Cylance Multi-Tenant Console

Administration Guide

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 for the first time

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.

Signing in with single account experience

The single account experience for the Cylance Multi-Tenant Console allows partner users to sign into multiple partner accounts in a given region using the same email address. A partner user needs to have their email address added in each of their desired partners by a partner administrator. To add a partner user's email address, follow the steps in Create a partner user. An invitation email will be sent to the partner user with a registration link that must be clicked on to complete the registration. Once registration is complete, the partner user can sign in to the partner account using a short name.

A short name is a globally unique name for a partner that is set to a system-generated GUID by default. The short name of a partner can be edited by an administrator and is included in the invitation email. On the sign-in screen, a partner user can enter the short name of the partner account they want to sign in to. Valid characters are lowercase letters, 0 to 9, and hyphen (-) with no spaces. The short name field is optional; however, if a partner user has completed registration in multiple partners, a short name will be required to sign in.

If a partner user is registered with multiple partners, they can use the same MTC and one-time passwords for all partners when signing in. The use of MTC passwords, including one-time passwords, and external identity providers when signing in will depend on the configuration of the individual partner account.

Note: Users were previously able to use external identity providers to sign in without clicking on the registration link in the invitation email. However, to improve the security of the sign in process, users must now click on the registration link in the invitation email to complete registration in each partner.

The single account experience is available in all regions except Gov Cloud.

Edit a partner short name

A short name is a globally unique name for a partner that is set to a system-generated GUID by default. The short name of a partner is included in the invitation email and can be edited by an administrator.

1. In the Cylance Multi-Tenant Console, click **Partners**.
2. Click the name of the partner that you want to edit.
3. In the **Partner Information** section, click .
4. In the **Partner short name** field, edit the short name. Valid characters are lowercase letters, 0 to 9, and hyphen (-) with no spaces.
5. Click ✓.

After you finish: After a short name is changed, all invited partner users will receive an email with the new short name.

Sign in to a different partner account using the single account experience

You can sign in to other partner accounts that your email address has been added after you sign in to the Multi-Tenant Console.

Before you begin: Verify that the partner user has been created in each partner account that you want to access. For instructions see, Create a partner user. If the task requires four or more prerequisites, create a separate Prerequisites topic.

1. In the Multi-Tenant Console, click the **User information** icon on the top right.

2. Click on ⌄ below the user information to display a list partner accounts.
3. Click the partner account that you want to sign in to. If necessary, use the search bar to filter the list.
4. If prompted, follow the on-screen prompts to complete any additional authentication requirements of the partner account.

Enhanced authentication sign in for the Cylance Multi-Tenant Console

The management console provides enhanced authentication capabilities, including local multi-factor authentication and more granular authentication policies and policy assignments. You can configure the environment to specify the types of authentication that partner users must complete to sign in to the Cylance Multi-Tenant Console. By default, partner users use their BlackBerry Online Account password and a one-time password to access the console after they set up their account.

You can create authentication policies that specify the types of authentication that must be completed by all partner users in the console. Only one default authentication policy can be created for signing in to the console. You can create separate authentication policies the specify the authentication methods that partner users must complete. The authentication types added to the default authentication and user authentication policies must be completed in the order specified in the policy. As a failsafe, you may configure one partner administrator to access the Cylance Multi-Tenant Console using their username and a strong password.

To configure enhanced authentication for sign-in, perform one of the following actions:

Configure enhanced authentication for signing in to the console

If your Cylance Multi-Tenant Console account was created before July 2024, complete these steps if you want to configure your users to authenticate with the console using an authenticator such as One-Time Password in addition to the BlackBerry Online Account password.

Step	Action
1	Sign in to the Cylance Multi-Tenant Console using your existing username and password.
2	Add an authenticator (for example, One-Time Password or SAML). By default, the following authenticators are configured for use in your environment: "One-Time Password" and BlackBerry Online Account.
3	Add a One-Time Password authenticator to the default authentication policy for partner administrators and users.
4	Create an authentication policy that uses the password and the authenticator that you created (optional). **Note:** As a failsafe, create one authentication policy that only uses the Cylance console password and assign it to one administrator.
5	Test the authentication policy by signing in to the console.

Remove One-Time Password authentication for signing in to the console

Cylance Multi-Tenant Console accounts created in July 2024 or later require users to enter a One-Time Password after they enter the Cylance console password each time before they can access the console. Complete these steps if you want to remove the One-Time Password requirement for users to authenticate with the console.

Step	Action
1	Sign in to the Cylance Multi-Tenant Console using your existing username, password, and one-time password.
2	Remove the One-Time Password authenticator from the default authentication policy.
3	Test the authentication policy by signing in to the console.

Configure a new IDP SAML authenticator for SSO and IDP-initiated access to the console

Complete these steps if you want to configure a new identity provider (IDP) SAML authenticator for users to authenticate with the Cylance Multi-Tenant Console. Users can use their IDP credentials to access the console from the IDP sign-in page or from the IDP-initiated SSO portal.

Step	Action
1	In the IDP environment, create a new SAML application.
2	Configure the IDP to communicate with the Cylance Multi-Tenant Console.
3	In the Cylance Multi-Tenant Console, Add an authenticator.
4	Create an authentication policy that uses the authenticator that you created. **Note:** As a failsafe, create one authentication policy that only uses the BlackBerry Online Account password and assign it to one administrator.
5	Verify whether you need to Generate a new SSO callback URL for an authenticator. If necessary, update it in the IDP environment.
6	Test the authentication policy by signing in the console.

Update an existing IDP SAML authenticator to enable IDP-initiated access to the console

Complete these steps only if your IDP SAML authenticator was created before July 2024 and you want to enable IDP-initiated SSO for users to access the console from the IDP user portal. For a walkthrough, see How do I update IDP (SAML) authenticators to enable IDP-initiated access to the Cylance console and select your IDP.

Step	Action
1	Sign in to the Cylance Multi-Tenant Console using your existing username and password.
2	Verify whether you need to Generate a new SSO callback URL for an authenticator. If necessary, update it in the IDP environment.
3	Update the authentication policy to use the authenticator with the new SSO callback URL. **Note:** As a failsafe, create one authentication policy that only uses the BlackBerry Online Account password and assign it to one administrator.
4	Test the authentication policy by signing in the console.

Add an authenticator

You add authenticators so that you can add them to authentication policies. An authenticator typically defines one authentication method, such as a password (for example, a BlackBerry Online Account password) or a connection to a third-party for authentication like Active Directory, Okta, or Ping Identity. You add them to authentication policies to specify the types of authentication that administrators must complete to sign in to the Cylance Multi-Tenant Consoleconsole and users must complete to activate Cylance Endpoint Security apps or agents (for example, the CylancePROTECT Mobile app or CylanceGATEWAY). You can combine multiple authenticators in an authentication policy to provide multiple authentication steps. For example, you can combine the Enterprise authenticator with a one-time password prompt in a policy to require users to authenticate with both their work or BlackBerry Online Account password and a one-time password.

Before you begin:

- **Important:** Verify that you have reviewed and completed the appropriate steps for Enhanced authentication sign in for the Cylance Multi-Tenant Console to the Cylance console before you configure your IDP SAML authenticator. If the required steps are not completed, the third-party authenticator will be unable to communicate with Cylance Endpoint Security. For more information, see the following:
  - For steps to configure an IDP for enhanced authentication and IDP-initiated access to the Cylance console, see Enhanced authentication sign in for the Cylance Multi-Tenant Console.
  - For a walkthrough of the steps to configure a new IDP SAML, see How do I configure IDP SAMLs for enhanced authentication and IDP-initiated access to the Cylanceconsole.
  - For a walkthrough of the steps to enable IDP-initiated access to the console for an existing IDP SAML that was created before December 2023, see How do I update external IDP (SAML) authenticators for SSO to access the Cylance console.
- If you add a SAML authenticator, download a copy of the signing certificate for your IDP.

