Cylance Multi-Tenant Console

Administration Guide

5.1

Contents

What is the Cylance Multi-Tenant Console?

Cylance Endpoint Security detects, protects against, and remediates threats on an organization's devices using an AI-powered solution for Zero Trust across devices, networks, apps, and people. The Zero Trust approach modernizes network security while simultaneously enhancing and improving the network experience for end users. The Zero Trust security model trusts nothing and no one by default, including users inside the work network. For more information about Cylance Endpoint Security, see the Cylance Endpoint Security documentation.

The Cylance Multi-Tenant Console integrates the security capabilities of Cylance Endpoint Security services into an environment that centralizes your tenant management activities. From the console, you can create and manage the tenants you support, their users, and device policies. Each tenant resides in its own environment within the console, which makes it easy for you to switch from one tenant to another.

Supported browsers for the Cylance Multi-Tenant Console

Item	Requirements

Browser	• Latest version of:
	  • Google Chrome
	  • Mozilla Firefox
	  • Microsoft Edge

Signing into the Cylance Multi-Tenant Console

If your organization is new to the Cylance Multi-Tenant Console, BlackBerry will send an email invitation to an administrator account that you've provided with a link to create a sign-in password. When this administrator signs in to the console, they can create users for your organization. Console users receive an email invitation with a link to create a password for their account. They can then sign in at https://admin.cylance.com and use their work email address as their username.

Configuring single sign-on for the Cylance Multi-Tenant Console

The Cylance Multi-Tenant Console supports single sign-on (SSO) user authentication with any identity provider (IdP) that uses SAML 2.0.

For more information about single sign-on, visit support.blackberry.com to read KB66452.

Configure SAML for the Cylance Multi-Tenant Console

1. In the Cylance Multi-Tenant Console, hover over and click **Account Overview**.
2. Under **Authentication Settings**, click .
3. Turn on **Enable SSO**.
4. In the **Provider** drop-down list, click your IdP provider. If your IdP is not listed, click **Custom**.
5. In the **X.509 certificate** field, paste your X.509 certificate information. Include `-----BEGIN CERTIFICATE-----` before the certificate text and `-----END CERTIFICATE-----` after it.
6. In the **Login URL** field, paste the login URL provided by the IdP.
7. Click .

Use SSO to log in to the Cylance Multi-Tenant Console

After you configure the Cylance Multi-Tenant Console to use your IdP authentication, users in your organization can then login using SSO.

1. Visit https://admin.cylance.com/#/auth/external-login.
2. In the **Email** field, type your work email address.
3. In the **Region** drop-down list, click the appropriate region.
4. Click **Sign In**.
5. On the IdP authentication page, specify your IdP username and password.
6. Click **Sign In**.

Configure SAML using an IDP

You can configure SSO for the Cylance Multi-Tenant Console using any IDP that supports SAML 2.0. When you configure SSO, type the information listed below in the appropriate fields.

Field	User input
Entity ID, Issuer, Application name	`CylancePROTECTMulti-TenantConsole`

Field	User input

Sign-on URL, SAML response URL	`https://admin.cylance.com/<regionCode>/api/auth/external-auth/consumesaml/< partnerid>`
	• Replace <*partnerid*> with your partner ID, and replace <*regionCode*> with the appropriate region code:
	  • us: North America
	  • au: Asia-Pacific South East (including Australia)
	  • eu: Europe Central
	  • gc: Gov Cloud
	  • jp: Asia-Pacific North East (including Japan)
	  • sp: South America East

Configure an ADFS trust

When you configure a relying party trust, type the information listed below in the appropriate fields.

Field	User input
Relying Party Identifier	`Cylance Multi-Tenant Console`

SAML Assertion Consumer Endpoint	`https://admin.cylance.com/<regionCode>/api/auth/external-auth/consume-saml/<partnerid>`
	• Replace <*partnerid*> with your partner ID, and replace <*regionCode*> with the appropriate region code:
	  • us: North America
	  • au: Asia-Pacific South East (including Australia)
	  • eu: Europe Central
	  • gc: Gov Cloud
	  • jp: Asia-Pacific North East (including Japan)
	  • sp: South America East

Turn off password login to enable single sign-on

With single sign-on (SSO) enabled, you might need to turn off the option for administrators to log in to the Cylance Multi-Tenant Console using an email address and password. For security purposes, an organization may require their users to log in using an external identity provider only.

