantined or safelisted or from clicking Acknowledge on the Events page).&lt;br&gt;  - All - Displays all events including acknowledged and unacknowledged. &lt;br&gt;<strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Application Events</td>
<td>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 <strong>Events &gt; Application Events</strong> page.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Clicking this widget opens the <strong>Configuration &gt; Settings</strong> page.</td>
</tr>
<tr>
<td>Device Events</td>
<td>Displays the total number of USB mass storage device events in your organization. Clicking this widget opens the <strong>Events &gt; Device Events</strong> page.</td>
</tr>
<tr>
<td>Devices</td>
<td>Displays the total number of devices communicating with this CylanceON-PREM virtual appliance. Clicking this widget opens the <strong>Device List</strong> page.</td>
</tr>
<tr>
<td>Global Lists</td>
<td>The Global Lists page displays events that were added to the Global Quarantine or Global Safe lists. Clicking this widget opens the <strong>Global Lists</strong> page.</td>
</tr>
<tr>
<td>Memory Events</td>
<td>Displays the total number of malicious memory events in your organization. Clicking this widget opens the <strong>Events &gt; Memory Events</strong> page.</td>
</tr>
<tr>
<td>Policies</td>
<td>Clicking this widget opens the <strong>Policies</strong> page.</td>
</tr>
<tr>
<td>Reported On</td>
<td>Filters the event widgets based on a date/time or date range set in this filter. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Script Events</td>
<td>Displays the total number of malicious script events in your organization. Clicking this widget opens the <strong>Events &gt; Script Events</strong> page.</td>
</tr>
<tr>
<td>Threat Events</td>
<td>Displays the total number of malicious file events in your organization. Clicking this widget opens the <strong>Events &gt; File Events</strong> page.</td>
</tr>
</tbody>
</table>
Filter Lists

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

1. Click the Filter icon (⚙️) on the right side above the list to expand the list of filters available.

![Page Name](image)

2. Set one or more filters from the following types.

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

     ![Search by hash, file name, file path, and interpreter](image)

   - **Text Entry fields**: Enter a full or partial name of the term you are searching for in the column, such as the full file name, then click the Save Filter icon (✔️).

     **Note**: Wildcards are not supported.

   - **Date Range fields**: Enter a date range or select a range by clicking on the date entry region. To remove a date range, click Clear.

   - **Selectable fields**: Click one or more options from a list. To remove a selected option, click the green X to the right of the selected option.

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

3. Click the Filter icon again to hide the filter options. A green circle appears on the Filter icon (⚙️) to indicate that filters are applied.
To Remove a Filter from a List