1. On the menu bar, click **Settings > Administration**.
2. Click the **Authenticators** tab.
3. Click **Add Authenticator**.
4. In the **Authenticator Type** drop-down list, select one of the following authentication methods:

Authentication method	Description
Entra (SAML)	Select this option if you want users to enter their Entra credentials in the primary sign-in page and enable IDP-initiated access to the Cylance console. For a walkthrough of the steps to configure your Entra (SAML), see the following: • Configure a new Entra (SAML): Configure the Entra (SAML) Authenticator for enhanced authentication • Enable Entra-initiated access for an existing Entra (SAML): Update the Entra (SAML) authenticator to enable IDP-initiated access to the Cylance console **Note:** The SSO Callback URL is generated when you save the authenticator and will be in the format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. Do the following: **a.** Enter a name for the authenticator. **b.** If you want users to validate their email with a one-time code when they log in for the first time, turn on **Validation required**. The code is sent to the email address that is associated with the user in your tenant. **c.** In the **Login request URL** field, enter the Login URL that is specified in the app registration single sign-on settings for your identity provider. For example, in the Entra Portal, go to Enterprise Application > <*Name of the newly created application*> > Setting up *application name* section > Login URL. **d.** In the **IDP signing certificate** field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. When you copy and paste the body of the certificate, make sure that you don't alter any line breaks or the format of the certificate information. **e.** In the **SP entity ID** field, enter the **Identifier (Entity ID)** that you recorded from the SAML configuration in the Entra portal. This field is required. The "SP Entity ID" value must match the “Identifier (Entity ID)” value that you recorded in the IDP console. **f.** Enable **Show Advanced** settings, in the **Email claim** field, paste the value from the “Claim Name” that you recorded in the Entra portal (e.g. http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress). **g.** Specify any other optional settings. **h.** Click **Save**. **i.** Open the authenticator that you added. Record the **SSO callback URL**. This URL will be required in the Entra portal > Basic SAML Configuration > Reply URL (Assertion Consumer URL) field.

Authentication method	Description
Custom (SAML)	Select this option if you want users to enter custom credentials in the primary sign-in page and enable IDP-initiated access to the Cylance console. For a walkthrough of the steps to configure your Custom (SAML), see the following: • Configure a new Custom (SAML): Configure the Custom (SAML) Authenticator for enhanced authentication • Enable Custom-initiated access for an existing Custom (SAML): Update the Custom (SAML) authenticator to enable IDP-initiated access to the Cylance console **Note:** The SSO Callback URL is generated when you save the authenticator and will be in the format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. **a.** Enter a name for the authenticator. **b.** If you want users to validate their email with a one-time code when they log in for the first time, turn on **Validation required**. **c.** In the **Login request URL** field, enter the identity provider's single sign-on URL. **d.** In the **IDP signing certificate** field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. When you copy and paste the body of the certificate, make sure that you don't alter any line breaks or the format of the certificate information. **e.** In the **SP Entity ID** field, enter the “Audience URI (SP Entity ID)” that you recorded in the custom IDP portal. This field is required. The "SP Entity ID" value must match the “Audience URI (SP Entity ID)” value that you recorded in the IDP console. **f.** In the **Name ID format** field, specify the name identifier format to request from the IDP (for example, urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress). **g.** In the **Email claim** field, type `NameID`. This value must match the “NameID Format” that you specified in the IDP console. The Email address ensures the correct user is signing in to the management console. **h.** Specify any other optional settings. **i.** Click **Save**. **j.** Open the authenticator that you added. Record the **Single Sign On URL**. This URL will be added to the custom IDP.

Authentication method	Description
Duo MFA (Deprecated) Duo has ended support for their Traditional Duo Prompt. For more information, see the Duo Knowledge Base. If this authenticator has been added, it will be visible in the console as read only. For Duo multi-factor authentication, see Duo Universal MFA, below.	Select this option if you want users to authenticate using Duo multi-factor authentication. Before you add Duo as an authenticator, you should create an Auth API application. For instructions, see the information from Duo. Do the following: **a.** Enter a name for the authenticator. **b.** In the **DUO MFA Configuration** section, enter the API hostname, Integration key, and Secret key. You can find this information on the Applications tab in your organization's Duo account. For more information, see the Duo documentation.
Duo Universal MFA	Select this option if you want users to authenticate using Duo multi-factor authentication. Before you add Duo as an authenticator, you must create a Web SDK application. For instructions, see the Duo documentation. Do the following: **a.** Enter a name for the authenticator. **b.** In the **DUO Universal MFA Configuration** section, enter the API hostname, Client ID, and Client Secret. You can find this information on the Applications tab in your organization's Duo account. For more information, see the Duo documentation.
Okta MFA	Select this option if you want users to authenticate using Okta. Do the following: **a.** Enter a name for the authenticator. **b.** In the **Okta MFA Configuration** section, enter the Auth API Key and the Auth Domain. **c.** Click **Save**.
Okta (OIDC)	Select this option if you want users to authenticate using Okta. Do the following: **a.** In the drop-down list below **Okta**, select **OIDC**. **b.** Enter a name for the authenticator. **c.** In the **Identity Provider Client** section, enter the OIDC discovery document URL, the Client ID, and the Private key JWKS. **d.** Click **Save**.

Authentication method	Description
Okta (SAML)	Select this option if you want users to enter their Okta credentials in the primary sign-in page and enable IDP-initiated access to the Cylance console. For a walkthrough of the steps to configure your Okta (SAML), see the following: • Configure a new Okta (SAML): Configure the Okta (SAML) Authenticator for Enhanced Authentication • Enable Okta-initiated access for an existing Okta (SAML): Update the Okta (SAML) authenticator to enable IDP-initiated access to the Cylance console **Note:** The SSO Callback URL is generated when you save the authenticator and will be in the format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. **a.** In the drop-down list below**Okta**, select **SAML**. **b.** Enter a name for the authenticator. **c.** If you want users to validate their email with a one-time code when they log in for the first time, turn on **Validation required**. **d.** In the **Login request URL** field, enter the identity provider's single sign-on URL. **e.** In the **IDP signing certificate** field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. When you copy and paste the body of the certificate, make sure that you don't alter any line breaks or the format of the certificate information. **f.** In the **SP Entity ID** field, enter the “Audience URI (SP Entity ID)” that you recorded in the Okta portal. This field is required. The "SP Entity ID" value must match the “Audience URI (SP Entity ID)” value that you recorded in the IDP console. **g.** In the **IDP entity ID** field, paste the "IdentityProvider Issuer" that you recorded from Okta. **h.** In the **Name ID format** field, select the NameID format that you specified in the Okta (for example, urn:oasis:names:tc:SAML:2.0:nameid-format:persistent). **i.** In the **Email Claim** field, type `Email`. This must match the “Attribute” name that you configured in the Okta console. The Email address ensures the correct user is signing in to the management console. **j.** Specify any other optional settings. **k.** Click **Save**. **l.** Open the Authenticator that you added. Record the Single Sign On URL. This URL will be added to the following fields in the Okta console > SAML Settings screen. • Single Sign On URL • Requestable SSO URLs The SSO Callback URL is generated when you add the authenticator and will be in the format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>.

Authentication method	Description
One-Time Password	Select this option if you want users to enter a one-time password in addition to another type of authentication. You must add another authenticator to the authentication policy and rank it higher than the One-Time Password authenticator. For a walkthrough of the steps to add and remove one-time password authentication for administrators, see the following: • Add one-time password authentication for administrators • Remove one-time password authentication for administrators Do the following: **a.** Enter a name for the authenticator. **b.** In the **One-Time Password Configuration** section, in the first drop-down list, 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. **c.** In the **One-Time Password Configuration** section, in the second drop-down list, specify the number of times that users can skip the OTP app setup and authenticate without entering a code. When users log in to the console for the first time after you have enabled time-based one-time password authentication, they need to follow the instructions on the screen and use a QR Code to enroll with a multi-factor authentication app (such as Google Authenticator, Microsoft Authenticator, Okta Verify, or Authy).
Ping Identity (OIDC)	Select this option if you want users to authenticate using Ping Identity.Do the following: **a.** In the drop-down list below **Ping**, select **OIDC**. **b.** Enter a name for the authenticator. **c.** In the **Identity Provider Client** section, enter the OIDC discovery document URL, the client ID, and the private key JWKS. **d.** In the **ID token signing algorithm** drop-down list, select a signing algorithm. **e.** Click **Save**.

Authentication method	Description
Ping Identity (SAML)	Select this option if you want users to enter their Ping Identity credentials in the primary sign-in page and enable IDP-initiated access to the Cylance console. For a walkthrough of the steps to configure your Ping Identity (SAML), see the following: • Configure a new Ping Identity (SAML): Configure the Ping Identity (SAML) Authenticator for enhanced authentication • Enable Ping Identity-initiated access for an existing OneLogin (SAML): Update the Ping Identity (SAML) authenticator to enable IDP-initiated access to the Cylance console **a.** In the drop-down list below **Ping Identity**, select **SAML**. **b.** Enter a name for the authenticator. **c.** If you want users to validate their email with a one-time code when they log in for the first time, turn on **Validation required**. **d.** In the **Login request URL** field, enter the identity provider's single sign-on URL. **e.** In the **IDP signing certificate** field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. When you copy and paste the body of the certificate, make sure that you don't alter any line breaks or the format of the certificate information. **f.** In the **SP Entity ID** field, enter the “Entity ID” that you recorded in the PingOne console. This field is required. The "SP Entity ID" value must match the “Entity ID” value that you recorded in the IDP console. **g.** Specify any other optional settings. **h.** Click **Save**. **i.** Open the Authenticator that you added. Record the **Single Sign On** URL. This URL will be required in the following PingOne console, Configuration screen fields: • Assertion Consumer Service (ACS) • Application URL The SSO Callback URL is generated when you add the authenticator and will be in the format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>.

