BlackBerry Protect

Multi-Tenant Console

1.0

Contents

Overview

BlackBerry Protect products detect and block malware before it can affect a computer. Protect uses a mathematical approach to malware identification, using machine learning techniques instead of reactive signatures, trust-based systems, or sandboxes. Protect's approach renders new malware, viruses, bots, and future variants useless. Protect analyzes potential file executions for malware in the operating system (OS) and memory layers to prevent the delivery of malicious payloads. Optics collects a diverse set of disparate information, then aggregates that information into a localized data store to track, alert upon, and respond to, complex malicious situations.

Managed security service providers (MSSPs) are partners who promote BlackBerry products to their customers. These partners provide various services to their clients, including tenant creation, onboarding, managing, reporting, and support.

The BlackBerry Multi-Tenant Console allows partners to manage and service their customers who use the Protect product. The Multi-Tenant Console allows partners a way to create tenants and view all the tenants they are servicing in a centralized location. This guide provides information about the console features and includes tasks showing how to use the console.

Browser support

- Google Chrome (latest version)
- Mozilla Firefox (latest version)
- Microsoft Edge (latest version)
- Microsoft Internet Explorer version 10 or higher (with latest updates)

Multi-Tenant Console login

If your organization is new to the BlackBerry Multi-Tenant Console, an email invitation will be sent to one email address in your organization. The email invitation contains a link to create a login password. Once this user logs in to the Multi-Tenant Console, they can create Multi-Tenant Console users for your organization.

If your Multi-Tenant Console administrator has created a Multi-Tenant Console account for you, you will receive an email invitation that contains a link to create a password for your account.

After your account is created and you create your password, you can go to https://admin.cylance.com and log in. Your username is your work email address. Select your region from the drop-down list.

Note:

- For single sign-on, see Use SSO for Multi-Tenant Console login.
- You will be logged out of the Multi-Tenant Console after one hour of inactivity.

Single sign-on

The BlackBerry Multi-Tenant Console supports single sign-on (SSO) user authentication with any identity provider (IDP) using SAML 2.0.

Multi-Tenant Console information needed for IDP

Use the following information when you create a new application with your IDP.

- **Entity ID / Issuer / Application Name**: Cylance Multi-Tenant Console
- **Sign-On / SAML Response URL**: https://admin.cylance.com/us/api/auth/external-auth/consume-saml/<partnerid>

Note:

- The entity ID name could differ, depending on the IDP.
- Replace <partnerid> with your partner ID for the Multi-Tenant Console.

Information for configuring an ADFS trust

Use the following information when configuring a relying party trust.

- **Relying Party Identifier**: Cylance Multi-Tenant Console
- **SAML Assertion Consumer Endpoint**: https://admin.cylance.com/us/api/auth/external-auth/consume-saml/<partnerid>

Replace <partnerid> with your partner ID for the Multi-Tenant Console.

IDP information needed for Multi-Tenant Console

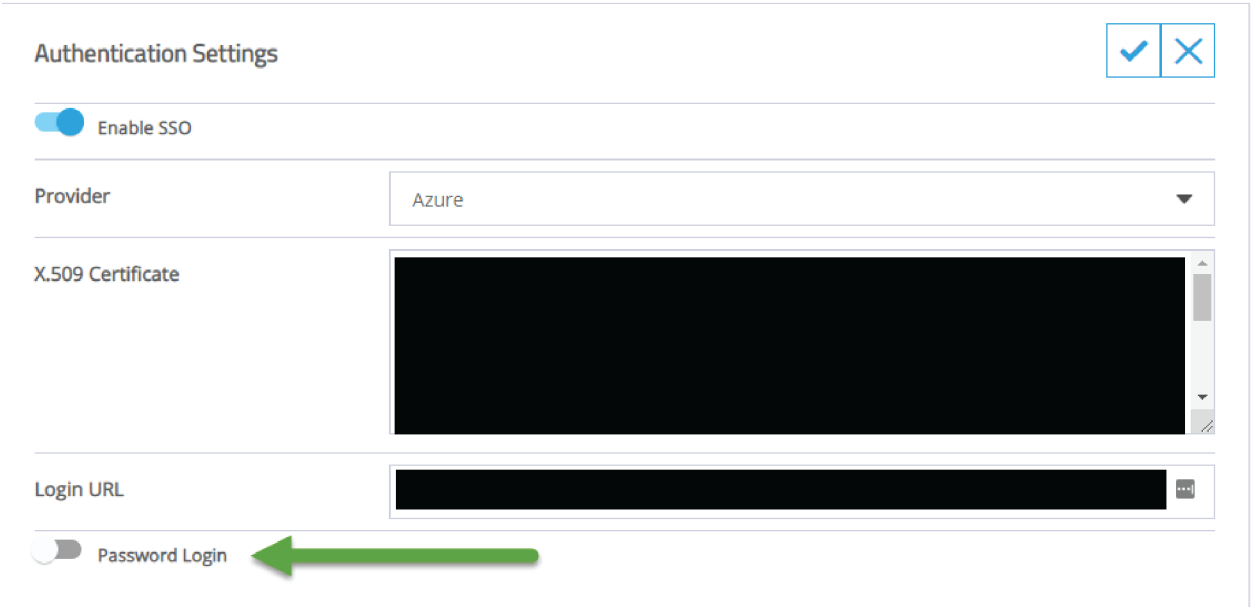
When configuring an IDP (using SAML 2.0) in the Multi-Tenant Console, you will need:

- X.509 certificate
- Login URL for the IDP

Disable password login

With single sign-on (SSO) enabled, you might need to disable the option to login to the console using an email and password. An organization may need their users to only log in using an external identity provider for security reasons.

1. Log in to the Multi-Tenant Console.
2. Hover-over the My Profile icon, then select **Account Overview**.
3. Click the edit icon for authentication settings.
4. Make sure **Password Login** is disabled, then click the save icon (green checkmark).



Configure SAML using Okta

The following is an example for configuring the Cylance Multi-Tenant Console in an IDP application. This example uses Okta.

Note: The IDP must support SAML 2.0.

1. In Okta, go to the **Applications** page.
2. Click **Create New App**.
3. Select **Web** for platform, select **SAML 2.0** for sign on method, then click **Create**.
4. Enter an **App name**, add an **App logo**, then click **Next**.
5. For SAML settings:
   - **Single sign on URL**: https://admin.cylance.com/us/api/auth/external-auth/consume-saml/<partnerid>

     Note: Replace <partnerid> with the tenant ID for your Cylance Multi-Tenant Console
   - **Audience URI**: Use your tenant ID
   - Click **Advanced Settings**
   - **SAML Issuer ID**: Enter Cylance Multi-Tenant Console
6. Complete the new application and assign to users and groups.
7. For the new Okta application, go to the **General** tab.
8. Copy the **App Embed Link**. Use this link for the login URL for authentication settings in the Multi-Tenant Console.

Configure SAML for Cylance Multi-Tenant Console

After you configure your IDP for the Cylance Multi-Tenant Console, go to the Multi-Tenant Console to complete the single sign-on configuration.