1. Click the Filter icon ( ) on the right side above the list to view the filters applied.
2. Click the X beside the applied filter(s) to remove in the Quick Search field:

```
<table>
<thead>
<tr>
<th>Safe</th>
<th>Acknowledged</th>
<th>Hash</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

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

Policies

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

Once created, 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" on page 70.
information about automatically assigning policies to devices, see "Add a Policy Rule " on page 43.

Tip: You can filter entries in this list to make finding information faster using the Filter icon (🔧). See "Filter Lists" on page 28 for more information.

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 Policy Name and select policy options. Descriptions for each policy option are listed below.

4. Click Save.

Threat Settings

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

<table>
<thead>
<tr>
<th>Threat Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Execution in Threat Exclusion Folders</td>
<td>Allows execution of files in Threat Exclusion folders in addition to exclusion of threats found during File Watcher and Background Threat Detection.</td>
</tr>
<tr>
<td>Auto Delete Quarantine</td>
<td>Automatically deletes quarantined files after a specified number of days. This applies to all devices assigned to the policy. The minimum number of days is one.</td>
</tr>
<tr>
<td>Threat Setting</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Auto Quarantine Abnormal Files</strong></td>
<td>The number of days starts when the file was first quarantined. This action is included in the Agent log file for verification. If this feature is not enabled, the quarantined files will remain on the device until the quarantined files are manually deleted.</td>
</tr>
</tbody>
</table>
| **Auto Quarantine Unsafe Files**   | Quarantines an Abnormal file to prevent it from executing. On a device, quarantining a file will move the file from its original location to the Cylance Quarantine directory.  
  - **For Windows**: C:\ProgramData\Cylance\Desktop\q  
  - **For macOS**: /Library/Application Support/Cylance/Desktop/q  
  Some malware is designed to drop other files in certain directories. This malware will continue to do so until the file is successfully dropped. To stop the malware from continually dropping the removed file, the Agent will modify the dropped file so it won’t execute and leave it in the folder.  
  **Note**: Auto Quarantine Unsafe Files must be selected for Auto Quarantine Abnormal Files to be available. |
| **Background Threat Detection**    | Performs a full disk scan to detect and analyze any dormant threats on the disk. The full disk scan is designed to minimize impact to the end-user by using a low amount of system resources.  
  The user can choose to run the scan once (upon installation only) or run recurring (which performs a scan every 9 days). A significant upgrade to the Cylance model, like adding new operating systems, will also trigger a full disk scan. Each time a new scan is performed, all files will be rescanned.  
  It is recommended that users set Background Threat Detection to Run Once. Due to the predictive nature of the CylancePROTECT technology, periodic scans of the entire disk are not necessary but can be implemented for compliance purposes. |
| **Copy File Samples**              | Allows user to specify a network share where file samples can be copied. This allows users to do their own analysis of files the Agent considers Unsafe or Abnormal.  
  - Supports CIFS/SMB network shares. |
Threat Setting | Description
---|---
| Specify one network share location. Using the fully qualified path is recommended. For example: \server_name\shared_folder | All files meeting 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 | Detects and analyzes any new or modified files for dormant threats. It is recommended that users 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 the user prefers to quarantine a file as it is added to a disk (File Watcher) but before execution (Auto-Quarantine).

Scan Archive | Sets the maximum archive file size the Agent will scan. This setting applies to Background Threat Detection and File Watcher.

Memory Protection

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

For descriptions of the different Violation, Process, and Escalation Types, see Memory Protection Violation Types.

**WARNING:** Enabling Memory Protection may cause errors if there is another application that also monitors running processes. It is recommended to disable the other application’s memory protection before enabling Cylance’s. If that is not possible, then leave Cylance’s Memory Protection disabled in your 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

<table>
<thead>
<tr>
<th>Exploitation Violation Types</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stack Pivot</strong> — 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).</td>
<td>Windows macOS</td>
</tr>
<tr>
<td><strong>Stack Protect</strong> — 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).</td>
<td>Windows macOS</td>
</tr>
<tr>
<td><strong>Overwrite Code</strong> — Code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass Data Execution Prevention (DEP).</td>
<td>Windows</td>
</tr>
<tr>
<td><strong>RAM Scraping</strong> — A process is trying to read valid magnetic stripe track data from another process. Typically related to point of sale systems (POS).</td>
<td>Windows</td>
</tr>
<tr>
<td><strong>Malicious Payload</strong> — A generic shellcode and payload detection associated with exploitation has been detected.</td>
<td>Windows</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process Injection Violation Types</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Allocation of Memory</strong> — 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.</td>
<td>macOS</td>
</tr>
<tr>
<td><strong>Remote Mapping of Memory</strong> — 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.</td>
<td>Windows</td>
</tr>
<tr>
<td><strong>Remote Write To Memory</strong> — 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.</td>
<td>Windows macOS</td>
</tr>
<tr>
<td><strong>Remote Write PE To Memory</strong> — 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.</td>
<td>Windows</td>
</tr>
<tr>
<td><strong>Remote Overwrite Code</strong> — 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.</td>
<td>Windows</td>
</tr>
</tbody>
</table>
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.

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.

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.

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

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.

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.
Note:

- 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. Recommended for initial deployment or testing.

- Block only allows scripts to run from specific folders. Use after testing in Alert mode.

![Script Control PowerShell Settings Console](image)

**Figure 2: Script Control PowerShell Settings Console**

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

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

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

As part of a Device Control policy, administrators can also define exceptions to the policy. This is done by using the Vendor ID, Product ID, and Serial Number to specify the exception. Minimally, the Vendor ID must be entered, but the Product ID and Serial Number can also be used for a more specific exception.

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

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

<table>
<thead>
<tr>
<th>Device Control Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked</td>
<td>This device type is blocked from accessing the endpoint it is connected to.</td>
</tr>
<tr>
<td>Full Access</td>
<td>This device type is allowed to access the endpoint it is connected to.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Agent Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Notifications</td>
<td>Agent Notification popups can be configured at the policy-level.</td>
</tr>
<tr>
<td>Prevent Service Shutdown</td>
<td>The Cylance service is protected from being shutdown either manually or by another process.</td>
</tr>
</tbody>
</table>

Exclusions

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

**Add New Exclusion**

<table>
<thead>
<tr>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Safe List</td>
</tr>
<tr>
<td>Threat Exclusion</td>
</tr>
<tr>
<td>External Device Exclusion List</td>
</tr>
<tr>
<td>Application Control Exclusion</td>
</tr>
<tr>
<td>Memory Violation Exclusion</td>
</tr>
<tr>
<td>Script Exclusion</td>
</tr>
</tbody>
</table>

*Figure 3: Create a Policy Exclusion*

<table>
<thead>
<tr>
<th>Exclusion Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Application Control Exclusion | Adding an Application Control exclusion allows application changes and additions to the specified folders. For Windows, use an absolute path, including the drive letter.  
Example for Windows: C:\Application |
<p>| External Device         | Adding an External Device exclusion allows the USB mass storage device to connect to a device.                                             |</p>
<table>
<thead>
<tr>
<th>Exclusion Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Exclusion List** | - 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 to allow Full Access or to Block the external device. |
| **Memory Violation Exclusion** | Adding a Memory Violation exclusion allows the specified file to run or be installed on any device assigned to the policy. The Memory Violation exclusion uses a relative file path.  
Example for Windows: \Application\Subfolder\application.exe  
Example for macOS (without spaces): /Applications/SampleApplication.app/Contents/MacOS/executable  
Example for macOS (with spaces): /Applications/Sample Application.app/Contents/MacOS/executable  
See "Wildcards in Memory Violation Exclusions" on the next page for more information. |
| **Policy Safe List** | Adding a Policy Safe List exclusion means all Agents assigned to the policy will treat the file as Safe, even if Cylance ranks it as Unsafe or Abnormal. This lets you allow a file to a group of devices but not for the rest of your organization.  
- SHA256 (required) – Include the SHA256 hash for the file you want to allow.  
- MD5 – Include the MD5 hash of the file. This is optional.  
- File Name – Include the filename of the file. This is optional.  
- Category (required) – Use this to categorize files to identify why it is allowed.  
- Reason (required) – Include a reason for allowing this file. |
| **Script Exclusion** | Adding a Script exclusion allows scripts to run from the specified folder, including subfolders. Use the relative path to the folder.  
Example for Windows: \Application\Subfolder\ |
| **Threat Exclusion** | Adding a Threat exclusion means the folder is excluded from Background Threat Detection and File Watcher. This includes subfolders.  
For Windows, use an absolute path, including the drive letter. For macOS, use a relative path, escaping any spaces in the path.  
Example for Windows: C:\Application  
Example for macOS (without spaces): /Applications/SampleApplication.app  
Example for macOS (with spaces): /Applications/Sample\ Application.app |
Wildcards in Memory Violation Exclusions

Memory violation exclusions can include the following special characters (all OS):

\^ & \* @ \{ \} \[ \] \$ = ! - # ( ) \% . + ~ _

In Agent 1560 or higher, the following additional special characters are also supported for Windows:

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

**Pattern Syntax for * Wildcard on Windows**

<table>
<thead>
<tr>
<th>Characters</th>
<th>Usage</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Excluding executables and applications.</td>
<td>Matches zero or more characters, except the platform-specific path separator (\ on Windows).</td>
</tr>
<tr>
<td>**</td>
<td>Excluding drives and directories. Can be used to include child directories.</td>
<td>Matches zero or more layers of a directory (e.g. &quot;**&quot;).</td>
</tr>
</tbody>
</table>

**Notes:**

- 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.

**Examples of Correct Exclusions:**

- `\Application\TestApp\MyApp\program.exe`
  - Relative path exclusion without any wildcards.
- `C:\Application\**\MyApp\program.exe`
  - Would exclude program.exe as long as program.exe is located under "MyApp" child directory in C: drive.
- `C:\Application\**\MyApp\*.exe`
<table>
<thead>
<tr>
<th>Characters</th>
<th>Usage</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Would exclude any .exe extension file as long as the executable is located under &quot;MyApp&quot; child directory in C: drive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Application**\MyApp*</td>
<td></td>
<td>Would exclude any executable as long as the executable is located under &quot;MyApp&quot; child directory in C: drive.</td>
</tr>
<tr>
<td>C:\Application\TestApp**\program.exe</td>
<td></td>
<td>Would exclude program.exe as long as program.exe is located under any child directory that belongs to &quot;TestApp&quot; parent directory in C: drive.</td>
</tr>
<tr>
<td>**\Application\TestApp\MyApp*.exe</td>
<td></td>
<td>Would exclude any .exe extension file as long as the executable is located under any child directory that belongs to &quot;TestApp\MyApp*&quot; under any drive.</td>
</tr>
<tr>
<td>**\Application\TestApp\MyApp*</td>
<td></td>
<td>Would exclude any executable as long as the executable is located under any child directory that belongs to &quot;TestApp\MyApp*&quot; under any drive.</td>
</tr>
</tbody>
</table>

**Example of Incorrect Exclusions:**

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

**Not Recommended Exclusions:**

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

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

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

Note: When importing a policy from CylancePROTECT:

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

To Import a Policy

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

5. Click **Import**. The imported policy displays in the Policy list with the name you specified.

### Export a Policy

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

1. Select **Policies** from the menu.

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

### Policy Rule Sets

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

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

You can also manually assign policies to individual devices. For information on manual assignment, see ["Assign a Policy" on page 70](#).

### Policy rule priority

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

### Evaluating policy rules

Rules are evaluated in the following scenarios:

- After you edit a rule set and click **Save**. The process of saving the rule set causes all devices to be evaluated against the newly saved rule set.

- Newly added devices will be evaluated when the Agent registers with the CylanceON-PREM Console.
When the Agent reports updated device attributes to the CylanceON-PREM Console (found under the General Info section on the Device List > select a device > Device Details page). If the device IP or other attribute changes, the rules will be re-evaluated and applied for that device only.

If a tag is added or removed on a device, the rules will be re-evaluated and applied for that device only.

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

Add a Policy Rule

Best Practice: Create tags and tag rules first to group the devices. Then create a policy rule that uses the Tag condition to apply a policy to the group of devices. See "Add a Device Tag" on page 73 and "Add a Tag Rule" on page 74 for more information.

Review the following:

- Policies can only be associated with one rule. If the Add New Rule button is disabled, it means no policies exist or all policies are assigned to a rule and you will need to create a new policy. See "Add a Policy" on page 30 for more information.

- Policy rules are not evaluated until the rule set is saved.

1. Add a policy. See "Add a Policy" on page 30 for more information.


3. Click Add New Rule.

   You can add multiple rules to the rule set at the same time.

4. (Optional) Rules run based on their order in the rule set with the first rule running first, and so on. To reorder the rule, click and drag the rule to the correct location in the rule set.

5. Enter a Rule Name.

6. (Optional) Enter a Rule Description.

7. Select a policy for Devices affected will receive the following policy.

8. Create a rule condition. Rule conditions contain three parts that are used to determine whether a policy rule will be applied: evaluation property, operator, and value. If the rule condition evaluates to True, the policy will be applied to a device.

   a. Click an evaluation property from the drop-down list beside Device Name.

   b. Click an operator from the drop-down list beside Starts With.
See "Policy Rule Operators" below for a description of all available operators.

C. Enter or select a value for the conditions. This varies depending on the other conditions selected. For example, selecting Device Name will require entering some device name information; selecting Operating System will require selecting a target OS from a list.

9. To add another condition to the rule, click Add "And" condition or Add "OR" condition block, then enter the condition information.

10. Click Save.

Policy Rule Operators

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

<table>
<thead>
<tr>
<th>Operators</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Uses the information provided to see if the device name matches the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Contains</strong>: The device name must contain the provided information, but it can be anywhere within the name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Contain</strong>: The device name must not contain the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not End With</strong>: The device name must not end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Start With</strong>: The device name must not start with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Ends With</strong>: The device name must end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Starts With</strong>: The device name must start with the provided information.</td>
</tr>
<tr>
<td></td>
<td>The Device Name value is case sensitive.</td>
</tr>
<tr>
<td>Distinguished Name (LDAP)</td>
<td>Uses the information provided to see if the distinguished name matches the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Contains</strong>: The distinguished name must contain the provided information, but it can be anywhere within the name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Contain</strong>: The distinguished name must not contain the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not End With</strong>: The distinguished name must not end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Start With</strong>: The distinguished name must not start with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Ends With</strong>: The distinguished name must end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Starts With</strong>: The distinguished name must start with the provided information.</td>