1. In the Cylance Multi-Tenant Console, hover over and click **Account Overview**.
2. In the **Authentication Settings** section, click .
3. Turn off **Password Login**.
4. Click .

Using time-based one-time password authentication

You can configure Cylance Multi-Tenant Console to work with a multi-factor authentication app and use a time-based one-time password as a second-factor authentication method. After you enable time-based one-time

password authentication, when a user logs in to the console for the first time, they will be provided with a QR code that allows them to enroll with a multi-factor authentication app such as Google Authenticator, Microsoft Authenticator, Okta Verify, or Authy.

Configure time-based one-time password authentication

1. In the Multi-Tenant Console, hover-over and select **Account Overview**.
2. Under **Authentication Settings**, click .
3. Click the **Time-based OTP** option. Note that you must enable the Password Login setting first.
4. In the **Time-Step Window** section, select a number of intervals in the drop-down list. Any code within the window is valid if it precedes or follows the expected code by the number of refresh intervals that you specify. The refresh interval is 30 seconds, and the default setting is 1.
5. Click **Save**.

Disable time-based one-time password authentication for a user

You can disable time-based one-time password authentication for individual users.

1. In the Multi-Tenant Console, click **Partner Users**.
2. On the **Partner Users** tab, click for the user you want to edit.
3. Disable the time-based one-time password authentication option for the user.

Note: If the user was enrolled with time-based one-time password before you disable it, the user to continue using their previous enrollment with the multi-factor authentication app when you re-enable it.

View which users are configured to use time-based one-time password authentication

On the **Partner Users** page, in the **OTP** column, you can see which user is enabled for time-based one-time password authentication. Note that you can filter on the OTP column.

Enroll with multi-factor authentication

The first time users log in to the console after you have enabled time-based one-time password authentication, they will be asked to enroll with a multi-factor authentication app using a QR code.

1. On the Multi-Tenant Console sign-in page, enter your credentials.
2. Click **Continue**.
3. Open your organization's authentication app on your device, and on the Multi-factor enrollment page, scan the QR code.
4. In the **One time password** field, enter the six digit code that is displayed in your organization's authentication app on your device.
5. Click **Sign in**.

   Note: You can click **Skip for now** up to three times to sign in without entering a one-time password.

Sign in to the Multi-tenant console using a one-time password

1. On the Multi-Tenant Console log in page, enter your credentials.
2. Click **Continue**.
3. In the **One time password** field, enter the six digit code that displays on your device in your organization's authentication app.
4. Click **Sign in**.

Regenerate the enrollment secret for a user

You can regenerate the enrollment secret for a user that has already enrolled with time-based one-time password authentication. After you regenerate the secret, the user will need to re-enroll with an authentication app the next time that they log in to the console.

1. In the Multi-Tenant Console, click **Partner Users**.
2. On the **Partner Users** tab, click the edit icon for the user you want to regenerate the enrollment secret for.
3. Click **Regenerate enrollment secret**.
4. Click **Regenerate**.

View and manage your account

1. In the Cylance Multi-Tenant Console, hover over .
2. Do any of the following:

Task	Steps
Update your password.	**a.** Click **My Profile**. **b.** Type your current password. **c.** Type your new password. **d.** Click **Update Password.**
View the audit log.	**a.** Click **Audit Log**. The audit log lists all user activity from your console.
View your account information.	**a.** Click **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 console's information.
Download product usage .csv files.	**a.** Click **Account Overview**. **b.** On the **Product Usage** tab, click **Download CSV** for the appropriate billing cycle.

Creating partner users in the Cylance Multi-Tenant Console

You can create other Cylance Multi-Tenant Console users that are known as partner users. You can assign a partner user to one or more tenants that they can manage.

You can assign a role to a partner user that defines the level of access that is granted to the user. Users that are assigned the administrator role can create and manage tenants, create tenant users, and create and manage console users. Partner read-only users have read-only access to the tenants that are assigned to them and they can't make changes to tenants.