Authentication method	Description
IP Address	Select this option if you want to restrict users' access based on their IP address. You can create multiple IP address authenticators and use them to manage access for different groups, but you can only assign one IP address authenticator in a policy. For a walkthrough of the steps to add or remove IP Address restrictions for the console, see Add an IP Address restriction authenticator for the Cylance console. **a.** Enter a name for the authenticator. **b.** In the **IP address ranges** field, specify one or more IP addresses, IP ranges, or CIDRs. Separate entries with a comma. For example, IP range: 192.168.0.100-192.168.1.255 or CIDR: 192.168.0.10/24. **c.** Click **Save**.
OneLogin (OIDC)	Select this option if you want users to authenticate using OneLogin. Do the following: **a.** In the drop-down list below **OneLogin**, select **OIDC**. **b.** Enter a name for the authenticator. **c.** If you want users to validate their email with a one-time code when they log in for the first time, turn on **Validation required**. **d.** In the **OneLogin Configuration** section, enter the OIDC discovery document URL, the Client ID, Client Secret, and Authentication Method. **e.** Click **Save**.

Authentication method	Description
OneLogin (SAML)	Select this option if you want users to enter their OneLogin credentials in the primary sign-in page and enable IDP-initiated access to the Cylance console. **a.** Enter a name for the authenticator. **b.** If you want users to validate their email with a one-time code when they log in for the first time, turn on **Validation required**. **c.** In the **Login request URL** field, enter the identity provider's single sign-on URL. **d.** In the **IDP signing certificate** field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. When you copy and paste the body of the certificate, make sure that you don't alter any line breaks or the format of the certificate information. **e.** In the **SP Entity ID** field, enter the “Identifier (Entity ID)” that you recorded in the OneLogin console. This field is required. The "SP Entity ID" value must match the “Identifier (Entity ID)” value that you recorded in the IDP console. **f.** Specify any other optional settings. **g.** Click **Save**. **h.** Open the Authenticator that you added. Record the Single Sign On URL. This URL will be added to the following fields in the OneLogin console: • ACS (Consumer) URL Validator* • ACS (Consume) URL* • Single Logout URL The SSO Callback URL is generated when you add the authenticator and will be in the format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>.
FIDO	Select this option if you want users to register a FIDO2 device and use it verify their identity. Supported device types include smartphones, USB security keys, or Windows Hello. **a.** Enter a name for the authenticator. **b.** Click **Save**. When FIDO is the first factor of authentication and a user registers a device for the first time, a one-time password is also sent to the email address that they use to sign in. When FIDO is used as a second factor in a policy, a one-time password isn’t required when a user registers a device for the first time. For information about how to remove registered devices from a user account, see Remove a registered FIDO device for a user account in the Administration content.

Authentication method	Description
Local Account	Select this option if you want users to enter their BlackBerry Online Account (*my*Account) credentials. Do the following: **a.** Enter a name for the authenticator. **b.** Click **Save**.
Deny Authentication	Select this option if you want to use an authentication policy to prevent users or groups of users from accessing the Cylance console or another service. You can add another policy or an app exception to allow access to a subset of users. **a.** Enter a name for the authenticator. **b.** Click **Save**.

5. Click **Save**.

After you finish: Create an authentication policy.

Considerations for adding SAML authenticators

When you add a SAML authenticator, the login request URL and IDP signing certificate values are required. You should note the following considerations for optional fields.

Note: When you configure an external identity provider, you must add the Cylance Endpoint Security login request URL. The URL must be in the format of https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. Because external SAML configurations support a list of single sign-on or assertion consumer service reply URLs, in existing configurations, you can add the new or newly generated URL to the list as a secondary option or replace the original. If you created your authenticator before December 2023, and you want users to access the Cylance console using single sign-on, you must generate an updated login request URL. For more information on updating your authenticator, see Considerations for adding SAML authenticators.

Item	Description
NameID format	You can use this field to specify an optional name identifier format to request from the identity provider.
Federated ID claim	You can use this field to specify an optional claim value that is used as your federated ID to link accounts across systems. The default value is NameID. If your IDP is setup to return the email address in a claim other than “NameID”, you must specify the claim in this field. You should use a unique, immutable, and persistent value in this claim (for example, an objectGUID or UUID). Using a value that is not unique or susceptible to change like an email address is not recommended. When users log in, Cylance Endpoint Security will use the value in the Federated ID claim to create a unique ID for the user to map their identities in both systems. After you specify the value to use as the federated ID claim it cannot be changed because it is used to link a user in the external identity provider and Cylance Endpoint Security after they log in for the first time.
Active Directory claim	You can use this field to specify an optional claim value that is used to match Active Directory objectGUIDs across systems to validate users.

Item	Description
Email claim	You can use this field to specify an optional claim value that is used to match email addresses across systems. The default value is 'email'. Cylance Endpoint Security requires that all SAML responses must contain the users full email address, and it must match the email address that is registered with Cylance Endpoint Security. If your IDP is setup to return the email address in a claim other than “email”, you must specify the claim in this field. For example, if the claim configured in your IDP is called “emailAddress”, then you must set “emailAddress” in the Email Claim field. If these do not match, users cannot sign in.
SP entity ID	You can use this field to specify an optional service provider entity ID to send to the identity provider (also known as the issuer string). For Entra SAML authenticators this field is required, and the value that you enter must match the Identifier (Entity ID) in the SAML configuration in Entra.
IDP entity ID	You can use this field to specify an optional identity provider entity ID (also known as the IDP Issuer). If provided, the IDP issuer will be validated on all responses.
Accepted clock drift	You can use this field to specify, in milliseconds, the acceptable clock drift between client and server.
Signature algorithm	You can use this field to specify the signature algorithm for signing requests.
Signature private key	You can use this field to specify, in PEM format, an optional private key that is used to sign all outgoing requests.

Settings to 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

Settings to 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

Regenerate the enrollment secret for a user with OTP authentication

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 Cylance Multi-Tenant Console, click **Settings > Administration**.
2. Click the **Users** tab.
3. Search for and click the user that you want to regenerate the enrollment secret for.
4. Click **Regenerate Enrollment Secret**.
5. Click **Regenerate**.

Create an authentication policy

You create an authentication policy to specify the types of authentication that partner users must complete to sign in to the Cylance Multi-Tenant Console console. Users must complete the types of authentication in the order that you specify in the policy. For example, if you add Local Authentication before One-Time Password, users enter their BlackBerry Online Account credentials before they receive a one-time password prompt.

Before you begin: Add an authenticator.

1. On the menu bar, click **Settings > Administration**.
2. Click the **Authentication Policies** tab.
3. In the **User Authentication Policies** section, click **Add policy**.
4. Enter a name and description for the policy.
5. In the **Authentication rules** section, click **Add Authenticator**.
6. In the **Add authenticator** dialog box:
   a) Select an authenticator in the drop-down list and click **Save**.
   b) Repeat the previous step to add more authenticators to the policy.
   c) To set the order, click **Set Order** and drag the authenticators to the order that you want.
   d) Click **Set Order** again to save the order.
7. Click **Save**.

After you finish: Assign an authentication policy.

Assign an authentication policy

By default, the Default Authentication policy is assigned to partner users. You can assign User Authentication policies which you create to users.

Before you begin: Create an authentication policy

1. On the menu bar, click **Settings > Administration**.
2. Click the **Users** tab.
3. Search for the partner user that you want to assign an authentication policy to.
4. Beside the name of the user, in the **Authentication Policy** column, click the name of the authentication policy which is currently assigned.
5. In the **Assign user authentication policy** dialog, select the authentication policy that you want to assign.
6. Click **Save**.

Generate a new SSO callback URL for an authenticator

You can use the copy option to copy your current authenticator information and create new authenticator. When the new authenticator is saved, a new SSO callback URL is generated and associated with it.

Important: Complete this task only if you configured your environment for enhanced sign in, your authenticator was created before December 2023, and you want to enable the IDP-initiated single sign-on (SSO) to the console. To verify if the authenticator was created before December 2023, you can view the SSO callback URL that is in the current authenticator.

- If the SSO callback URL is in the format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>, no further action is required.

- If the SSO callback URL is “https://idp.blackberry.com/_/resume”, complete the following steps to generate the updated URL.

1. In the Cylance Multi-Tenant Console, go to **Settings > Administration**.
2. In the **Authenticators** tab, click the current IDP SAML authenticator that you need to update the SSO callback URL for.
3. In the top right corner of the screen, click the **Copy** icon.
4. Update the name of the copied authenticator.
5. Click **Save**.
6. Open the Authenticator that you copied. Record the **SSO callback URL**.
7. Delete the previous IDP authenticator.