</tr>
<tr>
<td>Domain name</td>
<td>Uses the information provided to see if the domain name matches the condition.</td>
</tr>
<tr>
<td>Operators</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Contains</strong>: The domain name must contain the provided information, but it can be anywhere within the name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Contain</strong>: The domain name must not contain the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not End With</strong>: The domain name must not end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Start With</strong>: The domain name must not start with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Ends With</strong>: The domain name must end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Starts With</strong>: The domain name must start with the provided information.</td>
</tr>
<tr>
<td>IPv4 Address in Range</td>
<td>Provide an IPv4 address range. Any device with an IP address within the given range meets this condition.</td>
</tr>
<tr>
<td>Member of (LDAP)</td>
<td>Uses the information provided to see if the device’s group membership matches the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Contains</strong>: The Member Of must contain the provided information, but it can be anywhere within the member information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Contain</strong>: The Member Of must not contain the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Is</strong>: The Member Of must match the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Is Not</strong>: The Member Of must not match the provided information.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Uses the information provided to see if the device’s operating system matches the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Is</strong>: The device operating system must match the selected OS.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Is Not</strong>: The device operating system must not match the selected OS.</td>
</tr>
<tr>
<td>Tag</td>
<td>Uses the information provided to see if the device has any tags that match the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Is Any Of</strong>: The device must match one or more of the tags in this condition. You can add multiple tags to this condition.</td>
</tr>
</tbody>
</table>
Devices are added to your organization by installing the CylancePROTECT Agent on each system. Once connected to the CylanceON-PREM console, you can apply policies (to manage identified threats) and organize your devices based on your needs.

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

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

**Important Note About Initial Deployment**

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

**Add Root CA Certificate to Every Endpoint**

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

**Add Root CA Certificate to Windows**

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

Add 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, then click the Terminal icon.

3. In Terminal, type cd ./Downloads, then press Return.

4. Type sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain rootCA.crt, then press Return. In this example, the root CA certificate is named rootCA.crt. If your certificate has a different file name, be sure to change it in the command before running it.

5. Type your password, then press Return.

Copy Installation Token

An Installation Token is required when installing the CylancePROTECT Agent.

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

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

Ensure that your endpoint meets or exceeds the following system requirements.

System Requirements

The device can be a physical or virtual machine.

Supported Microsoft Windows Operating Systems

<table>
<thead>
<tr>
<th>OS</th>
<th>32-bit</th>
<th>64-bit</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP SP3</td>
<td>X</td>
<td>X</td>
<td>KB 968730* and KB 2868626 hotfix must be installed.**</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The trusted root certificates listed in KB 293781 must be installed.</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>X</td>
<td>X</td>
<td>The trusted root certificates listed in KB 293781 must be installed.</td>
</tr>
<tr>
<td>Windows 7</td>
<td>X</td>
<td>X</td>
<td>KB4054518 must be installed on Windows 7 (32-bit and 64-bit) and Windows 7 Embedded (32-bit and 64-bit) systems that use CylancePROTECT Agent 1494 or Agent 1550 and higher. For more information, read the KB article here. *** The trusted root certificates listed in KB 293781 must be installed.</td>
</tr>
<tr>
<td>OS</td>
<td>32-bit</td>
<td>64-bit</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------</td>
<td>--------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Support includes <strong>Windows Embedded Standard 7</strong> and Embedded POSReady 7. Windows POSReady 7 - Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td>Windows 8 and 8.1</td>
<td>X</td>
<td>X</td>
<td>Windows 8 Embedded - Requires CylancePROTECT Agent 1480 or higher. Windows RT is not supported.</td>
</tr>
<tr>
<td>Windows 10</td>
<td>X</td>
<td>X</td>
<td>Supports Enterprise, Pro, and Home editions - Requires CylancePROTECT Agent 1480 or higher. Windows 10 Anniversary Update (v1607) - Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Microsoft Windows 10 Device Guard and Credential Guard are supported with CylancePROTECT Agent version 1480 or higher.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Microsoft has also introduced a version of Windows Subsystem for Linux (WSL) in the Windows 10 Anniversary Update. WSL lets users run a bash shell on Ubuntu on Windows and has been received very positively by the developer community. WSL is disabled by default and Microsoft is likely to introduce more features before it becomes generally available. BlackBerry is following these updates and will introduce necessary controls for WSL when it becomes mainstream. Until then, BlackBerry recommends disabling this feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Windows 10 Creators Update (v1703) - Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>Note</strong>: Windows 10 Creators Update has the same known issues as the Windows 10 Anniversary Update.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Windows 10 Fall Creators Update (v1709 - Redstone 3) - Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CylancePROTECT Agent 1480 added the detection of Microsoft OneDrive files. <strong>Note</strong>: There is one known issue with OneDrive files changing status from &quot;Online-only file&quot; to &quot;Locally available file.&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enabling Windows Defender Device Guard Code Integrity will cause Modern Apps to fail with error 0xC000047E when Memory Protection or Script Control is enabled. This issue was resolved with the release of CylancePROTECT Agent 1480. Please read: <a href="#">Memory Protection: Conflict with</a></td>
</tr>
<tr>
<td>OS</td>
<td>32-bit</td>
<td>64-bit</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Windows 10 IoT Enterprise</strong></td>
<td>X</td>
<td>X</td>
<td>Limited support is available in CylancePROTECT Agent 1510.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Windows 10 IoT Core and Windows 10 IoT Core Services are not supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ARM is not supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The CylancePROTECT agent does not support the Unified Write Filter (UWF) on Windows 10 IoT. The UWF is an optional feature within Windows OS. To ensure you do not experience a conflict, make sure that the UWF is disabled before installing the agent.</td>
</tr>
<tr>
<td><strong>Windows Server 2003 SP2 and</strong></td>
<td>X</td>
<td>X</td>
<td>KB 968730* and <a href="#">KB 2868626</a> hotfix must be installed.**</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>** ***</td>
</tr>
<tr>
<td>OS</td>
<td>32-bit</td>
<td>64-bit</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2003 R2</td>
<td></td>
<td></td>
<td>The trusted root certificates listed in <a href="#">KB 293781</a> must be installed on Windows Server 2003 SP2.</td>
</tr>
</tbody>
</table>
| Windows Server 2008 and 2008 R2 | X (2008 only) | X | **KB 3004394** hotfix must be installed. The trusted root certificates listed in [KB 293781](#) must be installed.  
**KB4054518** must be installed on Windows Server 2008 R2 (64-bit) systems that use CylancePROTECT Agent 1494 or Agent 1550 and higher. For more information, read the KB article [here](#).  
Windows Server 2008 and 2008 R2 Foundation editions require CylancePROTECT Agent 1540 or higher.  
Windows Server 2008 Server Core and 2008 R2 Server Core are not supported. |
| Windows Server 2012 and 2012 R2 | – | X | Requires CylancePROTECT Agent 1480 or higher.  
Supports Standard, Data Center, Essentials, Server Core, Embedded, and Foundation editions.  
- Windows Server 2012 and 2012 R2 - Embedded edition requires CylancePROTECT Agent 1480 or higher.  
- Windows Server 2012 and 2012 R2 Foundation editions require CylancePROTECT Agent 1540 or higher.  
- Windows Server 2012 and 2012 R2 - Minimal Server Interface is not supported.  
- Windows Storage Server 2012 is not supported. |
| Windows Server 2016      | –      | X      | Requires CylancePROTECT Agent 1480 or higher.  
Supports Standard, Data Center, Essentials, and Server Core editions.  
- Windows Server Core 2016 requires CylancePROTECT Agent 1480 or higher  
- Windows 2016 Nano Server is not supported.  
- Windows Storage Server 2016 is not supported. |
| Windows Server 2019      | –      | X      | Requires CylancePROTECT Agent 1510 or higher.  
Supports Standard, Data Center, and Core editions.  
- Windows Storage Server 2019 is not supported.  
- Windows Server 2019 Data Center edition is supported on CylancePROTECT Agent 1530 or higher.  
- Windows Server 2019 Core edition is supported on CylancePROTECT Agent 1560 or higher.  
**Note:** Windows Server 2019 Data Center does not |
support the following features:

- Hyper-V Server Role is not supported with Shielded Virtual Machines
- Host Guardian Hyper-V Support
- Software-defined Networking
- Storage Spaces Direct

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

** For additional information about errors when accessing secure Cylance hosts, click [here](#).

*** BlackBerry Support does not provide assistance in searching and implementation of any Microsoft related KB's or other 3rd party patches. For any issues with finding or implementing Microsoft related KB's, please reach out to Microsoft for assistance.

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

## Additional Windows Requirements

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Requires at a minimum a two core processor.</td>
</tr>
<tr>
<td></td>
<td>Supports the SSE2 Instruction set.</td>
</tr>
<tr>
<td></td>
<td>Supports x86_64 instruction set.</td>
</tr>
<tr>
<td></td>
<td>Does not support ARM instruction set.</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
</tr>
<tr>
<td>Available Hard Drive Space</td>
<td>600 MB</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Disk space usage can increase depending on features enabled, like setting the log level to Verbose.)</td>
</tr>
<tr>
<td>Additional Software/Requirement</td>
<td>.NET Framework 3.5 (SP1) or higher (Note: .NET 4.0 must be the full version, not the .NET 4 Client Profile.)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A fully functioning installation of .NET Framework that meets the above specifications is a requirement for the CylancePROTECT Agent to be installed and function as expected.</td>
</tr>
<tr>
<td></td>
<td>Internet Browser</td>
</tr>
<tr>
<td></td>
<td>Internet access to login, access the installer, and register the product</td>
</tr>
<tr>
<td></td>
<td>Local administrator rights to install the software</td>
</tr>
<tr>
<td></td>
<td>Root Certificates:</td>
</tr>
<tr>
<td></td>
<td>• VeriSign Class 3 Public Primary Certification Authority - G5</td>
</tr>
</tbody>
</table>

CylanceON-PREM Administrator Guide, 1.7.2 rev2, July 2020 | 53
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• GeoTrust Global CA</td>
</tr>
<tr>
<td></td>
<td>• thawte Primary Root CA</td>
</tr>
<tr>
<td></td>
<td>• DigiCert Global Root CA</td>
</tr>
<tr>
<td><strong>Note:</strong> Devices missing any of the above root certificates may experience issues with the Cylance service not starting or the device being unable to communicate with the Console. Please see this <a href="#">article</a> for more details about missing root certificates.</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>• TLS 1.2 is supported and requires .NET Framework 4.5.2 or higher</td>
</tr>
</tbody>
</table>

### Installation Parameters – Windows

The Agent must be installed through GPO, SCCM, MSIEXEC, or 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).

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIDKEY</td>
<td>Installation Token</td>
<td>The Installation Token from your CylanceON-PREM Console.</td>
</tr>
<tr>
<td>LAUNCHAPP</td>
<td>0 or 1</td>
<td>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.</td>
</tr>
<tr>
<td>SELFPROTECTIONLEVEL</td>
<td>1 or 2</td>
<td>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.</td>
</tr>
<tr>
<td>APPFOLDER</td>
<td>Target Installation Folder</td>
<td>Specifies the Agent install directory. The default location is: C:\Program Files\Cylance\Desktop.</td>
</tr>
<tr>
<td>REGWSC</td>
<td>0 or 1</td>
<td>0: The Agent is not registered with Windows as an anti-virus program. This allows CylancePROTECT and Windows Defender to run at the same time on the endpoint. 1: The Agent is registered with Windows as an anti-virus program. This is the default setting.</td>
</tr>
<tr>
<td>InstallRegistrationURL</td>
<td>CylanceON-</td>
<td>The URL for your CylanceON-PREM Console.</td>
</tr>
<tr>
<td>Property</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| PREM URL             | Example of third-level domain name: https://login.onprem.com  
Example of second-level domain name: https://onprem.com |
| InstallTrustedSuffix | Cy VanceON-PREM URL suffix   | The URL suffix for your Cy VanceON-PREM Console.  
Example: example.com |
| InstallInfinityURL   | Cy VanceON-PREM URL          | The URL for your Cy VanceON-PREM Console.  
Example of third-level domain name: https://login.onprem.com  
Example of second-level domain name: https://onprem.com |

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

**macOS Agent**

Ensure that your endpoint meets or exceeds the following system requirements.

**System Requirements**

The device can be a physical or virtual machine.

**Supported macOS Operating Systems**

<table>
<thead>
<tr>
<th>OS</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac OS X 10.9</td>
<td>Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td>Mac OS X 10.10</td>
<td>Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td>Mac OS X 10.11</td>
<td>Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td>macOS Sierra (10.12)</td>
<td>Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td>macOS High Sierra (10.13)</td>
<td>Requires CylancePROTECT Agent 1480 or higher.</td>
</tr>
<tr>
<td>macOS Mojave (10.14)</td>
<td>Requires CylancePROTECT Agent 1510 or higher.</td>
</tr>
<tr>
<td>macOS Catalina (10.15)</td>
<td>Requires CylancePROTECT Agent 1550 or higher.</td>
</tr>
</tbody>
</table>

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

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

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

- **macOS Mojave version 10.14.x (recommended)** - If you are running macOS Mojave and have installed CylancePROTECT, it is recommended that you enable Full Disk Access on your macOS system. If Full Disk Access is not enabled, CylancePROTECT will be unable to process files secured by user data protection.

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

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

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

### Additional macOS Requirements

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Requires at a minimum a two core processor</td>
</tr>
<tr>
<td></td>
<td>Supports the SSE2 instruction set</td>
</tr>
<tr>
<td></td>
<td>Supports x86_64 instruction set</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
</tr>
<tr>
<td>Available Hard Drive</td>
<td>600 MB</td>
</tr>
<tr>
<td>Space</td>
<td>Note: Disk space usage can increase depending on features enabled, like setting the log level toVerbose.</td>
</tr>
<tr>
<td>Additional Requirements</td>
<td>Internet Browser</td>
</tr>
<tr>
<td></td>
<td>Internet access to login, access the installer, and register the product</td>
</tr>
<tr>
<td></td>
<td>Local administrator rights to install the software</td>
</tr>
<tr>
<td></td>
<td>Root Certificates:</td>
</tr>
</tbody>
</table>
### Installation Parameters – macOS

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>YOURINSTALLTOKEN</td>
<td></td>
<td>The Installation Token from your CylanceON-PREM Console.</td>
</tr>
<tr>
<td>NoCylanceUI</td>
<td></td>
<td>The Agent icon should not appear on startup. The default setting is the icon is visible.</td>
</tr>
<tr>
<td>SelfProtectionLevel</td>
<td>1 or 2</td>
<td>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.</td>
</tr>
<tr>
<td>LogLevel</td>
<td>0, 1, 2, or 3</td>
<td>0: Error — Only error messages are logged. 1: Warning — Error and warning messages are logged. 2: Information (default) — Error, warning, and information messages are logged. This may provide some details during troubleshooting. 3: Verbose — All messages are logged. When troubleshooting, this is the recommended log level. However, verbose log file sizes can grow very large. It is recommended to turn Verbose on during troubleshooting and then change it back to Information when troubleshooting is complete.</td>
</tr>
<tr>
<td>InstallRegistrationURL</td>
<td></td>
<td>The URL for your CylanceON-PREM Console. Example of third-level domain name: <a href="https://login.onprem.com">https://login.onprem.com</a> Example of second-level domain name:</td>
</tr>
<tr>
<td>Property</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InstallTrustedSuffix</td>
<td>CylanceON-PREM URL suffix</td>
<td>The URL suffix for your CylanceON-PREM Console. Example: example.com</td>
</tr>
<tr>
<td>InstallInfinityURL</td>
<td>CylanceON-PREM URL</td>
<td>The URL for your CylanceON-PREM Console. Example of third-level domain name: <a href="https://login.onprem.com">https://login.onprem.com</a> Example of second-level domain name: <a href="https://onprem.com">https://onprem.com</a></td>
</tr>
</tbody>
</table>