Partner administrators can't disable CylanceOPTICS, CylancePERSONA, or CylanceGATEWAY services after they have been enabled for a tenant. They will have to contact BlackBerry Support to disable these services.

Create a partner user

When you create a partner user, an invitation is sent to the user's email address. The invitation includes a link that allows them to create a password for their console's account.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Partner Users**.
2. On the **Partner Users** tab, click **Add Partner User**.
3. Specify the required information.
4. In the **Select A Role** drop-down list, click the appropriate role for the partner user.
5. Click **Save & Finish**.

After you finish:

- To edit a partner user, on the **Partner Users** page, click . Click **Save & Finish**.
- To reset a partner user password, on the console's login page, click **Forgot Password?** Specify the required information and click **Send Reset Link**. The partner user will receive an email with a link to reset their password.
- To delete a partner user, on the **Partner Users** page, click beside the partner user that you want to delete. Click **Confirm**.

Create and customize partner roles

In the Cylance Multi-Tenant Console, you can create new user roles using custom permission sets. This allows you to create roles with customized access to the console's features.

1. In the Cylance Multi-Tenant Console, click **Partner Users**.
2. On the **Roles and Permissions** tab, click **Add Role**.
3. Type a role name.
4. Select permissions for the role. For more information about the available permissions, see Permissions for user roles.
5. Click **Save New Role**.

After you finish:

- To edit a partner role, on the **Roles and Permissions** tab, click beside the role that you want to modify. Click **Save Role**.

- To delete a partner role, on the **Roles and Permissions** tab, click beside the role that you want to delete. Click **Confirm**.

Permissions for user roles

Tenant

These permissions relate to the tenant in the Cylance Multi-Tenant Console that the user is assigned to.

Permission	Description
Shutdown tenants	This permission allows users to shutdown a tenant.
View tenant list	This permission allows users to view a list of tenants in the console.
Read tenant details	This permission allows users to read the tenant details, such as tenant information, purchase information, licensing, and evaluation EULA.
Add or modify tenant details	This permission allows users to create or modify tenants in the console.

Policy template

These permissions relate to the policy template in the Cylance Multi-Tenant Console.

Permission	Description
Read policy template details	This permission allows users to read the policy template details, including the policy settings.
View policy template list	This permission allows users to view a list of policy templates in the console.
Add or modify policy template information	This permission allows users to create or modify policy templates in the console.
Delete policy templates	This permission allows users to delete policy templates in the console.

Report

These permissions relate to the Cylance Multi-Tenant Console reports.

Permission	Description
Read report details and report lists	This permission allows users to read the console reports.
Add or modify report information	This permission allows users to create or modify reports in the console.
Delete report	This permission allows users to delete a report from the console.

Partner-App

These permission relate to the use of API integrations with partner apps in the Cylance Multi-Tenant Console.

Permission	Description
List partner-app API integration details	This permission allows users to list partner-app API integration details in the console.
Read partner-app API integration details	This permission allows users to read partner-app API integration details in the console.
Add or modify partner-app API integrations	This permission allows users to add or modify partner-app API integrations in the console.
Delete partner-app API integrations	This permission allows users to delete partner-app API integrations in the console.

Ghost-Login

These permissions relate to the Ghost-Login feature in the Cylance Multi-Tenant Console.

Permission	Description
Ghost-login as tenant user	This permission allows a partner to log in with the user's account as if they were a tenant user, even if the user is assigned a different user role. The console will log the email address of the partner who logs in as the user.
Ghost-login as tenant admin	This permission allows a partner to log in with the user's account as if they were a tenant administrator, even if the user is assigned a different user role. The console will log the email address of the partner who logs in as the user.
Ghost-login as tenant zone manager	This permission allows a partner to log in with the user's account as if they were a tenant zone manager, even if the user is assigned a different user role. The console will log the email address of the partner who logs in as the user.
Ghost-login as tenant read only	This permission allows users to log in with the user's account as if they were a tenant read only user, even if the user is assigned a different user role. The console will log the email address of the partner who logs in as the user.

Partner

These permissions relate to partner users in the Cylance Multi-Tenant Console.