1. In the Multi-Tenant Console, select **My Profile > Account Overview**.
2. For authentication settings, click the edit icon.
3. Click the **Enable SSO** toggle to enable the feature.
4. Select a provider from the **Provider** list. If your IDP is not listed, select **Custom**.
5. Paste your X.509 certificate information into the X.509 certificate field. This includes the **-----BEGIN CERTIFICATE-----**, **-----END CERTIFICATE-----** and the certificate string in between.
6. Paste the login URL, provided by the IDP, into the login URL field.
7. Click the **Save** icon.

Use SSO for Multi-Tenant Console login

After you configure the Multi-Tenant Console to use your IDP authentication, users complete the following steps to log in.

1. Go to https://admin.cylance.com/#/auth/external-login.

   If users go to https://admin.cylance.com/#/auth/login, they can click **Sign in with your external account**.
2. Enter an email address.
3. Select the region from the which the user is logging in.
4. Click **Sign In**.

   Users are redirected to the IDP authentication page. If users are already authenticated with the IDP, the tenants page displays.
5. Enter the username and password for the IDP login, then click **Sign In**.

Account information

The account information menu is accessed by clicking on the user icon in the upper-right corner of the Multi-Tenant Console.

View my profile

The profile page contains information about the partner account you belong to, your role, and your email address. From the profile page, you can also update your password.

1. Select the **My Profile** icon, then select **My Account**.
2. To change your password:
   a) Type in your current password.
   b) Type in your new password. Your new password must be at least eight characters long.
   c) Click **Update Password**.

View audit log

The audit log lists all user activity for your Multi-Tenant Console. This includes successful log in, modifying information, or adding information.

1. Select the **My Profile** icon (upper-right).
2. Select **Audit Log**.

View account overview

The account overview page provides information about your multi-tenant account, billing information, and a list of partner users who can access your Multi-Tenant Console information. You can also download your product usage .csv files, which lists the number of Protect and Optics devices by tenant. The number of devices is the high watermark, meaning the highest number of devices using a product within the billing cycle

Download a .csv file

1. Select the **My Profile** icon, then select **Account Overview**.
2. Select **Product Usage**.
3. Click **Download CSV** for the billing cycle details you want to view.

Partner users

Multi-Tenant Console administrators can create other Multi-Tenant Console users (referred to as partner users). A partner user can be assigned to one tenant, or multiple tenants, which allows users to manage them. Administrators can also assign a role to a user, which sets the level of access granted (like read-only).

Create a partner administrator or user

When a new Multi-Tenant Console user is created, an invitation is sent to the user's email address. The invitation includes a link that allows the user to create their own password for their Multi-Tenant Console account.

Note: Multi-Tenant Console login credentials do not work on the Cylance console.

1. In the Multi-Tenant Console, click **Partner Users**.
2. On the users page, click **Add Partner User**.
3. Type in the partner user's information. The email address must be unique for the Multi-Tenant Console.
4. Select a role for the partner user.
5. Click **Save & Finish**.

User Type	Description
Partner administrator	The Multi-Tenant Console partner administrator can create and manage tenants, create tenant users, and create and manage Multi-Tenant Console users.
Partner read-only	The Multi-Tenant Console partner read-only user has read-only access to the tenants assigned to the user. The read-only user cannot make any changes to any of the tenants.

Edit a partner user

1. In the Multi-Tenant Console, click **Partner Users**.
2. On the users page, click the edit icon for the user you want to edit.
3. Edit the user information, then click **Save & Finish**.

Reset a partner user password

Partner users can reset their password.

Note: Protect users must go to the Cylance console to reset their password.

1. In the Multi-Tenant Console, click **Forgot password?** The forgot password page displays.
2. Type in the email address related to your account.
3. click **Send Reset Link**. You should receive an email with a link to reset your password.

Delete a partner user

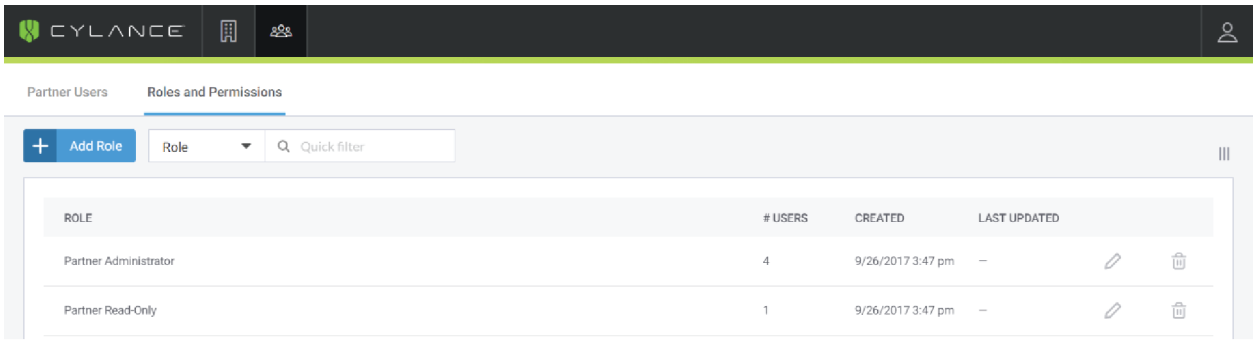
1. In the Multi-Tenant Console, click **Partner Users**.
2. Click the delete icon for the user you want to delete. A confirmation message displays.
3. Click **Confirm**.

Customize partner roles

The Multi-Tenant Console allows administrators to create new user roles using custom permission sets. This provides customized access to the Multi-Tenant Console features.

Create a partner role

1. In the Multi-Tenant Console, click **Partner Users**, then click **Roles and Permissions**.



2. Click **Add Role**.
3. Type in a role name.
4. Select permissions for the role.
5. Click **Save New Role**.

Edit a partner role

1. In the Multi-Tenant Console, click **Partner Users**, then click **Roles and Permissions**.
2. Click the edit icon for the role you want to edit.
3. Modify the permissions or role information.
4. Click **Save & Finish**.

Delete a partner role

1. In the Multi-Tenant Console, click **Partner Users**, then click **Roles and Permissions**.
2. Click the delete icon for the role you want to delete.
3. Click **Confirm**.

Permissions for user roles

Permission	Description
Tenant	These are permissions related to the tenant the Multi-Tenant Console that the user is assigned to.
Shutdown tenants	This permission grants the ability to shutdown a tenant.
Ghost-login as tenant user	This setting allows users to log in with the user's account as if you were a tenant user, even if the user is assigned a different user role. The console will log the Multi-Tenant partner's email address logging in as the user.
Ghost-login as tenant admin	This setting allows users to log in with the user's account as if you were a tenant administrator, even if the user is assigned a different user role. The console will log the Multi-Tenant partner's email address logging in as the user.
Ghost-login as tenant zone manager	This setting allows users to log in with the user's account as if you were a tenant zone manager, even if the user is assigned a different user role. The console will log the Multi-Tenant partner's email address logging in as the user.
View tenant list	View a list of tenants in the Multi-Tenant Console.
Read tenant details	Read the tenant details - tenant info, purchase info, licensing, and evaluation EULA.
Add or modify tenant details	Create or modify tenants in the Multi-Tenant Console.
Ghost-login as tenant read only	Log in with the user's account as if you were a tenant read only user, even if the user is assigned a different user role. The console will log the Multi-Tenant partner's email address logging in as the user.
Policy template	These are permissions related to the policy template in the Multi-Tenant Console.
Read policy template details	Read the policy template details, including the policy settings.
View policy template list	View a list of policy templates in the Multi-Tenant Console.
Add or modify policy template information	Create or modify policy templates in the Multi-Tenant Console.
Delete policy templates	Delete policy templates in the Multi-Tenant Console.
Report	These are permissions related to the Multi-Tenant Console reports
Read report details and report lists	Read the Multi-Tenant Console reports.
Add or modify report information	Create or modify reports in the Multi-Tenant Console.