```bash
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 /
```

**Linux Agent**

Ensure that your endpoint meets or exceeds the following system requirements.
System Requirements

The device can be a physical or virtual machine.

To download the CylancePROTECT Linux Agent for CylanceON-PREM, see the CylanceON-PREM Linux Agent Download KB article.

**Note:** Do not download the CylancePROTECT Linux Agent from the Cloud Console.

Supported Linux Operating Systems

<table>
<thead>
<tr>
<th>OS</th>
<th>32-bit</th>
<th>64-bit</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL/CentOS 6.6</td>
<td>X</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 6.7</td>
<td>X</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 6.8</td>
<td>X</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 6.9</td>
<td>X</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 6.10</td>
<td>X</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 7.0</td>
<td>X</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 7.1</td>
<td>–</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 7.2</td>
<td>–</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 7.3</td>
<td>–</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 7.4</td>
<td>–</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 7.5</td>
<td>–</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 7.6</td>
<td>–</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>RHEL/CentOS 7.7</td>
<td>–</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher.**</td>
</tr>
<tr>
<td>Ubuntu LTS/Xubuntu 16.04</td>
<td>X</td>
<td>X</td>
<td>Requires CylancePROTECT Agent 1560 or higher. ***</td>
</tr>
</tbody>
</table>
### Additional Linux Requirements

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Requires at a minimum a two core processor</td>
</tr>
<tr>
<td></td>
<td>Supports the SSE2 instruction set</td>
</tr>
<tr>
<td></td>
<td>Supports x86_64 instruction set</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
</tr>
<tr>
<td>Available Hard Drive Space</td>
<td>600 MB</td>
</tr>
<tr>
<td>Other</td>
<td>TLS 1.2 is supported</td>
</tr>
<tr>
<td></td>
<td>Required packages:</td>
</tr>
<tr>
<td></td>
<td>glibc.i686</td>
</tr>
<tr>
<td></td>
<td>dbus-libs.i686</td>
</tr>
<tr>
<td></td>
<td>RHEL/CentOS 7.x - dbus version 1.10.x or higher</td>
</tr>
<tr>
<td></td>
<td>openssl-libs.i686</td>
</tr>
<tr>
<td></td>
<td>libgcc.i686</td>
</tr>
<tr>
<td></td>
<td>sqlite.i686</td>
</tr>
</tbody>
</table>
Configure Linux Agents

Convert and Distribute Certificates

Agents must trust the certificate that the virtual appliance has been configured with to communicate with the virtual appliance. Linux Agents do not use a central certificate store like Windows or macOS systems. Instead, the Linux Agent uses the certificate store from the Mono framework. These certificates must be formatted in a Mono-specific format. Once the x509 certificate is converted into the Mono format, the certificate files can be distributed to Linux endpoints.

By converting the certificates, you do not need to install Mono on each Linux Agent endpoint.

Mono for Linux Steps

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

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

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

   The certificate needs to be in PEM format.

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

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

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

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

   Example Output: cert-sync rootCA.crt
4. Mono stores the synced certificate to:
   
   `/usr/share/.mono/new-certs/Trust`

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

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

   **Example:** The red boxed certificate is the certificate that was synced using the above steps. All other certificates were inserted upon installation of Mono.
5. On each Linux device that will use the appliance, create the following directory:

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

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

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

Example method to create the directory:

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

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

**Mono for Windows Steps**

The following steps use a Windows 10 machine as an example.

2. In the Start menu, right-click **Open Mono x64 Command Prompt** and select **More**
> Run as administrator. Please refer to Mono's documentation here for more information.

Example: Windows 10 Installation

The following command prompt window displays:

3. Change directories to the location where your certificate is stored.
   
   **Note:** The certificate needs to be in PEM format.
   
   **IMPORTANT:** The certificate required is the one used to sign the certificate and key for your CylanceON-PREM virtual appliance.

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

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

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

   Example Output: `cert-sync rootCA.crt`
5. Mono stores the synced certificates in the ProgramData directory:

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

The mono certificate will look like this:

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

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

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

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

Example method to create the directory:

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

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

**Install the Linux Agent**

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

1. Download the CylancePROTECT Linux Agent for CylanceON-PREM. See the CylanceON-PREM Linux Agent Download KB article for more information.

   **Note:** Do not download the CylancePROTECT Linux Agent from the Cloud Console.

2. Copy synced certificates to the proper directory for all target Linux machines. See "Convert and Distribute Certificates" on page 61 for more information.

3. Create the config_defaults.txt file and include the installation parameters.
   a. Enter `mkdir /opt/cylance`, then press **Enter**. This creates the installation folder.
   b. Enter `cd /opt/cylance`, then press **Enter**.
   c. Enter `echo InstallToken=YourInstallationToken > config_defaults.txt`, then press **Enter**. Replace `YourInstallationToken` with the installation token from the Console.
   d. Enter `echo InstallRegistrationURL=<onpremurl> > config_defaults.txt`, then press **Enter**. Replace `<onpremurl>` with the fully-qualified domain name for the server.

      **Example:** https://onprem.example.com. See more examples in the next section.
   e. Enter `echo InstallTrustedSuffix=<onpremsuffix> > config_defaults.txt`, then press **Enter**. Replace `<onpremsuffix>` with the URL suffix for the server.

      **Example:** example.com. See more examples in the next section.
   f. Enter `echo InstallInfinityURL=<onpremurl> > config_defaults.txt`, then press **Enter**. Replace `<onpremurl>` with the fully-qualified domain name for the server.

      **Example:** https://onprem.example.com. See more examples in the next section.

Install the Linux Agent

1. Navigate to the folder with the Linux Agent installation file. For example, if the installation file is in the Downloads folder and you are logged on as root: enter `cd /root/Downloads`, then press **Enter**.

2. Type the following and press **Enter**. This installs the Linux Agent.

   - **RHEL/CentOS:** `rpm -ivh CylancePROTECT.el7.rpm`
   - **Ubuntu:** `dpkg -i cylance-protect.1604.i686.deb`
This example installs the Linux Agent for RHEL/CentOS 7 and Ubuntu 16.04. Change the RPM or deb file name as needed during installation.

3. (Optional) Type the following and press Enter. This installs the UI for the Linux Agent. The UI is not required to run the Agent.

   - **RHEL/CentOS**: `rpm -ivh CylancePROTECTUI.el7.rpm`
   - **Ubuntu**: `dpkg -i cylance-protect.ui.1604.i686.deb`

   This example installs the Linux Agent UI for RHEL/CentOS 7 and Ubuntu 16.04. Change the RPM or deb file name as needed during installation.

### Examples for the Linux Configuration File

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

**Example**: Third-level domain name (onprem.example.com):

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

**Example**: Second-level domain name (example.com):

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

**Example**:

```
echo InstallToken=YourInstallationToken > config_defaults.txt
```

```
echo InstallRegistrationURL=<onpremurl> >> config_defaults.txt
```

```
echo InstallTrustedSuffix=<onpremurlsuffix> >> config_defaults.txt
```

```
echo InstallInfinityURL=<onpremurl> >> config_defaults.txt
```
Upgrade Agents

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

1. Download the latest Agent upgrade package for your operating system(s).
   - **Windows and macOS:** See [FAQ – Where can I download the latest upgrade package for CylancePROTECT](#) for more information.
   - **Linux:** See [CylanceON-PREM Linux Agent Download](#) for more information.

2. Use a 3rd party deployment tool to deploy the Agent upgrade package.

Virtual Machines

Below are some recommendations for using the CylancePROTECT Agent on a virtual machine image. For best practices, see the Virtual Desktop Infrastructure (VDI) Best Practices section in the CylancePROTECT Admin Guide.

- For non-persistent VDI environments, you can use Agent 1490 (or higher) and an installation parameter to instruct the Agent during installation that will be running in a pool of cloned images. This will enable the Agent to recognize each clone as a unique endpoint and persist their identification when they refresh. See the Virtual Desktop Infrastructure (VDI) Best Practices section in the CylancePROTECT Administrator Guide for more information.

- Some virtual machine software has security settings that conflict with CylancePROTECT’s Memory Protection feature. This conflict may result in an unresponsive virtual machine. If this happens, it is recommended to 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.

![Device List page](image)

**Tips:**
- You can filter entries in this list to make finding information faster using the Filter icon (🔍). See "Filter Lists" on page 28 for more information.
- To use entries in this list in other applications click ➡️ See "Export Lists" on page 29 for more information.

**Assign a Policy**

Policies can be assigned manually using this procedure or automatically using policy rules. When assigning policies manually, you can select one or more devices and manually assign them to a policy. For more information about automatically assigning policies, see "Policy Rule Sets" on page 42.

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

**Remove a Device**

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

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

4. Click **Remove Device**.

**Notes:**

- 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 Install Token. Either input the Install Token or uninstall the Agent from the endpoint.

**Device Details**

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

**Change a Policy**

A device can only be assigned to one policy.

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

1. Select **Devices > Device List**, then click a device. The Device Details page displays.
2. Select a policy from the **Policy** list.
3. Click **Save**.

**Change a Tag**

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

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

1. Select **Devices > Device List**, then click a device. The Device Details page displays.
2. Select one or more tags from the **Tags** list.
3. Click **Save**.
View Events

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

These events pages display the same information as the global events pages (accessed from the Events menu) filtered for the selected device except for the Script Events page. For more information about the global events, see the relevant sections under “Threat Management” on page 79. For information about the Script Events page, see the section below.

Device Script Events

<table>
<thead>
<tr>
<th>Script Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledged</td>
<td>Acknowledging an event means it has been reviewed.</td>
</tr>
<tr>
<td>Drive Type</td>
<td>The drive or storage type the script was discovered on.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Internal Hard Drive or Network Drive.</td>
</tr>
<tr>
<td>File Path</td>
<td>The path where the script was found.</td>
</tr>
<tr>
<td>Interpreter</td>
<td>The script interpreter responsible for executing the script. This could be</td>
</tr>
<tr>
<td></td>
<td>PowerShell, Active Script, or Microsoft Office Macros.</td>
</tr>
<tr>
<td>Last Reported</td>
<td>The date and time the script was last discovered on devices in your</td>
</tr>
<tr>
<td></td>
<td>organization.</td>
</tr>
<tr>
<td>Hash</td>
<td>The SHA256 hash for the script file.</td>
</tr>
<tr>
<td>Safe</td>
<td>The current status of the event.</td>
</tr>
<tr>
<td>Username</td>
<td>The username associated with the event.</td>
</tr>
</tbody>
</table>

Device Tagging

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

Once created, you can assign tags to a device manually or automatically, but not both. For information about manually assigning tags to devices, see "Assign a Tag" on the next page or "Change a Tag" on the previous page. For information about automatically assigning tags to devices, see "Add a Tag Rule" on page 74.
Add a Device Tag

You can manually add a tag to a device

1. Click Devices > Device Tags.
2. Click Add New Device Tag.
3. Type a name for the tag.
4. Click Add New Tag.

Assign a Tag

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

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

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

Tag Rules

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

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

Example: If a device is located in the Portland office and the user transfers to the Austin office, if you manually assigned tags, you will need to remove the Portland tag from the device and then assign the Austin tag. If you use tag rules to assign tags, when the user transfers to Austin, the tag rule for Portland will evaluate to false and automatically remove the Portland tag. When the tag rule for the Austin office evaluates to True, the Austin tag will be assigned to the device.
Tag rules are independent of each other and there are no priorities like those used in policy rule sets.

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

**Tag rules are deterministic**

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

- For automatic tagging to be useful, you want the tags to reflect a device's current state and not the device's past state. This means tags are both automatically assigned and removed from devices. In the example above, a device originally sat in the Portland office. When the user transferred to Austin, it would have both Portland and Austin tags assigned unless Portland was removed.

- If you can manually remove a tag that was assigned by a tag rule, it is no longer deterministic. For example, if you have 10 devices that should have the same tag assigned, but the tag could be manually removed from one device, you wouldn't have any way to know why the tag wasn't applied to that device and might wonder if there was an issue with the rule.

**Evaluating tag rules**

Tag rules are evaluated in the following scenarios:

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

**Add a Tag Rule**

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

1. Add a device tag. See "Add a Device Tag" on the previous page for more information.
2. Click Rules > Tag Rules.
3. Click Add New Tag Rule.
4. Enter a Tag Rule Name.
5. (Optional) Enter a rule description.
6. Select a tag for **Devices affected will receive the following tag**.

7. Create a rule condition.

Rule conditions contain three parts that are used to determine whether a tag rule will be applied: evaluation property, operator, and value. If the rule condition evaluates to *True*, the tag will be applied to a device.

   a. Click an evaluation property from the drop-down list beside **Device Name**.
   
   b. Click an operator from the drop-down list beside **Starts With**.
      
      See *"Tag Rule Operators" on the next page* 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, selecting Device Name will require entering some device name information; selecting Operating System will require selecting a target OS from a list.

8. To add another condition to the rule, click **Add "And" condition** or **Add "OR" condition block**, then enter the rule condition information.

9. Click **Add New Tag Rule**.

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

**Best Practice: Exclude a Device from a Tag Rule**

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

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

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

- Evaluation property = Device
- Operator = Is Not
- Value = Sal123East
Tag Rule Operators

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

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Uses the information provided to see if the device name matches the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Contains</strong>: The device name must contain the provided information, but it can be anywhere within the name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Contain</strong>: The device name must not contain the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not End With</strong>: The device name must not end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Start With</strong>: The device name must not start with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Ends With</strong>: The device name must end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Starts With</strong>: The device name must start with the provided information.</td>
</tr>
<tr>
<td></td>
<td>The Device Name field is case sensitive.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Uses the information provided to see if the selected device matches the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Is Not</strong>: The device name must not match the provided information.</td>
</tr>
<tr>
<td>Distinguished Name (LDAP)</td>
<td>Uses the information provided to see if the distinguished name matches the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Contains</strong>: The distinguished name must contain the provided information, but it can be anywhere within the name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Contain</strong>: The distinguished name must not contain the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not End With</strong>: The distinguished name must not end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Start With</strong>: The distinguished name must not start with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Ends With</strong>: The distinguished name must end with the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Starts With</strong>: The distinguished name must start with the provided information.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Uses the information provided to see if the domain name matches the condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Contains</strong>: The domain name must contain the provided information, but it can be anywhere within the name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not Contain</strong>: The domain name must not contain the provided information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Does Not End With</strong>: The domain name must not end with the provided information.</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Does Not Start With:</strong></td>
<td>The domain name must not start with the provided information.</td>
</tr>
<tr>
<td><strong>Ends With:</strong></td>
<td>The domain name must end with the provided information.</td>
</tr>
<tr>
<td><strong>Starts With:</strong></td>
<td>The domain name must start with the provided information.</td>
</tr>
<tr>
<td>IPv4 Address in Range</td>
<td>Provide an IPv4 address range. Any device with an IP address within the given range meets this condition.</td>
</tr>
<tr>
<td>Member of (LDAP)</td>
<td>Uses the information provided to see if the device’s group membership matches the condition.</td>
</tr>
<tr>
<td><strong>Contains:</strong></td>
<td>The Member Of must contain the provided information, but it can be anywhere within the member information.</td>
</tr>
<tr>
<td><strong>Does Not Contain:</strong></td>
<td>The Member Of must not contain the provided information.</td>
</tr>
<tr>
<td><strong>Is:</strong></td>
<td>The Member Of must match the provided information.</td>
</tr>
<tr>
<td><strong>Is Not:</strong></td>
<td>The Member Of must not match the provided information.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Uses the information provided to see if the device’s operating system matches the condition.</td>
</tr>
<tr>
<td><strong>Is:</strong></td>
<td>The device operating system must match the selected OS.</td>
</tr>
<tr>
<td><strong>Is Not:</strong></td>
<td>The device operating system must not match the selected OS.</td>
</tr>
</tbody>
</table>

**Edit a Tag Name**

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

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

**Remove a Tag from a Device**

You can use this feature to manually remove a tag. If a tag has been automatically assigned to a device using a Tag Rule, it cannot be manually removed from a device. Instead, you will need to modify the Tag rule so it will be unassigned.
1. Click Devices > Device Tags.
2. Click on a tag. A list of devices assigned to the tag displays.
3. Select the checkboxes for the devices for which you want to remove the tag.
4. Click Remove Tag From Device.

Remove a Tag from the CylanceON-PREM Console

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

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

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

**Actions on Threat Events**

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

1. Select **Events > Threat Events**. Or click the Threat Events widget on the Dashboard.

2. (Optional) Click **<number> Removed Threats** above the right side of the list to view the total number of threat events automatically removed by the Agent.

   If your policy has **Auto Delete Quarantine** enabled for a specified number of days in Threat Settings, files automatically quarantined by the Agent will be deleted after a specified number of days and will be removed from the Threat Events page. This button allows you to view all removed threats that were automatically deleted by the Agent since the beginning of time.

   **Note:** This button only displays if threat events were automatically removed by the Agent.

3. (Optional) If you clicked the **<number> Removed Threats** button in the previous step, click **<number> Threat Events** to return to the original view of threats.

4. Click the checkbox for one or more events and select an action:

   - **Globally Quarantine** – Click to add events to the Global Quarantine list and set the event status to Acknowledged. These events are automatically quarantined on all devices in your organization.