Permission	Description
Ability to approve creation of tenants	This permission allows users to approve the creation of tenants.
View partner list	This permission allows users to view the partner list.
Read partner details	This permission allows users to read partner details.
Add or modify partner information	This permission allows users to add or modify partner information.
Delete partners	This permission allows users to delete partners.

User

These permissions relate to the users associated to a tenant in the Cylance Multi-Tenant Console.

Permission	Description
View user list	This permission allows users to view a list of users in the console.
Read user details	This permission allows users to read user information.
Add or modify user information	This permission allows users to create or modify users in the console.
Delete users	This permission allows users to delete users from the console.

Role

These permissions relate to the roles in the Cylance Multi-Tenant Console.

Permission	Description
View role list	This permission allows users to view list of roles in the console.
Read role details	This permission allows users to read role information.
Add or modify role information	This permission allows users to create or modify roles in the console.
Delete roles	This permissions allows users to delete roles from the console.

Managing tenants in the Cylance Multi-Tenant Console

In the Cylance Multi-Tenant Console, a tenant represents a customer's organization. Each tenant in the console resides in an independent customer environment with its own associated devices. After you create a tenant in the console, you can create tenant users and assign them to the appropriate tenant. If one or more Cylance Endpoint Security services cannot be successfully enabled in the tenant, an error icon displays in the status column.

Tenants with an evaluation license (a trial license) have 60 days to manually convert to a customer license. Sixty days after the tenant creation date, the tenant will automatically be converted to a customer license. Fourteen days before the automated license conversion, an icon will appear next to the tenant's name to remind the tenant about the pending conversion.

Create a tenant

1. In the Cylance Multi-Tenant Console, click **Tenants** > **Add New tenant**.
2. In the **Tenant name** field, type the name for the tenant.
3. Optionally, in the **Unique admin email** field, type the email address of the tenant user.
4. Optionally, in the **Custom Domain** field, type a custom domain name to make it easier for your users to access the tenant.
5. In the **Tenant Address** section, specify the tenant's address information.
6. In the **Tenant Features** section, choose the features or services that you want to turn on for the tenant.
7. In the **Enter Licensing Details** section, specify the total number of licenses granted for each service.

   The CylancePROTECT license count is required when you add licenses to a tenant. By default, only CylancePROTECT is enabled for the tenant. To turn on additional services such as CylanceOPTICS, CylancePERSONA, and CylanceGATEWAY, in the **Tenant Services** section, turn on the desired services. If a service cannot be successfully enabled in a tenant, an error icon displays under the service.
8. If you want to turn on additional CylanceOPTICS services, under **Tenant Services**, turn on **Optics v2**. Choose the features that you want to turn on.
9. Click **Save & Finish**.

Tenant creation is an asynchronous process that prevents you from making edits to the tenant until the process is complete.

After you finish:

- To view a list of your customers' tenants, click the **Active Tenants** tab.
- To edit a tenant, on the **Active Tenants** tab, click the tenant that you want to edit. Click ✎ beside the section that you want to edit. To save your changes, click ✓.

Manage tenant threats from a global list

You can view the policies, zones, devices, agent versions, and tenant users for the tenants you manage, which allows you to help manage your customers' organizations and assist with troubleshooting.

You can add a file to the global quarantine list to block it from all devices in a tenant, and you can add a file to the global safelist to allow it on all devices in the tenant.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Tenants**.
2. On the **Active Tenants** tab, click a tenant.

3. On the **Threats** tab, click the threat that you want to take action on.
4. To add a threat to the global quarantine list, click **Globally Quarantine**. To add the threat to the global safelist, click **Globally Safelist**.
5. Choose 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 or global safelist.
8. Click **Next**.
9. Click **Globally Quarantine** or **Globally Safelist**.

After you finish:

- To remove an item from the global quarantine list, on the **Active Tenants** tab, click a tenant. On the **Quarantine List** tab, choose the files that you want to remove. Click **Remove Selected** > **Yes, Remove from List**.
- To remove an item from the global safelist, on the **Active Tenants** tab, click a tenant. On the **Safelist** tab, choose the files that you want to remove. Click **Remove Selected** > **Yes, Remove from List**.