Permission	Description
Delete report	Delete a report from the Multi-Tenant Console.
User	These are permissions related to the users related to the tenant.
View user list	View a list of users in the Multi-Tenant Console.
Read user details	Read the user details - email address, role, and last login.
Add or modify user information	Create or modify users in the Multi-Tenant Console.
Delete users	Delete users from the Multi-Tenant Console.
Role	These are permissions related to the roles in the Multi-Tenant Console.
View role list	View list of roles in the Multi-Tenant Console.
Read role details	Read the role details - role, number of users, created, and last updated.
Add or modify role information	Create or modify roles in the Multi-Tenant Console.
Delete roles	Delete roles from the Multi-Tenant Console.

Tenant management

In the Multi-Tenant Console, a tenant represents a customer's organization. Each tenant isolates its devices from other tenants. After creating a tenant, administrators can create tenant users and assign them to a tenant.

Tenants page

As a Multi-Tenant Console administrator or user, you can view a list of tenants created for your customers. Clicking on a tenant name displays the tenant details page.

About automated license conversion

For tenants with an evaluation license, 60 days after the tenant creation date, the tenant will automatically be converted to a customer license. Fourteen days before the automated conversion, an icon will appear next to the tenant name to indicate the pending license conversion.

Tenants page columns

You can display or hide various tenant related information, like product license count and usage. Click the columns icon to see a list of available columns, then display or hide columns.

Create a tenant

1. In the Multi-Tenant Console, click **Tenants**, then click **Add New tenant**.
2. In the tenant name field, enter the name for the tenant.
3. In the unique admin email field, enter the email address for the tenant administrator (user). This field is optional.
4. In the tenant address fields, enter the tenant's address information.
5. Select any optional tenant features for the user. These features are disabled by default and hidden from the user. See Tenant field information for more information about the tenant features.
6. In the product license count fields, enter the number of licenses granted for each product. The Protect license count is required. The Optics license count is optional.
7. Click **Save & Finish**.

   Note: Adding Optics licenses does not enable Optics for that tenant. The **Optics v2** , **Optics ML**, and **Optics Refract Packages** features must be enabled under tenant features.

Tenant field information

Tenant info

Field	Description
Tenant name	This is the name of the tenant. Must be unique to your Multi-Tenant Console. **Note:** It is recommended to use the following naming convention: *MSSP PartnerName ClientName*
Unique administrative address (UAE)	This is the primary email account for this tenant. **Note:** The email address must be unique to the Protect product.
Tenant address	This is the street address, suite (or floor or building), city, state, and zip code for the tenant.

Tenant features

Field	Description
API V2	With the Cylance API, users can programmatically manage their tenant, like devices, policies and users.
Data privacy	Console administrators can select the data types the agent will not upload to the console. For example, username, IP address, or hostname. **Note:** Enabling data privacy will affect the data displayed in the console. For example, enabling file path in data privacy disables displaying the file path for threats found. This will make it more difficult to resolve issues.
Device control	Console administrators can protect endpoints by controlling USB mass storage devices connecting to endpoints in their organization.
Linux	Users can download the Protect Linux agent from the application page in the console. **Note:** The Linux agent consists of two files, the agent and the UI. The UI is optional.
Notification for quarantine events	Users can receive email notifications for new quarantined threat events. Users can enable this email notification on the my account page.
Optics V2	Users can access Optics in the console and can download the Optics agent.
Optics ML	Users have access to the Optics machine learning feature. **Note:** Optics V2 must be enabled.

Field	Description
Optics refract packages	Users have access to the Optics refract packages in the console. **Note:** Optics V2 must be enabled.
Read only user role	Console administrators can create users with the read-only role. Read-only users have permission to view the Cylance console, but they cannot take any actions or change any settings. For example, someone conducting a compliance review.
Script control global safelist by hash	Console administrators can add script hashes to the global safe list on the global list page.
Ubuntu	Users can download the Protect Ubuntu agent from the application page in the console. **Note:** The Ubuntu agent consists of two files, the agent and the UI. The UI is optional.

Licensing details

Field	Description
Protect license count	The total number of endpoints the Protect product was purchased to protect.
Optics license count	The total number of endpoints for which the Optics product was purchased.
License type	This allows you to set the tenant to evaluation or production. Use evaluations for users trying out the product and use production for users who have purchased the product.

Note: After 60 days, the evaluation license is automatically converted to production. This applies to tenants with 10,000 endpoints or less. Two-weeks before the automatic conversion, an icon will appear next to the evaluation tenant name on the tenants page.

Pending approval

If a tenant has less than 10,000 endpoints, it is approved automatically. For tenants with more than 10,000 endpoints, Cylance's approval is required. Tenants requiring approval will appear on the pending approval list until they are approved.

Edit a tenant

Partner administrators can edit the information for a tenant, including the purchase info and licensing.

1. In the Multi-Tenant Console, click **Tenants**, then click the tenant name you want to edit. The tenant details page displays.
2. To edit the tenant info:
   a) Click the edit icon.
   b) Update the tenant information.
   c) Click the save icon.
3. To edit the purchase info and licensing information:
   a) Click the edit icon.
   b) Update the licensing information.
   c) Click the save icon.

Edit a tenant field information

Field	Description
Tenant name	The name of the tenant. Must be unique to your Multi-Tenant Console
Email	Shows the email address of the tenant administrator selected
Address	The user's address, including the city, state, and zip code
Created date	Displays the date the tenant was created
License type	Displays the license, which could be evaluation or customer
Protect license usage	Allows you to enter the total number of devices for which the user has paid, and the number of licenses used and view license usage
Optics license usage	Allows you to enter the total number of devices for which the user has paid, and the number of licenses used and view license usage
Term	Displays how often the user must renew their Cylance product license. **Note:** This field is not editable. Tenants can have an annual term, but this must be set by Cylance and requires pre-payment. Contact Cylance for more information.
Evaluation EULA	For evaluation tenants, there is a version of the end-user license agreement (EULA) that the first user to log in to the customer's tenant must accept. The date the EULA was accepted, and which user's email accepted, are listed. This information cannot be edited.
Customer EULA	For customer tenants, there is a version of the end-user license agreement (EULA) that the first user to log in to the customer's tenant must accept. The date the EULA was accepted, and which user's email accepted, are listed. This information cannot be edited.

Shut down a tenant

Shutting down a tenant removes user access to the console and all agents will no longer communicate with the console. Agents will display a message stating an installation token is required to connect to the console. Shutting down a tenant is not immediate. A 7-day grace period is initiated to allow time for the tenant user to renew their subscription. After the 7-day grace period, the tenant user logins are blocked, and the agents are unregistered.

To cancel a shut down, log in to the Multi-Tenant Console, go to the pending list, then click cancel for the tenant you want to cancel the shutdown for.