   - **Globally Safelist** – Click to add events to the Global Safelist and set the event status to Acknowledged. These events are allowed on all devices in your organization.

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

Tips:

- You can filter entries in this list to make finding information faster using the Filter icon (🔍). See "Filter Lists on page 28 for more information.
- To use entries in this list in other applications click ➔ See "Export Lists" on page 29 for more information.

### Threat Event Field Definitions

The following information displays in the Events List:

<table>
<thead>
<tr>
<th>File Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledged</td>
<td>Acknowledging an event means it has been reviewed.</td>
</tr>
<tr>
<td>Detected By</td>
<td>The name of the CylancePROTECT feature that detected the event.</td>
</tr>
<tr>
<td>Device Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>File Owner</td>
<td>The owner of the file that is considered to be a threat.</td>
</tr>
<tr>
<td>File Path</td>
<td>The path where the threat was found.</td>
</tr>
<tr>
<td>File Status</td>
<td>The status of the file on the device (Unsafe, Quarantined, Waived, or Abnormal).</td>
</tr>
<tr>
<td>Global List</td>
<td>Indicates whether an event has been added to the Global List (Quarantine or Safe) or blank if the event is new.</td>
</tr>
<tr>
<td>Hash</td>
<td>The SHA256 hash for the file.</td>
</tr>
<tr>
<td>Reported On</td>
<td>The date and time the event was first discovered in your organization.</td>
</tr>
<tr>
<td>Score</td>
<td>The Cylance Score for the event. The range is -1 to -1,000. See &quot;Cylance Score&quot; below for more information.</td>
</tr>
</tbody>
</table>

### Cylance Score

When viewing 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.

### Script Events

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

**Note**: This page aggregates the same event for all devices to help "keep the noise down". A separate Script Events page is available that provides more information on the Device List > select a device > Script Events widget. For more information, see "View Events" on page 72.

### Actions on Script Events

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

1. Select **Events > Script Events**. Or click the Script Events widget on the dashboard.
2. Click the checkbox for one or more events and select an action:
3. Click an action.
   - **Globally Safelist** – Adds events to the Global Safelist. These events are allowed on all devices in your organization.
   - **Acknowledge** – Click to change the event status from No to Acknowledged (Yes). Acknowledged means that a user has manually acknowledged an event by either clicking on this button or by manually adding the event to the Global Quarantine or Safe List. If you do not want to take any other action on an event (like adding it to the Quarantine or Safe List), and know the event isn't a threat, the Acknowledge button is an easy way to lower the threat in the list so you can focus on events that do require attention. By default, the events list displays events that have not been acknowledged first.

**Tips:**

- You can filter entries in this list to make finding information faster using the Filter icon (🔍). See "Filter Lists" on page 28 for more information.
To use entries in this list in other applications click ➡️ See “Export Lists” on page 29 for more information.

**Script Event Field Definitions**

The following information displays in the Events List:

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

**Memory Events**

Displays a list of memory-related events that are considered threats, that were found on devices in your organization.

**Actions on Memory Events**

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

1. Select **Events > Memory Events**. Or click the Memory Events widget on the dashboard.

2. Click the checkbox for one or more events and select an action:

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

**Tips:**

- You can filter entries in this list to make finding information faster using the Filter icon (🔍). See “Filter Lists” on page 28 for more information.

- To use entries in this list in other applications click ➡️ See “Export Lists” on page 29 for more information.

**Memory Event Field Definitions**

The following information displays in the Events List:

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

Displays a list of USB mass storage device events that occurred on devices in your organization.

Actions on Device Events

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

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

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

Tips:

- You can filter entries in this list to make finding information faster using the Filter icon ( ). See "Filter Lists" on page 28 for more information.
- To use entries in this list in other applications click See "Export Lists" on page 29 for more information.

Device Event Field Definitions

The following information displays in the Events List:

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

**Application Events**

Displays a list of application events that are considered threats, that were found on devices in your organization.

**Actions on Application Events**

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

1. Select **Events > Application Events**. Or click the Application Events widget on the dashboard.

2. Click the checkbox for one or more events and select an action:

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

**Tips:**

- You can filter entries in this list to make finding information faster using the Filter icon (🔍). See "Filter Lists" on page 28 for more information.

- To use entries in this list in other applications click ➔ See "Export Lists" on page 29 for more information.
## Application Event Field Definitions

The following information displays in the Events List:

<table>
<thead>
<tr>
<th>Application Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledged</td>
<td>Acknowledging an event means it has been reviewed.</td>
</tr>
<tr>
<td>Action</td>
<td>The action taken on the event.</td>
</tr>
<tr>
<td>Device Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>File Path</td>
<td>The path to the file that triggered the memory event.</td>
</tr>
<tr>
<td>Hash</td>
<td>The hash (SHA256) or other identifier for the application event.</td>
</tr>
<tr>
<td>Last Reported User</td>
<td>The last user that logged into the device.</td>
</tr>
<tr>
<td>Reported On</td>
<td>The date and time the event was first discovered in your organization.</td>
</tr>
<tr>
<td>Type</td>
<td>The exploit type.</td>
</tr>
</tbody>
</table>
Global Lists
The list of all events (file, script, memory, etc.) that are considered Safe or must be Quarantined on devices in your organization.

Tip: You can filter entries in this list to make finding information faster using the Filter icon (filter). See "Filter Lists" on page 28 for more information.

Add a Global List Entry

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

Import a Global List

You can import a Global List from CylancePROTECT or CylanceON-PREM so that you don't have to manually add hashes to the Global List.
Note: Importing a CylanceON-PREM Global List that was exported from CylanceON-PREM is available in CylanceON-PREM v1.7.1 or higher.

1. Click Global Lists. Or click the Global Lists widget on the dashboard.
2. Click the Import icon 🔄. The Import Global List window displays.
3. Select the type of list you are importing. Quarantine, Safe, or Script.
4. Browse for a .csv file or drag and one in the box.
5. Click Import. Once imported a dialog displays the results:
   - **Imported** - Number of entries that were imported.
   - **Skipped** - Number of entries were not imported because they already exist in the Global List.
   - **Conflicts** - 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.

Tip: To use entries in this list in other applications click ➡️ See "Export Lists" on page 29 for more information.

Global List Import File Format

The Global List import file is a CSV file that conforms to the same format as an exported Global List from the CylancePROTECT Console. This allows you to export an existing Global List and import it into CylanceON-PREM.

When creating an import file, include the following fields: Warning, Name, SHA256 Hash, Cylance Score, Classification, AV Industry, First Seen, Type, Added, Added By, Reason.

Remove a Global List Entry

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

Create a User

CylanceON-PREM has two pre-defined roles: Administrator and Read-Only. You can create custom roles and assign them to users. See "Role Management" on page 95 for more information.

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" on the next page for important information about setting passwords.
5. Select an Associated Role for the user.
6. Click Create. You must communicate the username and password to the appropriate user. It is highly recommended the user change the password the first time they log in.

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

Create a User with Identity Provider Settings Enabled

With CylanceON-PREM version 1.5.4.1 or higher, administrators can enable Identity Provider Settings for Single Sign-On access to the console. Read "Configure Identity Provider Settings" on page 118 for settings information.
1. Click **Access Management > User Management**. Or click the User Management widget on the Dashboard.

2. Click **Create User**.

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

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

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

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

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

### Password Requirements

Passwords in CylanceON-PREM have the following requirements:

- Passwords must be a minimum of 14 characters and include all of the following:
  - At least one upper-case letter (A through Z)
  - At least one lower-case letter (a through z)
  - At least one numeric (0 through 9)
At least one special character (e.g. ~!@#$%^&*()_+ = ' ] ? > < )

Passwords cannot contain personally identifiable information
- Passwords cannot be the same as the last 10 passwords
- Passwords expire after 180 days
- Users will be locked out for 5-minutes after three failed attempts to enter their password

**WARNING:** Administrators should generate a random password when changing or resetting a user's password. Do not use a generic password because the password may already be in the user's history (last 10 passwords) so it will be prohibited.

### Change a User Password

Administrators can change a user's password.

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

**WARNING:** Administrators should generate a random password when changing or resetting a user's password. Do not use a generic password because the password will already be in the user's history (saved for minimum of 10 generations) so it will be prohibited.

1. Click **Access Management > User Management**.
2. Click *** beside the user whose password you want to change.
3. Click **Change Password**.
4. Type and confirm the new password. See "[Password Requirements](#) on the previous page for important information about setting passwords.
5. Click **Update**.

### Edit a User

Administrators can edit a user's First Name, Last Name, and Email address.

1. Click **Access Management > User Management**.
2. Click 🆕 for the user you want to edit.
3. Update the user's information.
4. Click **Update**.
Deactivate a User

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

1. Click Access Management > User Management.
2. Click for the user you want to deactivate.
3. Click Deactivate.

Activate a Deactivated User

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

Delete a User

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

1. Click Access Management > User Management.
2. Click beside the user you want to delete.
3. Click Delete. A message displays prompting you to confirm the deletion.
4. Click Remove User.

Role Management

Roles allow or restrict access to your CylanceON-PREM console. CylanceON-PREM has two default roles: Administrator and Read Only. Administrators can create custom roles and assign these to users. Custom roles display as checkboxes below the default roles.

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

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

1. Click Access Management > Role Management.
2. Click Create Role.
3. Type in a name for the new role. The role name must be unique.
4. Select the permissions granted to the role. See "Role Permissions" below for more information.
   
   **Note:** If a role can create, update, or delete something, that role must also be able to view it.
5. Click Create.

Role Permissions

The following table describes the available permissions:

<table>
<thead>
<tr>
<th>Role Permission Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Applications allow access to the CylanceON-PREM API.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>View:</strong> Allows users to view the Application list. The user can view Application Settings and the Application ID, but cannot view the Application Secret.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Create:</strong> Allows users to add a new application.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Update:</strong> Allows users to edit and update an application.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Delete:</strong> Allows users to delete an application.</td>
</tr>
<tr>
<td>Audit Logs</td>
<td>Audit Logs record all user interactions with your CylanceON-PREM Console. This includes creating, updating, and deleting things.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>View:</strong> Allows user to view the Audit Logs page. The user can also download the Audit Logs as a CSV file.</td>
</tr>
<tr>
<td>Detection Events</td>
<td>Detection Events are threat events discovered on your devices.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>View:</strong> Allows user to view the Events page. This includes File Events, Script Events, Memory Events, Device Events, and Application Events.</td>
</tr>
<tr>
<td>Devices</td>
<td>Devices are your endpoints with Agents. Agents must be configured to communicate with your CylanceON-PREM Console.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>View:</strong> Allows user to view the Device List page.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Create:</strong> Allows users to add a new device using the installation token.</td>
</tr>
</tbody>
</table>

Note: This option must be selected if the user can create, update, or delete devices.
<table>
<thead>
<tr>
<th>Role Permission Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update:</strong> Allows users to edit and update device information.</td>
<td></td>
</tr>
<tr>
<td><strong>Delete:</strong> Allows users to delete devices from the CylanceON-PREM Console.</td>
<td></td>
</tr>
</tbody>
</table>

**Exclusions**

Exclusions define what is on the Safe List or the Quarantine list.