Create tenant users

As a Cylance Multi-Tenant Console administrator, you can add tenant users, which represent the employees within an organization. When you add a tenant user, they will receive an invitation email message to create a password and set up their account.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Tenants**.
2. On the **Active Tenants** tab, click a tenant that you want to add a user to.
3. On the **Tenant Users** tab, click **Add Tenant User**.
4. Specify the tenant user's first name, last name, and email address.
5. Click **Save & Finish**.

After you finish:

- To edit a tenant user, on the **Active Tenants** tab, click the tenant that the tenant user belongs to. On the **Tenant Users** tab, click beside the tenant user. Click **Save & Finish**.
- To delete a tenant user, on the **Active Tenants** tab, click the tenant that the tenant user belongs to. On the **Tenant Users** tab, click beside the tenant user that you want to delete. Click **Confirm**.

Use support login to log in as a tenant or tenant user

Support login, also known as ghost login, allows you to conveniently log in to a tenant's Cylance console as the tenant or as a tenant user to manage their account. With support login, you don't need a password to access a tenant or tenant user's Cylance console. You can only view and modify what their permissions allow.

The user's audit log will show that you logged in to the Cylance console as the user.

Before you begin: To use the support login feature, contact a tenant administrator to verify that support login is enabled in the tenant's Cylance console. On the menu bar, the administrator should click **Settings** > **Application** and confirm that **Enable Support Login** is selected.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Tenants**.
2. Do one of the following:

Task	Steps
Use support login to login as a tenant	a. On the **Active Tenants tab**, click beside the tenant you want to log in as. b. Click **Confirm**.
Use support login to login as a tenant user	a. On the **Active Tenants** tab, click the tenant. b. On the **Tenant Users** tab, click beside the user you want to log in as. c. Click **Confirm**.

You will be taken directly to the Cylance console using the tenant or tenant user's account.

Shut down a tenant

If a customer's license to the Cylance console expires, you can shut down the tenant, which removes their access to the Cylance console. Because the agents will no longer communicate with the Cylance console, they will display a message stating that the user will need an installation token to connect to the console.

After you shut down a tenant, you cannot recover the tenant's data unless you turn on the 7-day grace period. This grace period allows you to cancel the shutdown and it gives the tenant time to renew their Cylance licenses.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Tenants**.
2. On the **Active Tenants** tab, click the tenant that you want to shut down.
3. Click **Shut Down Tenant**.
4. Do one of the following:

Action	Description
Turn off the 7-day grace period.	• The tenant will be removed from your system and you won't be able to recover its data. The process may take up to 24 hours to complete.
Turn on the 7-day grace period.	• The tenant will be removed after the 7-day grace period. After the grace period ends, the tenant is removed and you won't be able to recover its data. • During the grace period, you can cancel the shutdown by clicking **Tenants** > **Pending** > **Cancel Shutdown**.

5. Click **Shut down tenant**.

Managing device policies from the Cylance Multi-Tenant Console

A device policy defines how the CylancePROTECT agent handles malware it detects on a user's device. A device policy is also used to enable and configure other services, including CylanceOPTICS and CylancePERSONA Desktop. Every device must be assigned a device policy. If you do not assign a custom policy to a device, the device is assigned the default policy.

The device policy templates allow you to configure and customize policy settings, apply them to new and existing tenants, and manage device policy assignments for all tenants directly from the Cylance Multi-Tenant Console.

Policy template actions are recorded in the console audit log, which includes the user who performed the action and the time of the action.

Policy template role permissions allow you to grant console users access to the policy template. Enabling a policy template permission does not automatically enable any dependencies. For example, if you enable the read policy template details permission, you must also enable the view policy template list permission. For more information, see Create and customize partner roles.

Note that there is no automated synchronization between the device policy template and the tenant policies. If you update the template, you will have to re-apply the template to a tenant.

Step	Action
1	Create a device policy template.
2	Apply a device policy template to a tenant.
3	Assign a device policy to a device.