After you finish: Edit the authentication policy to use the new authenticator. You can remove the authenticator that uses the old SSO callback URL.

View and manage your account

1. In the Cylance Multi-Tenant Console, on the top-right of the screen, click the **User Information** icon.
2. Do any of the following:

Task	Steps
Reset your password.	**a.** Click **My Profile**. **b.** Beside **Password**, click **Reset Password** **c.** Follow the instructions on the screen to reset your password.
View your account information.	Click **Account Overview**. The Account Overview page provides information about your Multi-Tenant Console user 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.
View the audit log.	You can view the audit log to see the partner account activity. Click **Audit Log**.

Managing alerts in the Cylance Multi-Tenant Console

The Alerts view gives you a comprehensive way to review alerts that are detected and correlated across all your tenants from a single partner account in the Cylance Multi-Tenant Console. This makes it easier for you to identify and track prevailing threat patterns in your corporate ecosystem and resolve collections of alerts more efficiently. The correlation of alerts across all tenants offers a more complete view of potential threats and allows for a more holistic approach to protecting your organization's employees and data.

The Alerts view is a superset of the alert groups found within each tenant. It augments the alert triage experience for individual tenants and contains a Tenant column that correlates an alert group to a specific tenant. For information on how to filter by tenant, see View and manage aggregated alerts. You can use the Alerts view to search, sort, and investigate alerts through a read-only experience. To access and operate on individual tenants within your organization, you can use the Tenants view from the Cylance console. When an individual alert within a group contains a **Detection Detail** button, this indicates that relevant cyber-security data is available from the Cylance console.

Service	Supported by the Alerts view
CylancePROTECT Desktop	Threat telemetry and memory protection alerts from the CylancePROTECT Desktop agent on desktop devices.
CylancePROTECT Mobile	Alerts detected by the CylancePROTECT Mobile app.
CylanceOPTICS	Alerts detected by the CylanceOPTICS agent on desktop devices.
CylanceGATEWAY	Network protection settings that you have configured or the destination reputations that CylanceGATEWAY has determined to be high risk.
CylanceAVERT	Exfiltration events from the CylanceAVERT agent on desktop devices.

The initial Alerts view is a summary that groups similar alerts based on criteria such as priority, alert classification, configured responses, and other key alert attributes. For more information about the criteria, see How the Cylance Multi-Tenant Console groups alerts.

The automated grouping of alerts reflects both the frequency and prevalence of alerts, giving analysts a clear view of how often threats occur and where they occur. By default, the alert groups are sorted in descending order by priority to provide a top-down view of all relevant security telemetry. Each group displays icons for the types of key indicator artifacts that are associated with the group (for example, File, Process, Email, and so on). You can click a key indicator icon to review the attributes of the key indicator, and, where applicable, you can copy or filter by those values. As new alerts are detected and processed from the telemetry sources, they are added to an existing group or to a new group.

The Alerts view supports single detection and multi-detection alerts. Alert detection rules can sometimes perform multiple detections before an alert is generated and displayed in the Alerts view. Each detection is modeled using an event (for example, File Opened, Registry Key Added, and so on).

You can click an alert group to access the following information:

- The alert overview tab that summarizes detection details and key indicators relevant to the group.
- The key indicators tab shows the detection attributes that were identical in each individual alert within the group. For example, if the key indicator was a file hash, that hash was detected in each alert, whether it was from the same device or different devices. The key indicators are represented visually to show the relationship between parent, child, and sibling objects. For multi-detection alerts, the key indicators are included within each event and are summarized in the order of execution.

- The list of individual alerts in the group. You can click an individual alert to open granular details. You can also view the full set of artifacts, represented as icons, that are associated with the alert. The artifacts contain the full set of facets captured by the underlying detection engine. Like key indicators, these artifacts are represented visually to show the relationship between parent, child, and sibling objects. For multi-detection alerts, the key indicators are included within each event and are summarized in the order of execution.

Depending on the types of alerts in a group, you may also be able to perform management actions. For example, for CylancePROTECT Desktop threat alerts, you can add a file to or remove a file from the global safe list or global quarantine list at the tenant level. The performed actions will only apply against the individual tenants.

How the Cylance Multi-Tenant Console groups alerts

The Cylance Multi-Tenant Console uses the following criteria to group alerts from all your tenants and Cylance Endpoint Security services, automating the process to allow you to scope and optimize your threat-hunting and resolution activities to logical groupings of related alerts. The grouping logic is built and maintained by BlackBerry, and is dynamically designed to handle alerts from a range of integrated services. The result is a zero-touch experience that automates frequency and prevalence analysis, making it easier for you to triage and prioritize your cybersecurity efforts.

A new alert is added to an existing alert group when all of the following conditions are met:

- The priority, classification, sub-classification, description, key indicators, and response of the alert match that group.
- The alert occurs within 24 hours of the most recent alert in that group.
- The alert is detected within 7 days (168 hours) of the oldest alert in that group.

A new alert group is created when an alert is detected that does not satisfy all of these conditions.

Priority

The priority of an alert, which correlates to the urgency of the issue and the potential impact on your organization's environment, is factored into how alerts are grouped. The Alerts view groups the highest priority alerts across the telemetry sources to help you view and resolve the most important alerts first.

The factors that determine the priority of an alert vary by service:

Service	Factors
CylancePROTECT Desktop	• For threat alerts, the priority is always high in the Alerts view, even if the priority of the alert is lower in Protection > Threats in the management console. The purpose of this elevated priority in the Alerts view is to indicate the urgency of malware detections. • For memory protection alerts, the priority is determined by the nature of the memory protection event, as configured by BlackBerry cybersecurity analysts. The priority of the events are based on the overall severity and relevance for investigation.
CylancePROTECT Mobile	Alerts use a priority value that corresponds to the severity that is displayed in the management console and in the CylancePROTECT Mobile app.
CylanceOPTICS	The priority is determined by the configuration of the CylanceOPTICS detection rules.

Service	Factors

CylanceGATEWAY	Priority is based on the network protection settings that you configure or the reputation of a destination, as determined by CylanceGATEWAY, with a high risk level. For example, CylanceGATEWAY might generate alerts to display in the Alerts view in the following scenarios:
	• Destination reputation detections:
	  • When enabled, the alerts are generated based on the risk level that you set. For example, if you set the risk level to "Medium and higher", alerts are generated for all the detections with the risk level of medium and high.
	  • When not enabled, alerts that are determined to have a high risk level are generated by default.
	• Signature detections:
	  • When enabled, alerts are generated for blocked signature detections and are displayed with a high risk level.
	  • When not enabled, CylanceGATEWAY will not generate alerts.
	• For DNS Tunneling and Zero Day detections, alerts are generated for detections with a high risk level.

CylanceAVERT	The priority is always high in the Alerts view.

Classification and sub-classification

The alert classification and sub-classification identifies and labels the underlying detection type to provide structured alert content that can better describe the alert detected by a given service. Each service will define a specific set of classifications and sub-classifications to clarify the nature of the alert.

Classification and sub-classification data are used to identify and group similar alerts.

The factors that determine the classification and sub-classification of an alert vary by service:

Service	Factors
CylancePROTECT Desktop	• For threat alerts, the classification and sub-classification correspond to the file classifications for CylancePROTECT Desktop threat alerts. • For memory protection alerts, the classification and sub-classification correspond to the memory protection violation types.
CylancePROTECT Mobile	The classification corresponds to an overall category of alerts (for example, Device Security or Network threats) and the sub-classification corresponds to the specific alert type that displays in the management console and in the app (for example, Malicious app, Sideloaded app, Insecure Wi-Fi, and so on).
CylanceOPTICS	Detection rules contain MITRE tactics, techniques, and sub-techniques to define the classification and sub-classification of an alert.
CylanceGATEWAY	The classification corresponds to the overall category of alerts (for example, Network Access Control) and the sub-classification corresponds to the specific alert type that displays in the management console (for example, Reputation, DNS Tunneling, Signature detection, and Zero-Day detection).

Service	Factors
CylanceAVERT	The classification is determined by the exfiltration event.

Description

The description of an alert is a characteristic that provides a short segment of information about the alert. Alerts with matching descriptions are more likely to be grouped together.

Key indicators

Key indicators are the detection content that are common across every individual alert in an alert group. The aggregation process compares the key indicators of alerts to determine whether they should be grouped together. For example, if a file contains a key indicator SHA256 hash, the hash value is identical within each alert inside an alert group.