Note: There is no way to recover tenant data after a tenant has been deleted.

Managing tenants

As a Multi-Tenant Console administrator or user, you can view the policies, zones, devices, agent versions, and users for the tenants you manage. This allows you to help your customers manage their organization and troubleshoot some issues.

Tenant details	Tenant details include the tenant name, email address, and license information. The tenant details can be edited.
Policies	Polices allow users to apply different Cylance security settings to different devices. One policy could have memory protection enabled, while a different policy can have this feature disabled. The Multi-Tenant Console lists the policies the user created for their tenant.
Zones	Zones allow users to group their devices. One device can be associated with multiple zones.
Devices	A device is a system that has Protect installed.
Tenant users	A list of Cylance console usernames for the user's tenant.
Threats	Partner administrators can help their tenant users manage threats in the user's console. Partner administrators can add threats to the global quarantine or the global safelist for a tenant.

Add a threat to a global list

Adding a threat to the global quarantine list will quarantine the file on all devices in the tenant.

Note: This example shows how to globally quarantine a threat. To globally safelist, follow the same steps, just select globally safelist instead of globally quarantine.

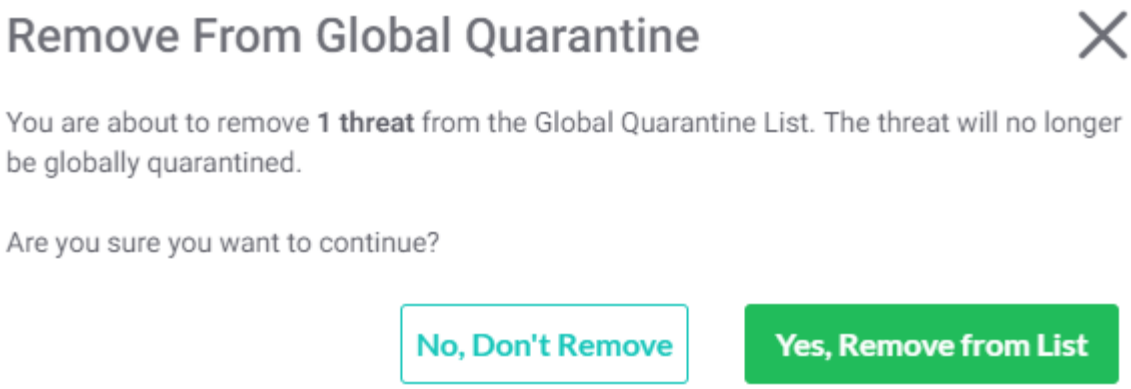
1. In the Multi-Tenant Console, on the tenants page, click the name of the tenant.
2. Click **Threats**. A list of threats in the threat displays.
3. Select the threats you want to add to the global quarantine list. Click the checkbox to select a threat.
4. Click **Globally Quarantine**.
5. Select the tenants to add the threat to their global quarantine list.
6. Click **Next**

7. Type a reason for adding this to the global quarantine list.
8. Click **Next**
9. Confirm the action, then click **Globally Quarantine**.

Remove an item from a global list

Removing a file from a global list moves the file to the threats list.

1. In the Multi-Tenant Console, click **Tenants**, then click the tenant name.
2. Click **Global Lists**, then select **Global Quarantine List** or **Global Safelist**.
3. Select the file to remove from the list. You can select multiple files.
4. Click **Remove Selected**. A message appears, asking you to confirm the action.
5. Click **Yes, Remove from List**



Add or remove tenant users

Multi-Tenant Console administrators can add tenant users. A tenant user can log in to the Cylance console. When a tenant user is added, they will receive an invitation email to create their account password.

Note: Only tenant administrators can be created from the Multi-Tenant Console.

Add a tenant user

1. In the Multi-Tenant Console, click **Tenants**, then click the tenant name.
2. Click **Tenant Users**.
3. Click **Add Tenant User**.
4. Type in the first name, last name, and email address for the tenant user.
5. Click **Save & Finish**.

Edit a tenant user

1. In the Multi-Tenant Console, click **Tenants**, then click the tenant name.
2. Click **Tenant Users**.

3. Click the edit icon (pencil) in the same row as the user's name.
4. Edit the user's information.
5. Click **Save & Finish**.

Delete a tenant user

1. In the Multi-Tenant Console, click **Tenants**, then click the tenant name.
2. Click **Tenant Users**.
3. Click the delete icon (trashcan) in the same row as the user's name you want to delete.
4. Click **Confirm**.

Use support login

Allows Multi-Tenant Console administrators to log in to the Cylance console as if they were the user. The Multi-Tenant Console administrator can view settings and make changes on behalf of the user, making troubleshooting some issues more effective. Multi-Tenant Console administrators can access policy settings, device details, global lsits, and zones. The Cylance console audit log will show the Multi-Tenant Console administrator's email address logging in as the user. This is also known as "ghost-login."

Note: If the user disables "Enable Support Login" (Settings > Application in the Cylance console), then this feature is disabled for that tenant.

Support login for tenant

1. In the Multi-Tenant Console, click **Tenants**, then click the support login icon for that tenant.
2. Click **Login**. A new tab opens and displays the Cylance console.
3. On the Multi-Tenant Console tab, click **Cancel** to close the support login message.

Support login as a user

1. In the Multi-Tenant Console, click **Tenants**, then click the tenant name. The tenant details page displays.
2. Click **Users**.
3. Find the user you want to log in as, then click the support login icon for that user. A message displays the URL to use.
4. Click **Login**. A new tab opens and displays the Cylance console. On the Multi-Tenant Console tab, click **Cancel** to close the support login message.

Note: The user's audit log will display that the Multi-Tenant Console administrator logged in as a user.

Policy management

A policy defines how the Protect agent handles malware it encounters - automatically quarantine, ignore if in a specified folder, watch for new files, etc. Every device must be in a policy. If no policy is assigned, the device is placed in the default policy.

Applying a policy to a device takes effect as soon as the agent receives the new or updated policy (the policy must be saved, and the policy must be assigned to the device). Policy changes do not require the device to reboot for the update to take effect.

A policy can be applied to multiple devices, but a device can only have one policy. The last policy assigned to a device (whether manually or automatically) is the one used.

Policy template

The policy template management gives partners the ability to configure and customize policy settings, apply them to new and existing tenants, and manage device policy assignments for all tenants directly from the Multi-Tenant Console. This functionality can drastically speed up the customer onboarding, product enablement, and implementation process for partners and their customers.

Create a policy template

Multi-Tenant Console administrators can create policy templates and apply those templates to their customers' tenants to help them protect their endpoints.

1. In the Multi-Tenant Console, click **Settings**, then click **Add New Template**.
2. Type a name for the template. The template name must be unique within your console.
3. Select the policy settings to enable. For a list of policy settings and descriptions, see Policy settings.
4. Click **Save & Finish**.

Apply a policy template to a tenant

Policy templates allow administrators to create a set of standardized templates containing policy settings, designed for types of endpoints typically found in a customer's environment. Administrators can then apply any of those templates to any of their customers' tenants. After a policy template has been created, it can then be applied to one or more tenants. This adds a policy to the selected tenants, with the same settings as the policy template. This can be done on the settings page or within a tenant's details page.