Create a device policy template

You can create device policy templates to apply to your customers' tenants. This feature can streamline customer onboarding, product enablement, and the implementation process.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Settings** > **Add New Template**.
2. Type a name for the template.
3. Configure the device policy settings.

   For more information about device policy settings and description. see Device policy settings.
4. Click **Save & Finish**.

After you finish: Apply a device policy template to a tenant.

Apply a device policy template to a tenant

To assign the same device policy to multiple devices in a tenant, you will first need to apply the device policy template to the tenant that those devices belong to.

Before you begin: Create a device policy template.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Tenants**.
2. On the **Active Tenants** page, click a tenant.
3. On the **Policies** tab, click **Apply a Policy Template**.
4. Select one or more policy templates to assign to the tenant. You can use keywords to filter the policy templates.
5. Click **Apply**.

After you finish: Assign a device policy to a device.

Assign a device policy to a device

After you assign a device policy template to a customer's tenant, you can apply the device policy to devices that belong to that tenant. You can apply a device policy to multiple devices, but a device can only have one policy.

Before you begin: Apply a device policy template to a tenant.

1. In the Cylance Multi-Tenant Console, click **Tenants**.
2. On the **Active Tenants** tab, click a tenant.
3. On the **Devices** tab, select the devices that you want the device policy to apply to.
4. Click **Assign Policy**.
5. Select a policy to apply to the devices.
6. Click **Assign Policy**.

Device policy settings

Cylance Endpoint Security administrators use device policies to configure and define the behavior of the CylancePROTECT Desktop agent, the CylanceOPTICS agent, and the CylancePERSONA Desktop agent on users' devices.

For more information about each device policy setting, see the Device policy documentation.

Using linked policy templates

You can create a linked policy template and link it to all of your tenants or to a subset of your tenants. If you make a change to a setting in one of the linked policy templates, that change applies to all of the tenants that use the policy. This allows you to quickly make changes to multiple tenants instead of updating each tenant separately.

Create a linked policy template

A linked policy template allows you to select a set of options that you can apply to multiple tenants simultaneously.

1. In the Cylance Multi-Tenant Console, click **Settings > Linked Policy Templates**.
2. Click **Add New Template**.
3. Type a name for the template.
4. Turn on the **Default Template** option if you want the linked policy template to override the policy template in your linked tenants.

   Note that after you set a policy template as a default template, it remains linked with the tenant's default policies and cannot be modified.
5. Click the options in the left-hand menu and select the settings that you want to apply to the linked policy template.
6. Click **Create**.

Link a linked policy template with multiple tenants

You can link a linked policy template with multiple tenants, which allows you to make a change to the linked policy and update all of the tenants that you have linked with the policy simultaneously.

For a non-default linked template, when the linking request creates a new policy in all tenants selected for linking, an email message with linking status details is sent to the administrator. For a default linked template, when the linking operation updates the default policy in all tenants selected for linking, an email message with linking status details is sent to the administrator.

1. In the Cylance Multi-Tenant Console, click **Settings > Linked Policy Template**.
2. Click the linked policy template that you want to link.
3. Click **Linked Tenants**.
4. Click **Link Tenant**.
5. Select the tenants that you want to link the policy template to, or use the search field to find the tenants and add them.
6. Click **Link Tenant**.

   Note that while linking is taking place, you cannot make any changes to the associated template.

Unlink a linked policy template from tenants

When a linked policy template is unlinked from selected tenants, the corresponding policy in the linked tenant is not deleted.

1. In the Cylance Multi-Tenant Console, click **Settings > Linked Policy Templates > Linked Tenants**.

2. Select the tenants that you want to unlink the linked policy template from.
3. Click **Unlink Tenant > Unlink**.

Update a linked policy template

When a linked policy template is updated, the corresponding policy in any linked tenants is updated. If you have made changes to a linked policy in the tenant directly, those changes will be overwritten.

For a non-default linked template, when the linking operation finishes updating the linked policy in all linked tenants, an email message with linking status details is sent to the administrator. For a default linked template, when the linking operation finishes updating the default policy in all linked tenants, an email message with linking status details is sent to the administrator.

1. In the Cylance Multi-Tenant Console, click **Settings > Linked Policy Templates**.
2. Click the template that you want to update.
3. Make your changes.