The key indicators of an alert vary by service:

Service	Factors
CylancePROTECT Desktop	• For threat alerts, the key indicator is the SHA256 hash. • For memory protection alerts, the key indicators are the unique characteristics of the event (for example, file data such as the SHA256 hash and the risk score).
CylancePROTECT Mobile	Key indicators correspond to the unique characteristics of a given mobile alert (for example, the package name of a sideloaded app, the SSID of an insecure Wi-Fi network, the model of an unsupported device, and so on).
CylanceOPTICS	Key indicators are the uniquely identifying facets of the artifacts that are associated with an alert. For example, for process artifacts, the key indicators are the following facets: SHA256 hash, file path, and command line argument. These facets establish a unique signature for the process artifact type that can be compared to other alerts. The key indicator facets for an alert group are common across the individual alerts in the group.
CylanceGATEWAY	The key indicators are "Network connection" and "DNS request".
CylanceAVERT	The key indicators vary by the artifact type. For email alert artifacts, the key indicator is the conversationID. For browser and file exfiltration alert artifacts, the key indicator is the UserName.

Response

For services that execute mitigation actions, this is the action that you configured the service to execute in response to the detection. For example, for CylancePROTECT Desktop threat alerts, a response may be one of the following: waived, quarantined, unsafe, or abnormal.

For services that don't execute mitigation actions, this captures relevant information from the integrated service. Alerts with matching responses are more likely to be grouped together.

Time

The time that an alert occurs relative to other alerts is factored into how alerts are grouped. An alert is added to an existing group if the priority, classification, sub-classification, description, key indicators, and response of the alert match that group, the alert occurs within 24 hours of the most recent alert in that group, and the alert occurs within 7 days (168 hours) of the oldest alert in that group. If the alert matches the above criteria but occurs outside of the 24 hour window from the most recent alert in the group, or outside of the 7 day window from the oldest alert in the group, it is added to a new group.

The 7 day window ensures that alert groups have a fixed period and do not grow indefinitely.

View and manage aggregated alerts

Before you begin: Verify that your administrator role has the permissions required to use the Alerts view. The permissions for the Alerts view are contained in the Common section. The View alerts permission provides read-only access to the Alerts view. You require the Edit alerts and Delete alerts permissions to make changes to alert groups and individual alerts in this view. For more information, see Setting up administrators.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Alerts**.

   To select the columns that you want to display, scroll to the right and click |||.
2. Do any of the following:

Task	Steps

Filter and sort alert groups.	**a.** Click ⏷ on a column and type or select the filter criteria. You can do any of the following:
	• Apply multiple filter criteria at once. To remove a filter, click x for that filter.
	• If you want to filter by Classification, Sub-classification, Description, or Key Indicators, do one of the following:
	  • To find exact matches, click ⚙ > **is equal to**. Type a value to view matches. Click up to 5 matches to add to the filtering list, then click **Apply**.
	  • To find matches that contain the specified value, click ⚙ > **contains**.
	  Type one or more values (click + to add additional values). Click **Apply**.
	  When you view the results, you can click the filter displayed at the top of the screen to add or remove filter criteria.
	• If you filter by **Count**, click ⚙ for additional options (greater than, less than, and so on).
	• Filter by **Product** to scope results to specific Cylance Endpoint Security services.
	• Filter by **Detection Time** to scope results to a specific date and time range.
	• Filter by **Tenant** to scope results from a specific tenant.
	b. To sort the alert groups in ascending or descending order by a column, click the name of the column (where applicable).

Task	Steps
View details for key indicators of an alert group and filter alert groups by key indicator type or value.	**a.** Hover over a key indicator icon to see the type of object or event. Click an icon to view details. **b.** Where applicable, to view the full text of a truncated string value, hover over it and click . **c.** Where applicable, to copy a value, hover over it and click . **d.** To filter alert groups by key indicator, hover over it and click .
View details for an alert group and individual alerts.	**a.** Click an alert group. **b.** To view the details for key indicators associated with the group, in the left pane, click **Key Indicators**. Expand the key indicators to review details and view relationships between instigating and target objects. This view will show a single set of key indicators associated with individual events (files, users, executables, processes, and so on). For example, you may see a "parent" process object or executable file that is the instigating process for a "child" process. Events or objects at the same level are considered "siblings" under the same parent. Where applicable, you can hover over values and click to view full text strings or to copy the value. **c.** For the individual device alerts, do any of the following: • Sort and filter the alert information. • Add or change labels for the alerts. The alert status and assigned user can be managed through the individual tenant. **d.** To open the details panel for an individual alert, click the alert. Do any of the following: • If applicable, you can click **Detection Detail** to view further details and actions from a tenant's Cylance console with support login. The Detection Detail link will remain active for 60 days for CylancePROTECT Desktop threat alerts and for 30 days for other types of alerts. • Expand the artifacts associated with the alert to review details and view relationships between instigating and target objects and events. The complete set of objects associated with a detection rule are included in the artifacts view. Where applicable, you can hover over values and click to view full text strings or to copy the value.
Change the status of alert groups.	Do any of the following: • To change the status of an alert group, in the **Status** drop-down list, click the appropriate status. • To change the status of multiple alert groups, select the alert groups, click **Change Status**, click the appropriate status, and click **Apply**. See Status changes for alerts.

Task	Steps
Add or change the label for alert groups.	You can add custom labels to alert groups to provide short notes or reminders or to use as filter criteria. To view labels you must set the Labels column to display. **a.** Select one or more alert groups. **b.** Click **Change Labels**. **c.** Type a label and press ENTER or search for and select an existing label. **d.** Click **Apply**. To remove a label, click the x icon, and click **Apply**.
Export alert data to a CSV file.	Do any of the following: • To export details for all alert groups, click . • To export details for all of the alerts within a group, click an alert group, then click .
Remove alert groups.	**a.** Select one or more alert groups. **b.** Click **Delete**. **c.** Click **Delete** again to confirm.

Status changes for alerts

The status of individual alerts from various sections of the Cylance console (for example, Protection > Threats, CylanceOPTICS > Detections, and Protection > Protect Mobile alerts) correspond to an equivalent status in the Cylance Multi-Tenant Console Alerts view. When an alert status changes from the Cylance console, the status is also updated in the Alerts view. For example, if the status of an alert in the Cylance Detections view changes to False Positive, the status in the Alerts view changes to Closed.

When you change the status of individual alerts in the Alerts view, an equivalent status change is displayed in the Cylance Detections view for CylanceOPTICS. Currently, status changes that you initiate in the Alerts view will not be displayed in the Protection > Threats view or in the Protection > Protect Mobile alerts view in the Cylance console.

Note the following equivalent states from the Cylance console for CylancePROTECT Desktop threat alerts:

- Alerts displayed in Protection > Threats with an Unsafe, Abnormal, or Quarantined status have a New status in the Alerts view.
- Alerts displayed in Protection > Threats with a Waived status have a Closed status in the Alerts view.

If you set a status for an alert group, the individual alerts in that group are assigned the status that you selected. If the individual alerts in an alert group have different statuses, either from manual status changes or as a result of status changes that come from another view (for example, CylanceOPTICS > Detections), the status of the alert group changes to Multiple. If all of the individual alerts in an alert group have the same status, the alert group will also have the same status. For example, if all of the individual alerts have a status of Closed, the status of the alert group is also Closed.

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, on the menu bar, click **Tenants**.
2. Click the **Active Tenants** tab.
3. Click **Add New Tenant**.
4. In the **Tenant name** field, type the name for the tenant.
5. In the **Short name** field, type a short name for the tenant. Valid characters are lowercase letters, 0 to 9, and hyphen (-) with no spaces.
6. Optionally, in the **Unique admin email address** field, type the email address of the tenant admin user.
7. In the **Address** section, specify the tenant's address information.
8. In the **License Usage** section, specify the total number of licenses granted for each service, the service term, and license type.

   The CylancePROTECT license count is required when you add licenses to a tenant.
9. In the **Tenant Features** section, choose the features or services that you want to turn on for the tenant.
10. In the **Tenant Services** section, turn on additional services such as CylanceOPTICS and CylanceGATEWAY.
11. 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, return to the **Active Tenants** tab and search for the tenants.
- To edit a tenant, on the **Active Tenants** page, click the tenant that you want to edit. Make your changes, click **Submit**.

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**.

Manage tenant services

In the Cylance Multi-Tenant Console, you can control which services are available for your tenants. If you disable a tenant service, it will be marked for removal after a 30-day grace period, but you can request to cancel the removal within that time. The services marked for removal will continue to work as normal during the grace period.

1. In the Cylance Multi-Tenant Console, click **Tenants**.
2. On the **Active Tenants** tab, click a tenant.
3. Click the **Features and Services** tab.
4. In the **Tenant Features** section, choose any of the features you want to make available for the tenant.
    - Custom application integration: Enable this option to display the Integration page in the console Settings menu. When enabled, you can use the Cylance User API to programmatically manage the Cylance Multi-Tenant Console settings and configurations. For more information, see Enable access to the Cylance User API.
    - Data privacy: Enable this option to display the Data privacy setting in the device policy on the Tenant Configurations > Policies > Device Policy page. When enabled, you can specify the data that you want to block the agent from sending to the Cylance console. For more information, see Create a device policy template.
5. In the **Tenant Services** section, choose the services you want to enable or disable for the tenant.
6. To save your changes, click **Save**.

After you finish:

- A message banner indicating a disabled service will be displayed on the tenant's console during the grace period.
- The removal date of a disabled service will be displayed in the **Service Pending Removal** column on the **Active Tenants** tab.

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 **Submit**.

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 the tenant user that you want to edit. Click **Save**.
- 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 allows you to conveniently log in to a tenant's Cylance console as the tenant or a tenant user to manage their account. With support login, you don't need a password to log in and can only view and modify what the tenant or tenant user's permissions allow.

The audit log in both the Cylance Multi-Tenant Console and the Cylance console will record the email addresses of the partner user used to initiate the support login and the tenant user that was used to log in.

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**.

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, control tenant services, 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.

Create a partner user

When you create a partner user, an invitation email is sent to the user's email address with a registration link that allows them to complete the registration and create a password for their account if required.

1. In the Cylance Multi-Tenant Console, on the menu bar, click **Settings > Administration**.
2. On the **Users** tab, click **Add Partner User**.
3. Specify the required information.
4. In the **Partner** drop-down list, select the partner account that they belong to.
5. In the **Role** drop-down list, click the appropriate role for the partner user.
6. Click **Save**.

After you finish:

To change the role assigned to a user, on the **Roles** tab, click the user whose role you want to modify. Change the role and click **Save**.

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 **Settings > Administration**.
2. On the **Roles** tab, click **Add Role**.
3. Type a name for the role.
4. Select permissions for the role. For more information about the available permissions, see Permissions for user roles.
5. Click **Save**.

After you finish: To edit a partner role, on the **Roles** tab, click the role that you want to modify. Modify the permissions and click **Save**.

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
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 information	This permission allows users to create or modify tenants in the console.
Shutdown tenants	This permission allows users to shutdown a tenant.
Ability to import/migrate tenants from venue	This permission allows users to import or migrate tenants from venue.
Delete tenants	This permission allows users to delete tenants.

Support Login

These permissions relate to the Support Login feature in the Cylance Multi-Tenant Console. When logging in with Support Login, the role of the tenant user used to log in is inherited regardless of a partner user's role.

Permission	Description
Support Login as tenant user	This permission allows a partner to log in with a tenant user's account as if they were the tenant user. The tenant user's account must also be assigned the tenant User role for the partner to log in.
Support Login as tenant admin	This permission allows a partner to log in with a tenant user's account as if they were a tenant administrator. The tenant user's account can be assigned any default role for the partner to log in.
Support Login as tenant zone manager	This permission allows a partner to log in with a tenant user's account as if they were a tenant zone manager. The tenant user's account must also be assigned the tenant Zone Manager role for the partner to log in.
Support Login as tenant read only	This permission allows users to log in with a tenant user's account as if they were a tenant read only user. The tenant user's account must also be assigned the tenant Read only role for the partner to log in.

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.

Permission	Description
Delete users	This permission allows users to delete users from the console.

Partner

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

Permission	Description
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.
Ability to approve creation of tenants	This permission allows users to approve the creation of tenants.

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.

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.

Policy-Template

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

Permission	Description
View policy template list	This permission allows users to view a list of policy templates in the console.
Read policy template details	This permission allows users to read the policy template details, including the policy settings.
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.

Alerts view

These permission relate to the Alerts screen in the Cylance Multi-Tenant Console.

Permission	Description
Read alerts	This permission allows users to read alerts in the console.
Update alerts	This permission allows users to update alerts in the console.
Delete alerts	This permission allows users to delete alerts in 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.

Audit

These permission relate to the audit logs in the Cylance Multi-Tenant Console.

Permission	Description
View audit list	This permission allows users to view the audit log in the console.

Create a report

You can create custom reports with the data collected across all your tenants.

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	Reports user activities performed in the console.
Account Data	Reports data regarding user accounts.
Partner User	Reports data regarding partner users.
Tenant Devices	Reports data regarding tenant devices.
Tenant Detections	Reports data regarding detected threats.
Tenant User	Reports data regarding tenant users.
Policy Details	Reports data regarding device policies.
Health Report	Automatically reports data regarding the health of your environment on a monthly basis. You can download the reports from the **Reports > Recently Run** tab.

5. In the **Report Fields** section, select the desired report fields.
6. In the **Report Filters** section, select the desired filter and configure it's parameters if needed.
7. If you want to specify a schedule to run a report, 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.** Select the recurrence period. **c.** Set the start and end dates you want the report to run on.

8. Do one of the following:
   - To save and run the report, click **Save and Run Report**.
   - To save the report without running it, click **Save & Finish**. You can run a saved report from the **Reports** tab by clicking  beside the desired report.
9. To view and download recently generated reports, on the **Reports** page, click **Recently Run**.

After you finish:

- You will receive an email notification after a report is generated and available to view.

- To edit a report, on the **Reports** tab, click beside the desired report.

Managing device policies

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. 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 **Tenant Configurations > Policies**.
2. On the **Device Policy Templates** tab, click **Add Template**.
3. Type a name for the template.
4. Configure the device policy settings.

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

   Data privacy: The Data privacy option can be found in the Tenant Configurations > Policies > device policy, Data Privacy tab. You can enable this option and select the fields for which the agent will not send the associated data (for example, IP address, username, and hostname or FQDN) to the Cylance console. Note that when enabled, this feature might affect other functions such as the "Auto-upload of log files" on the Agent Settings tab will be disabled.
5. Click **Save**.

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** tab, 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 Using device policies to manage CylancePROTECT Desktop devices in the Cylance Endpoint Security Setup guide.

Managing 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

You can create a linked policy template so that when you update the template, it is automatically updated for all tenants that it is applied to.

1. In the Cylance Multi-Tenant Console, click **Tenant Configurations > Policies**.
2. On the **Linked Device Policy Templates** tab, click **Add 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 default 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. Configure the device policy settings.

   For more information about each device policy setting, see the Device policy documentation.
6. Click **Create**.

After you finish: Link a linked policy template with multiple tenants

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.

Before you begin: Create a linked policy template

1. In the Cylance Multi-Tenant Console, click **Tenant Configurations > Policies**.
2. On the **Linked Device Policy Templates** tab, click a linked policy template.
3. Click the **Linked Tenants** tab.
4. Click **Link Tenant**.
5. Select the tenants that you want to link the policy template to. You can filter the list of tenants.
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 **Tenant Configurations > Policies**
2. Click the **Linked Device Policy Templates** tab.
3. Click a tenant.
4. Click the **Linked Tenants** tab.
5. Select the tenants that you want to unlink the linked policy template from.
6. 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 **Tenant Configurations > Policies**.
2. On the **Linked Device Policy Templates** tab, click a linked policy template that you want to update.
3. Make your changes to the template.

   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 **Tenant Configurations > Policies**.
2. On the **Linked Device Policy Templates** tab, select a linked policy template that you want to delete.
3. Click **Delete**.
4. Click **Remove**.

Create a bulk update request

You can update the agent version update rules of your tenants simultaneously by submitting a bulk update request.

1. In the Cylance Multi-Tenant Console, click **Tenant Configurations > Agents**.
2. Click the **New Bulk Update Request** tab.
3. In the **New Request For Bulk Agent Update** section, click **Select Tenants**.
4. Select the desired tenants and click **Save**.
5. Click **Select Update Rules**.
6. In the **General Information** section, select a rule name. The supported rules are Test, Pilot, and Production.
7. In the **Assign Zones** section, enter a zone name and press the Enter key to complete specifying the zone. You can enter multiple unique zone names (the values that you enter are not case-sensitive). The specified list of zones will replace all the zones currently assigned to the rule in the target tenant. If a specified zone does not exist in the target tenant, the zone will be skipped and indicated in the status report. If none of the specified zones exist, the rule update will fail.
8. In the **CylancePROTECT** and **CylanceOPTICS** sections, choose the update settings for the respective agents.

   The CylancePROTECT and CylanceOPTICS versions can be set to Auto Update for the Production rule, however in this case your bulk update request cannot include Test and Pilot rules at the same time. If CylanceOPTICS is not enabled in the target tenant, the rule update will only be performed for the specified CylancePROTECT version. If the selected CylancePROTECT and CylanceOPTICS versions are not available in the target tenant, the rule update will not be successful.
9. Click **Select**.
10. If you want to add additional tenants or rules, repeat the previous steps.
11. When all your tenants and rules have been added, click **Submit**.

After you finish:

- While the agent bulk update is in progress, you cannot make any new updates until it is finished.
- You will receive an email notification when the bulk process is complete.
- On the **Bulk Update History** tab, you can download the status report of your bulk request and view your previous bulk update requests from the last 30 days.

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 is 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.

Viewing CylanceMDR dashboards in the Cylance Multi-Tenant Console

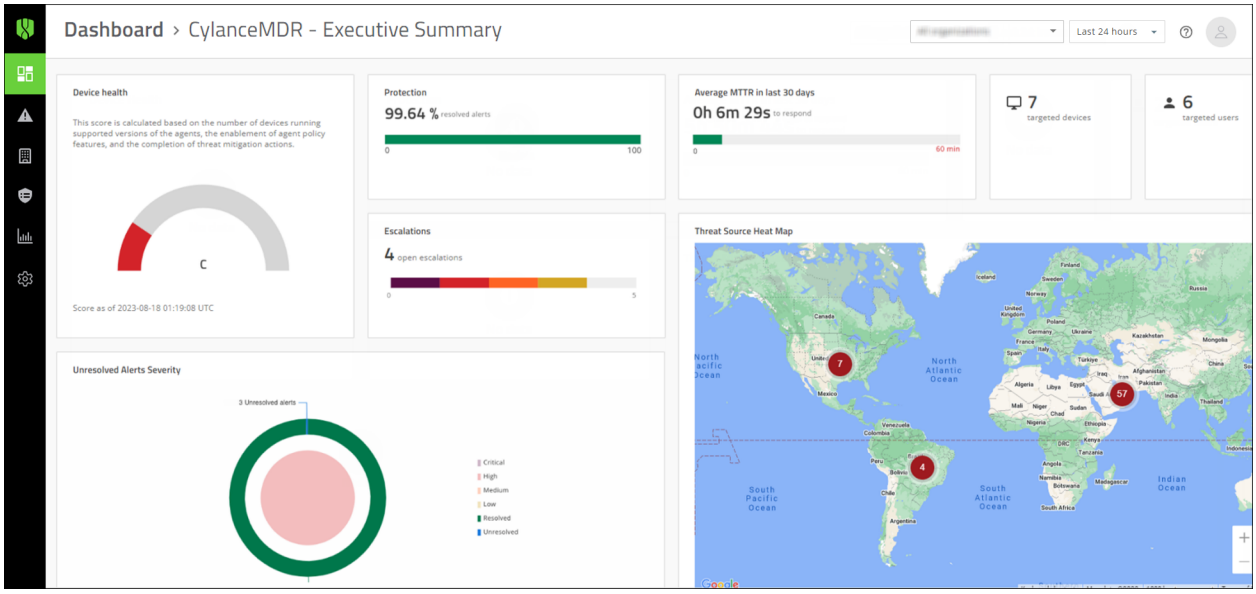
The dashboard pages for CylanceMDR in the Cylance Multi-Tenant Console have an interactive layout that visually displays the various types of alerts that were escalated to an organization, as well as top threats by alert type or target.

You can filter the data by organizations that you are managing and set the timeframe to limit the data that is presented on the dashboard. For example, you can limit the data to the last 24 hours so that you view only a list of escalations that occurred in that timeframe. These settings can be found on the top right of the Dashboard page. If there is no data available according to the specified timeframe, the widget will display "No data".

The following dashboard views are available out of the box:

- **Executive Summary**: This view provides a high level view of the overall protection status and threat landscape, such as visualizations of open and resolved alerts, as well as a map of threat sources.
- **Operations**: This view provides a quick report of the open escalations and top types of threats allowing users to target high-priority threats and resolve them as soon as possible.
- **Threat Summary**: This view provides a quick report of the number of incidents, escalated incidents, open escalations, and the top rules that were applied to fewest devices, allowing users to see the effectiveness of their threat strategy and take necessary actions.

Executive Summary dashboard

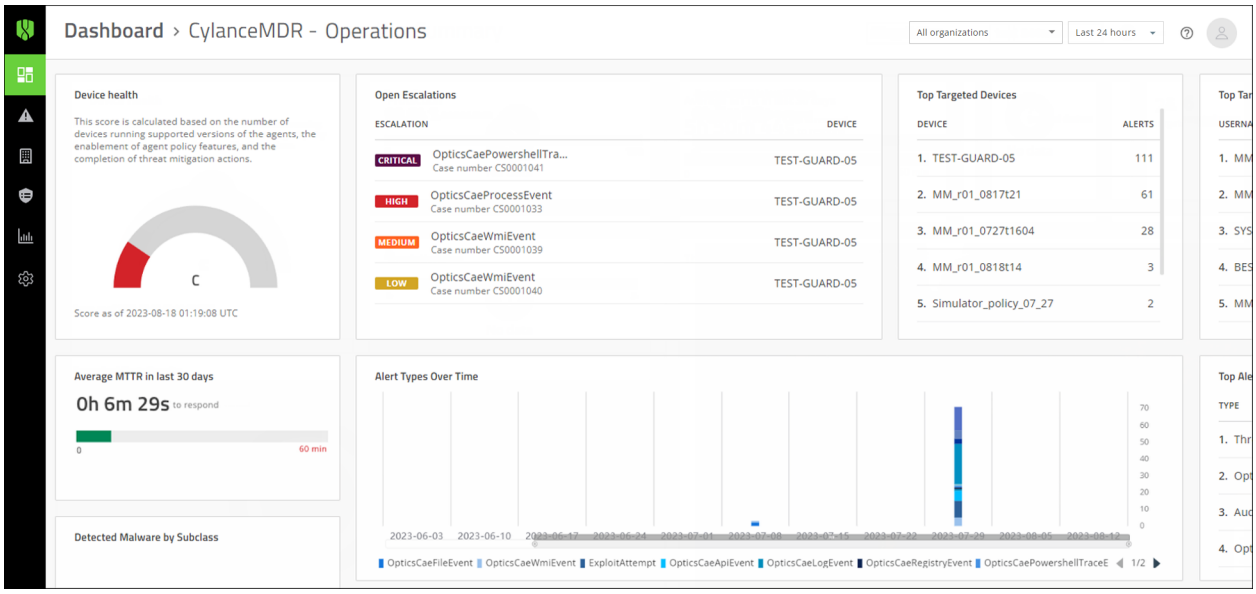


The following alert metrics are displayed in the Executive Summary tab of the dashboard:

- **Device health**: View a score that is calculated based on the number of devices running supported versions of the Cylance agents, the enablement of agent policy features, and the completion of threat mitigation actions.
- **Protection**: View the current percentage of alerts that are resolved.
- **Escalations**: View a graph of escalations to see the ratio of unresolved threats by severity, as well as threats that were already resolved. You can click on parts of this widget to view a list of all open escalations, or view a list of open escalations of a specific severity. Escalations are alerts that are brought to the attention of the organization.

- **Average MTTR in last 30 days**: View the average time for analysts to escalate and close alerts in the last 30 days.
- **Targeted users**: View the number of users that were targeted.
- **Targeted devices**: View the number of devices that were targeted.
- **Unresolved Alerts Severity**: View a graph that shows the status of overall alerts by severity. At a glance, you can see the ratio of resolved and unresolved alerts. Unresolved alerts are incoming alerts that CylanceMDR analysts are working on that may or may not be escalated to the organization for attention.
- **Threat Source Heat Map**: View a map of threat sources to understand where attacks are originating from. You can click the numbers that appear on the map to see the severity of threats for each geographic area.

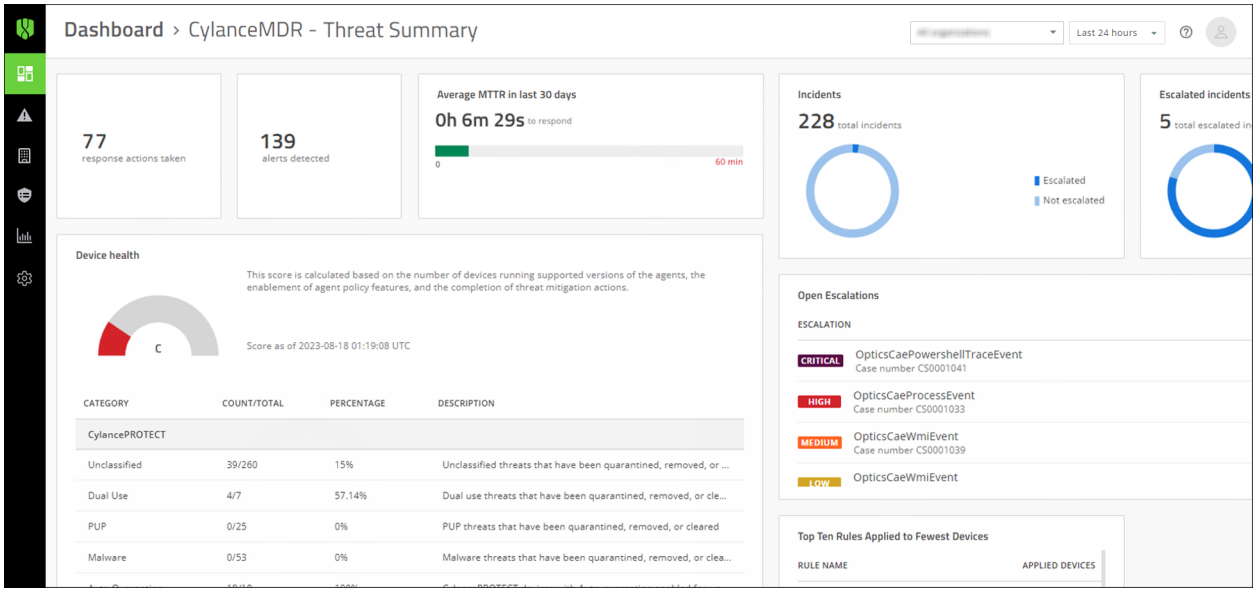
Operations dashboard



The following alert metrics are displayed in the Operations tab of the dashboard:

- **Device health**: A score that is calculated based on the number of devices running supported versions of the Cylance agents, the enablement of agent policy features, and the completion of threat mitigation actions.
- **Average MTTR in last 30 days**: View the average time for analysts to escalate and close alerts in the last 30 days.
- **Open Escalations**: View a list of open escalations that might require your attention, such as those with critical and high severity. You can click on an alert to quickly jump to its details.
- **Top Alert Types**: View the top alert types to see the alert types (such as memory exploit attempts, script control threats, and network threats) that are reported most frequently in the organization.
- **Detected Malware by Subclass**: View the top malware types by subclass, such as whether a threat was a trojan, virus, or worm.
- **Top Scripts Convicted**: View the top scripts to see the scripts that are run the most often in the organization that are also generating alerts. Hover over a script in the list to see the full directory path to the script.
- **Alert Types Over Time**: View the top alert types that have occurred over a period of time. You can adjust the timeframe by sliding the bar below the x-axis and click the alert types to show or hide them in the graph.
- **Top Targeted Processes**: View the top targeted processes to see the processes that are most often targeted by threats.
- **Top Targeted Devices**: View the top targeted devices to see the devices that are generating the most alerts.
- **Top Targeted Users**: View a list of users that have encountered the most threats.
- **Top Response Actions By Type**: View a list of the top response actions that were used to resolve threats.

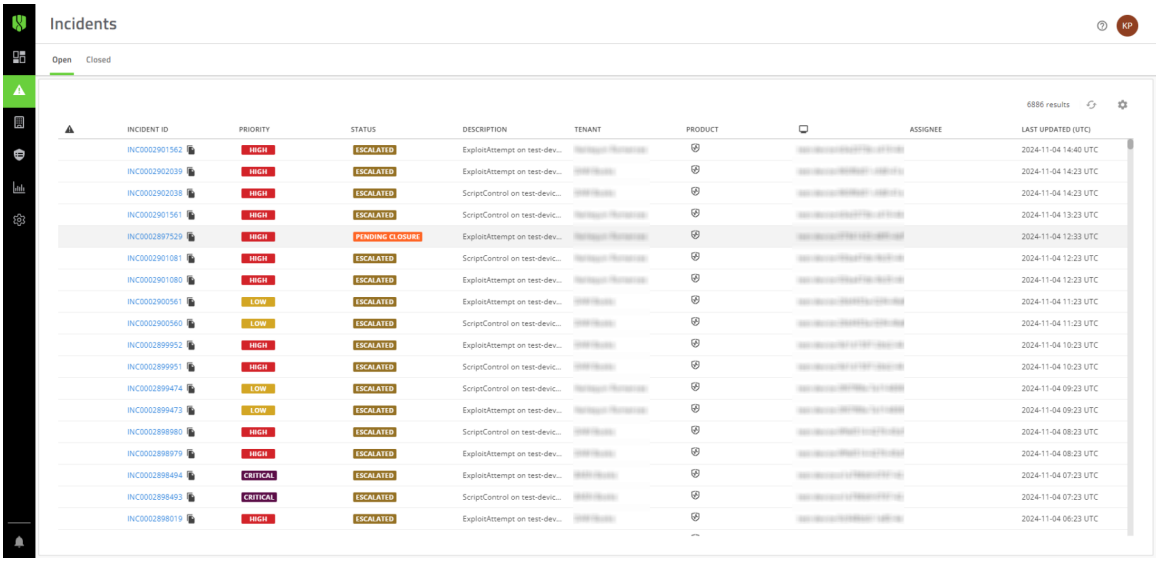
Threat Summary dashboard



The following alert metrics are displayed in the Operations tab of the dashboard:

- **Response actions taken**: The number of actions taken within the specified timeframe.
- **Alerts detected**: The number of alerts detected within the specified timeframe.
- **Average MTTR in last 30 days**: View the average time for analysts to escalate and close alerts in the last 30 days.
- **Incidents**: View the total number of incidents that were escalated and not escalated.
- **Escalated incidents**: View a list of incidents that were recently escalated.
- **Device health**: A score that is calculated based on the number of devices running supported versions of the Cylance agents, the enablement of agent policy features, and the completion of threat mitigation actions.
- **Open Escalations**: View a list of open escalations that might require your attention, such as those with critical and high severity. You can click on an alert to quickly jump to its details.
- **Top Ten Rules Applied to the Fewest Devices**: View a list of CylanceOPTICS rules that were applied to the fewest devices.

Managing CylanceMDR incidents in the Cylance Multi-Tenant Console



If an organization is subscribed to CylanceMDR Standard, Advanced, or Pro, analysts monitor alerts for them and will escalate the alerts as incidents to them if they require attention. When an analyst identifies a threat and escalates it to an organization, designated escalation groups in the organization are notified and you can view them on the Alerts > Incidents page in the Cylance Multi-Tenant Console.

If an organization is subscribed to CylanceMDR On-Demand, you must manually request CylanceMDR support from the details screen of an alert from the Alerts page. These requests are escalated to CylanceMDR analysts so they can investigate. You can follow up on these requests from the Alerts > Incidents page in the Cylance Multi-Tenant Console console.

On the Incidents page, you can do the following:

- In the Open or Closed tabs, click an incident in the list to view its details.
- Click beside one of the columns to filter the results. For example, you can filter certain tenants.
- Click to select the fields that you want to display.
- Export the current list of incidents to a .csv file, or print it as a PDF.

Respond to escalated incidents in the Cylance Multi-Tenant Console

When an incident is escalated to an organization, its details need to be verified to determine whether the incident was expected behavior in your environment. You can use the chat feature to communicate with a CylanceMDR analyst to share information and take appropriate steps to resolve the incident.

1. In the Cylance Multi-Tenant Console console, click **Alerts > Incidents**.
2. Click the **Open** tab.
3. Click an incident.
4. Do any of the following:

Task	Steps
Report whether the incident was expected or unexpected	If you confirm that the incident was based on expected behavior, the incident will be automatically closed. If you report that it was from unexpected behavior, you will be presented additional information and recommended actions to help resolve the threat. **a.** In the dialog message at the top of the screen, click **Expected** or **Unexpected**. **b.** Confirm your selection.
Assign the incident to an administrator user	**a.** In the left pane, in the **Assignee** field, search for and select another administrator user. **b.** Click **Save**.
Send a message to a CylanceMDR analyst	**a.** In the right pane, click ▭. **b.** Type your message. **c.** Click **Add**.
Upload attachment to this incident	**a.** In the right pane, click ⚭. **b.** Click **Upload**. **c.** Select the file that you want to upload.
View the history of this incident	In the right pane, click ⟲. A history of activity for this incident is displayed.
Close an incident	Send a message to the CylanceMDR analyst (using ▭) indicating that you want to close the incident. When an incident is closed, it cannot be reopened. You can find closed incidents in the **Closed** tab.

Manage CylanceMDR escalation groups

You can add partner administrators to CylanceMDR escalation groups so that when a CylanceMDR analyst escalates an incident, the appropriate partner administrators are notified based on the severity status of the incident. For example, when the severity of an incident is set to High, members that are in the "-High" escalation group receive a notification.

You can only manage other partner administrators in escalation groups for the organizations that you manage from the Cylance Multi-Tenant Console. Escalation groups for customer administrators are managed from the Cylance console.

Before you begin: You must be a partner administrator to manage escalation groups.

1. Click **Settings > Administration**.
2. Click the **CylanceMDR Escalation Groups** tab.
   Escalation groups are listed for each of the organizations that you can manage.
3. In an organization's section, click the escalation group that you want to manage.
4. To add a member to the group, click **Add member**.

5. Search for and select the administrators that you want to add.
6. Click **Submit**.

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