Apply policies from the policy templates page

1. In the Multi-Tenant Console, click **Settings**, then click **Policy Templates**.
2. Select the checkbox next to the policy name you want to assign. You can select multiple policies to assign to a tenant.
3. Click **Apply Template**. The apply Policy Template To Tenant window displays.
4. Select one tenant, multiple tenants, or all tenants that you want to apply the selected policies to.

Note: If duplicate policy names are detected, then a (#) will be automatically appended to the name of the new policy. **Example**: Test Policy (2).

5. Click **Apply**.

Apply policies from the tenant details page

1. In the Multi-Tenant Console, click a tenant name.
2. Click **Policies**, then click **Apply a Policy Template**. The Apply A Policy Template window displays.
3. Select one or more policy templates to assign to the tenant. Use the filter field to filter policy templates by a keyword.
4. Click **Apply**. The policy template is added to the customer's tenant.

Assign a policy to a device

After a policy template has been assigned to a customer's tenant, Multi-Tenant Console administrators can apply a policy to a customer's device.

Note: A policy can be applied to multiple devices, but a device can only have one policy. The last policy assigned to a device (whether manually or automatically) is the one used.

1. Log in to the Multi-Tenant Console.
2. Click on the tenant name.
3. Click **Device**
4. Select the checkbox for the device (or devices) for which you want to assign a policy.
5. Click **Assign Policy**
6. Select the policy to apply from the policy list.
7. Click **Assign Policy**.

Audit logging for policy template

Policy template actions are recorded in the Multi-Tenant Console audit log (Profile > Audit Log). This includes the user who performed the action and the timestamp.

Policy template role permissions

Allows Multi-Tenant Console administrators to grant Multi-Tenant Console users access to the policy template (Settings > Policy Templates). Enabling a policy template permission does not automatically enable any dependencies. For example: enabling read policy template details requires also enabling view policy template list.

See Customize partner roles for more information.

Things to know about policy templates

When using policy templates, consider the following:

- There is no automated synchronization between the policy template and the tenant policies.
- Assigning a policy template with the same name as an existing policy within the tenant results in the policy template name being appended with a number. Example: Test Policy (2).
- Changes to a specific policy can be made at the tenant-level and will have no impact to the policy template in the Multi-Tenant Console.

Multi-tenant reports

The custom reports functionality allows partners to customize reports based on data across their tenants that is output as a .csv file. The report types include an audit log report, account data report, tenant details report, and a partner user report.

Create a report

1. In the Multi-Tenant Console, click **Reports**, then click **Create Report**.
2. Enter a name for the report.
3. Select a report type.
   - Audit Log: Logs actions performed in the Multi-Tenant Console.
   - Account Data: Details about a tenant.
   - Partner User: Details about partner users and roles.
   - Tenant Details: Report that includes tenant information.
4. Select **Report Fields**. See descriptions in the tables below.
5. Select **Report Filters**. See descriptions in the tables below.
6. Enable **Schedule Report** to run at a specified time.
   - One-Time: Schedule the report to run one-time on a specified date. See Schedule report for more information.
   - Recurring: Schedule the report to run at a selected time, like daily, weekly, monthly, or annual. See Schedule report for more information.
7. Save the report.
   - Save and Run Report: Saves and runs the report, including running on a schedule.
   - Save & Finish: Saves the report but does not run it.

After you finish: View Recently Run Reports. All recently generated reports can be viewed and re-downloaded from the recently run tab, under reports.

Audit log report

The audit report includes actions performed in the Multi-Tenant Console, including adding, modifying, and deleting tenants.

Report fields

Field	Description
Action	The action performed in the console. This can include: adding a user, successful login, or deleting a role
Category	The category in the console affected by the action. This can include: device, tenant, partner, and partner user

Field	Description
Details	The details about the action, including tenant name, tenant features, policy name, and source IP address (on login)
User	The name of the user who performed the action
When	The date and time the action was performed

Report filters

Add filters to include or exclude data when generating a report. Report filters are related to the report fields available for a report type. See Report filters.

Account data report

The account data report includes details about a tenant, including license count, license usage, and EULA acceptance.

Field	Description
Address	The address for the tenant account
Address 2	Additional address information for the tenant account
City	The city for the tenant account
Country	The country for the tenant account
Created	The date and time the tenant account was created
Created by	The name of the partner user who created the tenant account
Customer EULA accepted by	The name of the tenant user who accepted the customer EULA
Customer EULA accepted date	The date and time the customer EULA was accepted
Customer EULA start date	The date the customer EULA was assigned to the tenant account
Customer EULA version	The customer EULA version used when the tenant account was created
Evaluation EULA accepted by	The name of the tenant user who accepted the evaluation EULA
Evaluation EULA accepted date	The date and time the evaluation EULA was accepted
Evaluation EULA start date	The date the evaluation EULA was assigned to the tenant account
Evaluation EULA version	The evaluation EULA version used when the tenant account was created
Installation token	The installation token for the tenant account

Field	Description
License type	The license type for the tenant account
Modified	The date and time the tenant account was last modified
Modified by	The name of the partner user who last modified the tenant account
Optics license count	The number of Optics licenses purchased for the tenant account
Optics license usage	The number of Optics licenses currently used by the tenant account
Protect license count	The number of Protect licenses purchased for the tenant account
Protect license usage	The number of Protect licenses currently used by the tenant account
State	The state for the tenant account
Tenant name	The name of the tenant account
Term	The frequency at which the tenant account fees are charged
Zip/Postal code	The zip code or postal code for the tenant account

Report filters

Add filters to include or exclude data when generating a report. Report filters are related to the report fields available for a report type. See Report filters.

Partner user report

The partner user report includes details about partner users and roles, including last login, date created, and email address.

Field	Description
Date partner created	The date and time the partner user account was created
Date role created	The date and time the partner role was created
Date role last updated	The date and time the partner role was last updated
Email	The email address for the partner user
First name	The first name of the partner user
Last login	The date and time the last time the partner user logged in to the console
Last name	The last name of the partner user

Field	Description
Role name	The name of the partner role

Report filters

Add filters to include or exclude data when generating a report. Report filters are related to the report fields available for a report type. See Report filters.

Policy details report

The Multi-Tenant Console policy details report allows administrators to see all of the settings for a policy, including the name, each setting, each value selected for a setting, and a short description of each setting.

Field	Description
Key	The policy setting
Policy name	The name of the policy
Section	The section of the policy the setting belongs to
Tenant name	The name of the tenant
Value	The value selected for the policy setting (example: disabled)

Report filters

Add filters to include or exclude data when generating a report. Report filters are related to the report fields available for a report type. See Report filters.

Tenant user report

The Multi-Tenant Console tenant user report includes user information and roles across all tenants.

Create a tenant user report

1. In the Multi-Tenant Console, click **Reports**.
2. Click **Create Report**.
3. Enter a report name, then select **Tenant User** for the report type.
4. Select the report fields you want for the report.
5. Add any report filters.
6. Click **Save And Run Report** or click **Save & Finish**. If you click Save & Finish, you must select the report, then click Save And Run Report to view any results.

View a tenant user report

1. In the Multi-Tenant Console, click **Reports**.
2. Click **Recently Run**.
3. Click on the report name to download the report.