   Note that after you set a policy template as a default template, it remains linked with the tenant's default policies and cannot be modified.
4. Click **Save**.

Delete a linked policy template

You cannot delete templates that are linked with a tenant. You must remove them from the tenant first.

1. In the Cylance Multi-Tenant Console, click **Settings > Linked Policy Templates**.
2. Select the templates that you want to remove.
3. Click **Delete**.
4. Click **Remove Template**.

Create a report

You can use the reports feature to produce custom reports that collect data from across the tenants that you manage.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Reports**.
2. On the **Reports** tab, click **Create Report**.
3. Type a report name.
4. From the **Report Type** drop-down list, select one of the following reports:

Report type	Description
Audit Log	This report logs actions performed in the console.
Account Data	This report includes information about the tenant.
Partner User	This report includes information about partner users and roles.
Tenant Devices	This report includes information about tenant devices.
Tenant Detections	This report includes information about detected threats.
Tenant User	This report includes user information and information about roles across all tenants.
Policy Details	This report includes information about device policy settings.

5. In the **Report Fields** section, select the report fields that you want to apply to the report.
6. In the **Report Filters** section, add a filter and configure its parameters.
7. If you want to run the report on a schedule, turn on **Schedule Report** and do one of the following:

Action	Steps
Run the report once on a specific date.	**a.** Click **One-Time**. **b.** Set the date you want the report to run on.
Run the report on a regular basis.	**a.** Click **Recurring**. **b.** Set the frequency you want the report to run on. **c.** Set the start date of the report, the date the report will run on, and the date the report will end on.

8. Do one of the following:
   - To save the report and run it immediately, click **Save and Run Report**.
   - To save the report without running it, click **Save & Finish**.

After you finish:

- To view and download recently generated reports, on the **Reports** page, click **Recently Run**.
- To edit a report, on the **Reports** tab, click beside the report that you want to edit. To save your changes, click **Save and Run Report** or **Save & Finish**.

Report filters

Report filters that require filter text

Filter	Description
Contains	The data that is returned from this filter contains the contents that you type into the filter text field. For example, if you type "ol" into the Contains filter text field, "policy" is included in the report, but "template" is excluded from the report.
Does not contain	The data that is returned from this filter does not contain the contents that you type into the filter text field. For example, if you type "po" into the Does not contain filter text field, "partner" is included in the report, but "policy" is excluded from the report.
Ends with	The data that is returned from this filter ends with the contents that you type into the filter text field. For example, if you type "ing" into the Ends with filter text field, "reporting" is included in the report, but "reported" is excluded from the report.
In	With this filter, you can select the type of content that you want to include in the report, such as usernames and actions.
Is equal	The data that is returned from this filter match the contents that you type into the filter text field.
Is not equal	The data that is returned from this filter does not match the contents that you type into the filter text field.
Starts with	The data that is returned from this filter start with the contents that you type into the filter text field. For example, if you type "po" into the Starts with filter text field, "policy" is included from the report, but "partner" is excluded from the report.

Report filters for counts and dates

Filter	Description
Greater than	For counts or for filters that use an integer, the data that is greater than the number that you specify 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 for filters that use an integer, the data that is greater than or equal to the number that you specify is included in the report. For dates, the data that is newer than or equal to the selected date is included in the report.

Filter	Description
Is equal	For counts or for filters that use an integer, the data that is equal to the number that you specify 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 that is not equal to the number that you specify 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 for filters that use an integer, the data that is less than the number that you specify is included in the report. For dates, the data that is older than the selected date is included in the report.
Less than or equal	For counts or for filters that use an integer, the data that is less than or equal to the number that you specify is included in the report. For dates, the data that is older than or equal to the selected date is included in the report.

Generating an API token for the Cylance Multi-Tenant Console

The Cylance Multi-Tenant Console API allows you to generate an API token, access policy templates, and administer tenants.

To learn about how to create a partner application, generate a bearer token, and make an API health check, see the Cylance MTC Partner API Documentation. There, you will find a downloadable JSON file that contains examples of the console's API that you can import into Postman. If you use other API software, you can copy the API requests directly from the API webpage.

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