- **View:** Allows user to view the Safe/Quarantine page.
  
  **Note:** This option must be selected if the user can create, update, or delete exclusions.

- **Create:** Allows user to create a new Exclusion.

- **Update:** Allows user to edit existing Exclusions.

- **Delete:** Allows user to delete existing Exclusions.

**Installation Token**

Installation Tokens are a randomly generated string of characters that enables the Agent to report to its assigned account on the CylanceON-PREM Console.

**Note:** View System Settings must also be enabled for users to view the Installation Token.

- **Regenerate:** Allows user to generate a new installation token.
  
  **Note:** Regenerating the Installation Token should only be used to prevent installation of new Agents with the existing token. All Agents installed using the token prior to regenerating it will continue to communicate with the Console.

**Network Configuration**

Network Settings define the IP Address for the CylanceON-PREM appliance as well as other configuration options.

**Note:** View System Settings must also be enabled for users to view the Installation Token.

- **Update:** Allows user to edit the fields in Network Settings.

**Policies**

Policies define what the Agent will do with threats.

- **View:** Allows user to view the Policies page.
  
  **Note:** This option must be selected if the user can create, update, or delete policies.

- **Create:** Allows user to create new Policies.

- **Update:** Allows user to edit existing Policies.

- **Delete:** Allows user to delete existing Policies.

**Roles**

Roles define what a user can do in the CylanceON-PREM Console.

- **View:** Allows user to view the Role Management page.
  
  **Note:** This option must be selected if the user can create, update, or delete roles.
<table>
<thead>
<tr>
<th>Role Permission Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td></td>
</tr>
<tr>
<td>Permission Type</td>
<td>Description</td>
</tr>
<tr>
<td>Create</td>
<td>Allows user to create new Roles.</td>
</tr>
<tr>
<td>Update</td>
<td>Allows user to edit existing Roles.</td>
</tr>
<tr>
<td>Delete</td>
<td>Allows user to delete existing Roles.</td>
</tr>
<tr>
<td>Rules</td>
<td>Rules can automatically assign a policy to a device, based on the selected conditions (like Device Name, IPv4 Address, or Operating System).</td>
</tr>
<tr>
<td>View</td>
<td>Allows user to view the Rules page.</td>
</tr>
<tr>
<td>Create</td>
<td>Allows user to create a rule.</td>
</tr>
<tr>
<td>Update</td>
<td>Allows user to edit existing rules.</td>
</tr>
<tr>
<td>Delete</td>
<td>Allows user to delete rules.</td>
</tr>
<tr>
<td>SSL Certificates</td>
<td>CylanceON-PREM requires a certificate to ensure secure communication between the server and the endpoints.</td>
</tr>
<tr>
<td>View</td>
<td>Allows user to view the Certificates page.</td>
</tr>
<tr>
<td>Install</td>
<td>Allows user to add a certificate.</td>
</tr>
<tr>
<td>Update</td>
<td>Allows user to update a certificate.</td>
</tr>
<tr>
<td>Delete</td>
<td>Allows a user to delete a certificate.</td>
</tr>
<tr>
<td>System Logging</td>
<td>System Logging Settings sets the level of information captured in the log file.</td>
</tr>
<tr>
<td>Settings</td>
<td>Note: View System Settings must also be enabled for users to view System Logging Settings.</td>
</tr>
<tr>
<td>Update</td>
<td>Allows user to change the logging level for the CylanceON-PREM virtual appliance.</td>
</tr>
<tr>
<td>System Logs</td>
<td>System Logs are the log files for the CylanceON-PREM virtual appliance. System logs can help when troubleshooting issues with the virtual appliance.</td>
</tr>
<tr>
<td>Note:</td>
<td>View System Settings must also be enabled for users to view System Version.</td>
</tr>
<tr>
<td>Downloads</td>
<td>Allows user to download System Logs.</td>
</tr>
<tr>
<td>System Settings</td>
<td>System Settings displays the Installation Token (used when installing the Agent) and System Settings (version, hostname, IP address, log level, and console language).</td>
</tr>
<tr>
<td>View</td>
<td>Allows user to view the System Settings page.</td>
</tr>
<tr>
<td>System Version</td>
<td>System Version provides a way to update the CylanceON-PREM virtual appliance.</td>
</tr>
<tr>
<td>Note:</td>
<td>View System Settings must also be enabled for users to view System Version.</td>
</tr>
<tr>
<td>Update</td>
<td>Allows user to update the CylanceON-PREM virtual appliance.</td>
</tr>
<tr>
<td>Tags</td>
<td>Device Tags allow you to group your devices based on your criteria.</td>
</tr>
<tr>
<td>Role Permission Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| View: Allows user to view the Device Tagging page.  
  **Note:** This option must be selected if the user can create, update, or delete tags.  
| Create: Allows user to create a Device Tag.  
| Update: Allows user to update a Device Tag.  
| Delete: Allows user to delete a Device Tag.  |

Users

Users have access to the CylanceON-PREM Console. Use Roles to grant or restrict access to the CylanceON-PREM Console.

- **View:** Allows user to view the User Management page.  
  **Note:** This option must be selected if the user can create, update, or delete users.
- **Create:** Allows user to create a User.  
- **Update:** Allows user to update a User.  
- **Delete:** Allows user to delete a User.

### Edit a Role

1. Click **Access Management > Role Management**.
2. Click the edit icon for the role you want to edit.
3. Make changes to the role.
   - **Note:** If a role can create, update, or delete something, that role must also be able to view it.
4. Click **Update**.

### Delete a Role

1. Click **Access Management > Role Management**.
2. Click the delete icon for the role you want to delete.
3. Click **OK** to confirm the action.

**Note:** If a role is assigned to one or more users, that role cannot be deleted. Reassign these users to another role, then delete the role.
My Account

The My Account page displays your profile information, lets you update your information, and change your password.

Update Profile Information

1. Click on your account name (upper-right corner).
2. Select My Account.
3. Under Update Information, change your profile information. You can change your First Name and Last Name only.
4. Click Update.

Change Your Password

1. Click on your account name (upper-right corner).
2. Select My Account.
3. Under Change Password, type in your old password, then type in and confirm your new password. See "Create a User" on page 92 for more information.
4. Click Update.

Audit Logs

The Audit Logs contain information pertaining to the following actions performed from the CylanceON-PREM Console.

- Agent Update (Edit)
- Device (Edit, Delete)
- Global List (Create, Delete)
- Login (Success, Failure)
- Logout (Success, Failure)
- Policy (Create, Edit, Delete)
- Policy Rule (Create, Edit, Delete, Auto Policy Applied) The Audit Log will have one entry per device when a rule is automatically applied because condition(s) 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 condition(s) were met.
- Threat (Quarantine, Waive, Global Quarantine, Safe List)
- User (Create, Edit, Delete, Assigned)
- Virtual Appliance Update (Enable or Disable Maintenance Mode)

Tips:
- You can filter entries in this list to make finding information faster using the Filter icon (🔍). See "Filter Lists on page 28" for more information.
- To use entries in this list in other applications click ➡️ See "Export Lists on page 29" for more information.

Certificates

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

- Syslog/SIEM
- LDAP
- External database

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

Notes:
- You cannot manage the CylanceON-PREM SSL certificate from this page. See "Update the CylanceON-PREM SSL Certificate" on page 107 for more information.
- The certificate is only needed if TLS/SSL is enabled.

Add a Certificate

To Add a Certificate

1. Select Configuration > Certificates.
2. Select an option:
   - To add a certificate, click Add Certificate.
     a. Type in the name for this certificate, such as postgres.crt.
     b. Drag the certificate to the Install certificate box or click Browse for a
file and select the certificate.

c. Click **Install Certificate**. The certificate should display on the page.

- To remove a certificate, click the Remove icon (🗑).
- To change or update a certificate, click the Edit icon (📝), then install the new certificate.
## Configuration

### Settings

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

<table>
<thead>
<tr>
<th>CylanceON-PREM Info</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Token</td>
<td>Displays the installation token used when installing the CylancePROTECT Agent. This is unique for each virtual appliance. See &quot;Regenerate an Installation Token&quot; on page 105 for more information.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the version for CylanceON-PREM. See &quot;Upgrade CylanceON-PREM&quot; on page 105 for more information.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Displays the fully qualified domain name (FQDN) for the virtual appliance. See &quot;Reboot the Virtual Appliance&quot; on page 106 for more information.</td>
</tr>
<tr>
<td>Console Language</td>
<td>Displays the language selected when the virtual appliance was initially configured.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Sets 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.</td>
</tr>
<tr>
<td>Certificate Expiration</td>
<td>Displays the date and time the CylanceON-PREM SSL certificate expires. See &quot;Update the CylanceON-PREM SSL Certificate&quot; on page 107 for more information.</td>
</tr>
<tr>
<td>Certificate Ciphers</td>
<td>Displays whether the certificate is running using strict mode of TLS 1.1 or higher (default) or the legacy TLS 1.0 mode. See &quot;Change the Certificate Cipher Mode&quot; on page 109 for more information.</td>
</tr>
<tr>
<td>Certificate Signing Request</td>
<td>Displays 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.</td>
</tr>
<tr>
<td>Maintenance Mode</td>
<td>Description</td>
</tr>
<tr>
<td>Maintenance Mode</td>
<td>Displays the status of Maintenance Mode. When enabled, this pauses activity between CylanceON-PREM and CylancePROTECT devices to allow making changes to the virtual appliance without interruption.</td>
</tr>
<tr>
<td>Network Settings</td>
<td>Description</td>
</tr>
<tr>
<td>IP Assignment</td>
<td>Displays how the IP address is assigned to the virtual appliance, whether it is DHCP or Static.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Displays the IP address for the virtual appliance.</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Displays the subnet mask.</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>Displays 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.</td>
</tr>
<tr>
<td><strong>DNS Servers</strong></td>
<td>Displays the IP addresses for the DNS servers with which CylanceON-PREM is communicating.</td>
</tr>
<tr>
<td><strong>Check an IP Address</strong></td>
<td>Allows you to ping an IP address to test the connection between CylanceON-PREM and the endpoint.</td>
</tr>
<tr>
<td><strong>Debug Logs</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| **Log Level** | Displays the log level for the virtual appliance.  
  **Note:** Debug logging can consume a high amount of disk space. Debug logging should only be used when troubleshooting server issues. Otherwise, the level should be set to Information (INFO). |
| **On or After** | Displays the start date to include when downloading the log files for the virtual appliance. |
| **Database Connection Settings** | **Description** |
| **Database Connection Settings** | Displays the connection information for the external database if it is configured. |
| **Syslog/SIEM** | **Description** |
| **Syslog/SIEM** | Displays the status of messaging being forwarded to a Syslog server. See "Configure Syslog/SIEM Settings" on page 112 for more information. |
| **LDAP** | **Description** |
| **LDAP** | Displays the status of LDAP/Active Directory integration. See "Configure Active Directory" on page 116 for more information. |
| **Identity Provider Settings** | **Description** |
| **Identity Provider Settings** | Displays the external identity provider (IdP) settings. See "Configure Identity Provider Settings" on page 118 for more information. |
Regenerate an Installation Token

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

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

Upgrade CylanceON-PREM

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

Note: It is recommended to enable Maintenance Mode and take a snapshot of the virtual appliance before upgrading.

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

1. Obtain the latest CylanceON-PREM file.
2. Log in to your CylanceON-PREM Console.
3. Click Configuration > Settings.
4. Click Maintenance Mode. This pauses site activity, including communication between the virtual appliance and the Agents, to ensure you can take a complete VM snapshot.

![Settings](image)

*Figure 5: Enable Maintenance Mode*

5. Take a snapshot of the CylanceON-PREM virtual appliance.
6. Under CylanceON-PREM Info, click Upgrade.
7. Select the I have taken a VM snapshot checkbox, then click Proceed with Upgrading.
8. Click Browse for a file, select the CylanceON-PREM file you want to use for this update, then click Open. You could drag and drop the file to select it.
9. Click **Start Upgrade**. During the upgrade, there are two things to look for: the update is in progress message and a successful update notification.

**Note:** 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.

![Upgrade CylanceON-PREM](image)

*Figure 6: Update in Progress (version 1.1.0)*

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

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

**Reboot the Virtual Appliance**

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

1. Log in to your CylanceON-PREM Console.
2. Click **Configuration > Settings**.
3. 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.
4. 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. On the **Configuration > Settings** page, click the edit icon for Session Timeout.
2. Use the slider to adjust the amount of time.
3. Click **Apply**.

Update the CylanceON-PREM SSL Certificate

Update CylanceON-PREM SSL Certificate Version 1.2.2.1 and Earlier

To update the CylanceON-PREM SSL certificate, go through the configuration process again, using the updated SSL certificate and key.

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

**Update CylanceON-PREM SSL Certificate Version 1.3.1 and Higher**

1. Log in to your CylanceON-PREM Console.
2. Click Configuration > Settings.

4. 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.

5. 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. Skip the remaining steps below and continue to Step 7.

6. 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.

7. Click **Save**.

**Change the Certificate Cipher Mode**

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

**To Change the Mode**

1. 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.