Report fields

Field	Description
Tenant name	The name of the tenant (selected by default when tenant details is selected)
Tenant first name	The first name of the user
Tenant last name	The last name of the user
Tenant user email	The email address of the user
Date added	The date and time the user's account was created
Tenant user role	The role assigned to the user
Tenant user last login	The date and time when the user last logged in to the Multi-Tenant Console

Report filters

Field	Description
Tenant name	The name of the tenant (selected by default when tenant details is selected)
Tenant first name	The first name of the user
Tenant last name	The last name of the user
Tenant user email	The email address of the user
Date added	The date and time the user's account was created
Tenant user role	The role assigned to the user
Tenant user last login	The date and time when the user last logged in to the Multi-Tenant Console

Tenant details report

The Multi-Tenant Console tenant details report includes tenant information, including global list, devices, and policies.

Report Fields

Field	Description
Tenant name	The name of the tenant (selected by default when tenant details is selected)
Global list	
Added on	The date and time the file was added to the global list
Category	The global list the file belongs to, either global quarantine or global safe
Global list file name	The name of the file on the global list
Global list SHA256 hash	The SHA256 hash for the file on the global list
List type	The file type, like executable
Reason	The reason for adding the file to the global list that is provided by the user who added the file to the global list
Tenant devices	
Device agent version	The Protect agent version installed on the device
Device date added	The date and time the agent first communicated with the Cylance console
Device name	The name of the device
Device policy	The name of the policy assigned to the device
Device state	The current state of the device, either online or offline
Tenant policy	
Policy date created	The date and time the policy was created
Policy date modified	The date and time the policy was last modified
Policy device count	The number of devices the policy is assigned to
Policy name	The name of the policy
Policy zone count	The number of zones the policy is assigned to
Tenant threat	
Classification	The type of threat, including potentially unwanted programs (PUPs), dual use, and malware

Field	Description
Cylance score	The score assigned to a file that is a potential threat • Abnormal: A file with a score ranging from 1-59 that might pose a threat to devices. • Unsafe: A file with a score ranging from 60-100 that can be used to negatively impact devices.
Globally quarantined	The file will be quarantined throughout the organization
Last found	The date and time the threat was last found in the organization
Sub-classification	The sub-classification provides more detail about the type of threat, including adware, ransomware, and viruses
Threat file name	The name of the threat
Threat SHA256 hash	The SHA256 hash of the threat
Threat zone	
Zone date added	The date and time the zone was added
Zone date modified	The date and time the zone was last modified
Zone name	The name of the zone

Report filters

Add filters to include or exclude data when generating a report. Report filters are related to the report fields available for a report type. See Report filters.

Threat classifications

Below is a list of possible file status entries that may appear under the classification for each threat, along with a brief description of each entry.

File unavailable

Due to an upload constraint (example: file is too large to upload) the file is unavailable for analysis.

UNKNOWN (blank entry)

The file has not been analyzed by Cylance's analysis team yet. Once the file is analyzed, the classification will be updated with a new status.

Trusted - local

The file has been analyzed by the Cylance research team and has been deemed safe (not malicious, not a PUP). A file identified as trusted - local can be globally safelisted so that the file will be allowed to execute and

not generate any additional alerts if found on other devices within your organization. The reason for the local designation is due to the fact that the file did not come from a trusted source (such as Microsoft or other trusted installer) and therefore cannot be added to our trusted cloud repository.

PUP

The file has been identified as a potentially unwanted program. This indicates that the program may be unwanted, despite the possibility that users consented to download it. Some PUPs may be permitted to run on a limited set of systems in your organization (example: a VNC application allowed to run on domain admin devices). A Cylance console Admin can choose to waive or block PUPs on a per device basis or globally quarantine or safelist based on company policies. Depending on how much analysis can be performed against a PUP, further sub-classification may be possible. Those subclasses are shown below and will aid an administrator in determining whether a particular PUP should be blocked or allowed to run.

Subclass	Definition	Examples
Adware	These are technologies that provide annoying advertisements (for example: pop-ups) or provide bundled third-party add-ons when installing an application. This usually occurs without adequate notification to the user about the nature or presence of the add-on, control over installation, control over use, or the ability to fully uninstall the add-on.	Gator, Adware Info
Corrupt	This is any executable that is malformed and unable to run.	
Game	These are technologies that create an interactive environment with which a player can play.	Steam Games, League of Legends
Generic	This is any PUP that does not fit into an existing category.	
Hacking tool	These are technologies that are designed to assist hacking attempts.	Cobalt Strike, MetaSpl0it
Portable application	This is a program designed to run on a computer independently, without needing installation.	Turbo
Scripting tool	This is any script that is able to run as if it were an executable.	AutoIT, py2exe
Toolbar	These are technologies that place additional buttons or input boxes on-screen within a UI.	Nasdaq Toolbar, Bring Me Sports

Subclass	Definition	Examples
Other	This is a category for things that don't fit anything else, but are still PUPs. There a lot of different PUPs, most of which aren't malicious but several that should still be brought to the attention of the system administrators through our product. Usually because they have potentially negative uses or negatively impact a system or network.	

Dual use

Dual use indicates the file can be used for malicious and non-malicious purposes. Caution should be used when allowing the use of these files in your organization. For example, while PsExec can be a useful tool for executing processes on another system, that same benefit can be used to execute malicious files on another system.

Subclass	Definition	Examples
Crack	These are technologies that can alter (or crack) another application in order to bypass licensing limitations or digital rights management protection (DRM).	
Generic	This is any dual use tool that does not fit into an existing category.	
KeyGen	These are technologies which can generate or recover/reveal product keys that can be used to bypass digital rights management (DRM) or licensing protection of software and other digital media.	
Monitoring tool	These are technologies that track a user's online activities without awareness of the user by logging and possibly transmitting logs of one or more of the following: • user keystrokes • email messages • chat and instant messaging • web browsing activity • screenshot captures • application usage	Veriato 360, Refog Keylogger

Subclass	Definition	Examples
Pass crack	These are technologies that can reveal a password or other sensitive user credentials either by cryptographically reversing passwords or by revealing stored passwords.	l0phtcrack, Cain & Abel
RemoteAccess	These are technologies that can access another system remotely and administer commands on the remote system, or monitor user activities without user notification or consent.	Putty, PsExec, TeamViewer
Tool	These are programs that offer administrative features but can be used to facilitate attacks or intrusions.	Nmap, Nessus, P0f

Malware

The Cylance research team analyze files to determine if any are malicious. When the team has definitively identified a file as a piece of malware, the file should be removed or quarantined as soon as possible. Verified malware can be further subclassified as one of the following.

Subclass	Definition	Examples
Backdoor	This is malware that provides unauthorized access to a system, bypassing security measures.	Back Orifice, Eleanor
Bot	This is malware that connects to a central command and control (C&C) botnet server.	QBot, Koobface
Downloader	This is malware that downloads data to the host system.	Staged-Downloader
Dropper	This is malware that installs other malware on a system.	
Exploit	This is malware that attacks a specific vulnerability on the system.	
FakeAlert	This is malware that masquerades as legitimate security software to trick the user into fixing fake security problems at a price.	Fake AV White Paper
Generic	This is any malware that does not fit into an existing category.	

Subclass	Definition	Examples
InfoStealer	This is malware that records login credentials and/or other sensitive information.	Snifula
Parasitic	Parasitic viruses, also known as file viruses, spread by attaching themselves to programs. Typically when you start a program infected with a parasitic virus, the virus code is run. To hide itself, the virus then passes control back to the original program.	
Ransom	This is malware that restricts access to system or files and demands payment for removal of restriction, thereby holding the system for ransom.	CryptoLocker, CryptoWall
Remnant	This is any file that has malware remnants post removal attempts.	
Rootkit	This is malware that enables access to a computer while shielding itself or other files to avoid detection and/or removal by administrators or security technologies.	TDL, Zero Access Rootkit
Trojan	This is malware that disguises itself as a legitimate program or file.	Zeus
Virus	This is malware that propagates by inserting or appending itself to other files.	Sality, Virut
Worm	This is malware that propagates by copying itself to another device.	Code Red, Stuxnet

Report filters

Report filter - enter filter text

Filter	Description
Contains	The data in the selected field must contain the contents of the filter. **Example:** If **ello** is the filter, then hello and mellow are included in the report, but hi and help are excluded.
Does not contain	The data in the selected field must not contain the contents of the filter. **Example:** If **ello** is the filter, then hi and help are included in the report, but hello and mellow are excluded.

Filter	Description
Ends with	The data in the selected field must end with the contents of the filter. **Example:** If **ing** is the filter, then helping and closing are included in the report, but help and closed are excluded.
In	The filter provides a list and allows selecting specific content to include in the report, like usernames, actions, or categories. **Note:** Only some filters provide this option.
Is equal	The data in the selected field must match the contents of the filter.
Is not equal	The data in the selected field must not match the contents of the filter.
None	No filter is applied.
Starts with	The data in the selected field must start with the contents of the filter. **Example:** If **hi** is the filter, then high and hill are included in the report, but help and hello are excluded.

Report filter - counts and dates

Filter	Description
Greater than	For counts (or filters that use an integer), the data with a number greater than the number provided is included in the report. For dates, the data that is newer than the selected date is included in the report.
Greater than or equal	For counts (or filters that use an integer), the data with a number greater than or equal to the number provided is included in the report. For dates, the data that is newer than or equal to the selected date is included in the report.
Is equal	For counts (or filters that use an integer), the data with a number that is equal to the number provided is included in the report. For dates, the data that has the same date as the selected date is included in the report.
Is not equal	For counts (or filters that use an integer), the data with a number that is not equal to the number provided is included in the report. For dates, the data that has a date that is not the same as the selected date is included in the report.
Less than	For counts (or filters that use an integer), the data with a number less than the number provided is included in the report. For dates, the data that is older than the selected date is included in the report.

Filter	Description
Less than or equal	For counts (or filters that use an integer), the data with a number less than or equal to the number provided is included in the report. For dates, the data that is older than or equal to the selected date is included in the report.
None	No filter is applied.

Note: To do a date range, add one filter that uses the greater than statement and the beginning date and another filter that uses the less than statement and the end date. This will filter out all dates before and after the desired range.

Schedule report

You can schedule a report to be run once or on a recurring basis.

Schedule one-time

1. Enable **Schedule Report**.
2. Select **One-Time**, under frequency.
3. Select a date, under run on. Clicking in the date field displays a calendar in a pop-up window. Only the current date and future dates are selectable.
4. Click **Save Changes**.

Schedule recurring

1. Enable **Schedule Reports**.
2. Select **Recurring**, under frequency.
3. Select how often to run the report.
   - **Annual**: Select a month and day to run the report.
   - **Daily**: The recurring report runs every day.
   - **Monthly**: Select a day of the month to run the report.
   - **Weekly**: Select a day of the week to run the report.
4. Select a date for **Starts After**. The recurring report will start after the selected date.
5. Select an end date for the recurring report.
   - **Never**: There is no end date for the recurring report.
   - **On**: Select a date for the recurring report to end.
6. Click **Save Changes**.

Multi-tenant console API

The Multi-Tenant Console API allows administrators to generate an API token, get policy templates, and administer tenants.

Link to the API: https://api-admin.cylance.com/public

Using the API

The following example shows how to generate an API token using Postman.

Create a partner application

1. In the Multi-Tenant Console, select **Settings**, then select **Application**.
2. Click **Add New Application**.
3. Enter a name and privileges.
4. Click **Submit**.
5. Copy application ID (Guid) and application secret (hash) to a text file.

Note: If you lose the application secret, you will have to regenerate a new one. This cannot be retrieved from the Multi-Tenant Console.

6. Click **OK**.

Generate a bearer token

1. Import the example JSON into Postman. The example JSON is available on the API page.
2. Select the `base_URL>:region/auth` endpoint.
   - **<base_URL>** is `https://api-admin.cylance.com/public`
   - **region** is the Multi-Tenant Console region you sign into.
   - Full URL for the US login region would be: `https://api-admin.cylance.com/public/us/auth`.
3. Click on the **Authorization** tab.
4. Select **Basic Auth** from the type drop down.
5. Enter your application ID as username and your application Secret as password.
6. Click on the **Body** tab.
7. Verify that the x-www-form-urlencded option is selected.
8. Verify that the value of grant_type is client_credentials.
9. Verify that the value of scope is api.
10. Click **Send**.

The API should respond with a 200 response code and string return like the following:

```
{
"access_token": string,
"expires_in": int,
"token_type": string
}
```

Making your first call to check

1. Select the `base_URL>:region/health-check` endpoint.
   - **<base_URL>** is `https://api-admin.cylance.com/public`.
   - **region** is the Multi-Tenant Console region you sign into.
   - Full URL for the US login region would be: `https://api-admin.cylance.com/public/us/health-check`.
2. Click on the **Authorization** tab.
3. Select **Bearer Token** from the type drop down.
4. Paste the **access_token** you generated previously.
5. Click **Send**.
6. The API should respond with a 200 response code and string return like the following:

```
{
"Version": x.x.x.x | Environment: 'Production'
}
```

API example for Postman - JSON file

On the API document page, there is a JSON file that contains examples of the Multi-Tenant Console API that can be imported into Postman. For people who use other API software, they can use the API document page and copy the API requests from there.

Link to the API: https://api-admin.cylance.com/public

Policy settings

Policy settings control what the agent does on the device. The following lists out policy settings and provides a description for each one.

File actions

Setting	Description
Auto-delete quarantine	Delete quarantined files after the designated time, from 14 days to 365 days.
Auto quarantine abnormal files	Quarantine abnormal files to prevent them from executing.
Auto quarantine unsafe files	Quarantine unsafe files to prevent them from executing.
Auto upload	Files that have never been analyzed by Cylance are uploaded for further analysis.
Background threat detection	Perform a full disk scan to detect and analyze any dormant threats on the disk. Settings include run once and run recurring. Run recurring performs the scan every 9 days. Also known as: BTD.
Copy file samples	Specify a network share that file samples can be copied to. This allows users to do their own analysis of files the agent considers unsafe or abnormal.
File watcher	Detect and analyze any new or modified files for dormant threats. Also known as: Watch for new files.
Scan archives	Set the maximum archive file size the agent can scan. This setting applies to background threat detection and watch for new files. Setting the file size to 0MB means no archive files will be scanned.

Memory actions

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.

Setting	Description
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.
Violation type	This is a list of memory protection violation types. Set actions to Ignore, alert, block, or terminate.