```
Change Certificate Ciphers

You’re about to enable less secure legacy SSL ciphers.
We do not advise enabling legacy ciphers unless required.
Legacy ciphers are provided for older unsupported operating systems.
Do you still wish to enable legacy SSL ciphers?

Do Not Enable  Yes, Enable Anyway
```

3. Select whether to enable the change. If you enable Legacy mode, a message displays informing you that you will need to close the current browser window and open a new one to see your change.

4. If you want to change back to Strict Mode, click **Change** beside **Certificate Ciphers** again. You will be prompted to close the current browser window and open a new one to update the settings.

**Enable Maintenance Mode**

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

Disabling Maintenance Mode requires you to confirm the action.
Change Network Settings

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

1. 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 the Edit icon. A warning message displays, reminding you to take a snapshot of your virtual appliance. You must acknowledge the message before you can continue.

4. Click I have taken a VM snapshot, then click Proceed to Edit Network Settings.

5. Change the network settings. For DHCP, the network settings are provided by your
DHCP server. For Static IP Addresses:

- Type in the IP address, Subnet Mask, Default Gateway, and DNS Servers.

6. Click the Save icon (checkmark).

7. Click **Maintenance Mode** and confirm disabling it. Site activity resumes.

### Check an IP Address

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

1. Click **Configuration > Settings**.

2. Under Network Settings, type the IP address in the **Enter a Custom IP Address** field.

3. Click **Ping**. Able to reach address(es) message appears with a successful ping.

![Enter a Custom IP Address](image)

### Change the Log Level

1. Click **Configuration > Settings**.

2. Under Debug Logs, click the Log Level edit icon.

3. Select a logging level from the list.

4. Click the checkmark icon to save your changes.

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

### Download Logs

1. Click **Configuration > Settings**.

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

![Debug Logs](image)

**Configure Syslog/SIEM Settings**

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

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

1. Click **Configuration > Settings**.

2. Click the Syslog/SIEM edit icon. This expands the Syslog settings.

![Syslog / SIEM](image)

3. Click the Syslog/SIEM toggle to enable the feature. Use this toggle to enable or disable the feature without losing any settings.

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

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

**IMPORTANT:** UDP does not support notifications when the Syslog server shuts
5. Click the Save icon.

6. To upload an SSL certificate, go to the "Certificates" on page 101 page (Configuration > Certificates), and add the certificate.

Notes:

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

- To remove a Syslog server shut down notification, re-enable Syslog. If you no longer want to use Syslog, re-enable Syslog and then disable Syslog.

Syslog Message Failures

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

**Update Database Connection Settings**

Allows users to change the external database information. This section does not display when using the database shipped with CylanceON-PREM.

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

1. Click **Configuration > Settings**.
2. Click the Database Connection Settings edit icon.
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.

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

5. Click the Save icon.

6. To upload the external database certificate for SSL connection, go to the "Certificates" on page 101 page (Configuration > Certificates), and add the certificate.

**Configure Active Directory**

If the Lightweight Directory Access Protocol (LDAP) Server is configured, CylanceON-PREM user logins are authenticated and authorized using the corporate LDAP server, including Microsoft’s Active Directory.

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

1. Add the SSL certificate for the LDAP Server. See "Certificates" on page 101 for more information.

2. Click **Configuration > Settings**.

3. Click the LDAP edit icon. This expands the LDAP configuration settings.

4. Under LDAP, enable the LDAP toggle.
5. Enter your LDAP/Active Directory information:

   - **Base Distinguished Name**: The base distinguished name (DN) used as a base for the LDAP search to look for the user DN.

   - **Group Distinguished Name**: 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**: Modify the FQDN to the LDAP server’s fully qualified domain name (FQDN).

     The FQDN must be configured on the Domain Server.

   - **Port**: The port number of the LDAP server.

   - **TLS/SSL**: To ensure 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 on the Save icon (✓) in the top right of the section.

### Configure Identity Provider Settings

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

1. Click **Configuration > Settings**.
2. Click the edit icon for Identity Provider Settings.
4. Enter the IdP information.
   - **Single Sign-On**: The single sign-on or SAML response URL. This is provided by the identity provider.
   - **Entity ID**: The entity ID, issuer, or application name. This is provided by the identity provider.
   - **x.509 Certificate**: This is provided by the identity provider.
5. Click the save icon.
6. CylanceON-PREM will generate a **Service Provider Entity ID** that the identity provider will need to complete the single sign-on configuration.
Add a Banner to the Login Screen

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

1. Click Configuration > Settings.
2. Click the Edit icon for Login Screen Banner.
3. Under Login Screen Banner, 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 the Save icon. The Banner will display similar to the following example:
Applications

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

**Note:** If necessary, administrators can regenerate the Application Secret and provide API users with the new information.

Add an Application

**IMPORTANT:** CylanceON-PREM can have up to 10 custom applications.

1. Click **Configuration > Applications**.
2. Select an option:
   - To add an application:
     a. Click **Add Application**. The Add Application dialog displays.
     b. Type the name of 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.
     c. Set permissions for the application, then click **Save Application**.
     d. You will need to copy the Application ID and Application Secret to use when generating an Access Token. To copy this information at a later time, you can click the down arrow to the right of the application name on the Applications page to display and copy it.
     e. Click **OK, got it** to close the dialog.
   - To edit an application, click the Edit icon (edit), then update the application name or permissions.
   - To remove an application, click the Remove icon (trash).
   - 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)" on page 130** for more information.
### Add Application

<table>
<thead>
<tr>
<th></th>
<th>Enter Application Info</th>
<th>Configure Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>None</td>
<td>Read</td>
</tr>
<tr>
<td>Policies</td>
<td><img src="on" alt="Checkbox" /></td>
<td><img src="off" alt="Checkbox" /></td>
</tr>
<tr>
<td>Exclusions</td>
<td><img src="off" alt="Checkbox" /></td>
<td><img src="off" alt="Checkbox" /></td>
</tr>
<tr>
<td>Devices</td>
<td><img src="off" alt="Checkbox" /></td>
<td><img src="off" alt="Checkbox" /></td>
</tr>
<tr>
<td>Tags</td>
<td><img src="off" alt="Checkbox" /></td>
<td><img src="off" alt="Checkbox" /></td>
</tr>
<tr>
<td>Events</td>
<td><img src="off" alt="Checkbox" /></td>
<td><img src="off" alt="Checkbox" /></td>
</tr>
<tr>
<td>Rules</td>
<td><img src="off" alt="Checkbox" /></td>
<td><img src="off" alt="Checkbox" /></td>
</tr>
</tbody>
</table>

**Buttons**

- Go Back
- Cancel
- Save Application
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" on page 121 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)" on page 130 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" on page 132 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.

To Add an Application

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

1. Log in to the CylanceON-PREM Console as an administrator. Only administrators can create a custom application.
2. Select Configuration > Applications.
3. Click **Add Application**.

4. 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.

![Add Application](image)

*Figure 8: Add an Application Name*

5. Select which console features and the permission level accessible by the Application.
6. Click **Save Application**. A success message displays, including the Application ID and Application Secret. To view the Application Secret, click the eye icon.
Access Token

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

**Note:** Before generating an Access Token you will need to add an application in the CylanceON-PREM Console (**Configuration > Applications**) and copy the ApplicationID and ApplicationSecret. See "Applications" on page 121 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.

**IMPORTANT:** The following requirements and script are just an example. Things 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/](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
    ```

**IMPORTANT:** You will need to use the access token to execute the API requests.
**Example Script**

The following example code can be used to get an Access Token using Python.

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

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

# Make a POST request to get the application token.
token_headers = {
    "Content-Type": "application/json",
    "Accept": "application/json",
}
token_request_body = {
    "clientId": appID,
    "clientSecret": appSecret,
    "scope": "*"
}
token_url = f"{onprem_base_url}/cyapi/v1/application/token"
token_result = requests.post(token_url, json=token_request_body, headers=token_headers, verify=False)
token_url_json_results = token_result.json()
print("Got result from token request:")
print(token_url_json_results)
```

**Token Lifecycle**

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

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

**IMPORTANT:** 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.

   ![Figure 11: Edit Hostname in YAML File](image)

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 displays in the Swagger Editor.

![Swagger Editor](image)

**Figure 12: CylanceON-PREM API Documentation in Swagger**

6. To view the API documentation click on 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:
Figure 13: Example Generated Curl Command and Request URL

**IMPORTANT:** 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:

```
```
However, for this command to work, you must include the Access Token::


Note: Replace {{access-token}} with the Access Token you generated using your Application ID and Application Secret. See "Access Token" on page 127.

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:


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" on page 127.

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.

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 - OK</td>
<td>A successful call and operation. The response payload will be JSON, structured according to the nature of the request.</td>
</tr>
<tr>
<td>400 - Bad Request</td>
<td>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.</td>
</tr>
<tr>
<td>401 - Unauthorized</td>
<td>Invalid credentials were passed or some other failure in authentication.</td>
</tr>
<tr>
<td>Status Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>403 - Forbidden</td>
<td>Request has been successfully authenticated, but authorization to access the requested resource was not granted.</td>
</tr>
<tr>
<td>404 - Not Found</td>
<td>A request was made for a resource that doesn't exist. Common causes are either an improperly formed URL or an invalid API key.</td>
</tr>
<tr>
<td>409 - Conflict</td>
<td>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.</td>
</tr>
<tr>
<td>500 - Internal Server Error</td>
<td>A catch-all code response for any unhandled error that has occurred on the server. Contact Cylance Support for help with this issue.</td>
</tr>
<tr>
<td>501 - Not Implemented</td>
<td>A request was made against a resource with an operation that has yet to be implemented. Such operations should be identified accordingly in documentation.</td>
</tr>
<tr>
<td>Other</td>
<td>Contact Cylance Support if you encounter any status codes that are not on this list.</td>
</tr>
</tbody>
</table>
This section provides a list of questions to answer and files to collect when troubleshooting issues with CylanceON-PREM. This information will enable Cylance Support to assist in resolving any issues.

**Agent Not Communicating with CylanceON-PREM**

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

**Web Browser Reports Insecure Webpage**

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

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

**Unable to Connect to External Database**

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

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

![Figure 14: Error message for Dashboard and Devices pages when external database is not available](image)

*CylanceON-PREM Administrator Guide, 1.7.2 rev2, July 2020 | 136*
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 --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.

Before Contacting Support

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

Enable Verbose Logging

1. Log in to your CylanceON-PREM Console.
2. Select System.
3. For Log Level, click the Edit icon (pencil).

4. Select **Debug**.

5. Click the Save icon (checkmark).

![System Settings](image)

*Figure 17: Set Log Level to Debug*

**Download Logs**

1. Log in to your CylanceON-PREM Console.

2. Select **System**.

3. For Download Logs, select a date for **On or After**.

4. Click **Download**, then click **OK** to save the file.

![Debug Logs](image)

*Figure 18: Download Log File*

5. Create a Cylance Support ticket and include the CylanceON-PREM log file.
   
   a. Go to [support.cylance.com](https://support.cylance.com).
   
   b. Click **Get Help Now**, under Submit a Case.
   
   c. Submit your case.
Legal Notice
Legal Notice

©2020 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, WARRANTIES, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, WARRANTIES, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE,
OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

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

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

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED 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