Optics settings

Setting	Description
Optics auto upload	Enabling auto upload allows instance access to a Optics focus view (insight into the origin of a threat detected by Protect). Disabling auto upload will require manual requests for a Optics focus view for each threat. Select the event types to auto upload: memory protection, script control, and threats.
Configurable sensors	Allows the Optics agent to record additional events (beyond the standard process, file, network, registry, and thread events). **Note:** Enabling configurable sensors may reduce the length of time that data is stored in the local Optics database. • Advanced Powershell Visibility: Ability to record commands, arguments, scripts, and content entered directly into the Powershell console and the Powershell integrated scripting environment (ISE) • Advanced WMI Visibility: Ability to record additional Windows Management Instrumentation (WMI) attributes and parameters • DNS Visibility: Ability to record DNS requests, responses, and associated data fields such as domain name, resolved addresses, and record type made by processes • Enhanced Portable Executable Parsing: Ability to record data fields associated with portable executable (PE) files such as file version, import functions, and packer types • Enhanced Process and Hooking Visibility: Ability to record process information from the Win32 API and kernel audit messages to detect forms of process hooking and injection • Private Network Address Visibility: Ability to record network connections within the RFC 1918 and RFC 4193 address spaces • Windows Event Log Visibility: Ability to record Windows security events and their associated attributes
Optics desktop notification	Enabling desktop notifications for Optics will notify the end user of any actions or responses taken by Optics on the endpoint.
Optics detection settings	Enabling Optics detection settings applies the selected detection rule sets to the endpoint. Detection settings are configured on the Optics page in the console.

Application control

Setting	Description
Application control	Application control allows administrators to lockdown specified systems and restrict any changes on the device after being locked down. Only the applications that exist on the device before the lockdown are allowed to execute on the device. Any new applications or any changes to existing applications are denied. The agent updater is also disabled when application control is enabled.
Change window	Enabling the change window disables application control to allow new applications to be installed or to perform updates to existing applications. When all updates are complete, disable the change window.

Agent settings

Setting	Description
Auto-upload of log files	Enabling auto upload provides an automated way of accessing agent log files in the Cylance console.

Script control

Setting	Description
Alert	Monitors scripts running in your environment
Block	Only allows scripts to run from specific folders
Active script	Active scripts includes VBScript and JScript
Macors	Microsoft Office macros use Visual Basic for Application (VBA) to simplify routine actions, like manipulating data in a spreadsheet
PowerShell	PowerShell commands (one-liners)

Device control

Setting	Description
Block	Does not allow the USB mass storage device to connect to the endpoint
Full access	Allows the USB mass storage device to connect to the endpoint
Android	Android-based devices, like smartphones and tablets

Setting	Description
iOS	iOS-based (Apple) devices, like smartphones and tablets
Still image	Digital cameras and like devices
USB CD DVD RW	USB disc drives
USB drive	USB flash memory drives, like thumb drives
VMware USB passthrough	VMware allows connecting a USB device to the host system, then connecting that device to the guest virtual machine
Windows portable device	Windows-based devices, like smartphones

Data privacy

Setting	Description
Active directory	This is a Microsoft directory service for Windows domain networks. The domain name system (DNS) data is also affected when the active directory data privacy feature is enabled. Data affected: • Zone details - Zone rule • Zone details - Zone device list • Devices
Distinguished name	The lightweight directory access protocol (LDAP) references an object by its distinguished name (DN). Data affected: • Zone details - Zone rule
File owner	File owner information was included in a report that is no longer available. The file owner data is still collected by the agent and reported to the console, but it is not displayed in the console interface.

File path	The location on the endpoint where the threat was found. This information can include the user name in the file path.
	Example: c:\users\username\documents\filename
	The file path field is blank when this data privacy feature is enabled.
	Data affected:
	• Device details - Threats & activities:
	  • Threats
	  • Application control
	  • Threats & activities
	• Threat details - Affected devices and zones

Setting	Description
Hostname / FQDN	This is the name of the endpoint, which includes the fully qualified domain name (FQDN). This affects the device name in the console. The device name is part of the host name. Devices will display as unknown. • Example host name/FQDN: Computer1.corporatedomain.com • Example device name: Computer1 Data Affected: • Dashboard - Top Ten Lists: There is no link to the device details page for that device. • Devices • Device details: From the devices page, clicking on a device name link will take you to the details for that device. The device name is part of the title for the page. • Threat details - Affected devices and zones **Note:** If username is not blocked by data privacy, the host name will display as part of the last reported user information.
IP address	These are the IP addresses used by the endpoint. This includes IPv4 and IPv6 addresses. Data affected: • Zone details - Zone device list • Device details • Devices • Threat details - Affected devices and zones
MAC address	These are the MAC addresses used by the endpoint. Data affected: • Zone details - Zone device list • Device details • Devices • Threat details - Affected devices and zones
Username	This is the name of the user who logged on to the endpoint. This is also known as last reported user. Data affected: • Zone details - Zone device list • Device details • Devices • Threat details - Affected devices and zones

Exclusions

Setting	Description
Add exclusion	This opens the create exclusion windows. Select an exclusion type from the list. See exclusion types below for a list with descriptions.
Type	This setting displays the type of exclusion.
Values	This setting displays exclusion values, like a folder path.

Exclusion Type

Setting	Description
Application control	This setting specifies the absolute path of a folder to allow application changes and additions while application control is enabled.

Device control	This setting adds an external storage exclusion to either allow full access or block the storage device. Use the vendor ID of the storage device to add the exclusion.
	• Vendor ID: A unique identifier for the manufacturer of the product. This field is required.
	• Product ID: A unique identifier for the product. This is assigned by the manufacturer. This field is optional.
	• Serial Number: A unique identifier for the product. This field is optional.
	• Reason: Include a reason for adding this exclusion to the device control list. This field is optional.
	• Access:
	  • Full Access: Allows the USB mass storage device to connect with the endpoint.
	  • Block: Does not allow the USB mass storage device to connect with the endpoint.

Folder exclusions	This setting specifies the absolute path of a folder to exclude the folder, and sub-folders, from the background threat detection scan and watch for new files. • Allow Execution: Allows files in the excluded folder (or sub-folder) to execute.
Memory protection	This setting specifies the relative path to an executable file to exclude from memory protection. This will allow the specified files to run or be installed on any device assigned to the policy.

Setting	Description
Policy safe list	This setting adds files that are considered safe to the policy. Adding a file to the policy safe list means all agents assigned to this policy will treat the file as safe, even if Cylance scores it as unsafe or abnormal. Use this to allow a file for a group of devices, but not the entire organization. • SHA256: The SHA256 hash for the file. This field is required. • MD5: The MD5 hash for the file. This field is optional. • Filename: The name of the file. This field is optional. • Category: A tag for categorizing the file into a group, like admin tool or internal application. This field is required. • Reason: Include a reason why the file was added to the exclusion list. This field is required.
Script control	This setting specifies the relative path of a folder that contains authorized scripts. This will exclude any scripts in this folder, and sub-folders, from script control. **Wildcard Exclusions for Script Control**: Supports the use of wildcards when creating script control exclusions. Wildcards can exclude a folder or a script, including full or partial script names. Example: /users/*/temp would cover: • \users\john\temp • \users\jane\temp

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada