



Cylance Endpoint Security

Setup Guide

Contents

- Configuring a new Cylance Endpoint Security tenant.....7**
 - Default configuration settings for a new Cylance Endpoint Security tenant..... 8
 - Export, import, or reset the configuration of a Cylance Endpoint Security tenant..... 11
- Cylance Endpoint Security requirements..... 13**
 - Requirements: Cylance console..... 13
 - Requirements: CylancePROTECT Desktop..... 13
 - Root certificates required for the CylancePROTECT Desktop agent for Windows..... 17
 - Requirements: CylanceOPTICS..... 18
 - Requirements: CylancePROTECT Mobile app..... 22
 - Requirements: BlackBerry Connectivity Node..... 22
 - Requirements: CylanceGATEWAY Connector..... 23
 - Requirements: CylanceGATEWAY agents..... 23
 - Requirements: CylanceAVERT..... 24
 - Cylance Endpoint Security network requirements..... 24
 - Cylance Endpoint Security proxy requirements..... 30
- Accessing the management console and configuring authentication.....32**
 - Logging in to the management console..... 32
 - Enhanced authentication sign in..... 32
 - Sign in to the Cylance console using enhanced authentication..... 35
 - Generate a new SSO callback URL..... 36
 - Using authentication policies to access the Cylance console and activate agents..... 36
 - Add an authenticator..... 37
 - Manage the default authentication policies for your tenant..... 49
 - Create an authentication policy..... 49
 - Custom authentication..... 50
 - Configure custom authentication..... 51
 - Custom authentication descriptions..... 51
 - Migrate external IDPs from Custom Authentication to an authenticator..... 51
 - Migrate custom authentication settings to the authenticators list..... 52
- Setting up administrators.....55**
 - Add an administrator..... 55
 - Permissions for administrator roles..... 56
 - Managing roles..... 64
 - Add a role..... 64
 - Configure the session and idle timeout limits..... 64
- Setting up zones to manage CylancePROTECT Desktop and CylanceOPTICS.. 66**
 - Add and configure a zone..... 66

| | |
|--|----------------|
| Setting up CylancePROTECT Desktop..... | 69 |
| Testing your CylancePROTECT Desktop deployment..... | 69 |
| Create a CylancePROTECT Desktop test policy..... | 70 |
| Exclusions and when to use them..... | 72 |
| Create and manage a device policy..... | 74 |
| Device policy: Malware Protection settings..... | 75 |
| Device policy: Memory Protection settings..... | 80 |
| Device policy: Script Control settings..... | 89 |
| Device policy: External Device Control settings..... | 96 |
| Device policy: Application Control settings..... | 98 |
| Device policy: Agent Settings..... | 99 |
| Installing the CylancePROTECT Desktop agent for Windows..... | 100 |
| Install the Windows agent..... | 101 |
| Windows installation parameters..... | 101 |
| Installing the CylancePROTECT Desktop agent for macOS..... | 104 |
| Install the CylancePROTECT Desktop agent for macOS..... | 105 |
| Troubleshooting macOS installations..... | 109 |
| Installing the CylancePROTECT Desktop agent for Linux..... | 110 |
| Linux installation prerequisites..... | 111 |
| Install the Linux agent automatically..... | 113 |
| Install the Linux agent manually..... | 114 |
| Updating the Linux driver..... | 115 |
| Upgrade the Linux agent manually..... | 117 |
| Linux commands for the agent..... | 118 |
| Troubleshooting Linux agent installations..... | 118 |
| Require users to provide a password to remove the CylancePROTECT Desktop and CylanceOPTICS agents..... | 120 |
| Setting up CylanceOPTICS..... | 121 |
| Install the CylanceOPTICS agent on devices..... | 121 |
| Configuration requirements for macOS 11.x and later..... | 122 |
| OS commands for the CylanceOPTICS agent..... | 123 |
| Enable and configure CylanceOPTICS..... | 126 |
| CylanceOPTICS sensors..... | 127 |
| CylanceOPTICS optional sensors..... | 128 |
| Data structures that CylanceOPTICS uses to identify threats..... | 132 |
| Managing updates for the CylancePROTECT Desktop and CylanceOPTICS agents..... | 143 |
| Manage updates for the CylancePROTECT Desktop and CylanceOPTICS agents..... | 144 |
| Best practices for deploying CylancePROTECT Desktop on Windows virtual machines..... | 146 |
| Requirements and considerations for using CylancePROTECT Desktop on virtual machines..... | 146 |
| Deploy CylancePROTECT Desktop on virtual machines..... | 148 |
| Update CylancePROTECT Desktop on cloned devices..... | 149 |

| | |
|---|------------|
| Using RMM solutions to install the Cylance agents on devices..... | 150 |
| Use Datto RMM to install or remove the Cylance agents..... | 150 |
| Use Kaseya VSA 10 to install or remove the Cylance agents..... | 151 |
| Installing the BlackBerry Connectivity Node..... | 154 |
| Set an environment variable for the Java location..... | 154 |
| Download the installation and activation files for the BlackBerry Connectivity Node..... | 155 |
| Install and configure the BlackBerry Connectivity Node..... | 155 |
| Copy directory connection configurations..... | 157 |
| Configure proxy settings for a BlackBerry Connectivity Node instance..... | 157 |
| Linking to your company directory..... | 158 |
| Configure Cylance Endpoint Security to synchronize with Entra Active Directory..... | 158 |
| Update the Microsoft Entra ID Active Directory connection credentials..... | 159 |
| Connect to Microsoft Active Directory..... | 159 |
| Connect to an LDAP directory..... | 160 |
| Configure onboarding and offboarding..... | 162 |
| Configure directory synchronization schedules..... | 162 |
| Synchronize with your company directory..... | 163 |
| Adding users and devices..... | 164 |
| Add CylancePROTECT Mobile app and CylanceGATEWAY users..... | 164 |
| Adding user groups..... | 165 |
| Add a directory group..... | 165 |
| Add a local group..... | 165 |
| Assign policies to administrators, users, and groups..... | 166 |
| Rank policies..... | 167 |
| Setting up CylancePROTECT Mobile..... | 168 |
| Create a CylancePROTECT Mobile policy..... | 168 |
| Integrating Cylance Endpoint Security with Microsoft Intune to respond to mobile threats..... | 170 |
| Connect Cylance Endpoint Security to Intune..... | 171 |
| Use Intune app protection policies with CylancePROTECT Mobile..... | 171 |
| Setting up CylanceGATEWAY..... | 173 |
| Defining your private network..... | 174 |
| Setting up the CylanceGATEWAY Connector..... | 175 |
| Specify your private network..... | 191 |
| Specify your private DNS..... | 192 |
| Specify your DNS suffixes..... | 192 |
| Specify private CylanceGATEWAY agent IP ranges..... | 192 |
| Bring your own IP addresses (BYOIP)..... | 193 |
| Network Address Translation with CylanceGATEWAY..... | 193 |
| Define network services..... | 194 |
| Controlling network access..... | 194 |
| Applying ACL rules..... | 195 |

| | |
|--|-----|
| ACL parameters..... | 196 |
| Destination content categories..... | 199 |
| Evaluate the risk level of a network destination..... | 202 |
| Configure the access control list..... | 202 |
| Configuring network protection..... | 203 |
| Destination reputation risk threshold..... | 204 |
| Configure network protection settings..... | 204 |
| Searching ACL rules and Network Services..... | 206 |
| Using source IP pinning..... | 206 |
| Configuring the Gateway service options..... | 207 |
| Gateway Service policy parameters..... | 207 |
| Configure Gateway service options..... | 213 |
| Specifying how devices activated with an EMM solution use the CylanceGATEWAY tunnel..... | 214 |
| Connecting Cylance Endpoint Security to MDM solutions to verify whether devices are managed..... | 218 |
| Prerequisites: Verifying that devices are MDM managed..... | 219 |
| Add a BlackBerry UEM connector..... | 221 |
| Use BlackBerry UEM to install the CylancePROTECT Mobile app on devices..... | 221 |
| Connect Cylance Endpoint Security to Intune..... | 222 |
| Installing the CylanceGATEWAY agent..... | 222 |
| Perform a silent installation and upgrade of the CylanceGATEWAY agent..... | 223 |

Enrolling CylancePROTECT Mobile and CylanceGATEWAY users..... 225

| | |
|---|-----|
| Create an enrollment policy..... | 225 |
| Supported enrollment email variables..... | 226 |

Setting up CylanceAVERT..... 227

| | |
|---|-----|
| Installing the CylanceAVERT agent..... | 227 |
| Install CylanceAVERT..... | 227 |
| Define sensitive content using information protection settings..... | 228 |
| Manage evidence collection..... | 228 |
| Add allowed and trusted domains..... | 229 |
| Use templates to group data types..... | 229 |
| Specify sensitive data types..... | 230 |
| Verify domains using trusted certificates..... | 232 |
| Send notifications to specified email addresses..... | 232 |
| Managing information protection policies..... | 232 |
| Best practices for policy consolidation..... | 232 |
| Create an information protection policy..... | 233 |

Connecting Cylance Endpoint Security to external services.....235

| | |
|--|-----|
| Integrating Cylance Endpoint Security with Okta..... | 235 |
| Prerequisites for adding an Okta connector..... | 236 |
| Add and configure an Okta connector..... | 236 |
| Integrating Cylance Endpoint Security with Mimecast..... | 237 |
| Prerequisites for adding a Mimecast connector..... | 237 |
| Add and configure a Mimecast connector..... | 238 |

Legal notice..... 239

Configuring a new Cylance Endpoint Security tenant

When you create a new Cylance Endpoint Security tenant, or when you reset a tenant to the recommended default state, the tenant includes preconfigured [zones](#) and preconfigured [device policies](#) that are designed to help you tune your environment to the desired security posture.

A new tenant, or a tenant that has been reset to the recommended default state, includes three preconfigured zones, one for each desktop OS (Windows, macOS, and Linux). These zones are configured to automatically assign new desktop devices to the appropriate OS zone. The preconfigured zones are assigned the stage 1 device policy described below.

A new or reset tenant includes three preconfigured device policies to control the features and functionality of CylancePROTECT Desktop and CylanceOPTICS. See [Default configuration settings for a new Cylance Endpoint Security tenant](#) for the complete configuration of each preconfigured policy.

| Preconfigured policy | Description |
|----------------------|---|
| Stage 1 | <p>The starter configuration that allows devices to listen for malware threats. Advanced policy settings are turned off. Use this policy in your environment first to observe the initial detections from devices and to configure the appropriate exceptions.</p> <p>When you are comfortable with the performance and impact of this policy, you can progress devices to the stage 2 policy.</p> |
| Stage 2 | <p>This device policy enables the detection of a wider range of threats, including abnormal malware, unsafe scripts, and memory exploits. Assign this policy to a small number of devices to gauge the volume and frequency of detections and the level of investigation required. This will allow you to refine the policy configuration before assigning it to more devices.</p> <p>When you are comfortable with the performance of this policy, you can progress devices to the stage 3 policy.</p> |
| Stage 3 | <p>This device policy builds on stage 2 by adjusting settings so that devices can both listen for threats and take certain preventative actions. Use this device policy only after sufficient testing with the stage 2 policy, and only after applying the fine tuning from the stage 2 policy to this policy as well.</p> |

As you test and evaluate the preconfigured zones and device policies, you can adjust the configuration as needed, including making changes to the preconfigured options or copying and modifying a zone or policy to determine the configuration that best suits your organization's environment.

Cylance Endpoint Security also offers additional options that make it easier for you to quickly configure a new tenant to meet your organization's needs. You can export the configuration of a tenant and import it to a new tenant, or reset a tenant to the recommended defaults detailed in [Default configuration settings for a new Cylance Endpoint Security tenant](#). For more information, see [Export, import, or reset the configuration of a Cylance Endpoint Security tenant](#).

Default configuration settings for a new Cylance Endpoint Security tenant

Preconfigured Zones

| Preconfigured Zones | Assigned device policy | Default Zone rules |
|---------------------|------------------------|---|
| Windows Zone | Stage 1 | Automatic zone assignment to move all new Windows devices into this zone. |
| Mac Zone | Stage 1 | Automatic zone assignment to move all new macOS devices into this zone. |
| Linux Zone | Stage 1 | Automatic zone assignment to move all new Linux devices into this zone. |

Preconfigured device policies

| Device policy setting | Stage 1 policy | Stage 2 policy | Stage 3 policy |
|--|----------------|----------------|----------------|
| File Actions | | | |
| Auto Quarantine with Execution Control: Unsafe | Off | On | On |
| Auto Quarantine with Execution Control: Abnormal | Off | Off | On |
| Enable auto-delete for quarantined files | Off | On | On |
| Auto Upload: Executable | On | On | On |
| Memory Actions | | | |
| Memory Protection | Off | On | On |
| Exploitation: Stack Pivot | Off | Ignore | Ignore |
| Exploitation: Stack Protect | Off | Ignore | Ignore |
| Exploitation: Overwrite Code | Off | Ignore | Ignore |
| Exploitation: RAM Scraping | Off | Alert | Block |
| Exploitation: Malicious Payload | Off | Ignore | Ignore |
| Exploitation: System Call Monitoring | Off | Ignore | Ignore |
| Exploitation: Direct System Calls | Off | Ignore | Ignore |

| Device policy setting | Stage 1 policy | Stage 2 policy | Stage 3 policy |
|--|----------------|----------------|----------------|
| Exploitation: System DLL Overwrite | Off | Ignore | Ignore |
| Exploitation: Dangerous COM Object | Off | Ignore | Ignore |
| Exploitation: Injection via APC | Off | Ignore | Ignore |
| Exploitation: Dangerous VBA Macro | Off | Ignore | Ignore |
| Process Injection: Remote Allocation of Memory | Off | Alert | Block |
| Process Injection: Remote Mapping of Memory | Off | Alert | Block |
| Process Injection: Remote Write to Memory | Off | Alert | Block |
| Process Injection: Remote Write PE to Memory | Off | Alert | Block |
| Process Injection: Remote Overwrite Code | Off | Ignore | Ignore |
| Process Injection: Remote Unmap of Memory | Off | Ignore | Ignore |
| Process Injection: Remote Thread Creation | Off | Ignore | Ignore |
| Process Injection: Remote APC Scheduled | Off | Ignore | Ignore |
| Process Injection: DYLD Injection | Off | Ignore | Ignore |
| Process Injection: Doppelganger | Off | Ignore | Ignore |
| Process Injection: Dangerous Environmental Variable | Off | Ignore | Ignore |
| Escalation: LSASS Read | Off | Alert | Block |
| Escalation: Zero Allocate | Off | Alert | Block |
| Escalation: Memory Permission Changes In Other Processes | Off | Ignore | Ignore |
| Escalation: Memory Permission Changes In Child Processes | Off | Ignore | Ignore |
| Escalation: Stolen System Token | Off | Ignore | Ignore |
| Escalation: Low Integrity Process Start | Off | Ignore | Ignore |
| Protection Settings | | | |
| Prevent service shutdown from device | On | On | On |
| Kill unsafe running processes and their sub processes | Off | Off | Off |

| Device policy setting | Stage 1 policy | Stage 2 policy | Stage 3 policy |
|--|----------------|----------------|----------------|
| Background Threat Detection | On | On | On |
| Run setting | Recurring | Recurring | Recurring |
| Days | 10 | 10 | 10 |
| Watch For New Files | On | On | On |
| MB | 150 | 150 | 150 |
| Exclude Specific Folders | Off | Off | Off |
| Copy File Samples | Off | Off | Off |
| CylanceOPTICS Settings | | | |
| CylanceOPTICS | Off | Off | Off |
| Enable CylanceOPTICS Desktop Notifications | Off | Off | Off |
| Detection Settings | None | None | None |
| Application Control | | | |
| Application Control | Off | Off | Off |
| Agent Settings | | | |
| Enable auto-upload of log files | Off | Off | Off |
| Enable Desktop Notifications | Off | Off | Off |
| Enable Software Inventory | On | On | On |
| Script Control | | | |
| Script Control | Off | On | On |
| Active Script | Off | Alert | Block Unsafe |
| PowerShell Script | Off | Alert | Block Unsafe |
| PowerShell Console | Off | Disabled | Disabled |
| Macros | Off | Disabled | Disabled |
| Python | Off | Disabled | Disabled |
| .NET DLR | Off | Disabled | Disabled |

| Device policy setting | Stage 1 policy | Stage 2 policy | Stage 3 policy |
|--|----------------|----------------|----------------|
| XLM Macros | Off | Disabled | Disabled |
| Advanced: Score All Scripts | Off | On | On |
| Advanced: Upload Script to Cloud | Off | On | On |
| Advanced: Alert On Suspicious Scripts Execution Only | Off | On | On |
| Device Control | | | |
| Windows Device Control | On | On | On |
| Android | Full Access | Full Access | Full Access |
| iOS | Full Access | Full Access | Full Access |
| Still Image | Full Access | Full Access | Full Access |
| USB CD DVD RW | Full Access | Full Access | Full Access |
| USB Drive | Full Access | Full Access | Full Access |
| VMWare USB Passthrough | Full Access | Full Access | Full Access |
| Windows Portable Device | Full Access | Full Access | Full Access |

Export, import, or reset the configuration of a Cylance Endpoint Security tenant

You can configure a new Cylance Endpoint Security tenant by exporting the configuration of an existing tenant and importing it into the new tenant. You also have the option to reset a new tenant to use the [recommended default settings](#).

The following settings are included when you export the configuration of an existing tenant, and are changed when you import or reset the tenant configuration:

- Device policies
- Zone configurations
- Agent update settings
- Global safe and quarantine lists
- Syslog settings

Note: The export, import, and reset options are designed specifically to help you configure a new tenant and test settings before you enroll devices. The export feature is not intended to be used to create a backup configuration file for an existing tenant. When you import a configuration to a new tenant or you reset a tenant, the previous configuration of the items detailed above are removed and cannot be recovered.

1. In the management console, on the menu bar, click **Settings > Tenant Settings**.
2. Do any of the following:

| Task | Steps |
|---|---|
| Export the configuration of the current tenant. | <p>Note that only zones and zone rules that were created with a saved query are included in the exported configuration. The configuration file that you export can only be imported to a new tenant in the same region. The exported configuration file is not valid for tenants with a different region.</p> <ol style="list-style-type: none"> Click Export. Specify a name for the .zip file. Click Export. See the instructions below to import the configuration to a new tenant. |
| Import configuration settings that you exported from another tenant to this tenant. | <p>Note that importing a tenant configuration will remove the current configuration of a tenant, including any association between devices and device policies and zones. Once removed, the configuration cannot be recovered.</p> <ol style="list-style-type: none"> Click Import. Browse to and select the configuration .zip file. In the confirmation field, type import. Click Import. Confirm the import. <p>If the process fails, any changes that were applied to the tenant are rolled back.</p> |
| Reset a tenant to the recommended default settings . | <p>Resetting the tenant configuration to the default settings will remove the current configuration, including any association between devices and device policies and zones. Once removed, the configuration cannot be recovered.</p> <ol style="list-style-type: none"> Click Reset. In the confirmation field, type reset. Click Reset. Confirm the reset. <p>If the process fails, any changes that were applied to the tenant are rolled back.</p> |

Details of the import or reset are written to the [audit log](#).

Cylance Endpoint Security requirements

To get started setting up Cylance Endpoint Security, review this section and verify that your organization's environment satisfies the requirements of the solution's features and components.

Requirements: Cylance console

| Item | Requirements |
|---------------------|--|
| Supported browsers | <p>Latest version of:</p> <ul style="list-style-type: none">• Google Chrome (recommended)• Microsoft Edge• Mozilla Firefox <p>Note: If you are using Firefox to access the management console, do not use private browser mode, do not enable "Delete cookies and site data when Firefox is closed", and do not disable service workers. Any of these configurations can cause some screens in the console to not load as expected.</p> |
| Supported languages | <p>Set your browser to any of the following supported languages:</p> <ul style="list-style-type: none">• English• French• German• Italian• Japanese• Korean• Portuguese• Spanish |

Requirements: CylancePROTECT Desktop

For information about the operating systems that each of CylancePROTECT Desktop agents supports, see the [Cylance Endpoint Security compatibility matrix](#). To view the support timelines for all BlackBerry products, see the [BlackBerry Enterprise Software Lifecycle Reference Guide](#).

The following tables list the supported operating systems that have additional requirements or considerations. Note that these tables are not a comprehensive list of supported operating systems. If an operating system is not listed in the tables, it means that there are no additional requirements or considerations.

Windows OS

| Supported OS | Requirements |
|-----------------------------------|--|
| All supported Windows OS versions | <ul style="list-style-type: none"> • .NET Framework 4.6.2 or later • TLS 1.2 • For virtual machine requirements, deployment guidance, and best practices, see Best practices for deploying CylancePROTECT Desktop on Windows virtual machines. • CylancePROTECT Desktop does not support scanning unhydrated files from Microsoft OneDrive. • Verify that the latest Windows security updates have been installed on devices before installing or upgrading the CylancePROTECT Desktop agent. |
| Windows 11 (64-bit) | <ul style="list-style-type: none"> • All editions of Windows 11 are supported. • Case-sensitive file systems are not supported. |
| Windows 10 (32-bit, 64-bit) | <ul style="list-style-type: none"> • All editions of Windows 10 are supported. • Case-sensitive file systems are not supported. • Windows 10 (v1809, October 2018 update): Unified Write Filter (UWF) is not supported. Disable UWF before installing the agent. |
| Windows Server 2025 (64-bit) | <ul style="list-style-type: none"> • Standard, Data Center, and Core editions are supported. • For Data Center editions, the agent does not support: <ul style="list-style-type: none"> • Hyper-V Server Role for Shielded Virtual Machines • Host Guardian Hyper-V Support • Software-defined Networking • Storage Spaces Direct • Storage Server 2025 is not supported. |
| Windows Server 2022 (64-bit) | <ul style="list-style-type: none"> • Standard, Data Center, and Core editions are supported. • For Data Center editions, the agent does not support: <ul style="list-style-type: none"> • Hyper-V Server Role for Shielded Virtual Machines • Host Guardian Hyper-V Support • Software-defined Networking • Storage Spaces Direct • Storage Server 2022 is not supported. |
| Windows Server 2019 (64-bit) | <ul style="list-style-type: none"> • Standard, Data Center, and Core editions are supported. • For Data Center editions, the agent does not support: <ul style="list-style-type: none"> • Hyper-V Server Role for Shielded Virtual Machines • Host Guardian Hyper-V Support • Software-defined Networking • Storage Spaces Direct • Storage Server 2019 is not supported. |

| Supported OS | Requirements |
|--|--|
| Windows Server 2016 (64-bit) | <ul style="list-style-type: none"> Standard, Data Center, Essentials, and Server Core editions are supported. Nano Server and Storage Server are not supported. |
| Windows Server 2012 and 2012 R2 (64-bit) | <ul style="list-style-type: none"> Standard, Data Center, Essentials, Server Core, Embedded, and Foundation editions are supported. Minimal Server Interface and Storage Server are not supported. |

macOS

| Supported OS | Requirements |
|------------------------------|--|
| All supported macOS versions | <ul style="list-style-type: none"> TLS 1.2 Verify that the following root certificates are installed. If they are missing, the agent might not start, or the device might not be able to communicate with the management console. For more information, see KB 66608. <ul style="list-style-type: none"> VeriSign Class 3 Public Primary Certification Authority - G5 Thawte Primary Root CA DigiCert Global Root For virtual machine requirements, deployment guidance, and best practices, see Best practices for deploying CylancePROTECT Desktop on Windows virtual machines. Case-sensitive volume formats are not supported. |
| macOS Big Sur (11) and later | <ul style="list-style-type: none"> See KB 66578. Enable Full Disk Access. If Full Disk Access is not enabled, CylancePROTECT Desktop cannot process files secured by user data protection. For more information, see KB 66427. See Troubleshooting macOS installations. The following Memory Protection violations are supported: Remote Allocation of Memory, Remote Mapping of Memory, Remote Write to Memory, Remote Unmap of Memory. Other Memory Protection violations are not supported. |

Linux OS

| Supported OS | Requirements |
|---|--|
| All supported Linux OS versions | <ul style="list-style-type: none"> An internet connection is required. If the device cannot meet this requirement, consider the CylanceON-PREM solution instead. See the Supported Linux kernels spreadsheet. TLS 1.2 Required packages: <ul style="list-style-type: none"> bzip2(x86-64) dbus-libs (For RHEL/CentOS 7.x or 8.x, version 1.10.24 or higher is required.) glibc gtk3 (for RHEL/CentOS) libgcc libc6-dbg (for Debian 12) openssl (for RHEL/CentOS 6.x) openssl-libs (for RHEL/CentOS 7.x) sqlite Root certificates: <ul style="list-style-type: none"> VeriSign Class 3 Public Primary Certification Authority - G5 Thawte Primary Root CA DigiCert Global Root GNOME versions supported for the 2.1.1590 agent: <ul style="list-style-type: none"> 3.28 3.20 3.14 3.10 3.8 Virtual machines are supported. |
| Ubuntu 24.04 LTS (64-bit) Ubuntu 22.04 LTS (64-bit) Ubuntu 20.04 LTS (64-bit) Ubuntu 20.04 (64-bit) Ubuntu 18.04 (64-bit) | <ul style="list-style-type: none"> Azure Ubuntu kernels are not supported. Use the CylancePROTECT Desktop Secure Boot CA certificate to support UEFI Secure Boot. For more information, see KB 73487. |
| Red Hat Enterprise Linux 9 (64-bit) Red Hat Enterprise Linux/CentOS 8 (64-bit) Red Hat Enterprise Linux/CentOS 7 (64-bit) | <ul style="list-style-type: none"> Use the CylancePROTECT Desktop Secure Boot CA certificate to support UEFI Secure Boot. For more information, see KB 73487. FIPS is supported. For instructions to enable FIPS, see the Red Hat documentation for your OS. |

Using CylancePROTECT Desktop with other antivirus software

If third-party antivirus software is installed on devices with CylancePROTECT Desktop, you may need to perform some additional configuration tasks to ensure that those products do not interfere with the functionality of CylancePROTECT Desktop. For more information, see [KB 66448](#).

Hardware requirements

| Hardware component | Requirements |
|-------------------------|--|
| Processor (CPU) | Minimum of two processor cores that also: <ul style="list-style-type: none">• Supports the SSE2 Instruction set• Supports the x86_64 instruction set• Supports Apple silicon processors, including M1, M2, M3, and M4; requires Rosetta• Does not support the ARM instruction set for Windows and Linux |
| Memory (RAM) | 2 GB |
| Disk space (hard drive) | <ul style="list-style-type: none">• 600 MB• Disk space usage can increase depending on the features that are enabled (for example, setting the log level to verbose) |

Root certificates required for the CylancePROTECT Desktop agent for Windows

On some versions of Windows, the CylancePROTECT Desktop agent requires the following root certificates (see [Requirements: CylancePROTECT Desktop](#)). If root certificates are missing, the agent might not start or the device might not be able to communicate with the management console. For more information about missing root certificates, see [KB66608](#).

- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert High Assurance EV Root CA
- DigiCert Trusted Root G4
- GlobalSign Root CA
- Microsoft Root Certificate Authority 2010
- Microsoft Identity Verification Root Certificate Authority 2020
- Starfield Class 2 Certification Authority
- Thawte Primary Root CA
- Thawte Primary Root CA - G3
- Thawte Timestamping CA
- USERTrust RSA Certification Authority
- UTN-USERFirst-Object
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Universal Root Certification Authority

For more information, see the following resources:

- [Thawte Root Certificates](#)
- [PKI Repository - Microsoft PKI Services](#)

- [DigiCert Roots and Intermediates](#)
- [DigiCert Trusted Root Authority Certificates](#)
- [GlobalSign Root Certificates](#)
- [Microsoft Windows support for the Trusted Signing \(formerly Azure Code Signing\) program](#). For more information, see KB 140264.
- [How to Download & Install Sectigo Intermediate Certificates - RSA](#)
- [Obtain the VeriSign Class 3 Public Primary Certification Authority - G5 root certificate](#)

Requirements: CylanceOPTICS

Agents

| Agent | Requirements |
|------------------------------|--|
| CylancePROTECT Desktop agent | <ul style="list-style-type: none"> • You must install the CylancePROTECT Desktop agent on a device before you install the CylanceOPTICS agent. The CylanceOPTICS agent requires the CylancePROTECT Desktop agent to function. • BlackBerry recommends installing the latest available version of the CylancePROTECT Desktop agent to benefit from the latest features and fixes. • For the CylanceOPTICS agent version 3.4, the minimum required version of the CylancePROTECT Desktop agent for Windows and Linux is 3.3.x. The minimum required version of the CylancePROTECT Desktop agent for macOS is 3.4.x. • For the CylanceOPTICS agent version 3.3, the minimum required version of the CylancePROTECT Desktop agent is 3.1.x. The Windows sensors introduced in CylanceOPTICS 3.3 require CylancePROTECT Desktop agent for Windows is 3.2.x or later. • The CylanceOPTICS agent version 3.2 and 3.1 require the following minimum versions of the CylancePROTECT Desktop agent: <ul style="list-style-type: none"> • Windows: 2.1.1578.x • macOS: 3.0.1000.x • Linux: 2.1.1590.x • Review the CylancePROTECT Desktop compatibility matrix and the CylancePROTECT Desktop requirements to verify that you install a supported CylancePROTECT Desktop agent and meet all other requirements. |

| Agent | Requirements |
|---------------------|--|
| CylanceOPTICS agent | <ul style="list-style-type: none"> BlackBerry recommends installing the latest available version of the CylanceOPTICS agent on each device. CylanceOPTICS agent version 3.x is required to support automatically storing collected data in the CylanceOPTICS cloud database. Earlier versions of the agent store CylanceOPTICS data in a local database on the device. In agent 3.x, the data that is collected by the CylanceOPTICS sensors is cached locally before it is sent to the CylanceOPTICS cloud database. If the device is offline, the data is cached until the device can connect to the cloud database. A maximum of 1 GB of data can be stored locally. If more than 1 GB of data is stored before it can be uploaded, the lowest priority data will be deleted so that higher priority data can be cached. See the Cylance Endpoint Security Release Notes for considerations when upgrading from CylanceOPTICS agent 2.x to 3.x. When you upgrade from version 2.x to 3.x, the full contents of the CylanceOPTICS local database are uploaded to the cloud database in batches. After you upgrade to version 3.x, you cannot downgrade the agent to version 2.x. If you want to install version 2.x, you must uninstall version 3.x, then install version 2.x. |

OS support and additional requirements

For information about the operating systems that CylanceOPTICS supports, see the [Cylance Endpoint Security compatibility matrix](#). To view support timelines for all BlackBerry products, see the [BlackBerry Enterprise Software Lifecycle Reference Guide](#).

The following table lists the supported operating systems that have additional requirements or considerations. Note that this table is not a comprehensive list of supported operating systems. If an operating system is not listed in the table, it means that there are no additional requirements or considerations.

| OS | Additional requirements or considerations |
|--|--|
| Windows operating systems | |
| Windows 8.1 Windows 7 SP1 | See this Microsoft article for additional dependencies for .NetCore support . |
| macOS operating systems | |
| macOS Sequoia (15.x) macOS Sonoma (14.x) macOS Ventura (13.x) macOS Monterey (12.x) macOS Big Sur (11.x) | <ul style="list-style-type: none"> Enable full disk access. For more information, see KB 66427. See Configuration requirements for macOS 11.x and later. |
| macOS Catalina (10.15) | Enable full disk access. For more information, see KB 66427 . |
| Linux operating systems | |

| OS | Additional requirements or considerations |
|--|--|
| All supported Linux systems | <ul style="list-style-type: none"> • kernel-headers and kernel-devel are required, and the version must match the running kernel. During the installation, the package manager will indicate the versions that are required. For supported Ubuntu and Debian systems, linux-headers is the equivalent of kernel-headers. • One of the following Linux sensor suites is required: eBPF, Netlink (with multicast Netlink socket support 3.16 or later, or audit daemon uninstalled), or Auditdps (with the auditd and auditdps plugins enabled to start on boot). eBPF is recommended for the best performance with the CylanceOPTICS agent. If eBPF is not available, the agent tries to use Netlink for the next best level of performance. If Netlink is not available, the agent tries to use Auditdps. The available sensor suites vary depending on the version of your OS. • The Microsoft .NET Framework runtime packages depend on libicu and libssl but are not listed as package dependencies because their names differ on different Linux distributions. For the exact package names, see https://github.com/dotnet/core/blob/master/Documentation/linux-prereqs.md. In the case that any required libraries are missing, CylanceTcpService reports the missing library and exits. |
| RHEL 9.x RHEL/CentOS 8.x RHEL/CentOS 7.x AlmaLinux 9.4 AlmaLinux 8.10 Rocky Linux 9.4 Rocky Linux 8.10 | <ul style="list-style-type: none"> • For RHEL/CentOS 8.x, ncurses-compat-libs is required unless devices are running CylanceOPTICS agent version 3.2.1140-x or later. • Firewalld must be enabled and running to support the lockdown device feature. Firewalld is available by default with RHEL/CentOS, AlmaLinux, and Rocky Linux. |
| Amazon Linux 2023 Amazon Linux 2 | <ul style="list-style-type: none"> • ncurses-compat-libs is required unless devices are running CylanceOPTICS agent version 3.2.1140-15000 or later. • Firewalld must be enabled and running to support the lockdown device feature. |
| Oracle Linux Server UEK 9 (64-bit) Oracle Linux Server 9 (64-bit) Oracle Linux Server UEK 8 (64-bit) Oracle Linux Server 8 (64-bit) Oracle Linux Server UEK 7 (64-bit) Oracle Linux Server 7 (64-bit) | <ul style="list-style-type: none"> • ncurses-compat-libs is required unless devices are running CylanceOPTICS agent version 3.2.1140-37000 or later. • Firewalld must be enabled and running to support the lockdown device feature. Firewalld is available by default with Oracle Linux. |

| OS | Additional requirements or considerations |
|--|---|
| Ubuntu 24.04 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04 | <ul style="list-style-type: none"> Ubuntu 20.04 requires libtinfo5 unless devices are running CylanceOPTICS agent version 3.2.1140-x or later. Firewalld must be enabled and running to support the lockdown device feature. Firewalld must be installed manually for Ubuntu. |
| SUSE Enterprise Linux 15 SP4 SUSE Enterprise Linux 15 SUSE Enterprise Linux 12 | <ul style="list-style-type: none"> polycoreutils is required. For SUSE 15.x, kernel-default-devel to match the kernel is required. libncurses5 is also required unless devices are running CylanceOPTICS agent version 3.2.1140-29000 or later. Firewalld must be enabled and running to support the lockdown device feature on SUSE 15.x. Firewalld is available by default with SUSE 15.x. The lockdown device feature is not supported for SUSE 12. |
| Debian 12 Debian 11 Debian 10 | <ul style="list-style-type: none"> Debian 10 devices require iptables 1.8.5 or later to support the lockdown device feature. Firewalld must be enabled and running to support the lockdown device feature. Firewalld must be installed manually for Debian. |

Compatibility with other EDR solutions

The CylanceOPTICS agent is not compatible with other EDR (Endpoint Detection and Response) solutions installed on the same device. Remove any third-party EDR solutions from a device before you install and enable the CylanceOPTICS agent.

Hardware

| Item | Requirements |
|-------------------------|--|
| Processor (CPU) | <ul style="list-style-type: none"> In general use, as low as 1% additional CPU For heavy sustained workloads, additional 5% to 25% CPU bursts can be required, depending on the workload |
| Memory (RAM) | The agent requires 0.2 to 1.0 GB of additional memory, depending on the workload. |
| Disk space (hard drive) | <p>Minimum 1 GB</p> <ul style="list-style-type: none"> For CylanceOPTICS agent 2.x and earlier, 1 GB minimum is required for the local database. For CylanceOPTICS 3.0 and later, 1 GB minimum is recommended for caching CylanceOPTICS sensor data before the device can upload the data to the CylanceOPTICS cloud database when it is online. |

Virtual machines

CylanceOPTICS is supported for virtual machines. For requirements, deployment guidance, and best practices, see [Best practices for deploying CylancePROTECT Desktop on Windows virtual machines](#). If you use CylanceOPTICS on a virtual machine, BlackBerry recommends disabling the Advanced WMI visibility sensor to reduce the number of recorded events.

Requirements: CylancePROTECT Mobile app

| Item | Description |
|---------------------------|---|
| OS | See the Cylance Endpoint Security compatibility matrix . Note: <ul style="list-style-type: none">Sideload detection is not supported for iOS 17.5 and later.On iOS devices, backup and restore is not supported for the CylancePROTECT Mobile app. |
| Supported device browsers | Latest version of: <ul style="list-style-type: none">Android: Google Chrome, Samsung Internet, Firefox, BraveiOS: Safari |
| Device configuration | <ul style="list-style-type: none">Instruct users to enable JavaScript in their default mobile browser. This is required to activate the CylancePROTECT Mobile app.Instruct Android users to allow background activity for the CylancePROTECT Mobile app after it is installed. |

Requirements: BlackBerry Connectivity Node

Software

| Item | Description |
|--------------------------|--|
| Java Runtime Environment | JRE 17 (latest update version, 64-bit) |

Hardware

| Component | BlackBerry Connectivity Node |
|-------------------------|---|
| Processor (CPU) | Six processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent |
| Memory (RAM) | 12 GB |
| Disk space (hard drive) | 64 GB |

Additional BlackBerry Connectivity Node requirements

- Choose a directory account with read permissions for each configured directory connection that the BlackBerry Connectivity Node can use to access the company directories.
- Use a Windows account with permissions to install and configure software on the computer that will host the BlackBerry Connectivity Node.
- Verify that the following outbound ports are open in your organization's firewall so that the BlackBerry Connectivity Node components can communicate with the BlackBerry Infrastructure (<region>.bbsecure.com, for example ca.bbsecure.com):
 - 443 (HTTPS) to activate the BlackBerry Connectivity Node
 - 3101 (TCP) for all other outbound connections
- Install the software on a version of Windows Server supported by Microsoft.
- You can install the BlackBerry Connectivity Node on English, French, Spanish, Japanese, or German implementations of the operating system.

Requirements: CylanceGATEWAY Connector

Hardware

| Component | CylanceGATEWAY Connector |
|-------------------------|--------------------------|
| Processor (CPU) | Two processor cores |
| Memory (RAM) | 5 GB |
| Disk space (hard drive) | 2 GB |

AWS

| Item | Description |
|---------------|--|
| Instance type | BlackBerry recommends an instance type of c6in or c5n for production environments. |

Requirements: CylanceGATEWAY agents

If you enabled the CylanceGATEWAY feature for your mobile users, users can enable Work Mode from the CylancePROTECT Mobile app. For information on CylancePROTECT Mobile requirements, see the [Requirements: CylancePROTECT Mobile app](#).

| Item | Requirements |
|-----------------|--|
| Processor (CPU) | <ul style="list-style-type: none"> • Supports all Apple devices, including Apple Silicon devices via Rosetta 2 • Supports all x64-based processors • Does not support 32-bit operating systems • Does not support ARM devices |
| OS | For information about the operating systems that the CylanceGATEWAY agent supports, see the Cylance Endpoint Security compatibility matrix . To view support timelines for all BlackBerry products, see the BlackBerry Enterprise Software Lifecycle Reference Guide . |

Requirements: CylanceAVERT

| Item | Description |
|----------------------------------|--|
| CylanceAVERT agent | CylanceAVERT is a bundled installer which includes the CylanceAVERT Microsoft Outlook plugin and browser extensions for Chrome, Firefox, and Microsoft Edge. |
| CylancePROTECT Desktop agent | CylancePROTECT Desktop agent version 3.1 or later. |
| OS and Microsoft Outlook support | For information about the operating systems and Microsoft Outlook versions that CylanceOPTICS supports, see the Cylance Endpoint Security compatibility matrix . To view support timelines for all BlackBerry products, see the BlackBerry Enterprise Software Lifecycle Reference Guide . |
| .NET | <ul style="list-style-type: none"> • Microsoft .NET 4.6.2 or later • .NET Standard 2.0 or later |
| Microsoft Visual C++ | Microsoft Visual C++ 2017 Re-distributable or later |

Cylance Endpoint Security network requirements

Cylance Endpoint Security agents

Port 443 (HTTPS) must be open for the Cylance Endpoint Security desktop agents to communicate with the management console.

The agents communicate over secure websockets (WSS) and must be able to establish this connection directly. Configure your organization's network to allow connections to the following domains.

Note:

- The management console is hosted by AWS and does not have fixed IP addresses. You can allow HTTPS traffic to *.cylance.com. For the cylance-optics-files-use1.s3.amazonaws.com host (and similar hosts for other regions), it is recommended to allow that specific host. It is not recommended to allow *.amazonaws.com because it can open your network to other hosts.

- Please note that the domain `api2.cylance.com` is deprecated, but is kept open to support older CylancePROTECT Desktop agents. `api2.cylance.com` directs to the same destination as `api.cylance.com` for the purpose of threat analysis and risk scoring.

| Item | Description |
|---------------|--|
| North America | <p>Required for logging in to the Cylance console:</p> <ul style="list-style-type: none"> • <code>login.cylance.com</code> • <code>idp.blackberry.com</code> • <code>cdn.cylance.com</code> • <code>idp.cs.cylance.com</code> • <code>download.cylance.com</code> <p>Required for CylancePROTECT Desktop:</p> <ul style="list-style-type: none"> • <code>data.cylance.com</code> • <code>protect.cylance.com</code> • <code>update.cylance.com</code> • <code>api.cylance.com</code> • <code>download.cylance.com</code> • <code>venueapi.cylance.com</code> <p>Required for CylanceOPTICS:</p> <ul style="list-style-type: none"> • <code>cylance-optics-files-use1.s3.amazonaws.com</code> • <code>opticspolicy.cylance.com</code> • <code>content.cylance.com</code> • <code>rrws-use1.cylance.com</code> • <code>collector.cylance.com</code> • <code>scalar-api-use1.cylance.com</code> • <code>cement.cylance.com</code> <p>Required for the CylanceGATEWAY agent:</p> <ul style="list-style-type: none"> • <code>idp.blackberry.com</code> • <code>quip.webapps.blackberry.com</code> • <code>us1.cs.blackberry.com</code> <p>Required for the CylanceGATEWAY Connector: <code>deb.nodesource.com</code></p> <p>Required for the CylanceGATEWAY agent and the CylanceGATEWAY Connector: <code>us1.bg.blackberry.com</code></p> <p>For more information, see KB79017.</p> |

| Item | Description |
|------------------------|---|
| Asia-Pacific Northeast | Required for logging in to the Cylance console: |
| | <ul style="list-style-type: none"> • login-apne1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com • cylance-jp1.cs.cylance.com • apne1-consoleapi.cylance.com • protect-apne1.cylance.com • download.cylance.com |
| | Required for CylancePROTECT Desktop: |
| | <ul style="list-style-type: none"> • data-apne1.cylance.com • protect-apne1.cylance.com • update-apne1.cylance.com • api.cylance.com • download.cylance.com • venueapi-apne1.cylance.com |
| | Required for CylanceOPTICS: |
| Asia-Pacific Southeast | <ul style="list-style-type: none"> • cylance-optics-files-apne1.s3.amazonaws.com • opticspolicy-apne1.cylance.com • content-apne1.cylance.com • rrws-apne1.cylance.com • collector-apne1.cylance.com • scalar-api-apne1.cylance.com • cement-apne1.cylance.com |
| | Required for the CylanceGATEWAY agent: |
| | <ul style="list-style-type: none"> • idp.blackberry.com • quip.webapps.blackberry.com • jp1.cs.blackberry.com |
| | Required for the CylanceGATEWAY Connector: deb.nodesource.com |
| | Required for the CylanceGATEWAY agent and the CylanceGATEWAY Connector: jp1.bg.blackberry.com |
| | For more information, see KB79017 . |
| Asia-Pacific Southeast | Required for logging in to the Cylance console: |
| | <ul style="list-style-type: none"> • login-au.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com • download.cylance.com |

| Item | Description |
|----------------|--|
| | <p>Required for CylancePROTECT Desktop:</p> <ul style="list-style-type: none"> • data-au.cylance.com • protect-au.cylance.com • update-au.cylance.com • api.cylance.com • download.cylance.com • venueapi-au.cylance.com <p>Required for CylanceOPTICS:</p> <ul style="list-style-type: none"> • cylance-optics-files-apse2.s3.amazonaws.com • opticspolicy-au.cylance.com • content-apse2.cylance.com • rrws-apse2.cylance.com • collector-apse2.cylance.com • scalar-api-apse2.cylance.com • cement-au.cylance.com • cement-apse2.cylance.com <p>Required for the CylanceGATEWAY agent:</p> <ul style="list-style-type: none"> • idp.blackberry.com • quip.webapps.blackberry.com • au1.cs.blackberry.com <p>Required for the CylanceGATEWAY Connector: deb.nodesource.com</p> <p>Required for the CylanceGATEWAY agent and the CylanceGATEWAY Connector: au1.bg.blackberry.com</p> <p>For more information, see KB79017.</p> |
| Europe Central | <p>Required for logging in to the Cylance console:</p> <ul style="list-style-type: none"> • login-euc1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com • download.cylance.com <p>Required for CylancePROTECT Desktop:</p> <ul style="list-style-type: none"> • data-euc1.cylance.com • protect-euc1.cylance.com • update-euc1.cylance.com • api.cylance.com • download.cylance.com • venueapi-euc1.cylance.com |

| Item | Description |
|---------------|---|
| | <p>Required for CylanceOPTICS:</p> <ul style="list-style-type: none"> • cylance-optics-files-euc1.s3.amazonaws.com • opticspolicy-euc1.cylance.com • content-euc1.cylance.com • rrws-euc1.cylance.com • collector-euc1.cylance.com • scalar-api-euc1.cylance.com • cement-euc1.cylance.com <p>Required for the CylanceGATEWAY agent:</p> <ul style="list-style-type: none"> • idp.blackberry.com • quip.webapps.blackberry.com • eu1.cs.blackberry.com <p>Required for the CylanceGATEWAY Connector: deb.nodesource.com</p> <p>Required for the CylanceGATEWAY agent and the CylanceGATEWAY Connector: eu1.bg.blackberry.com</p> <p>For more information, see KB79017.</p> |
| South America | <p>Required for logging in to the Cylance console:</p> <ul style="list-style-type: none"> • login-sae1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com • download.cylance.com <p>Required for CylancePROTECT Desktop:</p> <ul style="list-style-type: none"> • data-sae1.cylance.com • protect-sae1.cylance.com • update-sae1.cylance.com • api.cylance.com • download.cylance.com • venueapi-sae1.cylance.com <p>Required for CylanceOPTICS:</p> <ul style="list-style-type: none"> • cylance-optics-files-sae1.s3.amazonaws.com • opticspolicy-sae1.cylance.com • content-sae1.cylance.com • rrws-sae1.cylance.com • collector-sae1.cylance.com • scalar-api-sae1.cylance.com • cement-sae1.cylance.com |

| Item | Description |
|----------|--|
| | <p>Required for the CylanceGATEWAY agent:</p> <ul style="list-style-type: none"> • idp.blackberry.com • quip.webapps.blackberry.com • br1.cs.blackberry.com <p>Required for the CylanceGATEWAY Connector: deb.nodesource.com</p> <p>Required for the CylanceGATEWAY agent and the CylanceGATEWAY Connector: br1.bg.blackberry.com</p> <p>For more information, see KB79017.</p> |
| GovCloud | <p>Required for logging in to the Cylance console:</p> <ul style="list-style-type: none"> • login.us.cylance.com • idp.blackberry.com • idp.cs.cylance.com • download.cylance.com <p>Required for CylancePROTECT Desktop:</p> <ul style="list-style-type: none"> • data.us.cylance.com • protect.us.cylance.com • update.us.cylance.com • api.us.cylance.com • download.cylance.com • download.us.cylance.com • venueapi.us.cylance.com <p>Required for CylanceOPTICS:</p> <ul style="list-style-type: none"> • cylance-optics-files.us.s3.amazonaws.com • opticspolicy.us.cylance.com • rrws.us.cylance.com • collector.us.cylance.com • scalar-api.us.cylance.com • cement.us.cylance.com |

CylancePROTECT Mobile app

The CylancePROTECT Mobile app requires a secure, direct connection to the following URLs to communicate with the CylancePROTECT Mobile cloud services. If devices are connected to your organization's Wi-Fi network, your network configuration must allow connections to:

- CylancePROTECT Mobile cloud service:
 - US: <https://us1.mtd.blackberry.com>
 - JP: <https://jp1.mtd.blackberry.com>
 - EU: <https://eu1.mtd.blackberry.com>
 - AU: <https://au1.mtd.blackberry.com>
 - SP: <https://br1.mtd.blackberry.com>

- Common services gateway:
 - US: https://us1.cs.blackberry.com
 - JP: https://jp1.cs.blackberry.com
 - EU: https://eu1.cs.blackberry.com
 - AU: https://au1.cs.blackberry.com
 - SP: https://br1.cs.blackberry.com
- https://score.cylance.com
- https://idp.blackberry.com
- https://mobile.ues.blackberry.com

Cylance Endpoint Security proxy requirements

Configuring a proxy for the CylancePROTECT Desktop and CylanceOPTICS agents

- If you want to configure both the CylancePROTECT Desktop agent and the CylanceOPTICS agent on a device to use a proxy server for outbound communication to BlackBerry servers, in the Registry Editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop and create String Value REG_SZ:
 - Value Name = ProxyServer
 - Value Data = <proxyIP:port> (for example, http://123.45.67.89:8080)
- The proxy must accept unauthorized requests. SSL inspection is not supported and must be bypassed for all agent traffic (*.cylance.com).
- For Windows environments, if you configured system wide proxy settings in HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings, you must specify the ProxyServer registry key value using <proxyIP:port>, or the value must start with http:// instead of https:// (HTTPS proxy connections are supported but the registry value must not start with https://).

Proxy options for the CylanceOPTICS agent

- The CylanceOPTICS agent is proxy aware and will query the .NET framework to identify and use the available proxy settings. If you configured the ProxyServer value in the registry, the CylanceOPTICS agent will use the specified proxy. The CylanceOPTICS agent will try to communicate first as the Local System, then as the currently logged in user.
- If you configure the CylanceOPTICS agent to use a proxy and the agent cannot communicate with the cloud services, the agent will attempt to bypass the proxy to make a direct connection. On Windows and macOS devices, you can disable this proxy bypass. Do the following before you install the CylanceOPTICS agent:

| Platform | Steps |
|----------|---|
| Windows | <p>In HKLM\SOFTWARE\Cylance\Optics\, create String Value REG_SZ:</p> <ul style="list-style-type: none"> • Value Name = DisableProxyBypass • Value Data = True |

| Platform | Steps |
|----------|--|
| macOS | <ul style="list-style-type: none"> In /Library/Application Support/Cylance/Desktop/registry/LocalMachine/Software/Cylance/Desktop/, add the following to the values.xml file: <pre><value name="ProxyServer" type="string">http://proxy_server_IP:port</value></pre> In /Library/Application Support/Cylance/Optics/Configuration, create an ExternalConfig.xml file with the following: <pre><?xml version="1.0" encoding="utf-8"? ><EnforceProxyServer>true</EnforceProxyServer></pre> |

- When CylanceOPTICS creates a detection event that involves a signed file as an artifact, it uses a command from the Windows API to validate the signature or certificate. The command sends a validation request to an OCSP server. The OCSP server address is determined by Windows. If your proxy server reports attempts to send external traffic to an OCSP server, update the proxy settings on devices to allow connections with the OCSP server.

Linux: Configure the CylancePROTECT Desktop and CylanceOPTICS agents to use a proxy server

On [supported versions](#) of RHEL, CentOS, Ubuntu, Amazon Linux 2, and SUSE 15, use the following commands to configure the agents to use an unauthenticated or authenticated proxy. You can use these commands before you install the agents. The commands below configure a proxy for the CylancePROTECT Desktop agent. To set a proxy for the CylanceOPTICS agent:

- Replace all instances of "cylancesvc" with "cyoptics"
- Duplicate each http_proxy line and replace "http_proxy" with "https_proxy". In most cases https_proxy will use the same value as http_proxy because HTTPS traffic is tunneled using TCP Connect, but if your organization uses an HTTPS termination proxy server, specify the appropriate value for https_proxy.

Unauthenticated proxy:

```
mkdir /etc/systemd/system/cylancesvc.service.d
echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf
echo "Environment=http_proxy=http://proxyaddress:port" >> /etc/systemd/system/
cylancesvc.service.d/proxy.conf
systemctl stop cylancesvc
systemctl daemon-reload
systemctl start cylancesvc
```

Authenticated proxy:

```
mkdir /etc/systemd/system/cylancesvc.service.d
echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf
echo "Environment=http_proxy=user:password@proxyaddress:port" >> /etc/systemd/
system/cylancesvc.service.d/proxy.conf
systemctl stop cylancesvc
systemctl daemon-reload
systemctl start cylancesvc
```

Accessing the management console and configuring authentication

The first time that you log in to the management console, you must create a password. You can then configure the types of authentication that you want your administrators to complete to access the management console, and that you want users to complete to activate Cylance services.

Logging in to the management console

Upon activation of your account, you will receive an email with your login information for the Cylance management console. Click the link in the email to open the login page or go to:

- **North America (US):** <https://login.cylance.com>
- **Asia-Pacific Northeast:** <https://login-apne1.cylance.com>
- **Asia-Pacific Southeast:** <https://login-au.cylance.com>
- **Europe Central:** <https://login-euc1.cylance.com>
- **South America East:** <https://login-sae1.cylance.com>
- **GovCloud:** <https://login.us.cylance.com>

The email address will serve as your account login. After you create a password, you can proceed to the console.

Password requirements

Your password must have three of the following characters:

- A lowercase character
- An uppercase character
- A special character (examples * # \$ %)
- A numeric character
- A Unicode character/data (examples ♥ ❄ ☆)

Session timeout

The session will time out 1 hour after the last successful authentication.

Enhanced authentication sign in

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 administrators must complete to sign in to the Cylance console and users must complete before they can activate the CylancePROTECT Mobile app and CylanceGATEWAY agent. By default, administrators use the Cylance console password to access the management console. Users will use their directory credentials (username only) or their BlackBerry Online Account credentials (full email address) to activate the CylancePROTECT Mobile app and CylanceGATEWAY agent based on how the depending on how the CylanceGATEWAY agent was activated. For tenants created in March 2024 or later, by default, administrators will be required to enter a one-time password to access the Cylance console after they set up their console password.

You can create authentication policies for your tenant that specify the types of authentication that must be completed by all administrators and users on the tenant. Only one tenant policy can be created for Cylance console sign-in, the CylancePROTECT Mobile app, and CylanceGATEWAY agent. You can create authentication policies for users that specify the types of authentication administrators and users on the tenant must complete.

The type of authentication added to the tenant policy and authentication policy must be completed in the order that they are specified in the policy. As a failsafe, you may configure one administrator to access the Cylance console using their username and a strong password.

Note: The updated sign-in flow is now the only method to access the Cylance console. Any authentication policies that you applied in your console during the preview period have taken effect.

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

Configure enhanced authentication for sign-in to the Cylance console

If your tenant was created before March 2024, complete these steps if you want to configure your users to authenticate with the Cylance console using an authenticator such as One-Time Password in addition to the Cylance password. For a walkthrough of how to add the One-Time Password authenticator to your tenant policy, see [Add the One-Time Password authentication for administrators to access the Cylance console](#).

| Step | Action |
|------|---|
| 1 | Sign in to the Cylance console using your existing username and password. |
| 2 | Add an authenticator (for example, One-Time Password or Enterprise). By default, the following authenticators are configured for use in your environment: One-time password, Cylance console password and enterprise authentication. |
| 3 | 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. |
| 4 | Create a tenant policy for administrators and users. |

Remove One-Time Password authentication for sign-in to the Cylance console

Tenants created in March 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. For a walkthrough of how to remove the One-Time Password authenticator from your tenant policy, see [Remove One-Time Password authentication for administrators to access the Cylance console](#).

| Step | Action |
|------|--|
| 1 | Sign in to the Cylance console using your existing username and password and one-time password. |
| 2 | Remove the One-Time Password authenticator from the Administration Console tenant policy . |

| Step | Action |
|------|--|
| 3 | Sign in to the Cylance console and test the Cylance console password policy. |

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

Complete these steps if you want to configure a new IDP SAML authenticator for users to authenticate with the Cylance console. Users can use their IDP credentials to access the console from the sign-in page or use IDP-initiated SSO to access the console from the IDP user portal. For a walkthrough of how to configure your IDP SAML, see [How do I configure IDP SAMLs for enhanced authentication and IDP-initiated access to the Cylance console](#) and select your IDP.

| Step | Action |
|------|---|
| 1 | In the IDP environment, create a new SAML application. |
| 2 | Configure the IDP to communicate with Cylance Endpoint Security. |
| 3 | In the Cylance console, Add an authenticator . |
| 4 | <p>Create an authentication policy that uses the password and the authenticator that you created.</p> <p>Note: As a failsafe, create one authentication policy that only uses the Cylance console password and assign it to one administrator.</p> |
| 5 | In the IDP environment, update the SSO Callback URL that you generated in the Cylance console. |
| 6 | Sign in to the Cylance console from the main sign in screen and test the external IDP sign in credentials policy. |
| 7 | (Optional) Disable Custom Authentication (Settings > Application). |

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

Complete these steps only if your IDP SAML authenticator was created before December 2023 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 console using your existing username and password. |
| 2 | In the current IDP SAML authenticator, generate a new SSO callback URL . |
| 3 | Update the current Authentication policy with the newly generated SSO callback URL . |
| 4 | In the IDP environment, update the existing SAML settings. |

Sign in to the Cylance console using enhanced authentication

You can configure authentication policies that specify the types of authentication that administrators must complete to sign in to the management console and users must complete to activate the CylancePROTECT Mobile app and the CylanceGATEWAY agent. A transitioning screen appears briefly before the management console is accessed.

If you sign in with an external IDP that was configured for custom authentication in the management console (Settings > Custom Authentication), you must continue to sign in using the 'Or sign in with your External Identity Provider' link with your external third-party IDP credentials. BlackBerry recommends that you configure your external IDP configuration as an authenticator so that you can use an authentication policy to sign in with your third-party IDP credentials from the main sign in screen. This provides more granularity and flexibility in the authentication configuration. For more information on how to configure your external IDP as an authenticator, see [Migrate external IDPs from Custom Authentication to an authenticator](#).

If you configured your external IDP configuration as an authenticator before December 2023, users will be unable access the Cylance console directly from their external IDP user portal using single sign on. To enable this feature, you must generate a new Cylance Endpoint Security single sign-on login request. For more information on how to enable IDP-initiated sign in to the Cylance console, see [Enhanced authentication sign in](#) and the [How Do I Update your external IDP to enable SSO access to the Cylance console](#).

Before you begin: [Create an authentication policy](#) and [assign it to administrators, users, and groups that administrators and users are a member of](#).

1. In a browser, navigate to the management console.
2. Complete one of the following tasks to access the management console.

| Access | Task | Steps |
|--|--|---|
| Main Cylance Endpoint Security sign in screen. | Sign in with your Cylance account. | <ol style="list-style-type: none"> a. Enter your email address. b. Click Sign In. c. Enter your password. d. Click Sign In. |
| | Sign in with your External Identity Provider that is configured as an authenticator. | <ol style="list-style-type: none"> a. Enter your email address. b. Click Sign In. c. Enter your password. d. Click Sign In. |

| Access | Task | Steps |
|----------------------------|--|--|
| | Sign in with your External Identity Provider. | <ol style="list-style-type: none"> Click Sign in with your External Identity Provider. In the browser, enter your email address. Click Sign In. Enter your password Click Sign In. |
| External IDP users' portal | Single sign on with your External Identity Provider credentials. | <ol style="list-style-type: none"> Log in to your IDP user portal. Click the application that is assigned to you. |

Generate a new SSO callback URL

You can use the copy option to copy your current authenticator information and create the new SSO callback URL. The copy option will remove the current SSO callback URL and generate a new URL when the copied authenticator is saved.

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, in the Cylance console, open the IDP SAML authenticator (Settings > Authentication).

- 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.

Before you begin: The IDP SAML authenticator was created before December 2023 and is using the deprecated SSO callback URL.

1. In the management console, on the menu bar, click **Settings > Authentication**.
2. Click the current IDP SAML authenticator.
3. Click the Copy icon in the upper right-hand corner of the screen.
4. Update the name of the copied authenticator. Click **Save**.
5. Open the Authenticator that you copied. Record the **SSO callback URL**.
6. Delete the previous IDP authenticator.

After you finish: [Update the current authentication policy with the copied authenticator.](#)

Using authentication policies to access the Cylance console and activate agents

You can use authentication policies to specify the type of authentications that administrators and users must complete. An authenticator defines one authentication method (for example, a console password) or a connection to a third-party for authentication (for example, Active Directory or Okta). An authentication policy contains one or more authenticators that you have added. The authentication policy specifies the type of authentications administrators and users must complete in the order that is specified in the policy to access the

console and CylancePROTECT Mobile app and CylanceGATEWAY agent, respectively. For more information, see [Manage authentication policies for your tenant](#).

You can also configure app exceptions and different authenticators for the CylancePROTECT Mobile or CylanceGATEWAY. When an app exception is configured, it takes precedence over the authentication policy that is created. For more information, see [Create an authentication policy](#).

By default, administrators must enter a one-time password to access the Cylance console after they set up their console password.

Add an authenticator

An authenticator defines one authentication method, such as a password (for example, a Cylance console 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 console and users must complete to activate the CylancePROTECT Mobile app or CylanceGATEWAY agent. 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 Cylance console 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](#) 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 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 Cylance console](#).
 - 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.
 - Verify that you have reviewed [Considerations for adding SAML authenticators](#).
1. On the menu bar, click **Settings > Authentication**.
 2. Click **Add Authenticator**.
 3. In the **Authenticator Type** drop-down list, select one of the following authenticators:

| Item | Description |
|--------------|--|
| Entra (SAML) | <p>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.</p> <p>For a walkthrough of the steps to configure your Entra (SAML), see the following:</p> <ul style="list-style-type: none"> • 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 <p>The SSO Callback URL is generated when you save the authenticator and will be in the format <code>https://login.eid.blackberry.com/_/resume/saml20/<hash></code>.</p> <p>Do the following:</p> <ol style="list-style-type: none"> 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 > <i><Name of the newly created application></i> > 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. <p>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.</p> <ol style="list-style-type: none"> 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. <code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</code>). 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. |

| Item | Description |
|--------------------------------|--|
| Custom (SAML) | <p>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.</p> <p>For a walkthrough of the steps to configure your Custom (SAML), see the following:</p> <ul style="list-style-type: none"> • 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 <p>The SSO Callback URL is generated when you save the authenticator and will be in the format <code>https://login.eid.blackberry.com/_/resume/saml20/<hash></code>.</p> <ol style="list-style-type: none"> Enter a name for the authenticator. 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. In the Login request URL field, enter the identity provider's single sign-on URL. In the IDP signing certificate field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. <p>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.</p> <ol style="list-style-type: none"> 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. In the Name ID format field, specify the name identifier format to request from the IDP (for example, <code>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</code>). In the Email claim field, type <code>NameID</code>. 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. Specify any other optional settings. Click Save. Open the authenticator that you added. Record the Single Sign On URL. This URL will be added to the custom IDP. |
| Cylance Administrator Password | <p>Select this option if you want users to enter their Cylance console credentials. Do the following:</p> <ol style="list-style-type: none"> Enter a name for the authenticator. Click Save. |

| Item | Description |
|--|---|
| Deny Authentication | <p>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.</p> <ol style="list-style-type: none"> Enter a name for the authenticator. Click Save. |
| <p>Duo MFA (Deprecated)</p> <p>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. To add Duo multi-factor authentication, see Duo Universal MFA, below.</p> | <p>Select this option if you want users to authenticate using Duo multi-factor authentication.</p> <p>Before you add Duo as an authenticator, you should create an Auth API application. For instructions, see the information from Duo.</p> <p>Do the following:</p> <ol style="list-style-type: none"> Enter a name for the authenticator. 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 | <p>Select this option if you want users to authenticate using Duo multi-factor authentication.</p> <p>Before you add Duo as an authenticator, you must create a Web SDK application. For instructions, see the Duo documentation.</p> <p>Do the following:</p> <ol style="list-style-type: none"> Enter a name for the authenticator. 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. |
| Enterprise | <p>Select this option if you want users to authenticate using their credentials for Active Directory, LDAP, or <i>myAccount</i>. The credentials that a user will use depends on the account type that is the source for their user account in the console. Do the following:</p> <ol style="list-style-type: none"> Enter a name for the authenticator. Click Save. |

| Item | Description |
|---|---|
| FIDO | <p>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.</p> <ol style="list-style-type: none"> Enter a name for the authenticator. Click Save. <p>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.</p> <p>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.</p> |
| Integrated Directory (Active Directory/Entra ID/LDAP) | <p>Select this option if you want users to enter their Active Directory password. If you select this option, your Cylance Endpoint Security tenant must have a connection to the company directory instance. For more information, see Linking to your company directory. Do the following:</p> <ol style="list-style-type: none"> Enter a name for the authenticator. Click Save. |
| IP Address | <p>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.</p> <p>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.</p> <ol style="list-style-type: none"> Enter a name for the authenticator. 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. Click Save. |
| Local Account | <p>Select this option if you want users to enter their BlackBerry Online Account (<i>myAccount</i>) credentials. Do the following:</p> <ol style="list-style-type: none"> Enter a name for the authenticator. Click Save. |
| Okta MFA | <p>Select this option if you want users to authenticate using Okta. Do the following:</p> <ol style="list-style-type: none"> Enter a name for the authenticator. In the Okta MFA Configuration section, enter the Auth API Key and the Auth Domain. Click Save. |

| Item | Description |
|-------------|--|
| Okta (OIDC) | <p>Select this option if you want users to authenticate using Okta. Do the following:</p> <ol style="list-style-type: none"> In the drop-down list below Okta, select OIDC. Enter a name for the authenticator. In the Identity Provider Client section, enter the OIDC discovery document URL, the Client ID, and the Private key JWKS. Click Save. |

| Item | Description |
|-------------|---|
| Okta (SAML) | <p>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.</p> <p>For a walkthrough of the steps to configure your Okta (SAML), see the following:</p> <ul style="list-style-type: none"> • 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 <p>The SSO Callback URL is generated when you save the authenticator and will be in the format <code>https://login.eid.blackberry.com/_/resume/saml20/<hash></code>.</p> <ol style="list-style-type: none"> In the drop-down list below Okta, select SAML. Enter a name for the authenticator. 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. In the Login request URL field, enter the identity provider's single sign-on URL. In the IDP signing certificate field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. <p>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.</p> <ol style="list-style-type: none"> 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. In the IDP entity ID field, paste the "IdentityProvider Issuer" that you recorded from Okta. In the Name ID format field, select the NameID format that you specified in the Okta (for example, <code>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</code>). In the Email Claim field, type <code>Email</code>. 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. Specify any other optional settings. Click Save. 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. <ul style="list-style-type: none"> • Single Sign On URL • Requestable SSO URLs |

| Item | Description |
|-----------------|---|
| OneLogin (OIDC) | <p>Select this option if you want users to authenticate using OneLogin. Do the following:</p> <ol style="list-style-type: none"> In the drop-down list below OneLogin, select OIDC. Enter a name for the authenticator. 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. In the OneLogin Configuration section, enter the OIDC discovery document URL, the Client ID, Client Secret, and Authentication Method. Click Save. |

| Item | Description |
|-----------------|---|
| OneLogin (SAML) | <p>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.</p> <p>For a walkthrough of the steps to configure your OneLogin (SAML), see the following:</p> <ul style="list-style-type: none"> • Configure a new OneLogin (SAML): Configure the OneLogin (SAML) Authenticator for enhanced authentication • Enable OneLogin-initiated access for an existing OneLogin (SAML): Update the OneLogin (SAML) authenticator to enable IDP-initiated access to the Cylance console <p>The SSO Callback URL is generated when you save the authenticator and will be in the format <code>https://login.eid.blackberry.com/_/resume/saml20/<hash></code>.</p> <ol style="list-style-type: none"> Enter a name for the authenticator. 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. In the Login request URL field, enter the identity provider's single sign-on URL. In the IDP signing certificate field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. <p>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.</p> <ol style="list-style-type: none"> 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. Specify any other optional settings. Click Save. 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: <ul style="list-style-type: none"> • ACS (Consumer) URL Validator* • ACS (Consume) URL* • Single Logout URL |

| Item | Description |
|----------------------|---|
| One-Time Password | <p>Select this option if you want users to enter a one-time password in addition to another type of authentication.</p> <p>Note: If you select this option, you must also add another authenticator to your authentication policy and rank it higher than the one-time password.</p> <p>For a walkthrough of the steps to add and remove one-time password authentication for administrators, see the following:</p> <ul style="list-style-type: none"> • Add one-time password authentication for administrators • Remove one-time password authentication for administrators <p>Do the following:</p> <ol style="list-style-type: none"> 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. |
| Ping Identity (OIDC) | <p>Select this option if you want users to authenticate using Ping Identity. Do the following:</p> <ol style="list-style-type: none"> 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. |

| Item | Description |
|----------------------|---|
| Ping Identity (SAML) | <p>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.</p> <p>For a walkthrough of the steps to configure your Ping Identity (SAML), see the following:</p> <ul style="list-style-type: none"> • 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 <p>The SSO Callback URL is generated when you add the authenticator and will be in the format <code>https://login.eid.blackberry.com/_/resume/saml20/<hash></code>.</p> <ol style="list-style-type: none"> In the drop-down list below Ping Identity, select SAML. Enter a name for the authenticator. 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. In the Login request URL field, enter the identity provider's single sign-on URL. In the IDP signing certificate field, paste the body of the signing certificate that you downloaded, including the Begin Certificate and End Certificate lines. <p>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.</p> <ol style="list-style-type: none"> 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. Specify any other optional settings. Click Save. 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: <ul style="list-style-type: none"> • Assertion Consumer Service (ACS) • Application URL |

4. Click **Save**.

After you finish: [Create an authentication policy](#) and [Manage the default authentication policies for your tenant](#).

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 [Enhanced authentication sign in](#).

| 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 | <p>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.</p> <p>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.</p> <p>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.</p> |
| 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. |
| Email claim | <p>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'.</p> <p>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.</p> |
| SP entity ID | <p>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).</p> <p>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.</p> |
| 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. |

| Item | Description |
|-----------------------|---|
| 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. |

Manage the default authentication policies for your tenant

By default, Cylance Endpoint Security has three tenant authentication policies that are used to manage the types of authentication that administrators must complete to sign in to the Cylance console and users must complete to activate the CylancePROTECT Mobile app or CylanceGATEWAY agent. The tenant policies are applied when no app exception or authentication policy is assigned to the user for the console or the app that they are trying to access. The default policies and their authenticators are:

- **Administration Console:** This policy uses the Cylance console password as the default authenticator. For tenants created after March 2024, this policy uses the Cylance console password and One-Time Password as the default authenticators. It is used for authentication to the Cylance Endpoint Security management console.
- **CylanceGATEWAY:** This policy uses the user's enterprise password as the default authenticator. It is used when users activate the CylanceGATEWAY app or desktop agent.
- **CylancePROTECT Mobile app:** This policy uses the user's enterprise password as the default authenticator. It is used when users activate the CylancePROTECT app on mobile devices. It is not applied when the user activates the desktop agent.

You can edit the policies to add other types of authentication that users must complete in the order that you specify in the policy. For example, if you add One-Time Password after the Enterprise authenticator, users enter their work or *myAccount* credentials before they receive a one-time password prompt.

Before you begin: [Add an authenticator](#).

1. On the menu bar, click **Settings > Authentication > Default Authentication**.
2. Click the policy that you want to edit.
3. In the **App Authentication** section, click **Add Authenticator**.

4. In the **Add authenticator** dialog box, in the drop-down list, select an authenticator. Click **Add**.

Repeat this step to add more authenticators to the policy. Users must complete the types of authentication in the order that you specify. To change the order, click **Set Order**, drag the authenticators to the order that you want and click **Set Order**.

Note: If you add One-Time Password as an authenticator, it must be set after the enterprise password. again.

5. Click **Save**.

If you add authenticators to a default policy, you can click **Revert to Default Method** on the policy list page to restore the default setting.

Create an authentication policy

You create an authentication policy to specify the types of authentication that administrators must complete to sign in to the Cylance Endpoint Security management console and users must complete to activate the

CylancePROTECT Mobile app or CylanceGATEWAY agent. Users must complete the types of authentication in the order that you specify in the policy. For example, if you add Enterprise before One-Time Password, users enter their work or *myAccount* credentials before they receive a one-time password prompt.



In a policy you can also configure app exceptions and specify different authenticators for specific apps. App exceptions take precedence over the authentication policy. Any authentication policies that are configured in your tenant are applied in the following order:

1. App exceptions in authentication policies that are assigned to users or groups
2. Authentication policies that are assigned to users or groups
3. Tenant authentication policy

Before you begin: [Add an authenticator](#)

1. On the menu bar, click **Policies > User Policy**.
2. Click the **Authentication** tab.
3. Click **Add policy**.
4. Enter a name and description for the policy.
5. In the **Authentication rules** section, click **Add Authenticator**.

If your authenticator was created before December 2023, and you updated Cylance Endpoint Security login request URL to enable the IDP-initiated Proxy to allow users to use single sign-on (SSO) to access the Cylance console after logging in to their users' IDP portal, add the updated authenticator and remove the original authenticator that was created. For more information, see [Enhanced authentication sign in](#).

6. In the **Add authenticator** dialog box, select an authenticator in the drop-down list.
Repeat this step to add more authenticators to the policy. Users receive prompts from each authenticator in the order that they are listed in the policy. If you add Duo Universal MFA to the policy, you should also add another authenticator so that Duo is used as a second factor for authentication. To change the order, click **Set Order**, drag the authenticators to the order that you want, and click **Set Order** again.
7. If you want to add app exceptions, click **Manage App Exceptions**.
8. In the **Manage App Exceptions** dialog box, select the apps that you want to include in the **Available apps** pane.
9. Click .
Click .
10. Click **Save**.
11. In the **Manage app exceptions** section, click the tab for one of the apps that you added as an exception.
12. Click **Add Authenticator**.
13. In the **Add authenticator** dialog box, select an authenticator from the drop-down list. Click **Save**.
Repeat this step to add more authenticators to the app exception. Users must complete the types of authentication in the order that you specify. To change the order, click **Set Order**, drag the authenticators to the order that you want and click **Set Order** again.
14. To save the policy, click **Save**.

After you finish: [Assign policies to administrators, users, and groups](#).

Custom authentication

Important: Custom authentication has been deprecated and will be removed in the near future. If you are using custom authentication to access Cylance Endpoint Security, you can migrate your external IDP to an authenticator and use enhanced authentication to access the Cylance console. For more information on enhanced authentication, see [Enhanced authentication sign in](#). To see a walkthrough on how to configure your

external IDP as an authenticator, see [Migrate external IDPs from Legacy Custom Authentication to the Modern Authenticator Framework](#).

Use external identity providers (IdP) to login to the management console. This requires configuring settings with your IdP to obtain an X.509 certificate and a URL for verifying your IdP login. Custom authentication works with Microsoft SAML 2.0. This feature has been confirmed to work with OneLogin, Okta, [Microsoft Azure](#), and PingOne. This feature also provides a custom setting and should work with other IdP's who follow Microsoft SAML 2.0.

Examples of using custom authentication, see the following articles.

- [Microsoft Azure](#)
- [Okta](#)
- [OneLogin](#)
- [PingOne](#)
- [Using SAML 2.0](#)

Note: Custom authentication does not support Active Directory Federation Services (ADFS).

Configure custom authentication

1. In the management console, click **Settings > Application** from the menu.
2. Select the **Custom Authentication** checkbox. Configuration options display.
3. Select the options you want to use for authentication. See [Custom authentication descriptions](#) for a description of options.
4. Click **Save**.

Custom authentication descriptions

| Option | Description |
|-----------------------|--|
| Strong authentication | Select this option to provide multi-factor authentication access. |
| Single sign-on | Select this option to provide single sign-on (SSO) access. Selecting strong authentication or SSO does not affect the custom authentication settings, because all configuration settings are handled by the identity provider (IdP). |
| Allow password login | Selecting this option allows you to login to the console directly and using SSO. This allows you to test your SSO settings without being locked out of the console. Once you have successfully logged into the console using SSO, it is recommended that you disable this feature. |
| Provider | Select the service provider for the custom authentication. |
| X.509 certificate | Enter the X.509 certification information. |
| Login URL | Enter the URL for the custom authentication. |

Migrate external IDPs from Custom Authentication to an authenticator

When you sign in to the management console using an external identity provider (IDP) that is configured for custom authentication, you must sign in using the 'Or sign in with your External Identity Provider' link with your external IDP credentials. BlackBerry recommends that you configure your external IDP as an authenticator and

use an authentication policy to sign in from the main sign in screen using your IDP credentials. Configuring your external IDP as an authenticator provides more granularity and flexibility in the authentication configuration.

To configure an external IDP to sign in to the management console from the main sign in screen, perform the following actions. For more information, see [How Do I Migrate external IDPs from custom authentication to an authenticator](#).

If you configured your existing IDP as an authenticator before December 2023 and you want to allow users to directly access the Cylance console from the IDP user portal, see [Enhanced authentication sign in](#).

| Step | Action |
|------|--|
| 1 | Review the Considerations for adding SAML authenticators . |
| 2 | Sign in to the Cylance console with your external IDP . |
| 3 | Configure the external IDP to communicate with Cylance Endpoint Security . <ul style="list-style-type: none">Record the custom authentication informationConfigure the authenticator |
| 4 | Manage the default authentication policies for your tenant that uses the authenticator that you created. Note: As a failsafe, create one user policy that only uses the Cylance console password and assign it to one administrator. |
| 5 | Verify that the Allow Password Login check box (Settings > Application > Custom Authentication) is selected. This option allows you to log in to the console directly and use SSO. Enable this option to test your SSO settings without being locked out of the console. |
| 6 | Sign in to the Cylance console from the main sign in screen and test the external IDP sign in credentials policy . |
| 7 | (Optional) Disable Custom Authentication (Settings > Application). |

Migrate custom authentication settings to the authenticators list

You can migrate your existing SAML authenticators to the authenticators list in Settings so that you add them to authentication policies for users and groups or your tenant. When you migrate the authenticators, you must update the single sign-on URL to the URL used by Cylance Endpoint Security. You must also update the NameID claim in your external IDP configuration so that it returns a persistent, immutable value instead of a user's email address or create a claim in the identity provider that can be used as the Federated ID claim.

Before you migrate your settings, as a failsafe, you should create one authentication policy that requires only the Cylance console password and assign it to one administrator.

Note: When you migrate the custom authentication settings, in the external identity provider, you must add the following Cylance Endpoint Security login request URL: https://idp.blackberry.com/_/resume. 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 URL to the list as a secondary option or replace the original.

For more information about SAML authenticators, see [Considerations for adding SAML authenticators](#).

Before you begin: Download a copy of the signing certificate for your IDP.

1. In the management console, on the menu bar, click **Settings > Application**.
2. In the **Custom authentication** section, complete the following:
 - a) Copy the following information to a text file:
 - Provider name
 - Login URL
 - b) Select the **Allow Password Login** checkbox. For more information about this setting, see [Custom authentication descriptions](#).
3. On the menu bar, click **Settings > Authentication**.
4. On the **Authenticators** tab, click **Add authenticator**.
5. In the **Authenticator Type** drop-down list, click the SAML authenticator that corresponds to the provider you copied in step 2 (for example, Entra or Okta) or click Custom SAML.
6. In the **General Information** section, enter a name for the authenticator.
7. In the **SAML Configuration** section, if you want to require users to validate their email with a one-time code when they log in for the first time, turn on **Validation required**.
8. In the **Login request URL** field, enter the single sign-on URL for the identity provider.
9. In the **IDP signing certificate** field, paste the 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.

10. Do one of the following:

| Task | Steps |
|---|--|
| Update the NameID and email claim values in the external identity provider. | <ol style="list-style-type: none">a. Sign in to your external identity provider.b. Update the single sign-on URL for Cylance Endpoint Security to <code>https://idp.blackberry.com/_/resume</code>. You can add this URL to the existing login.<region>.cylance.com URL.c. Edit the NameID claim so that it returns a persistent, immutable value (for example, objectGUID or a UUID) that can be used in the Federated ID claim instead of the user's email address. For instructions, see the documentation from the identity provider.d. Create a new email claim that will return the user's email address. |
| Create a new claim in your external identity provider and add it to the authenticator settings. | <ol style="list-style-type: none">a. Sign in to your external identity provider.b. Update the single sign-on URL for Cylance Endpoint Security to <code>https://idp.blackberry.com/_/resume</code>. You can add this URL to the existing login.<region>.cylance.com URL.c. Create a new claim that returns a persistent, immutable ID for a user. For instructions, see the documentation from the identity provider.d. In the Cylance management console, in the Email claim field, enter nameID. The nameID value must use a lowercase "n."e. In the Federated ID claim field, enter the name of the new claim that you created in the external identity provider. |

11. Click **Save**.

After you finish:


- [Create an authentication policy.](#)
- If you encounter issues logging in using the SAML authenticator in an authentication policy, you can download a sample SAML response from your IDP and validate the claim names.

Setting up administrators

You can control how administrator users access and use the management console by assigning predefined or custom roles to them. This role-based access control allows you to give administrators access to the specific console features needed for their role and restrict the features you don't want them to have access to.

For more information on roles and permissions, see [Permissions for administrator roles](#).

Add an administrator

You can add administrator users to the management console to grant those users the ability to control and configure your Cylance Endpoint Security environment. Existing and newly added administrator accounts are displayed on the User page (Assets > Users) in the management console. You can add the Administrator column to display an  icon beside each administrator account. The screens that an administrator user can view in the management console, and the features that the user is able to configure and change, depend on the role that you assign to that user. For more information on roles and permissions, see [Permissions for administrator roles](#).

1. In the management console, on the menu bar, click **Settings > Administrators**. Do any of the following:

| Task | Steps |
|-------------------------------|--|
| Add a new administrator. | <ol style="list-style-type: none">Under Add users, in the Enter email field, type the user's email addressIn the Select role drop-down list, click a role. For more information about roles and their associated permissions, see Managing roles.If you selected a zone manager or user role, in the Select Zone drop-down list, click a zone.Click Add. <p>Cylance Endpoint Security sends an email to the new administrator user with a link to create a password.</p> |
| Change an administrator role. | <ol style="list-style-type: none">Click an administrator user.In the drop-down list, click a new role.If you selected the Zone Manager or User role, do the following:<ol style="list-style-type: none">Choose the Default Zone Role to assign to the user when a new zone is created. The default is "None."Adjust the user's role for each zone accordingly.<p>Note that if a user is assigned Zone Manager for at least one zone, they will inherit some Zone Manager abilities such as the ability to view the list of device policies, download the installer, and view the global list. However, the user could only perform Zone Manager abilities on devices that are in zones where they are assigned the Zone Manager role. Likewise, the user could only perform User abilities on devices that are in zones where they are assigned the User role.</p>In the pop-up window, enter your password.Click Save. |

2. On the menu bar, click **Assets > Users**. Do any of the following:

- To add or remove columns, click **|||** and select the columns that you want to view.
- To sort users in ascending or descending order by a column, click the column.
- To filter users by a column, use the filter field and icon for the column.
- To view only administrator accounts, click **≡** and set the Administrator option to **True**.

Permissions for administrator roles

The following tables list out the default permissions for system-defined roles within the management console. Permissions in bold have child permissions that are only available after the main permission is selected.

The data that zone managers can view in the console is limited to the zones that they manage.

Dashboard

These permissions provide access to the dashboard page and cannot be disabled. The information displayed on the dashboard is determined by the role and permissions assigned to the administrator role.

| Permission | Administrator | Zone Manager | User | Read-Only |
|------------|---------------|--------------|------|-----------|
| Dashboard | ✓ | ✓ | ✓ | ✓ |

Endpoint Detection Response

These permissions allow you to manage CylanceOPTICS features.

| Permission | Administrator | Zone Manager | User | Read-Only |
|-----------------------------|---------------|--------------|------|-----------|
| View detections | ✓ | ✓ | | ✓ |
| Edit detections | ✓ | | | |
| Delete detections | ✓ | | | |
| View, create InstaQuery | ✓ | ✓ | | ✓ |
| Delete InstaQuery | ✓ | | | |
| View, create advanced query | ✓ | ✓ | | ✓ |
| Create shared template | ✓ | | | |
| Delete shared template | ✓ | | | |
| Delete shared snapshots | ✓ | | | |
| Delete shared export query | ✓ | | | |

| Permission | Administrator | Zone Manager | User | Read-Only |
|-------------------------------|---------------|--------------|------|-----------|
| Create scheduled query | ✓ | | | |
| Edit shared scheduled query | ✓ | | | |
| Delete shared scheduled query | ✓ | | | |
| View, create focus data | ✓ | ✓ | | ✓ |
| View package deploy | ✓ | | | ✓ |
| Create package deploy | ✓ | | | |
| Update package deploy | ✓ | | | |
| Delete package deploy | ✓ | | | |
| View playbook results | ✓ | ✓ | | ✓ |
| Delete playbook results | ✓ | | | |
| View package | ✓ | | | ✓ |
| Create package | ✓ | | | |
| Delete package | ✓ | | | |
| View playbook | ✓ | | | ✓ |
| Create, edit playbook | ✓ | | | |
| Delete playbook | ✓ | | | |
| View ruleset* | ✓ | | | |
| Edit ruleset | ✓ | | | |
| Delete ruleset | ✓ | | | |
| View rules | ✓ | | | |
| Create, edit custom rule | ✓ | | | |
| Delete custom rule | ✓ | | | |
| View exceptions | ✓ | | | |
| Create, edit exceptions | ✓ | | | |

| Permission | Administrator | Zone Manager | User | Read-Only |
|-------------------------------------|---------------|--------------|------|-----------|
| Delete exceptions | ✓ | | | |
| View lockdown configuration | ✓ | | | |
| Create, Edit lockdown configuration | ✓ | | | |
| Delete lockdown configuration | ✓ | | | |

*To view a rule set, you require an administrator role with the View ruleset and Edit ruleset permissions.

Users and Devices

These permissions control what you can do with users and devices in the management console. You have to have global list permissions to global quarantine or add a threat to the safe list from these pages.

| Permission | Administrator | Zone Manager | User | Read-Only |
|-------------------------|---------------|--------------|------|-----------|
| View users and groups | ✓ | | | ✓ |
| Create users and groups | ✓ | | | |
| Edit users and groups | ✓ | | | |
| Delete users and groups | ✓ | | | |
| View mobile devices | ✓ | | | ✓ |
| Delete mobile devices | ✓ | | | |
| View devices | ✓ | ✓ | ✓ | ✓ |
| Edit devices | ✓ | | | |
| Delete devices | ✓ | | | |
| Lock Optics device | ✓ | | | |
| Unlock Optics device | ✓ | ✓ | | |
| Execute remote response | ✓ | | | |
| Allow file download | ✓ | | | |
| View device policies | ✓ | ✓ | | ✓ |
| Create device policies | ✓ | | | |

| Permission | Administrator | Zone Manager | User | Read-Only |
|------------------------|---------------|--------------|------|-----------|
| Edit device policies | ✓ | | | |
| Delete device policies | ✓ | | | |
| View zones | ✓ | ✓ | ✓ | ✓ |
| Create zones | ✓ | | | |
| Edit zones | ✓ | | | |
| Delete zones | ✓ | | | |

Threat Protection

These permissions provide access to the protection menu, CylancePROTECT Mobile alerts, and vulnerabilities.

| Permission | Administrator | Zone Manager | User | Read-Only |
|------------------------------------|---------------|--------------|------|-----------|
| View, create, edit, delete Persona | ✓ | | ✓ | ✓ |
| View threat protection | ✓ | ✓ | ✓ | ✓ |
| Edit Protect Mobile events | ✓ | | | |
| View Protect Mobile policies | ✓ | | | ✓ |
| Create Protect Mobile policies | ✓ | | | |
| Edit Protect Mobile policies | ✓ | | | |
| Delete Protect Mobile policies | ✓ | | | |

Network

These permissions allow you to manage network protection settings, including network access control, CylanceGATEWAY settings, and CylanceGATEWAY alerts and events.

| Permission | Administrator | Zone Manager | User | Read-Only |
|---------------------------------|---------------|--------------|------|-----------|
| View Gateway service policies | ✓ | | | ✓ |
| Create Gateway service policies | ✓ | | | |

| Permission | Administrator | Zone Manager | User | Read-Only |
|---------------------------------|---------------|--------------|------|-----------|
| Edit Gateway service policies | ✓ | | | |
| Delete Gateway service policies | ✓ | | | |
| View network access controls | ✓ | | | ✓ |
| Edit network access controls | ✓ | | | |
| View Gateway settings | ✓ | | | ✓ |
| Create Gateway settings | ✓ | | | |
| Edit Gateway settings | ✓ | | | |
| Delete Gateway settings | ✓ | | | |
| View Gateway reporting events | ✓ | | | ✓ |
| View Gateway alerts and events | ✓ | | | ✓ |

Avert

These permissions allow you to manage CylanceAvert features.

| Permission | Administrator | Zone Manager | User | Read-Only |
|------------------------------|---------------|--------------|------|-----------|
| View Avert settings | ✓ | | | ✓ |
| Edit Avert settings | ✓ | | | |
| View Avert device identifier | ✓ | | | ✓ |
| View Avert risk scores | ✓ | | | ✓ |
| View Avert device events | ✓ | | | ✓ |
| View Avert policies | ✓ | | | ✓ |
| Create Avert policies | ✓ | | | |
| Edit Avert policies | ✓ | | | |
| Delete Avert policies | ✓ | | | |

| Permission | Administrator | Zone Manager | User | Read-Only |
|-----------------------------------|---------------|--------------|------|-----------|
| View Avert sensitive file summary | ✓ | | | |
| View Avert file content | ✓ | | | |
| Delete Avert files | ✓ | | | |

Common

These permissions allow administrators to manage tenant-level settings that affect multiple features in the Cylance Endpoint Security solution, including EMM providers and directories, enrollment for mobile devices and CylanceGATEWAY, and adaptive risk options and events. For directory connections, you can create Microsoft Entra ID active directories (AD) only.

| Permission | Administrator | Zone Manager | User | Read-Only |
|------------------------------------|---------------|--------------|------|-----------|
| View EMM connections | ✓ | | | ✓ |
| Create EMM connections | ✓ | | | |
| Edit EMM connections | ✓ | | | |
| Delete EMM connections | ✓ | | | |
| View directory connections | ✓ | | | ✓ |
| Create directory connections | ✓ | | | |
| Edit directory connections | ✓ | | | |
| Delete directory connections | ✓ | | | |
| View on-prem directory connector | ✓ | | | ✓ |
| Create on-prem directory connector | ✓ | | | |
| Edit on-prem directory connector | ✓ | | | |
| Delete on-prem directory connector | ✓ | | | |
| View authentication controls | ✓ | | | ✓ |
| Create authentication controls | ✓ | | | |
| Edit authentication controls | ✓ | | | |
| Delete authentication controls | ✓ | | | |
| View enrollment policies | ✓ | | | ✓ |

| Permission | Administrator | Zone Manager | User | Read-Only |
|-------------------------------|---------------|--------------|------|-----------|
| Create enrollment policies | ✓ | | | |
| Edit enrollment policies | ✓ | | | |
| Delete enrollment policies | ✓ | | | |
| View adaptive risk policies | ✓ | | | ✓ |
| Create adaptive risk policies | ✓ | | | |
| Edit adaptive risk policies | ✓ | | | |
| Delete adaptive risk policies | ✓ | | | |
| View adaptive risk settings | ✓ | | | ✓ |
| Create adaptive risk settings | ✓ | | | |
| Edit adaptive risk settings | ✓ | | | |
| Delete adaptive risk settings | ✓ | | | |
| View OneAlert Events | ✓ | | | ✓ |
| Edit OneAlert Events | ✓ | | | |
| Delete OneAlert Events | ✓ | | | |

Logging

These permissions allow you to view reports and the audit log.

| Permission | Administrator | Zone Manager | User | Read-Only |
|----------------|---------------|--------------|------|-----------|
| View reports | ✓ | | | ✓ |
| View audit log | ✓ | | | |

Settings

These permissions allow you to manage management console settings. User management permissions and role management permissions are associated. If a user is assigned a role with user management permissions selected, the user will also have access to role management functionality.

| Permission | Administrator | Zone Manager | User | Read-Only |
|-------------|---------------|--------------|------|-----------|
| Application | ✓ | ✓ | | ✓ |

| Permission | Administrator | Zone Manager | User | Read-Only |
|----------------------------------|---------------|--------------|------|-----------|
| Installation Token management | ✓ | | | |
| Installer Download | ✓ | ✓ | | |
| Invitation URL | ✓ | | | |
| Uninstall Password Management | ✓ | | | |
| Support Login | ✓ | | | |
| Syslog/SIEM | ✓ | | | |
| Custom Authentication | ✓ | | | |
| Threat Data Report | ✓ | | | |
| User Management | ✓ | ✓ | | |
| View Global List | ✓ | ✓ | | ✓ |
| Create Global List | ✓ | | | |
| Edit Global List | ✓ | | | |
| Delete Global List | ✓ | | | |
| View Agent Update Settings | ✓ | | | ✓ |
| Create Agent Update Settings | ✓ | | | |
| Edit Agent Update Settings | ✓ | | | |
| Delete Agent Update Settings | ✓ | | | |
| Certificates | ✓ | ✓ | | ✓ |
| Integrations | ✓ | | | ✓ |
| View device lifecycle settings | ✓ | | | ✓ |
| Create device lifecycle settings | ✓ | | | |
| Edit device lifecycle settings | ✓ | | | |
| Delete device lifecycle settings | ✓ | | | |
| View activation settings | ✓ | | | ✓ |
| Edit activation settings | ✓ | | | |

Managing roles

You can use predefined roles or create custom roles to manage administrator access to features in the management console. Predefined roles have set permissions that cannot be modified. Based on your role's permissions, some menu options, pages, and features may not be available. For example, if a user does not have access to the zones feature, the zones menu option does not display. The Dashboard screen is available for all predefined and custom roles, but the data it displays only reflects the zones that the logged in user is allowed to manage.

For a comprehensive list of user permissions allowed for each predefined role, see [Permissions for administrator roles](#). Users assigned to a custom role cannot enable notifications on the My Account page.

Add a role

Custom roles are globally scoped and provide full operational access to the related pages and actions for a defined area. For example, if a custom role has permissions allowed for the zone features, any user assigned to the role has access to all functionality available on the Zones or Zone Details pages.

If access is not selected for a role, users will not see that page in the menu or be able to navigate to the page from anywhere within the console. For example, if a custom role has permissions allowed for threats and disallowed for devices, the Threat Protection page displays in the menu while the Devices page does not. If the user views the Threat Details page for a threat, the affected devices and zones will display but the user will receive an error page when attempting to click the link for details for a specific device.

1. In the management console, on the menu bar, click **Settings > Administrators**.
2. Click **Roles**.
3. Click **Add New Role**.
4. Type a name for the role.
5. Click the **Access** checkbox beside any feature that you want to allow this role to access. Expand sections to see more options. See [Permissions for administrator roles](#) for more information.
6. Click **Add Role**.

After you finish:

- To edit a role, click an existing role and modify the name or permissions. The updated name or permissions will be applied to any users assigned to the existing role.
- If a predefined or custom role has users assigned, you can click the link in the **Assigned Users** column to view the email for any users assigned to that role. You can click the email to view the User Details page for that user.
- To delete a role, click a checkbox beside a role that does not have any users assigned to it, then click **Remove**. If a role has users assigned to it, you cannot select the checkbox.

Configure the session and idle timeout limits

You can specify how long an administrator can remain logged in to the management console before they are signed out, even if the session is active. You can also specify how long a session is allowed to remain idle before the administrator is logged out of the console.

1. In the management console, on the menu bar, click **Settings > Authentication**.
2. On the **Settings** tab, in the **Console Timeout** section, configure the **Session timeout** limit.

Administrators will receive a countdown prompt a few minutes before the session timeout limit is reached that will allow them to authenticate again to continue the session. If the administrator does not actively respond

to the prompt by clicking **Verify** and logging in again, they are logged out when the session timeout limit is reached.

3. Configure the **Idle timeout limit.**

Administrators are not warned prior to the idle timeout expiring and will be automatically logged out.

4. Click **Save.**

Setting up zones to manage CylancePROTECT Desktop and CylanceOPTICS

You can use zones to group and manage CylancePROTECT Desktop and CylanceOPTICS devices. You can group devices based on geography (for example, Asia and Europe), function (for example, Sales and IT staff), or by any criteria that your organization requires.

You can assign a device policy to a zone and apply that device policy to the CylancePROTECT Desktop and CylanceOPTICS devices that belong to that zone. You can also add a zone rule to add devices to a zone based on criteria specified in a saved query, like domain name, IP address range, or operating system. New devices will be automatically added to a zone if they match the zone rules criteria.

By default, devices that are added automatically to the zone will follow the zone rules. If the automatic device removal option is selected in the zone rules, devices that follow the zone rules will be automatically removed from the zone when they don't meet the zone rules criteria. You can also manually add devices that ignore the zone rules so they aren't automatically removed from the zone. When managing a zone, you can change whether a device follows or ignores the zone rules.

Note that administrator users with the Zone Manager role can install agents on devices, but they do not have access to the default zone (Unzoned), so they cannot assign devices to zones.

When you create a new Cylance Endpoint Security tenant, or when you reset a tenant to the recommended default state, BlackBerry provides preconfigured zones and preconfigured device policies that are designed to help you tune your environment to the desired security posture. For more information, see [Configuring a new Cylance Endpoint Security tenant](#).

Add and configure a zone

Before you begin: If you want to add a zone rule to the zone, you need to create and save a query from the Assets > Devices screen. The list of devices in the results of the saved query indicates the devices that will be automatically added to the zone.

1. In the management console, on the menu bar, click **Zones**.
2. Click **Add New Zone**.
3. In the **Zone Name** field, type a name for the zone.
4. In the **Policy** drop-down list, click a device policy to associate with the zone.
5. In the **Value** field, click the appropriate priority level for the zone. This setting has no impact on managing zones or devices.
6. Click **Save**.
7. In the zones list, click the name of the zone that you created.
8. Do any of the following:

| Task | Steps |
|--|--|
| Add a zone rule to automatically add devices. | <p>You need a saved query to add a zone rule.</p> <ol style="list-style-type: none"> Click Create Rule. Select a saved query. The query can contain any of the following fields only; if a query contains a field that is not in this list, you cannot use it: <ul style="list-style-type: none"> Device name DNS name IP addresses MAC addresses OS version OS build/kernel version Distinguished Name Member of (LDAP) If you want to automatically apply the device policy that's associated with the zone, select Apply zone policy to devices when they are added to the zone. This option is not available if the associated device policy is set to None. If you want to automatically remove devices that do not match the criteria of the zone rule from the zone, select Remove devices automatically from this zone. This only affects devices that follow the zone rules. If you don't want to associate and apply a device policy to devices in this zone, select None. Click Save. |
| Manually add devices to the zone. | <p>When you manually add a device to a zone, the device ignores the zone rules by default. A device that ignores the zone rules will remain in the zone even when it doesn't match the zone rule criteria.</p> <ol style="list-style-type: none"> On the Devices tab, click Add Device to Zone. Select the devices that you want to add. You can apply filters to find devices. If you want to apply the zone device policy to those devices, select the Apply zone policy to selected devices check box. Click Save. |
| Apply the zone device policy to all the users in the zone. | <p>This action replaces any device policies that are currently assigned to devices with the device policy that is currently assigned to the zone. If you choose None for the associated policy, the option to automatically assign a policy will no longer be available. You also cannot apply a policy to all devices as the option will not be available.</p> <ol style="list-style-type: none"> Select the Apply to all devices in this zone check box. Click Save. |

| Task | Steps |
|---|--|
| Set a device to follow or ignore a zone rule. | <p>In the list of devices in a zone, devices that follow that zone rule can be identified from the Zone Rule column. Devices that follow the zone rules are subject to automatic removal from the zone. Devices that ignore the zone rules will remain in the zone (unless you remove them manually).</p> <ol style="list-style-type: none"> On the Devices tab, select one or more devices. Click Follow Zone Rule or Ignore Zone Rule. Click Yes. |
| Copy devices to another zone. | <ol style="list-style-type: none"> On the Devices tab, select one or more devices. Click Copy Device. Select one or more zones. Click Save. |
| Remove devices from the zone. | <ol style="list-style-type: none"> On the Devices tab, select one or more devices. Click Remove Device from Zone. Click Yes. |

Setting up CylancePROTECT Desktop

| Step | Action |
|------|---|
| 1 | Review the CylancePROTECT Desktop requirements . |
| 2 | <p>Create and configure a device policy.</p> <ul style="list-style-type: none">• New tenants include preconfigured zones and device policies that make it easier for you to tune your environment to the desired security posture.• Review the recommendations for creating and testing device policies.• Review the recommendations for zone management. |
| 3 | <p>Install the CylancePROTECT Desktop agent on devices.</p> <ul style="list-style-type: none">• Installing the CylancePROTECT Desktop agent for Windows• Installing the CylancePROTECT Desktop agent for macOS• Installing the CylancePROTECT Desktop agent for Linux <p>If you want to use an RMM solution to install the CylancePROTECT Desktop agent on devices, see Using RMM solutions to install the Cylance agents on devices.</p> |
| 4 | Manage updates for the CylancePROTECT Desktop and CylanceOPTICS agents . |

Testing your CylancePROTECT Desktop deployment

Before you deploy the CylancePROTECT Desktop agent to devices, you should test how it behaves with other applications in a test environment so that you can verify that the applications that are used in your organization are allowed to run and work as expected. For example, if you discover that the agent blocks some applications from running properly, you can configure exclusions to allow them to do so.

When you create a new Cylance Endpoint Security tenant, or when you reset a tenant to the recommended default state, BlackBerry provides preconfigured zones and preconfigured device policies that are designed to help you tune your environment to the desired security posture. For more information, see [Configuring a new Cylance Endpoint Security tenant](#).

When you want to test the agent, install it on test systems that include applications that are used in your organization to make sure that it accurately represents a real-world environment.

To test the agent, you do the following:

1. Create test policies.
2. Create test zones.

Device policies contain the settings for the agent and tell it what to do when it encounters a threat. Zones help you group your systems by geographical location, business unit, operating system, or other group properties. Zone rules help you automatically assign systems to a zone based on the criteria that you set (for example, operating system, IP address range, and other criteria). You should test policies and zones to familiarize yourself with these features and to help you plan how to use these features in your organization.

Create a CylancePROTECT Desktop test policy

You should implement CylancePROTECT Desktop policy features in a phased approach to ensure performance and operations are not impacted. By default, when you create a device policy, policy features are not enabled and you must manually enable them. As you understand the types of threats that are logged in your environment and how the CylancePROTECT Desktop agent behaves, you can gradually enable more policy features.

It is recommended that you test device policies on devices that include the applications that are used in your organization. It is important that the devices that you use to test device policies accurately represent the devices that are in your production environment, and not just a clean machine, to ensure that applications are allowed to run properly when policies are enforced through the CylancePROTECT Desktop agent. For example, you might select a subset of devices in your production environment that include all applications (proprietary and custom) that users need for their daily activities.

The agent uses execution control and process monitoring to analyze running processes only. This includes all files that run at startup, that are set to auto-run, and that are manually executed by the user. The agent only sends alerts to the management console. By default, no files are blocked or quarantined.

1. In the management console, click **Policies > Device Policy > Add new policy**.
2. In the **Policy Name** field, type a name for the test policy.
3. Enable **Auto Upload** to analyze and send suspicious files to the CylancePROTECT cloud services for further analysis.
 - a) In the **File Actions** tab, in the **Auto Upload** section, select all the file types that are available.
 - b) Click **Create** to create the initial test policy.
 - c) Assign the initial test policy to the CylancePROTECT Desktop endpoints that you are using for testing.
 - d) Allow the devices that are assigned to the test policy to run for at least one day to allow applications and processes that are typically used on the device to run and be analyzed. You may want to consider any required applications that run periodically on a device (for example, once a week) that may need to be monitored outside of this test run.
 - e) While testing the policy, navigate to the **Protection > Threats** screen in the management console to view a list of applications and processes that CylancePROTECT considers to be a threat (abnormal or unsafe) and identify the ones that should be allowed to run on the endpoint. You can click a threat to view more information about it and download the malicious file to perform your own threat research. The malicious file is unaltered but renamed using the SHA256 hash without a file extension to prevent the accidental detonation of it. If you rename it to include the original file extension, the malicious file may be run. No personally identifiable information is shared with the console or with other tenants or organizations.
 - f) Navigate to **Policies > Device Policy** and edit the device policy to allow specific applications and processes to run on endpoints that have this policy assigned to them. You can add files to the **Policy Safe List** section in the **File Actions** tab.

You may also quarantine or waive files on specific devices or all devices in your organization. For more information, see [Managing safe and unsafe lists for CylancePROTECT Desktop](#).

4. Edit the device policy to enable the background threat detection scans to analyze executable files on the disk that may be dormant threats.
 - a) In the **Protection Settings** tab, enable the **Background Threat Detection** setting and select the **Run Once** option. Although periodic scanning is not necessary due to the predictive abilities of the solution, you may select **Run Recurring** to enable it, for example, for compliance purposes.
 - b) Enable the **Watch For New Files** setting. This setting may negatively impact performance on the device. Adding folder exclusions may help reduce the impact.
 - c) To exclude specific folders from background threat detection, select **Exclude Specific Folders (includes subfolders)** and specify the folders to exclude. To allow the execution of files in the folders that you specified, select **Allow execution**. For more information about these fields, see [Device policy: Malware Protection settings](#).
 - d) Click **Save** to save the policy.

- e) Test the policy again and make sure that any applications that users are required to use are allowed to run. Background threat detection scanning may take up to one week, depending on how busy the system is and the number of files that require analysis. If necessary, make sure to add files to the policy safe list, global safe list, or waive them for individual devices. You can also exclude the folder containing the file in the protection settings.
5. Edit the device policy to kill unsafe processes that are running on the system. For example, when a threat is detected in an executable file (.exe or .msi) and it is considered to be unsafe, this setting kills running processes and their sub-processes.
 - a) In the **Protection Settings** tab, enable the **Kill Unsafe Running Processes** setting.
6. Edit the policy to enable the auto-quarantine settings for unsafe and abnormal files.
 - a) In the **File Actions** tab, under the **Unsafe** table column, enable the **Auto Quarantine** setting beside **Executable** to automatically move unsafe files to the quarantine folder on the device. Unsafe files have malware attributes and are likely to be malware.
 - b) Under **Abnormal**, enable **Auto Quarantine** to automatically move abnormal files to the quarantine folder on the device. An abnormal file has fewer malware attributes than an unsafe file and is less likely to be malware.
7. Edit the policy to enable memory protection settings to handle memory exploits, process injections, and escalations.
 - a) In the **Memory Actions** tab of the device policy, enable **Memory Protection** and set the violation types to **Alert**. When a violation type is set to alert and a threat of that type is detected, the agent sends information to the console but does not block or terminate any processes running in the device memory.
 - b) While testing the policy, navigate to the **Protection > Memory Protection** screen in the console to view a list of memory protection alerts for processes may be a threat.
 - c) If you determined that any of the processes are safe for daily business activities, you can add exclusions for the processes that you want to allow to run. In the **Memory Actions** tab of the device policy, click **Add exclusion** and specify the relative path to the file.
 - d) After you have specified the exclusions for processes that you want to allow to run, set the action to **Block** for all violation types. When a violation type is blocked, the agent sends information to the console and blocks the malicious process from running in the memory. The application that called the malicious process is allowed to continue to run.
8. Edit the policy to enable the device control settings. This example demonstrates how to block access to all device types and allow the exceptions, but you may choose to allow full access to all device types and block the exceptions instead.
 - a) In the **Device Control** tab of the device policy, enable the **Device Control** policy.
 - b) Set the access level for each of the USB device types to **Full Access**.
 - c) Save the policy.
 - d) On the test device, insert a USB device.
 - e) In the management console, navigate to **Protection > External Devices** and identify the vendor ID, product ID, and serial number of any devices that you want to allow. Not all manufacturers use a unique serial number with their products; some manufacturers use the same serial number for multiple products.
 - f) In the **Device Control** tab of the device policy, in the **External Storage Exclusion List** section, click **Add device** to add any devices that you want to allow.
 - g) Once testing is complete, set the access level for each of the device types to **Block**. You can add any exclusions as needed.
9. Edit the policy to enable the script control settings. The suggested testing time is 1 to 3 weeks.
 - a) In the **Script Control** tab of the device policy, enable the **Script Control** policy.
 - b) Set the policy for each of the script types to **Alert**. The longer the time script control is set to alert, the more likely you are to find infrequently run scripts used in the organization.

Note: Enabling the script control setting can cause a high-volume of events if scripts are used to manage Active Directory settings.

- c) Navigate to **Protection > Script Control** and identify the scripts that were run on devices that you want to allow.
- d) In the **Script Control** tab of the device policy, in the **Exclude Files, Scripts or Processes** section, click **Add exclusion** and specify a relative process path of the scripts that you want to allow (for example, \Cases\AllowedScripts).
- e) After you have added the exclusions for scripts that you want to allow to run, you can set the policy for each of the script types to **Block**.

Exclusions and when to use them

The following table provides a description of each type of exclusion and general guidance about when and how to use them appropriately.

| Exclusion type | Description and example |
|---------------------------------|---|
| Policy safe list (File Actions) | <p>The policy safe list is specified in the File Actions tab in a device policy.</p> <p>When a device policy is assigned to a device, the device is allowed to run files that are specified in the policy safe list. The policy safe list is applied at the policy level for specific devices whereas the global safe list or quarantine list is applied at the global level for all devices. The policy safe list takes precedence over the global quarantine list. A file that is added to the policy safe list is allowed to run on any device that is assigned the policy, even if that file is in the global quarantine list, which blocks files from running on all devices.</p> <p>Example: You frequently use privilege escalation tools like PSEXEC to perform your daily tasks. You do not want other users to have the same ability, and you want to prevent them from using such tools without impacting your own daily duties. To do this, you can add PSEXEC to the global quarantine list and add the same file hash to your policy safe list. Then you ensure that only you and other authorized users are assigned to that particular device policy where you added PSEXEC to the safe list. The result is that all users that are not assigned to the device policy will have PSEXEC quarantined, but users that are assigned to the device policy are able to use it.</p> |

| Exclusion type | Description and example |
|---|--|
| Exclude executable or macro files (Memory Protection) | <p>Exclusions for the memory protection policy are specified in the Memory Actions tab in a device policy when Memory Protection is enabled.</p> <p>When you specify exclusions for memory protection, the agent ignores violations of specific types from each specific application. In other words, you avoid blocking or terminating an application when it performs an action that causes a violation of a certain type.</p> <p>When memory protection is enabled, the agent monitors application processes for specific actions that they perform. If a process performs a particular action that the agent is monitoring for, such as an LSASS read, the agent reacts to that action according to the device policy. Sometimes false positives occur and memory protection blocks an action that an application tried to perform, or terminates the application completely. In this situation, you can specify exclusions for memory protection so that certain applications are exempt from specific violation types and can run as intended without being blocked or terminated.</p> <p>Example: Your organization blocks all memory protection violations from all applications by default. You use Test.exe frequently and you understand that it has legitimate reasons for LSASS read violations only. You can add an exclusion so that the agent ignores only LSASS read violations from Test.exe. The agent still blocks Test.exe when a violation of any other type occurs.</p> <p>Memory protection exclusions use relative paths (drive letters are not required) and can be specified down to the executable level. For example:</p> <ul style="list-style-type: none"> • \Application\Subfolder\Test.exe • \Subfolder\executable <p>Note: It is not recommended to specify an exclusion at the executable level without a relative path. For example, if an exclusion is set for \Test.exe, a malicious file with the same name would be allowed to run from any folder on the device.</p> |
| Exclude specific folders (Protection Settings) | <p>Exclusions for background threat detection are specified in the Protection Settings tab in a device policy when Background Threat Detection is enabled. This may be known as directory safelisting. When a directory is excluded, the agent ignores any files in that directory during a scan, including any sub-folders.</p> <p>If you select Allow Execution, the agent ignores any executables that are launched from the excluded directories.</p> <p>Example: An application developer in your organization uses a directory (for example, C:\DevFiles\Temp) to store temporary files that are generated during compilation. The agent scans these files, considers them to be unsafe due to various characteristics found in them, and subsequently quarantines them. The developer submits a request to allow the temporary directory. You can add the C:\DevFiles\Temp directory so that the temporary files are ignored and the developer can perform their work.</p> |

| Exclusion type | Description and example |
|------------------------------------|---|
| Folder exclusions (Script Control) | <p>Exclusions for the script control policy are specified in the Script Control tab in a device policy when Script Control is enabled. You can add exclusions when you want to allow scripts to run in a specified directory. When adding script control exclusions, specify the relative paths. Subfolders are also included in the exclusion.</p> <p>Example: An IT administrator is attempting to run a script located in <code>C:\Scripts\Subfolder\Test</code>. The script is blocked by script control every time the IT administrator attempts to run it. To allow the script to run, you can add one of the following relative paths as an exclusion to the script control policy:</p> <ul style="list-style-type: none"> • <code>\Scripts\Subfolder\Test</code> • <code>\Subfolder\Test\</code> • <code>\Scripts\Subfolder\</code> • <code>\Scripts\</code> • <code>\Subfolder\</code> • <code>\Test\</code> |

Create and manage a device policy


You create and assign device policies to control the features of the CylancePROTECT Desktop and CylanceOPTICS agents, and to configure how you want the agents to detect and respond to threats.

Execution control is enabled by default in all device policies, allowing the CylancePROTECT Desktop agent to alert the management console when unsafe or abnormal files attempt to run. After the CylancePROTECT Desktop agent is installed, it analyzes all running processes and modules to determine whether there are threats that are already active.

You can create and assign different device policies to meet the needs of various groups within your organization. Each device is assigned to one device policy. The default policy is assigned to a device if no other policy is assigned.

1. In the management console, on the menu bar, click **Policies > Device Policy**.
2. Do any of the following:

| Task | Steps |
|-----------------------------|--|
| Create a new device policy. | <ol style="list-style-type: none"> a. Click Add Policy. b. On the General Info tab, specify a name for the policy. c. Configure the settings for the device policy (see the device policy settings links below). d. Click Save. |
| Edit a device policy. | <ol style="list-style-type: none"> a. Click the name of the device policy that you want to edit. b. Configure the settings for the device policy (see the device policy settings links below). c. Click Save. |

| Task | Steps |
|--|--|
| Copy a device policy. | <ol style="list-style-type: none"> Click the name of the device policy that you want to copy. Click . On the General Info tab, specify a name for the copied policy. Configure the settings for the device policy (see the device policy settings links below). Click Save. |
| Configure device policy settings. | <p>For more information about the available settings, see the following:</p> <ul style="list-style-type: none"> • Device policy: Malware Protection settings • Device policy: Memory Protection settings • Device policy: Script Control settings • Device policy: External Device Control settings • Device policy: Application Control settings • Device policy: Agent Settings <p>For more information about enabling and configuring CylanceOPTICS using the CylanceOPTICS Settings tab, see Enable and configure CylanceOPTICS.</p> |
| Automatically assign a device policy to devices in a zone. | <p>You can associate a device policy with a zone so that when devices are added to that zone, they are automatically assigned that device policy. For more information, see Add and configure a zone.</p> |
| Manually assign a device policy to a device | <ol style="list-style-type: none"> In the management console, on the menu bar, click Assets > Devices. Select the devices that you want to assign a device policy to. Click Assign Policy Select the device policy that you want to assign. Click Save |

Device policy: Malware Protection settings

Malware protection settings specify how the agent handles a file when it detects a threat that it considers to be [unsafe or abnormal](#). Add files that you want the agent to consider as safe to the policy safe list.

| Setting | Description |
|---|--|
| Auto-quarantine unsafe executables with execution control | <p>When enabled, CylancePROTECT Desktop will automatically quarantine unsafe files when they try to execute on a device. Once enabled, you can also choose whether to auto-quarantine abnormal executables when they try to execute (Auto-quarantine abnormal executables with execution control).</p> <p>Unsafe files contain significantly more malware attributes and are more likely to be malware than abnormal files.</p> <p>When a file is quarantined, it is renamed with a .quarantine extension and moved to the quarantine directory:</p> <ul style="list-style-type: none"> • Windows: C:\ProgramData\Cylance\Desktop\q • macOS: /Library/Application Support/Cylance/Desktop/q • Linux: /opt/cylance/desktop/q <p>The Access Control List (ACL) for the file is modified to prevent the user from interacting with the file.</p> <p>Some malware is designed to create files in other directories and continues to do so until it is successful. Instead of removing the files, CylancePROTECT Desktop modifies them so that the malware doesn't try to create them again and so that they cannot be executed.</p> |
| Stop unsafe running processes and their sub-processes | <p>When enabled, the CylancePROTECT Desktop agent will stop all unsafe running processes and child processes when it detects a .exe or .dll threat. This offers a high level of control over malicious processes that might be running on a device.</p> <p>The file must be auto-quarantined, manually quarantined, or quarantined using the global quarantine list. This feature must be enabled before the file is quarantined. If this feature is enabled but the file is not quarantined or auto-quarantined, the processes will continue to run.</p> <p>For example, a file is allowed to run, then you decide to quarantine the file. When this setting enabled, the file is quarantined and the process is terminated, along with any child processes. If this setting is disabled, the file would be quarantined, but because the file was allowed to run, any processes started by the file could continue to run.</p> |
| Auto-upload for .exe files | <p>When enabled, CylancePROTECT Desktop will automatically upload unfamiliar executable files that it detects to the CylancePROTECT cloud services to perform a deeper analysis of the file and provide additional data on the detection to assist with manual analysis and triage.</p> <p>CylancePROTECT Desktop only uploads and analyzes unknown files such as Portable Executable (PE), Executable and Linkable Format (ELF) and Mach Object file format (Mach-O) files. If the same unknown file is discovered on multiple devices, CylancePROTECT Desktop uploads one file only from a single device for analysis, not one file per device.</p> |

| Setting | Description |
|-----------------------------|---|
| Copy file samples (malware) | <p>When enabled, you specify a fully qualified network share (\\server_name\shared_folder) to store copies of file samples that are detected by Background threat detection, Watch for new files, and Auto-quarantine with execution control. This allows you to conduct your own analysis of files that CylancePROTECT Desktop considers to be unsafe or abnormal.</p> <p>CIFS/SMB network shares are supported. All files that meet the unsafe or abnormal criteria are copied. No uniqueness test is performed. Files are compressed and password protected. The password is "infected".</p> |
| Policy safe list | <p>Add files that your organization considers to be safe to the policy safe list to allow them to run on devices. The policy safe list takes precedence over the global safe list or global quarantine list.</p> <p>For more information about the policy safe list, see Exclusions and when to use them.</p> |

| Setting | Description |
|-----------------------------|---|
| Background threat detection | <p>When enabled, the CylancePROTECT Desktop agent performs a full disk scan on a specified interval to detect and analyze any dormant threats.</p> <p>The scan is designed to minimize impact to the device user by using a low amount of system resources. The background threat detection scan can take up to one week, depending on how busy the system is and the number of files on the system that require analysis. The date and time of the most recent completed scan is recorded in the management console.</p> <p>You can specify whether you want the scan to occur only once after the agent is installed, or on a recurring interval that you specify (default 10 days). Increasing the scan frequency may impact device performance. A significant update to the agent's detection model (for example, adding support for a new OS) can trigger a full disk scan.</p> <p>It is a best practice to set background threat detection to run once and to enable Watch for new files. Periodic scans of the entire disk are not necessary, but can be implemented for compliance purposes (for example, for PCI compliance).</p> <p>If background threat detection scans are running on several VM devices that are from the same VM host at the same time, device performance will be impacted. Consider incrementally enabling this feature for VM devices to limit the number of scans occurring at the same time.</p> <p>To manually start a background threat detection scan on a device, use one of the following commands:</p> <ul style="list-style-type: none"> Windows: <pre>C:\Program Files\Cylance\Desktop\CylanceSvc.exe / backgroundscan</pre> macOS: <pre>/Applications/Cylance/CylanceUI.app/Contents/MacOS/ CylanceUI -background-scan</pre> Linux: <pre>/opt/cylance/desktop/Cylance -b /opt/cylance/desktop/Cylance --start-bg-scan</pre> |

| Setting | Description |
|---------------------------------|---|
| Watch for new files | <p>When enabled, the CylancePROTECT Desktop agent scans and analyzes any new or modified files for dormant threats. If a threat is detected, the file can be quarantined (per the Auto-quarantine setting) even if there was no attempt to execute it. It is recommended that you enable this setting together with Background threat detection (run once).</p> <p>Auto-quarantine with execution control blocks unsafe or abnormal files when they try to execute, while Watch for new files can quarantine unsafe or abnormal files when they are detected. It is not necessary to enable Watch for new Files when Auto-quarantine is also enabled, unless you prefer to quarantine a malicious file as soon as the agent detects the threat during a scan.</p> <p>This setting might impact device performance. Consider monitoring disk or message processing performance to see if it has changed. Excluding specific folders might improve performance and ensure that certain folders and files do not get scanned or analyzed by the agent.</p> |
| Scan archives: Max archive size | <p>This setting is available if Background threat detection or Watch for new files are enabled.</p> <p>You can specify the maximum size of an archive file, in MB, that the CylancePROTECT Desktop agent can scan (Background threat detection and Watch for new files). If the file size is set to 0 (the default value), archive files are not scanned.</p> |
| Exclude folders: Add Exclusion | <p>This setting is available if Background threat detection or Watch for new files are enabled.</p> <p>You can specify folder and subfolder paths that you want to exclude from scanning (Background threat detection and Watch for new files):</p> <ul style="list-style-type: none"> • For Windows, use an absolute path with a drive letter. For example, C:\Test. • For macOS, use an absolute path from the root without a drive letter. For example, /Applications/SampleApplication.app. • For Linux, use an absolute path from the root without a drive letter. For example, /opt/application. <p>You can turn on the Allow execution setting if you also want to exclude the specified folder paths from Auto-quarantine with execution control. Note that files and threats that are dropped into exclusion folders will be allowed to execute and could compromise your device and organization. Take precautions to ensure that rogue files cannot be added to excluded folders.</p> <p>Exclusions are not applied retroactively. Adding an exclusion after an initial detection or conviction will not retroactively exclude the files. Any files that were previously detected or convicted will remain in that state until locally waived or added to the global safe list.</p> <p>See the details below for using wildcards for folder exclusions.</p> |

Using wildcards for folder exclusions

You can use the asterisk (*) as a wildcard for all operating systems when specifying folder exclusions. Use the asterisk to exclude folders and to represent a prefix or suffix for a folder name.

- The asterisk matches one or more characters, except the platform-specific path separator ('\\').
- Multiple wildcards are allowed in an exclusion path.
- "*" escaping is not supported. For example, you cannot exclude a folder that contains an asterisk "*" in the folder name.
- Previous folder exclusion functionality still applies, so exclusions will also apply to any child folders.
- A wildcard cannot be used in the file name of an executable. Use wildcards for folder or directory names only.
- Double asterisks (**) are not supported in folder exclusions.
- C:* is not recommended as it would exclude any directory and child directory in the entire C: drive.

Wildcard examples:

- Parent folder: C:\Application*\MyApp\
- Prefix: C:\Application*Folder1\MyApp\
- Suffix: C:\Application\TestFolder*\MyApp\
- Prefix and suffix: C:\Application*Folder*\MyApp\

Device policy: Memory Protection settings

Memory protection settings specify how the agent handles memory exploits, including process injections and escalations. Add exclusions for executable or macro files that you want to allow to run.

| Setting | Description |
|-------------------|--|
| Memory protection | <p>When enabled, the CylancePROTECT Desktop agent detects various types of process calls that may be a threat and handles each type according to the options that you configure.</p> <p>The violation type tables below provide more information about each violation type. For each violation type, you can configure the agent to respond with one of the following actions:</p> <ul style="list-style-type: none"> • Ignore: The agent does not take any action. • Alert: The agent logs the violation and reports the incident to the management console. • Block: The agent logs the violation, reports the incident to the management console, and blocks the process call. The application that made the call is allowed to run. • Terminate: The agent logs the violation, reports the incident to the management console, blocks the process call, and terminates the application that made the call. |

| Setting | Description |
|--|--|
| Exclude executable or macro files: Add Exclusion | <p>You can specify the relative path of the files that you want the CylancePROTECT Desktop agent to ignore when trying to detect memory protection threats. When you add a file to the exclusion list, you allow the file to be installed and run on devices that are assigned the policy.</p> <p>When you add an exclusion, you specify the relative path of the file and the violation types that you want to ignore. On Windows devices, you can also specify the absolute file path. Use shortened relative paths with caution because they may exclude other executables that have the same relative path.</p> <p>After applying the exclusion, all instances of that process must be terminated to stop the driver from injecting into it.</p> <p>Note: If you save an exclusion without adding at least one violation type to ignore, the exclusion is applied to both memory protection and script control events. Adding at least one violation type to ignore means the exclusion is applied to memory protection only.</p> <p>Windows examples:</p> <ul style="list-style-type: none"> • Relative path: \Application\Subfolder\application.exe • Absolute path: C:\Application\Subfolder\application.exe <p>Linux examples:</p> <ul style="list-style-type: none"> • Relative path: /opt/application/executable • Relative path for Dynamic Library files: /executable.dylib <p>macOS examples:</p> <ul style="list-style-type: none"> • Relative path without spaces: /Applications/SampleApplication.app/Contents/MacOS/executable • Relative path with spaces: /Applications/Sample Application.app/Contents/MacOS/executable • Relative path for Dynamic Library Files: /executable.dylib • You can also use wildcards for memory protection exclusions. For more information, see Wildcards in memory protection exclusions. <p>See the details below for using wildcards for executable or macro exclusions.</p> |

| Setting | Description |
|--|--|
| Add Exclusion: Treat as DLL exclusion | <p>Enable this setting when you want to add an exclusion for a third-party DLL. For example, if you are running third-party security products in addition to CylancePROTECT Desktop for Windows, you can add an exclusion for the appropriate .dll files so that CylancePROTECT ignores specific violations for those products.</p> <p>This feature supports the Malicious payload and System DLL overwrite violation types only. These violation types are supported for Windows devices only.</p> <p>Note the following when you specify a DLL exclusion:</p> <ul style="list-style-type: none"> • Devices must be running the CylancePROTECT Desktop agent for Windows version 3.1.1001 or later. • The file path that you specify must be the full, direct path to the .dll file. Wildcards are not allowed. • The .dll file must be signed using a certificate that is trusted on the device, otherwise it will not be excluded. • For more information about supporting DLL exclusions, see KB 108909. |
| Add Exclusion: Ignore specific violation types | <p>Enable this setting when you add a memory protection exclusion to select the violation categories and specific violation types that you want the CylancePROTECT Desktop agent to ignore.</p> <p>When adding exclusions, if you want the policy to apply to memory protection violations only and not script control violations, specify at least one violation type that you want to ignore. If you do not select any violation types to ignore, a warning message appears and the exclusion will apply to both memory protection and script control policies.</p> |

Using wildcards for executable or macro exclusions

Note the following considerations for using special characters and wildcards (*) in memory protection exclusions:

- Memory protection exclusions can include the following special characters: ^ & ' @ { } [] , \$ = ! - # () % . + ~ _ *
- On Windows devices, any letter value followed by a colon (for example, C:) is supported.
- Escaping an asterisk (*) is not supported. For example, you cannot use it to exclude a file that contains an asterisk in its file name.
- When adding DLL exclusions, wildcards are not allowed.
- A * wildcard matches zero or more characters, except for the platform-specific file path separators. The file path separators are '\' on Windows devices, and '/' on Linux and macOS.
- A ** wildcard matches zero or more directories in an absolute path to exclude drives, directories, and child directories. For example, C:\MyApp*****.\.
 - Always use ** with file path separators, such as **\ or /**/
 - The pattern **\ is valid if it is at the beginning of pattern for Windows devices only. It matches all directories inside all drives.
 - You can use **\ or /**/ multiple times in a path without limitation.
 - Avoid using ** immediately after a drive letter or at the beginning of an exclusion. For example, C:**\program.exe on Windows or /***/program.dmg on macOS, as this would exclude anything in any directory and child directories on the drive.

- For examples demonstrating the use of wildcards in memory protection exclusions, see [Windows examples of wildcards used in memory protection exclusions](#) and [macOS examples of wildcards used in memory protection exclusions](#).
- Three asterisks (***) are not valid for exclusions because it would hide typos. For example, in the pattern "C:***.exe", users might have wanted to type "C:***.exe" but missed one "\\". If "***" were treated as a single "*" it could result in different behavior than intended.

Exploitation violation types

| Violation type | Supported OS | Description |
|------------------------|------------------|---|
| Stack pivot | Windows Linux | Detects if the stack for a thread has been replaced with a different stack. Generally, the system only allocates a single stack for a thread. An attacker might use a different stack to control execution in a way that is not blocked by Data Execution Prevention (DEP). |
| Stack protect | Windows Linux | Detects if the memory protection of a thread's stack has been modified to enable execution permission. Stack memory should not be executable, so this can mean that an attacker is preparing to run malicious code stored in stack memory as part of an exploit, an attempt that would otherwise be blocked by Data Execution Prevention (DEP). |
| Overwrite code | Windows | Detects if the code that resides in a process's memory has been modified in a way that may indicate an attempt to bypass Data Execution Prevention (DEP). |
| RAM scraping | Windows | Detects if a process is trying to read valid magnetic stripe track data from another process. Typically, this violation is associated with point of sale (POS) systems. |
| Malicious payload | Windows | Detects shellcode and payloads that are associated with exploitation. This violation type supports DLL exclusions. |
| System call monitoring | Windows | Detects system calls made to an application or operating system. |
| Direct system calls | Windows | Detects attempts to silently inject malicious code into other processes. This violation type cannot be blocked. |
| System DLL overwrite | Windows | Detects attempts to overwrite a system DLL. This violation type supports DLL exclusions. |
| Dangerous COM object | Windows | Detects malicious code that has a reference to a Component Object Model (COM) object. |

| Violation type | Supported OS | Description |
|---------------------|--------------|--|
| Injection via APC | Windows | <p>Detects if a process is injecting arbitrary code into a target process using an asynchronous procedure call (APC), or starting a remote thread to call LoadLibrary, or a similar function.</p> <p>If the action is set to alert, you can expect to see alerts for both valid and malicious injections. The alert reports the application that received the injection, but you must determine the executable source that caused the alert. For more information, see KB 92422.</p> <p>If the action is set to block or terminate, it prevents reported apps from running on the device even if they are valid.</p> |
| Dangerous VBA macro | Windows | <p>Detects macros that contain dangerous implementations. Protects devices running agent version 2.1.1580 and later. Any memory protection exclusions are supported on agent version 3.0 and later.</p> |

Process injection violation types

| Violation type | Supported OS | Description |
|-----------------------------|------------------|---|
| Remote allocation of memory | Windows macOS | Detects if a process allocates memory in another process. Most allocations occur only within the same process. This might indicate an attempt to inject code or data into another process to reinforce a malicious presence on a system. |
| Remote mapping of memory | macOS | Detects if a process introduces code or data into another process. This might indicate an attempt to execute code in another process and reinforce a malicious presence. |
| Remote write to memory | Windows macOS | Detects if a process has modified memory in another process. This might indicate an attempt to store code or data in previously allocated memory, but it is possible that an attacker is trying to overwrite existing memory to divert execution for a malicious purpose. |
| Remote write PE to memory | Windows | Detects if a process has modified memory in another process to contain an executable image. This can indicate that an attacker is attempting to execute code without first writing that code to disk. |
| Remote overwrite of code | Windows | Detects if a process has modified executable memory in another process. Under normal conditions, executable memory is not modified, especially by another process. This can indicate an attempt to divert execution in another process. |
| Remote unmap of memory | Windows macOS | Detects if a process has removed an executable from the memory of another process. This might indicate an intent to replace the executable image with a modified copy for the purpose of diverting execution. |

| Violation type | Supported OS | Description |
|--------------------------------|--------------|--|
| Remote thread creation | Windows | Detects if a process has created a new thread in another process. A process's threads are usually only created by that same process. This method can be used by an attacker to activate a malicious presence that has been injected into another process. |
| Remote APC scheduled | Windows | Detects if a process has diverted the execution of another process's thread. An attacker can use this method to activate a malicious presence that has been injected into another process. |
| DYLD injection | Linux | Detects if an environment variable has been set that will cause a shared library to be injected into a launched process. Attackers can modify the list of applications or replace applications with bash scripts that allow their modules to be loaded automatically when an application starts. |
| Doppelganger | Windows | Detects if a new malicious process was started from a file that has not yet been written to the file system. The file write transaction is usually rolled back after the process starts (so that the malicious file is never committed to disk), and any attempt to scan the file on disk will only see the unmodified, benign file. |
| Dangerous environment variable | Windows | Detects an environment variable that might have malicious code attached to it. |

Escalation violation types

| Violation type | Supported OS | Description |
|--|--------------|--|
| LSASS read | Windows | Detects if memory belonging to the Windows Local Security Authority process has been accessed in a way that indicates an attempt to obtain user passwords. |
| Zero allocate | Windows | Detects if a null page has been allocated. The memory region is typically reserved, but in certain circumstances it can be allocated. Attackers can use this to setup privilege escalation by taking advantage of some known null de-reference exploit, typically in the kernel. |
| Memory permission changes in other processes | Windows | Detects if a violating process has modified memory access permissions within another process. This is usually done to inject code into another process and make memory executable by modifying access permissions. |
| Memory permission changes in child processes | Windows | Detects if a violating process has created a child process and has modified memory access permissions in that child process. |

| Violation type | Supported OS | Description |
|-----------------------------|--------------|--|
| Stolen system token | Windows | Detects if an access token has been modified to allow a user to bypass security access controls. |
| Low integrity process start | Windows | Detects if a process has been set to run with a low integrity level. |

Windows examples of wildcards used in memory protection exclusions

The following examples are based on excluding an executable that is stored in the following path: C:\Application\TestApp\MyApp\program.exe

Examples

Examples of valid exclusion paths

Relative path without any wildcards to exclude program.exe:

```
\Application\TestApp\MyApp\program.exe
```

Relative path with wildcards to exclude program.exe (or any file):

```
\Application\TestApp\MyApp\*
```

Relative path with wildcards to exclude program.exe (or any file) in the MyApp directory and any of its children :

```
\Application\TestApp\MyApp\**\*
```

Exclude program.exe as long as program.exe is located in the "MyApp" directory in C:\Application:

```
C:\Application\**\MyApp\program.exe
```

In this example, any directories between the Application folder and the MyApp folder are also excluded.

Exclude any .exe file that is located in the "MyApp" directory in C:\Application :

```
C:\Application\**\MyApp\*.exe
```

Exclude any executable (regardless of its file extension) as long as it is located in the "MyApp" directory in C:\Application :

```
C:\Application\**\MyApp\*
```

Exclude program.exe as long as it is located in any child directory of the C:\Application\TestApp:

```
C:\Application\TestApp\**\program.exe
```

Exclude program.exe as long as it is located in \Application\TestApp\MyApp\ of the C: drive:

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

Exclude any .exe executable as long as it is located in \Application\TestApp\MyApp\ of the C: drive:

```
C:\**\Application\TestApp\MyApp\*.exe
```

Exclude any executable (regardless of extension) as long as it is located \Application\TestApp\MyApp\ of the C: drive

```
C:\**\Application\TestApp\MyApp\*
```

| Examples | |
|--|--|
| Incorrect use of asterisks in exclusions | <p>Only use a single asterisk (*) to match characters in a folder name or file name. Double asterisks (**) are reserved to match directory paths or the end of a directory path, and cannot be used at the end of an exclusion.</p> <p>The following is a list of examples in the context of excluding C:\Application\TestApp\MyApp\program.exe.</p> <ul style="list-style-type: none"> • Incorrect: C:\Application\TestApp\MyApp**.exe Reason: Double asterisks are reserved for directory paths. Use single asterisks to match characters of a file name. • Incorrect: C:\Application**\MyApp\program.exe Reason: The double asterisk excludes folders whose names start with Application. Although the syntax is valid, the TestApp directory is not matched in this exclusion. • Incorrect: C:\Application\TestApp*\program.exe Reason: Use the double asterisks with file path separators instead of a single asterisk. • Correct: C:\Application\TestApp\MyApp*.exe • Correct: C:\Application**\program.exe |
| Exclusions that are not recommended | <p>Avoid using a double asterisk (**) immediately after a drive letter. For example:</p> <pre>C:**\program.exe</pre> <p>In this example, program.exe is allowed to run from any folder in the C: drive. Although this exclusion is technically correct, it would exclude anything in any directory (including child directories) located on the drive.</p> |

macOS examples of wildcards used in memory protection exclusions

The following examples are based on excluding an executable that is stored in the following path: /Application/TestApp/MyApp/program.dmg

| Type | Description |
|--|--|
| Correct use of exclusions | <p>Excludes program.dmg as long as it is located under the "MyApp" child directory:</p> <pre>/Application/**/MyApp/program.dmg</pre> <p>Excludes any executable with the .dmg as long as the it is located under the "MyApp" child directory:</p> <pre>/Application/**/MyApp/*.dmg</pre> <p>Excludes any executable as long as it is located under the "MyApp" child directory:</p> <pre>/Application/**/MyApp/*</pre> <p>Excludes program.dmg as long as it is located in any directory that is a child of the "TestApp" directory :</p> <pre>/Application/TestApp/**/program.dmg</pre> |
| Incorrect use of asterisks in exclusions | <p>Only use a single asterisk (*) to match characters in a folder name or file name. Double asterisks (**) are reserved to match directory paths and cannot be used at the end of an exclusion.</p> <p>The following is a list of examples in the context of excluding /Application/TestApp/MyApp/program.dmg.</p> <ul style="list-style-type: none"> • Incorrect: /Application/TestApp/MyApp/pro**am.dmg • Correct: /Application/TestApp/MyApp/progra*.dmg • Incorrect: /Application/** • Correct: /Application/**/* |
| Exclusions that are not recommended | <p>Avoid using a double asterisk (**) at the beginning of an exclusion. For example:</p> <pre>/**/program.dmg</pre> <p>In this example, program.dmg is allowed to run from any folder on the drive. Although this exclusion is technically correct, it would exclude anything in any directory (including child directories) located on the drive.</p> |

Device policy: Script Control settings

Script control settings specify how the CylancePROTECT Desktop agent handles the execution of scripts on Windows devices.

| Setting | Description |
|----------------|--|
| Script control | <p>You must enable this option to configure any script control settings.</p> <p>You can select one of the following control mode actions for each type of script:</p> <ul style="list-style-type: none"> • Disabled: Allows all scripts to run and does not report them to the management console. This setting is not recommended. • Alert: Allows all scripts to run and reports them to the management console. Use this setting when you want to monitor and observe all scripts that are running in your environment. Recommended for initial deployment while you determine which scripts you want to allow or block. • Block: Blocks all scripts from running and reports them to the management console. Only files that are added to the exclusion list are allowed to run. Use this setting after testing and monitoring for threats in alert mode. <p>Active script and PowerShell include additional enhanced script control options, see the appropriate rows below for more information.</p> <p>You can find script control alert and block events in Protection > Script Control.</p> |
| Active script | <p>Controls how the agent will handle active scripts, including VBScript and JScript.</p> <p>The following control modes are available for active scripts in addition to Disabled, Alert, and Block. These settings require agent version 3.2 or later (if the device is running an earlier agent, the script will be blocked by default):</p> <ul style="list-style-type: none"> • Block unsafe scripts: If the script is not already in the exclusion list, the agent obtains a threat score from the CylancePROTECT cloud services. If it receives an unsafe threat score, the script is blocked from executing. Unsafe files greatly resemble malware. Unscored and abnormal scripts are reported to the management console but are not blocked. • Block abnormal and unsafe scripts: If the script is not in the exclusion list, the agent obtains a threat score from the CylancePROTECT cloud services, and if it receives an abnormal or unsafe threat score, the script is blocked from executing. Abnormal files have some malware-like attributes but are less likely to be malware than an unsafe file. Unscored scripts are alerted to the console but are not blocked. |

| Setting | Description |
|--------------------|--|
| PowerShell | <p>Controls how the agent will handle PowerShell scripts.</p> <p>The following control modes are available for PowerShell scripts in addition to Disabled, Alert, and Block. These settings require agent version 3.2 or later (if the device is running an earlier agent, the script will be blocked by default):</p> <ul style="list-style-type: none"> Block unsafe scripts: If the script is not already in the exclusion list, the agent obtains a threat score from the CylancePROTECT cloud services. If it receives an unsafe threat score, the script is blocked from executing. Unsafe files greatly resemble malware. Unscored and abnormal scripts are reported to the management console but are not blocked. Block abnormal and unsafe scripts: If the script is not in the exclusion list, the agent obtains a threat score from the CylancePROTECT cloud services, and if it receives an abnormal or unsafe threat score, the script is blocked from executing. Abnormal files have some malware-like attributes but are less likely to be malware than an unsafe file. Unscored scripts are alerted to the console but are not blocked. |
| PowerShell Console | <p>Controls how the agent will handle the PowerShell console. Blocking the PowerShell console provides additional security by protecting against the use of PowerShell console in interactive mode.</p> <p>The Alert control mode requires CylancePROTECT Desktop agent version 3.2 or later. For agents that don't support Alert mode, the use of PowerShell console will be allowed by default and an alert won't be generated.</p> <p>If the control mode is set to Block and a script launches the PowerShell console, the script fails. It is a best practice for scripts to invoke the PowerShell scripts instead of the PowerShell console (a basic command to run a PowerShell script without invoking the console is Powershell.exe -file [script name]).</p> |
| Macros | <p>Controls how the agent will handle Microsoft Office macros. Macros use Visual Basic for Applications (VBA) which allows embedding code inside a Microsoft Office document. Malware creators can use macros to run commands and attack the system.</p> <p>This setting applies only to agent version 2.1.1578 and earlier. For newer agents, use the Dangerous VBA macro violation type on the Memory Protection tab. Any macro exclusions that you created previously for script control must be added to the memory protection exclusions for the Dangerous VBA macro violation type.</p> <p>Starting with Microsoft Office 2013, macros are disabled by default. Typically you do not need to enable macros for users to view the content of a Microsoft Office document. Enable macros only for documents from trusted users. It is a best practice to disable macros.</p> |
| Python | Controls how the agent will handle Python scripts version 2.7 and 3.0 to 3.8. |
| .NET DLR | Controls how the agent will handle .NET DLR scripts. |

| Setting | Description |
|--|--|
| XLM macros (Preview) | <p>Note: The XLM macros feature is currently available in Preview mode where it might behave unexpectedly.</p> <p>Controls how the agent will handle Excel 4.0 (XLM) macros.</p> <p>This feature requires:</p> <ul style="list-style-type: none"> • Microsoft Windows 10 or later • CylancePROTECT Desktop agent version 3.1 or later • VBA macros must be disabled in Excel. |
| Score all scripts | When enabled, all active script and PowerShell scripts are scored, even if the control mode is set to Alert or Block. If not enabled, Active script and PowerShell scripts are scored only if the control mode is set to "Block unsafe scripts" or "Block abnormal and unsafe scripts". |
| Upload script to cloud | When enabled, a copy of active script and PowerShell scripts are uploaded to the CylancePROTECT cloud services for threat analysis and scoring. If not enabled, CylancePROTECT attempts to obtain a score for active script and PowerShell scripts using the hash details. |
| Alert on suspicious scripts execution only | When enabled, only active script or PowerShell script executions that are determined to be unsafe or abnormal are reported to the management console. If not enabled, the execution of any active script or PowerShell script is reported to the console, regardless of whether a threat is detected. |
| Actions for Large Scripts | <p>When enabled, the agent takes the specified action when a threat is detected from a larger script (for example, PowerShell scripts larger than 5 MB):</p> <ul style="list-style-type: none"> • Ignore large scripts: The agent does not report the alert to the management console. • Alert only on large scripts: When the agent detects a large script, it will only report the script to the console, and take no other action. • Apply language specific policy settings: When the agent detects a large script, it will report the alert to the console and execute the selected action (control mode) that you configured for each type of script. |

| Setting | Description |
|---|---|
| Exclude files, scripts, or processes: Add Exclusion | <p>You can specify folders that are excluded from script control. Any script that is executed from within a specified folder (or sub-folder) are not subject to the control mode that you configured, and will not generate an alert.</p> <p>You can add exclusions for processes to allow scripts from certain applications that would otherwise be blocked. For example, if your IT department uses specific tools to run scripts, you can add the process for that tool as an exclusion so that scripts are allowed to run.</p> <p>You specify the relative path of the folder or sub-folder. The path can be to a local drive, a mapped network drive, or to a universal naming convention (UNC) path.</p> <p>Excluding folders and scripts:</p> <ul style="list-style-type: none"> • Folder exclusions cannot contain the script or macro file name. These entries are not valid and the agent ignores them. • If the “Everyone” group in your organization has write permissions to a folder, anyone inside or outside of the organization can drop a script in the folder and write to it. CylancePROTECT Desktop will continue to send alerts on scripts and block them. The write permissions apply not only to the direct parent folder, but also to all parent folders, all the way to the root. • If you want to exclude a specific script, you must use a wildcard. <p>Excluding processes:</p> <ul style="list-style-type: none"> • The executable in the process exclusion may be quarantined by execution control and blocked from running. If the executable is quarantined, you need to add it to the policy safe list. • Process exclusions allow scripts to run and do not restrict them from running from the specified folder. <p>See the details below for using wildcards for file, script, or process exclusions.</p> |

Using wildcards for file, script, or process exclusions

Note the following considerations for using wildcards (*) in script control exclusions:

- Only the asterisk (*) is supported as a wildcard for script control exclusions. The wildcard represents one or more characters.
- Exclusions must use Unix-style slashes (even for Windows systems), for example, /windows/system*/*.
- To exclude a folder, the exclusion must have a wildcard at the end of the path to distinguish the exclusion as a folder and not a file. For example: /windows/system32/test*/*.
- When you want to exclude a file, the exclusion must end with a file extension to distinguish the exclusion as a file and not a folder. For example: /windows/system32/script*.vbs.
 - Each wildcard represents one folder level only. The number of folder levels represented in the exclusion must match the level of the file that you are trying to exclude. For example, /folder/*/script.vbs matches \folder\test\script.vbs, but does not match \folder\test\001\script.vbs. This would require either /folder/*/001/script.vbs or /folder/*/*/*script.vbs.
 - The wildcard would need to persist down per level to where the script resides.
 - Two or more wildcards per level are not allowed. For example, /folder/*file*.ext is not allowed.

- Process exclusions with a wildcard must have a file extension to distinguish it as a process exclusion and not a folder. For example, /my*.exe (local drive),/directory/child/my*.exe (local drive), //my*.exe (network drive),// directory/child/my*.exe (network drive)
- Wildcards can lower your security stance if your exclusions are too broad. For example, avoid excluding entire folders such as /windows/temp. Instead, use a wildcard while specifying the full or partial filename of the script that you want to exclude (for example, /windows/temp/myscript*.vbs).
- Absolute paths are not supported in script control exclusions.
- If you can identify a common relative path, you can exclude Universal Naming Convention (UNC) paths with a wildcard. For example, if you use device names in a path such as "DC01" to "DC24": /dc*/path/to/script/*
- Network paths can be excluded. For example, //host*/application/*.
- For detailed examples, see [Examples of script control exclusions](#).

Examples of script control exclusions

Adding exclusions for dynamic scripts that are run from a specific directory location or for a script that is run from multiple different user folders is possible by using wildcards in script control exclusions. As an example, you can use the token "*" in the exception path to ensure it covers your variants.

The following table includes some example exclusions with matches that would be successfully excluded, and non-matches that won't be excluded.

| Exclusion example | Matches | Non-matches |
|-------------------------------------|---|---|
| /users/*/temp/* | <ul style="list-style-type: none"> • \users\john\temp • \users\jane\temp | <ul style="list-style-type: none"> • \users\folder\john\temp • \users\folder\jane\temp <p>These folders won't be excluded because the number of folder levels don't match.</p> |
| /program files*/app/script*.vbs | <ul style="list-style-type: none"> • \program files(x86)\app\script1.vbs • \program files(x64)\app\script2.vbs • \program files(x64)\app\script3.vbs | <ul style="list-style-type: none"> • \program files(x86)\app\script.vbs • \program files\app\script1.vbs <p>These folders won't be excluded because wildcards represent one or more characters.</p> |
| //*example.local/sysvol/script*.vbs | <ul style="list-style-type: none"> • \\ad.example.local\sysvol\script1.vbs | <ul style="list-style-type: none"> • \\ad.example.local\sysvol\script.vbs <p>This script won't be excluded because wildcards represent one or more characters.</p> |
| /users/*/*/*.vbs | <ul style="list-style-type: none"> • /users/john/temp/script.vbs • /users/john/temp/anotherScript.vbs | <ul style="list-style-type: none"> • /users/john/temp1/temp2/script.vbs <p>This script won't be excluded because the number of folder levels don't match.</p> |

Process Exclusion

You can add processes to the list of script control exclusions. This feature can be useful if you want to exclude specific processes that may be calling scripts. For example, you can exclude SCCM to allow it to launch PowerShell scripts in a temporary directory. A process is any process that calls a script interpreter to run a script.

- The following example allows the myfile.exe process to call an interpreter (such as PowerShell.exe) to run a script.
 - `/windows/*/myfile.exe`
- The following examples add myprocess.exe to the exclusion list so that it is allowed to run regardless of its folder path:
 - `\myprocess.exe` (on a local Windows drive)
 - `\\myprocess.exe` (on a network Windows drive)
- The following example adds myprocess.exe to the exclusion list so that it is only allowed to run from a specific folder path:
 - `\directory\child\myprocess.exe` (on a local Windows drive)
 - `\\directory\child\myprocess.exe` (on a network Windows drive)

Note:

- Absolute paths are not supported for exclusions.
- Ancestors are not supported.
- When an executable file (exe) is added to an exclusion, `/[CySc_process]/` is automatically added to the exclusion. If you added the above example exclusion, the result would be: `/[CySc_process]/ windows/*/myfile.exe`.

Alternative options for exclusions for script control

You can use the global safelist or add a certificate as an alternative method to excluding scripts.

- [Add a file to the CylancePROTECT Desktop global quarantine or global safe list](#)
 - This method requires a SHA256 hash value and assumes that this value won't change. Updates to the script or changes made by the script by design causes the hash value to change. Therefore, this method requires more administrative work to maintain if the script or macro is frequently updated or changes programmatically (for example, appends a new date or time, or makes system requests, pulls data). Each time the CylancePROTECT Desktop agent reports a script to the management console, it must report a SHA256 hash value. Each time the hash value changes, the agent reports the new value and you need to add the new value to the global safe list. If a hash value cannot be generated (for example, if the script doesn't execute properly, the file doesn't exist, or there are permission issues), then a generic hash is used when the script is reported to the console.
 - The following SHA256 hash value is a generic hash that the CylancePROTECT Desktop agent uses when a hash cannot be generated for a script. If you try to add this value to the global safe list, an error message displays due to the agent functionality.
 - `FE9B64DEFD8BF214C7490AA7F35B495A79A95E81F8943EE279DC99998D3D3440`
 - The following SHA256 hash value is a generic hash that the CylancePROTECT Desktop agent uses when a PowerShell one-liner is used and a hash cannot be generated for a script. If you try to add this value to the global safe list, an error message displays due to the agent functionality.
 - `FE9B64DEFD8BF214C7490BB7F35B495A79A95E81F8943EE279DC99998D3D3440`
- [Add a certificate to the CylancePROTECT Desktop global safe list](#)
 - This method requires you to submit a valid code signing certificate to the console and is only available for PowerShell and Active scripts (not macros).

Device policy: External Device Control settings



You can control how CylancePROTECT devices connect to USB mass storage devices. When you enable external device control, you can configure one of the following actions for the USB device types:

- Full access: Allows read, write, and delete access to the external USB storage device.
- Block: Blocks the device from accessing the external USB storage device.
- Read only: Allows read-only access to external USB storage devices.
 - For Windows devices, read only is not supported for Android and iOS external USB storage devices.
 - For macOS devices, the read only action is not supported.

Note the following considerations for external device control:

- Requires the CylancePROTECT Desktop agent for Windows version 2.1.1410 or later.
- Requires the CylancePROTECT Desktop agent for macOS version 3.3.1000 or later.
- Device control does not affect USB peripherals such as a mouse or keyboard.
- Device control is not supported for SD cards. However, if utilized with a USB card reader device, device control might detect the USB device.
- When device control is enabled, all USB mass storage devices that are inserted are logged, along with the action that was applied (full access, read only, or block). If the action is set to read only or block, and desktop notifications are enabled, a pop-up notification appears on the device when a USB mass storage device is connected. You can find the log of device control events in the management console (Protection > External Devices).

| Setting | Description |
|------------------------|--|
| Windows device control | Enable device control for Windows devices. See the table below for the USB device types that you can configure controls for. |
| macOS device control | Enable device control for macOS devices. See the table below for the USB device types that you can configure controls for. |

| Setting | Description |
|--|---|
| External device exclusion: Add Exclusion | <p>You can add exclusions to define the access level for specific mass storage devices using the vendor ID, product ID, and serial number. For example, you can block all USB mass storage devices, but create exclusions to allow full access to some authorized devices.</p> <p>The vendor ID is required. The product ID and serial number are optional and can be used if you want to make the exclusion more specific. To ensure that you are using the correct information for each exclusion, you can enable device control and insert a device to check the log entry in the management console (Protection > External devices).</p> <p>Note the following when adding exclusions:</p> <ul style="list-style-type: none"> • The exclusion list is shared between Windows and macOS devices when device control is enabled for both OS platforms. • Not all manufacturers use a serial number for their products. Some manufacturers use the same serial number for multiple products. • External storage exclusions are not editable. Add new exclusions as necessary and delete any exclusions that are no longer required. • Each device policy has a limit of 5000 exclusions. • If you want to import a large number of exclusions, click  > Download template. Populate the .csv template, then click  to upload the file. You can import a maximum of 500 entries per template file. The Vendor ID and Access (Full Access, Read Only, Block) values are required. For more information, see KB 65484. |

USB device types

| USB device type | Supported OS | Description |
|-----------------|--------------|---|
| Android | Windows | A portable device running Android OS (for example, a smartphone or tablet). When an Android device is connected, its device type might be identified as Android, Still image, or Windows portable device. If you want to block Android devices, consider blocking Still image and Windows portable device as well. |
| iOS | Windows | A portable Apple device running iOS (for example, iPhone or iPad). Some iOS devices will not charge when device control is enabled, and set to block unless the device is powered off. Apple includes their charging capability within functions of the device that are required for the CylancePROTECT iOS device blocking capability. |

| USB device type | Supported OS | Description |
|-------------------------|------------------|---|
| Still image | Windows | Devices with frame capture and frame grabbers, including scanners, digital cameras, and multi-mode video cameras. Note that Canon cameras are considered a Windows portable device, not a still image device. |
| USB CD DVD RW | Windows macOS | A USB optical drive. |
| USB drive | Windows macOS | A USB hard drive or USB flash drive. |
| VMWare USB passthrough | Windows | A VMware virtual machine client that has USB devices connected to the host. |
| Windows portable device | Windows | Portable devices that use the Windows Portable Device (WPD) driver technology, for example, mobile phones, digital cameras, and portable media players. |

Device policy: Application Control settings

You can use application control for Windows and Linux devices to restrict changes to executables on CylancePROTECT Desktop devices. Only the applications that are present on a device before application control is enabled are allowed to execute. Typically, application control is used for fixed function devices that are not changed after they are set up (for example, point-of-sale devices).

After you enable application control, any attempts to add applications or make changes to existing applications on devices are denied. Applications cannot be downloaded from browsers or copied from another device (for example, an external or shared drive). The main objectives of application control are to deny the execution of executable files from remote or external drives, to deny the creation of new executables on the local drive, and to deny changes to existing files on the local drive.

You can view application control activity in the device details in the management console.

Consider the following before you enable application control:

- If application control is enabled, [the CylancePROTECT Desktop and CylanceOPTICS agent update process](#) is disabled on devices that are assigned the policy.
- If application control is enabled, you cannot remove the CylancePROTECT Desktop or CylanceOPTICS agents from devices that are assigned the policy.
- It is not recommended to run CylanceOPTICS on systems that use application control. When application control is enabled, CylanceOPTICS does not function properly due to the restrictive nature of application control.
- To prevent production outages or excessive network activity, application control does not monitor file transfers to remote or external drives.
- On Linux devices:
 - Application control folder exclusions are not supported.
 - When application control is enabled, an inventory of all executable files on the local file system is generated. File execution is restricted to the files in the inventory.

- Executable files can be added to the device after application control is enabled, but the executables cannot run. Only applications that are in the inventory when application control is enabled are allowed to run.
- Allowing an update when application control is enabled may cause issues.

| Setting | Description |
|--------------------------------|---|
| Application control | <p>Enables application control. If you enable application control and save the device policy, the following policy settings are changed automatically (regardless of previous configuration):</p> <ul style="list-style-type: none"> • Malware protection: Auto-quarantine unsafe executables is enabled • Malware protection: Auto-quarantine abnormal executables is enabled • Malware protection: Watch for new files is enabled • Memory protection is enabled • Memory protection: All violation types are set to Terminate <p>You can change these settings by editing the device policy, but they are recommended for use with application control.</p> |
| Change window | <p>When enabled, application control is turned off, allowing for new applications to be installed or for changes to be made to applications on the device (including agent updates). After performing the necessary changes, turn off this setting to close the change window and enable application control again.</p> <p>When you use this setting to temporarily disable application control, changes such as folder exclusions are retained. If you disable the Application control setting, all settings are reset to the defaults.</p> |
| Exclude folders: Add Exclusion | <p>You can specify the absolute path of folders that are exempt from application control (for example, C:\Program Files\Microsoft SQL Server). Application control folder exclusions are supported for Windows devices only. Folder exclusions are available only for local internal drives. Exclusions for removable or remote drives are not supported.</p> |

Device policy: Agent Settings

Agent settings specify the agent features that you can use to protect devices.

| Setting | Description |
|--------------------------------------|--|
| Prevent service shutdown from device | <p>When enabled, device users cannot stop the service for the CylancePROTECT Desktop agent or for the following versions of the CylanceOPTICS agent:</p> <ul style="list-style-type: none"> • CylanceOPTICS agent for Windows 3.1 or later with CylancePROTECT Desktop 3.0 or later • CylanceOPTICS agent for macOS 3.3 or later with CylancePROTECT Desktop 3.1 or later <p>When enabled, a macOS user can stop the services only if the Self Protection Level in the device properties is set to Local Admin (Assets > Devices > click the device). Windows users cannot stop the agent services as long as this setting is enabled.</p> <p>CylancePROTECT Desktop agent version 3.1 and later runs as a trusted service using Antimalware Protected Process Light (AM-PPL) technology from Microsoft, which also helps prevent the agent from being shut down. This feature requires the device to be running Windows 10 1709 or later or Windows Server 2019 or later.</p> |
| Auto-upload log files | <p>When enabled, agent logs are uploaded to the management console where you can view them (Assets > Devices > click the device > Agent Logs tab). The log file name is the date of the log. Uploaded log files are stored for 30 days.</p> |
| Desktop notifications | <p>When enabled, the CylancePROTECT Desktop agent will display pop-up notifications to the device user. Note that device users can change this setting directly in the agent, and the user setting will take precedence over this device policy setting. In the agent on devices, the Events tab is cleared when the agent or device is restarted.</p> |
| Auto-delete quarantined files | <p>When enabled, quarantined files are deleted automatically from the device after a specified number of days (by default, 14). When a quarantined file is deleted, the action is included in the agent log file and the file is removed from the quarantine list in the agent.</p> |
| Monitor installed applications | <p>When enabled, the agent reports a list of applications that are installed on devices to the management console. This allows you to identify applications that may be a source of vulnerabilities and prioritize and manage actions against those vulnerabilities.</p> <p>This feature requires CylancePROTECT Desktop for Windows version 3.2 or later. You can view the list of applications and their associated devices in Assets > Installed Applications. You can also view a list of applications that are installed on individual devices in Assets > Devices > Device details > Installed Applications.</p> |

Installing the CylancePROTECT Desktop agent for Windows

CylancePROTECT Desktop detects and blocks malware before it can affect a device. BlackBerry uses a mathematical approach to malware identification, using machine learning techniques instead of reactive

signatures, trust-based systems, or sandboxes. This approach renders new malware, viruses, bots, and future variants useless. CylancePROTECT Desktop analyzes potential file executions for malware in the OS and memory layers to prevent the delivery of malicious payloads.

You can install the agent onto individual devices or can use the installation parameters to deploy it across your environment using a deployment tool.

If you want to use an RMM solution to install the CylancePROTECT Desktop agent on devices, see [Using RMM solutions to install the Cylance agents on devices](#).

Install the Windows agent

Before you begin:

- Download the CylancePROTECT Desktop installation files from the management console. Click **Settings > Deployments**. From the **Product** drop-down list, select **CylancePROTECT**, and set the target operating system, the agent version, and the file type. Click **Download**.
 - In the management console, copy the installation token from **Settings > Application**.
1. Double-click the CylancePROTECT Desktop installer.
 2. On the CylancePROTECT Desktop setup window, click **Install**.
 3. Type the installation token and click **Next**.
 4. Optionally, change the destination folder.
 5. Click **OK** to begin the installation.
 6. Click **Finish** to complete the installation. Ensure that the check box to launch CylancePROTECT Desktop is selected.

After you finish: If memory protection, script control, and/or device control are enabled in the device policy, a reboot of the device following the agent installation or upgrade is recommended, but not strictly required. A reboot will ensure that any new policy settings have taken full effect.

Windows installation parameters

The agent can be installed interactively or non-interactively through GPO, Microsoft System Center Configuration Manager (SCCM), MSIEXEC, and other third-party tools. The MSIs can be customized with the parameters below or the parameters can be supplied from the command line.

| Parameter | Value | Description |
|---------------------|----------------------|--|
| PIDKEY | <Installation Token> | This parameter automatically enters the installation token. |
| LAUNCHAPP | 0 or 1 | 0: This value hides the system tray icon the start menu folder at run-time. 1: This value displays the system tray icon and start menu folder at run-time. If no value is entered, the default value is 1. |
| SELFPROTECTIONLEVEL | 1 or 2 | 1: This value allows local administrators to make changes to the registry and services. 2: This value only allows the system administrator to make changes to the registry and services. If no value is entered, the default value is 2. |

| Parameter | Value | Description |
|-----------|---|--|
| APPFOLDER | <i><Target Installation Folder></i> | This parameter specifies the agent installation directory. The default location is C:\Program Files\Cylance\Desktop |
| REGWSC | 0 or 1 | <p>0: This value indicates that CylancePROTECT Desktop is not registered with Windows as an anti-virus program. It allows CylancePROTECT Desktop and Windows Defender to run at the same time on the device.</p> <p>1: This value indicates that CylancePROTECT Desktop is registered with Windows as an antivirus program.</p> <p>If no value is entered, the default value is 1.</p> <p>The above commands won't have an effect on Windows Server 2016 and 2019. To disable Windows Defender after installing CylancePROTECT Desktop on Windows Server 2016 and 2019, set the following registry value:</p> <pre>HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware</pre> <p>REG_DWORD</p> <p>Value = 1</p> <p>If the Windows Defender sub-key does not exist, you will need to manually create it,</p> <p>For more information about using group policy settings to manage Windows Defender, see Use Group Policy settings to configure and manage Windows Defender AV.</p> |
| VENUEZONE | <i>"<Zone_Name>"</i> | <p>Use this parameter to specify the name of a zone that you want to add devices to. If it can't find a zone with that name, it creates a zone with the name you provide.</p> <p>Zone names cannot contains whitespaces, tabs, carriage returns, equal signs, newlines, or other invisible characters.</p> |

| Parameter | Value | Description |
|--------------|---|--|
| VDI | <X> | <p>When you install CylancePROTECT Desktop on a master Image, use the install parameter <code>VDI=<X></code> where <X> is a "counter" for the total number of machines or images not connected to the domain (including the Master image) before creating a pool of workstations. The value for <X> determines when the agent should start identifying the virtual machine utilizing VDI fingerprinting instead of the default agent fingerprinting mechanism.</p> <p>The VDI parameter uses a counter "X" and has a delayed effect, whereas the AD parameter is immediate upon installation.</p> <p>For more information, see Requirements and considerations for using CylancePROTECT Desktop on virtual machines.</p> |
| AD | 1 | <p>This parameter requires agent version 1520 or later.</p> <p>Use the Active Directory (AD) parameter on a domain-connected master image during the initial installation. When it's installed on a domain connected master image, it immediately uses VDI fingerprinting on the master image and subsequently created pool of workstations.</p> <p>AD fingerprinting will take precedence over the <code>VDI=<X></code> installation parameter. For more information, see Requirements and considerations for using CylancePROTECT Desktop on virtual machines.</p> |
| PROXY_SERVER | <code><ip_address></code> : <code><port_number></code> | <p>This parameter specifies the IP address of the proxy server through that the agent must communicate with. Proxy server settings are added to the device's registry, and you can find proxy server information in the agent log file.</p> |
| AWS | 1 | <p>This parameter requires agent version 1500 or later.</p> <p>Use this parameter to capture and include the Amazon EC2 Instance ID to the device's name to help identify Amazon Cloud hosts.</p> <p>The device name is modified to include the hostname and the Instance ID. For example, if the device name is ABC-DE-12345678 and the AWS EC2 ID is i-0a1b2cd34efg56789, the complete device name is ABC-DE-123456789_i-0a1b2cd34efg56789.</p> <p>This feature is only available for the Amazon EC2 Instance ID.</p> |

| Parameter | Value | Description |
|-----------------|-------|---|
| PROTECTTEMPPATH | 1 | <p>This parameter requires agent version 1480 or later.</p> <p>Use this parameter to change the location of the CylanceDesktopArchive and CylanceDesktopRemoteFile folder to the Cylance ProgramData folder.</p> <p>For more information, see the KB 66457 Changing the location of the CylanceDesktopArchive and CylanceDesktopRemoteFile folders.</p> |

Example: PIDKEY, APPFOLDER, and LAUNCHAPP parameters

```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> LAUNCHAPP=0 /L*v
C:\temp\install.log
```

In this example, the installation is silent and the installation log is saved to the C:\temp folder. You may need to create this folder. When the agent runs, the system tray icon and the start menu Cylance folder are hidden. For more information about allowed command line options, see <https://docs.microsoft.com/en-us/windows/win32/msi/command-line-options>.

Example: PIDKEY, VDI, and LAUNCHAPP parameters

```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> VDI=2
LAUNCHAPP=1
```

In this example, the "2" for VDI is the total number of machines or images that are not connected to the domain (the master image plus the additional or parent image) before the pool of workstations is created.

Example: PIDKEY, AD, and LAUNCHAPP parameters

```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> AD=1 LAUNCHAPP=1
```

In this example, the AD parameter immediately uses VDI fingerprinting on the master image and the pool of workstations that is created. For information about editing the MSI installation file for deployment through a group policy, see KB 66391, [Editing the MSI Installer using Orca](#).

Installing the CylancePROTECT Desktop agent for macOS


CylancePROTECT Desktop detects and blocks malware before it can affect a device. BlackBerry uses a mathematical approach to malware identification, using machine learning techniques instead of reactive signatures, trust-based systems, or sandboxes. This approach renders new malware, viruses, bots, and future variants useless. CylancePROTECT Desktop analyzes potential file executions for malware in the OS and memory layers to prevent the delivery of malicious payloads.

You can install the agent onto individual devices or can use the installation parameters to deploy it across your environment using a deployment tool.

If you want to use an RMM solution to install the CylancePROTECT Desktop agent on devices, see [Using RMM solutions to install the Cylance agents on devices](#).

Install the CylancePROTECT Desktop agent for macOS

Before you begin:

- Download the CylancePROTECT Desktop installation files from the management console. Click **Settings > Deployments**. From the **Product** drop-down list, select **CylancePROTECT**, and set the target operating system, the agent version, and the file type. Click **Download**.
 - In the management console, copy the installation token from **Settings > Application**.
1. Double-click the CylancePROTECT Desktop installation file (.dmg or .pkg) to mount the installer.
 2. Double-click  from the CylancePROTECT Desktop user interface to begin the installation.
 3. Click **Continue** to verify that the OS and hardware meet the requirements.
 4. Click **Continue**.
 5. Type the installation token.
 6. Click **Continue**.
 7. Optionally, change the installation location.
 8. Click **Install**.
 9. Type your credentials.
 10. Click **Install Software**.
 11. On the summary screen, click **Close**.
 12. Click **OK > Finish**.
 13. If you are installing CylancePROTECT Desktop on macOS Catalina, a notification prompts you to allow CylanceUI to display notifications. Click **Allow**.

CylancePROTECT Desktop configuration requirements for macOS and later

When installing CylancePROTECT Desktop agent version 2.1 or later on devices running macOS, note the following configuration requirements. The requirements depend on whether devices are managed by an MDM solution (for example, Jamf Pro).

MDM managed devices

The information below uses Jamf Pro as the MDM solution, but it is applicable to other MDM solutions.

| Requirement | Steps |
|------------------|--|
| General settings | Create a configuration profile and specify the following settings in the General tab: <ul style="list-style-type: none">• Specify a name and description for the profile.• Level: Computer Level• Distribution Method: Install Automatically |

| Requirement | Steps |
|---|--|
| Enable the CylancePROTECT kernel extension. (macOS 10 only) | <p>Configure the following settings from the Approved Kernel Extensions option:</p> <ul style="list-style-type: none"> • Display Name: Cylance • Team ID: 6ENJ69K633 • In the Scope tab, verify that the configuration profile is scoped to apply to macOS 10 devices running CylancePROTECT Desktop and CylanceOPTICS. |
| Enable the CylancePROTECT system extension. (macOS 11+) | <p>Configure the following settings from the System Extensions option:</p> <ul style="list-style-type: none"> • Display Name: CylanceSystemExtension • System Extension Types: Allowed System Extensions • Team Identifier: 6ENJ69K633 • Allowed System Extensions: com.cylance.CylanceEndpointSecurity.extension |
| Enable full disk access for the CylancePROTECT agent and system extensions. | <p>Configure the following settings from the Privacy Preferences Policy Control option.</p> <p>Add an App Access configuration and specify the following settings:</p> <ul style="list-style-type: none"> • Identifier: com.cylance.Agent • Identifier Type: Bundle ID • Code Requirement: <ul style="list-style-type: none"> Copy the code requirement from the HTML version of this topic. The code requirement should be on one line and include no additional spaces or line breaks. • Add the SystemPolicyAllFiles service and set to Allow. <p>Add another App Access configuration and specify the following settings:</p> <ul style="list-style-type: none"> • Identifier: com.cylance.CylanceEndpointSecurity.extension • Identifier Type: Bundle ID • Code Requirement: <ul style="list-style-type: none"> Copy the code requirement from the HTML version of this topic. The code requirement should be on one line and include no additional spaces or line breaks. • Add the SystemPolicyAllFiles service and set to Allow. |
| Notifications | <p>In the Notifications tab of the configuration profile, the following settings are recommended:</p> <ul style="list-style-type: none"> • Critical Alerts: Enabled • Notifications: Enabled • Banner alert type: Persistent • Notifications on Lock screen: Displayed • Notifications in Notification Center: Displayed • Badge app icon: Displayed • Play sound for notifications: Enabled |

| Requirement | Steps |
|-----------------------------|---|
| Scope | Configure the following settings in the Scope tab: <ul style="list-style-type: none"> Verify that the configuration profile is scoped to apply to macOS devices that will be running CylancePROTECT Desktop. |
| Restart after installation. | After you complete the configuration steps above and install the CylancePROTECT Desktop agent, restart the device. |

Devices that are not MDM managed

On devices that are not MDM managed, the user receives a prompt to approve the "CylanceES System Extension" after installing the macOS agent on the device. Follow these instructions from the prompt to enable the system extension and allow full disk access. Users can also tap the notification from "CylanceUI" to configure its notification settings.

1. Click **Open Security Preferences**. This opens the **System Preferences > Security & Privacy > General** tab.
2. If necessary, click the lock to authenticate the changes and click **Allow**.
3. Beside the **System software from application 'CylanceES' was blocked from loading** message, click **Allow** to approve the extension.
4. To enable full disk access, on the device, navigate to **System Preferences > Security & Privacy > Privacy** tab.
5. If necessary, click the lock to authenticate the changes and click **Allow**.
6. Scroll down and click **Full Disk Access**.
7. Select **CylanceEsExtension**.
8. Allow notifications for the agent from the **System Preferences > Notifications > CylanceUI** tab.

Commands for installing the macOS agent using the command line

When using the command line to install the macOS agent, you must create a `cyagent_ install_token` file that includes the installation parameters. The file includes the installation token, along with other optional parameters that you can set.

The follow sections include examples on how to create the file from the command line, but you can create the file from a text editor that includes each parameter in their own separate line. The file must be in the same folder as the installation package.

Installing the macOS agent with the installation token only

Use the following example commands in the terminal to create the `cyagent_ install_token` file with the installation token and install the agent. If you are using the `.dmg` installer, change the file extension in the command accordingly.

```
echo YOURINSTALLTOKEN > cyagent_install_token
sudo installer -pkg CylancePROTECT.pkg -target /
```

The following is the installation command without the installation token:

```
sudo installer -pkg CylancePROTECT.pkg -target /
```

Installing the macOS agent with specified parameters

Use the following example commands in the terminal to create the `cyagent_install_token` file with the specified parameters and install the agent. If you are using the `.dmg` installer, change the file extension in the command accordingly.

```
echo YOURINSTALLTOKEN > cyagent_install_token
echo SelfProtectionLevel=2 >> cyagent_install_token
echo VenueZone=zone_name >> cyagent_install_token
echo LogLevel=2 >> cyagent_install_token
sudo installer -pkg CylancePROTECT.pkg -target /
```

Installation parameters

The CylancePROTECT Desktop agent can be installed using command line options in the terminal.

| Parameter | Value | Description |
|---------------------|----------------------|---|
| InstallToken | <installation_token> | The installation token is required when you install the agent. You can find it in the management console by clicking Settings > Application . |
| NoCylanceUI | | This parameter hides the system tray at startup. |
| SelfProtectionLevel | 1 or 2 | 1: This value only allows local administrators to make changes to the registry and services. 2: This value only allows the system administrator to make changes to the registry and services. If no value is specified, the default value is 2. |
| LogLevel | 0, 1, 2, or 3 | 0: This value indicates that only error messages are logged. 1: This value indicates that error and warning messages are logged. 2: This value indicates that error, warning, and information messages are logged. 3: This value enables verbose logging, where all messages are logged. Note that verbose log file sizes can grow very large. BlackBerry recommends turning on verbose logging during troubleshooting and then changing it back to 2 when troubleshooting is complete. If no value is specified, the default value is 2. |
| VenueZone | <zone_name> | Use this parameter to add devices to an existing zone, or to a zone that you want to create. If the zone does not exist, the zone is created using the name you type. You cannot use tabs, carriage returns, newlines, equal signs, whitespace or other invisible characters in the zone name. This parameter requires agent version 1380 or later. |

| Parameter | Value | Description |
|-------------|----------------------------|---|
| ProxyServer | <ip_address>:<port_number> | <p>This adds proxy server settings to the device's registry. You can find the proxy server information in the agent log file.</p> <p>This parameter requires agent version 1470 or later.</p> |

Troubleshooting macOS installations

The table below outlines the actions you can take to troubleshoot the macOS installation.

| Issue | Action |
|---|--|
| Troubleshooting with the installation token and verbose installer logging | <p>Type the following commands and replace "YOURINSTALLTOKEN" with the installation token found in the Settings > Application tab of the management console:</p> <pre>echo YOURINSTALLTOKEN >cyagent_install_token sudo installer -verboseR -dumplog -pkg CylancePROTECT.pkg -target /</pre> <p>The echo command outputs a cyagent_install_token file, which is a text file with one installation option per line. This file must be in the same folder as the CylancePROTECT.pkg installation package.</p> <p>If you install the CylancePROTECT Desktop agent using Terminal on macOS Catalina, a DYLD warning sometimes displays. This warning does not impact the installation because it is generated by the operating system, not by the CylancePROTECT Desktop.</p> |
| Start or stop the macOS agent service | <p>To start the agent service, run the following command:</p> <pre>sudo launchctl load /Library/launchdaemons/ com.cylance.agent_service.plist</pre> <p>To stop the agent service, run the following command:</p> <pre>sudo launchctl load /Library/launchdaemons/ com.cylance.agent_service.plist</pre> |

| Issue | Action |
|--|---|
| Supporting the Endpoint Security system extension on macOS Big Sur | <p>BlackBerry recommends using MDM to deploy a configuration profile that contains approval and full disk access for the CylancePROTECT Desktop system extension. By default, macOS Big Sur does not support remote silent installations of an MDM profile onto a system with a new installation of the Big Sur operating system.</p> <p>To install configuration profiles on remote macOS systems without user interaction (silent install), Apple Mobile Device Management (MDM) is required. Before upgrading to macOS Big Sur, the devices should be enrolled with an MDM vendor. Devices that are not enrolled prior to the upgrade require user interaction with administrative privileges.</p> <p>To support remote silent installations, do the following:</p> <ol style="list-style-type: none"> 1. Install macOS Catalina. 2. Apply the MDM profile. 3. Download the configuration profiles onto the device. 4. Upgrade the device to macOS Big Sur. <p>The CylancePROTECT Desktop agent versions and the extension types that they support are the following:</p> <ul style="list-style-type: none"> • The CylancePROTECT Desktop agent version 1570 or earlier includes the kernel extension which is supported on macOS Catalina or earlier. • The CylancePROTECT Desktop agent version 1580 and later includes the kernel extension which is supported on macOS Catalina or earlier, and the Endpoint Security system extension, which is supported on macOS Big Sur and later. |

Installing the CylancePROTECT Desktop agent for Linux

The agent can be installed directly on each system or through system management software, such as Ansible, SCCM, or cloud-init. When installing the agent, installation parameters are provided to configure some installation settings.

Ensure the target devices meet system requirements and that you have the proper permissions for installing software.

- Review the [CylancePROTECT Desktop requirements](#).
- Root permission is required to install the Linux agent.
- [Create a configuration file for the Linux agent installation](#)

After installing the CylancePROTECT Desktop agent on Linux devices, make sure to keep the Linux drivers updated to support the latest kernels on the systems. Updated driver packages are released regularly and independently from the agent releases. For more information, see [Updating the Linux driver](#).

Linux agent installation package

Starting with agent version 2.1.1590, the CylancePROTECT Desktop agent, agent UI, and driver packages are included in one compressed .tgz file.

| Debian package | Component |
|-----------------------------|--------------------------------------|
| cylance-protect-driver | Proprietary driver |
| cylance-protect-open-driver | Open driver |
| cylance-protect | CylancePROTECT Desktop agent/service |
| cylance-protect-ui | CylancePROTECT Desktop UI |

| RPM package | Component |
|--------------------------|--------------------------------------|
| CylancePROTECTDriver | Proprietary driver |
| CylancePROTECTOpenDriver | Open driver |
| CylancePROTECT | CylancePROTECT Desktop agent/service |
| CylancePROTECTUI | CylancePROTECT Desktop UI |

Linux installation prerequisites

The agent can be installed directly on each system or through system management software, such as Ansible, SCCM, or cloud-init. When installing the agent, installation parameters are provided to configure some installation settings.

Ensure the target devices meet system requirements and that you have the proper credentials for installing software.

- [CylancePROTECT Desktop requirements](#)
- Root permission is required to install the Linux agent.

Create a configuration file for the Linux agent installation

Before you install the CylancePROTECT Desktop agent on Linux devices, you must create configuration file which is used to register the device with your Cylance Endpoint Security tenant and define local agent settings. After the installation of the agent, the configuration file is removed from the device.

CylancePROTECT Desktop requires `config_defaults.txt` to only contain line feed as a line ending. If you are creating the file from a DOS/Windows computer, the line ending includes carriage return and line feed. For instructions on how to convert the `config_defaults.txt` file to a proper format, visit support.blackberry.com/community to read article 65749.

1. In the `/opt/cylance/` directory, create the `config_defaults.txt` file.
2. Edit the file with the following information.

```
InstallToken=YOUR_INSTALL_TOKEN
SelfProtectionLevel=2
LogLevel=2
VenueZone=ZONE_NAME
UiMode=2
AWS=1
```

- Replace `YOUR_INSTALL_TOKEN` with the installation token from the management console.

- Replace *ZONE_NAME* with the name of the zone that you want to add the device to. If the specified zone doesn't exist in the console, it will be automatically created.

| Parameter | Description |
|----------------------------|---|
| InstallToken | This field is required and specifies the Cylance Endpoint Security tenant that you want the device to register with. Use the installation token from the Settings > Application menu in the management console. |
| SelfProtectionLevel | <p>This setting restricts the level of access to the Cylance Service and folders.</p> <ul style="list-style-type: none"> • 1: Only Local Administrators can make changes to the registry and services. • 2: Only the System Administrator can make changes to the registry and services. <p>The default setting is "2".</p> |
| LogLevel | <p>This setting specifies the level of information gathered in the debug logs.</p> <ul style="list-style-type: none"> • 0: Error • 1: Warning • 2: Information • 3: Verbose <p>The default setting is "2". If verbose logging is selected, the file size of the log grows quickly.</p> |
| VenueZone | <p>This setting specifies the zone that you want to add the device to.</p> <ul style="list-style-type: none"> • If the specified zone name does not exist in the console, the zone is created using the name provided. • If the zone name or device name leads or ends with whitespace (for example, " Hello" or "Hello "), it is removed during device registration. Tabs, carriage returns, newlines, or other invisible characters are not permitted. • Zone names cannot contain an equal sign (=). For example, "Hello=World" is not permitted. |
| UiMode | <p>This setting specifies the agent user interface mode when the system starts.</p> <ul style="list-style-type: none"> • 1: Minimal user-interface • 2: Full user-interface <p>The default setting is "2".</p> |

| Parameter | Description |
|------------|--|
| AWS | <p>This setting specifies that the agent is running on an Amazon Web Services host. By default, the device's hostname is used as the Device Name in the management console. Enable this setting to allow the agent to capture the Instance ID from the host and store it with the hostname to the Device Name field in the console. This setting makes sure that each agent on a Amazon Web Services host reports a unique device name to the management console.</p> <p>1: Enable the agent to capture the Instance ID.</p> <p>The Device Name is modified to include Hostname + Instance ID. The instance ID is denoted with the "i-" prefix.</p> <p>ABC-DE-123456789_i-0a1b2cd34efg56789 where the device name is ABCDE-12345678 and the AWS EC2 ID is i-0a1b2cd34efg56789.</p> |

Install the Linux agent automatically

Before you begin:

- Review the [CylancePROTECT Desktop requirements](#).
 - Download the CylancePROTECT Desktop installation files from the management console. Click **Settings > Deployments**. From the **Product** drop-down list, select **CylancePROTECT**, and set the target operating system, the agent version, and the file type. Click **Download**.
 - In the management console, copy the installation token from **Settings > Application**.
 - Verify that you have root permissions.
1. [Create a configuration file for the Linux agent installation](#).
 2. Run the following commands in the specified order to install the driver and the agent. Use the files extracted from the .tgz file to determine the value of `<version>`.

| Linux distribution | Commands |
|--|---|
| <ul style="list-style-type: none"> • Red Hat Enterprise Linux • CentOS • Amazon Linux • Oracle • AlmaLinux • Rocky Linux | <p>Run the following commands to install the driver and the agent:</p> <ol style="list-style-type: none"> a. <pre>yum install CylancePROTECTOpenDriver-<version>.rpm CylancePROTECTDriver-<version>.rpm</pre> b. <pre>yum install CylancePROTECT.<version>.rpm CylancePROTECTUI.<version>.rpm</pre> |
| SUSE Linux Enterprise Server | <p>Run the following commands to install the driver and the agent:</p> <ol style="list-style-type: none"> a. <pre>zypper install CylancePROTECTOpenDriver-<version>.rpm CylancePROTECTDriver-<version>.rpm</pre> b. <pre>zypper install CylancePROTECT.<version>.rpm CylancePROTECTUI.<version>.rpm</pre> |

After you finish:

If the agent UI does not launch automatically after installation (for example, on CentOS, SUSE, or Ubuntu devices), you need to restart the GNOME shell to view the CylancePROTECT UI. See [Start the UI manually](#).

Install the Linux agent manually

Before you begin:

- Review the [CylancePROTECT Desktop requirements](#).
 - Download the CylancePROTECT Desktop installation files from the management console. Click **Settings > Deployments**. From the **Product** drop-down list, select **CylancePROTECT**, and set the target operating system, the agent version, and the file type. Click **Download**.
 - In the management console, copy the installation token from **Settings > Application**.
 - Verify that you have root permissions.
1. [Create a configuration file for the Linux agent installation](#).
 2. Run the following commands in the specified order to install the driver and the agent. Use the files extracted from the .tgz file to determine the value of `<version>`.

| Linux distribution | Commands |
|---|--|
| <ul style="list-style-type: none">• Red Hat Enterprise Linux or CentOS• Amazon Linux• Oracle• SUSE Linux Enterprise Server• AlmaLinux• Rocky Linux | <p>a. Install the open driver:</p> <pre>rpm -ivh CylancePROTECTOpenDriver-<version>.rpm</pre> <p>b. Install the agent driver:</p> <pre>rpm -ivh CylancePROTECTDriver-<version>.rpm</pre> <p>c. Install the agent:</p> <pre>rpm -ivh CylancePROTECT.<version>.rpm</pre> <p>d. Install the agent UI*:</p> <pre>rpm -ivh CylancePROTECTUI.<version>.rpm</pre> <p>* For devices running SUSE Linux Enterprise Server, you might need to install the Gnome 3 library (libgtk-3-0) prior to the agent UI installation. If necessary, use the following command: <code>zypper install libgtk-3-0</code></p> |
| <ul style="list-style-type: none">• Ubuntu• Debian | <p>a. Install the open driver:</p> <pre>dpkg -i cylance-protect-open-driver_<version>.deb</pre> <p>b. Install the agent driver:</p> <pre>dpkg -i cylance-protect-driver_<version>.deb</pre> <p>c. Install the agent:</p> <pre>dpkg -i cylance-protect.version.deb</pre> <p>d. Install the agent UI:</p> <pre>dpkg -i cylance-protect-ui.version.deb</pre> |

After you finish:

If the agent UI does not launch automatically after installation (for example, on CentOS, SUSE, or Ubuntu devices), you need to restart the GNOME shell to view the CylancePROTECT UI. See [Start the UI manually](#).

Updating the Linux driver

Each supported Linux kernel requires a supported driver so that the CylancePROTECT Desktop agent can run on the device. When you upgrade the Linux kernel on a device, you must make sure that the device is running a driver that supports it. Upgrading to the latest kernel ensures that your device receives the latest OS security updates, while using the latest agent and driver ensures that CylancePROTECT keeps it protected.

You have the following options to keep the Linux driver updated:

| Scenario | Actions |
|---|---|
| Automatically update the driver as soon as an update is available when you upgrade the Linux kernel | <ul style="list-style-type: none">• Make sure that the devices are running agent version 3.1 or later and driver 3.1 or later.• Enable the Auto-Update Linux Driver feature in the update rule. |
| Manually update the driver when you upgrade the Linux kernel | <ul style="list-style-type: none">• Each time you upgrade the Linux kernel, you need to manually download the driver package when it becomes available in the management console. To determine the minimum driver version that you need for the Linux kernel that you are using, see the Supported Linux drivers and kernels spreadsheet.• You can use a package manager or similar tools and methods to update the agent and driver.• If you choose to update the agent manually, BlackBerry recommends that you change the zone-based update Agent setting to Do Not Update for these devices. <p>Tip: The 3.1.1100 driver is compatible with agent 2.1.1590 and later. You can install the driver on devices that are running agent version 2.1.1590 and later so that you can benefit from the Auto-Update Linux Driver feature when you upgrade to agent 3.1.</p> |

Automatically update the Linux driver

When you upgrade the Linux kernel on a device, you must make sure that the device is running a driver that supports it. For devices running CylancePROTECT Desktop agent 3.1 and later, you can enable the Auto-Update Linux Driver feature, which allows the agent to automatically update the driver when an updated kernel is detected on the system, as soon as it becomes available. Upgrading to the latest kernel ensures that your device receives the latest OS security updates, while using the latest agent and driver ensures that CylancePROTECT keeps it protected.

1. In the management console, on the menu bar, go to **Settings > Update**.
2. Click an update rule that you use to manage updates for Linux devices. If you need to create one, see [Manage updates for the CylancePROTECT Desktop and CylanceOPTICS agents](#).
3. Expand the **Agent** section.
4. Select the **Auto-Update Linux Driver** option.
5. Click **Save**.

Manually update the Linux driver

When you upgrade the kernel on your Linux device, you must make sure that the device is running a driver that supports it. When a Linux distribution releases a kernel update, BlackBerry creates an updated Linux driver package and makes it available from the management console. A driver update package is only available if there is a more up-to-date version than the one included in the agent release.

BlackBerry recommends that you upgrade to agent version 3.1 or later, which enables a feature that allows the agent to [automatically update the Linux driver](#) after an updated kernel is detected, as soon as it becomes available. If you are running agent versions 3.0 or 2.1.1590, or you choose not to use the Auto-Update Linux Driver feature, you must manually install a supported driver for the Linux kernel. You can use tools and methods from your organization to deploy the compatible drivers to your devices.

Before you begin:

- Verify that you have root or sudo permissions.
- [Determine the minimum driver version that is required to support the Linux kernel on your device.](#)

1. In the management console, on the menu bar, click **Settings > Deployments**.
2. In the **Product** list, select **CylancePROTECT Driver**.
3. In the **OS** list, select the operating system that you want to download the driver for.
4. In the **Version** list, select the version of the driver.
5. In the **Format** list, select the format of the driver.
6. Click **Download**.
7. To upgrade the RPM package, use one of the following commands :

Paste both drivers in the same command line and replace "xx" with the package version number:

| Distribution | Commands |
|---|---|
| Oracle 6, Oracle UEK 6 | <pre>rpm -Uvh CylancePROTECTOpenDriver-xx.el6.noarch.rpm CylancePROTECTDriver-xx.el6.noarch.rpm</pre> |
| CentOS 7, RHEL 7, Oracle 7, Oracle UEK 7 | <pre>rpm -Uvh CylancePROTECTOpenDriver-xx.el7.x86_64.rpm CylancePROTECTDriver-xx.el7.x86_64.rpm</pre> |
| CentOS 8, RHEL 8, Oracle 8, Oracle UEK 8, AlmaLinux 8, Rocky Linux 8 | <pre>rpm -Uvh CylancePROTECTOpenDriver-xx.el8.x86_64.rpm CylancePROTECTDriver-xx.el8.x86_64.rpm</pre> |
| CentOS 9, RHEL 9, Oracle 9, Oracle UEK 9, AlmaLinux 9, Rocky Linux 9 | <pre>rpm -Uvh CylancePROTECTOpenDriver-xx.el9.x86_64.rpm CylancePROTECTDriver-xx.el9.x86_64.rpm</pre> |
| Amazon Linux 2 | <pre>rpm -Uvh CylancePROTECTOpenDriver-xx.amzn2.x86_64.rpm CylancePROTECTDriver-xx.amzn2.x86_64.rpm</pre> |
| SUSE Linux Enterprise Server | <pre>rpm -Uvh CylancePROTECTOpenDriver-xx.x86_64.rpm CylancePROTECTDriver-xx.x86_64.rpm</pre> |

| Distribution | Commands |
|--|---|
| Supported 32-bit Ubuntu and Xubuntu distros | <ul style="list-style-type: none"> Install the dependencies with the following command: <pre>apt-get update -y && apt-get install</pre> Install the CylancePROTECT Desktop driver DEB packages with the following commands: <pre>dpkg -i cylance-protect-open-driver_xx_i386_32.deb dpkg -i cylance-protect-driver_xx_i386_32.deb</pre> |
| Supported 64-bit Ubuntu, Xubuntu, and Debian distros | <ul style="list-style-type: none"> Install the dependencies with the following command: <pre>apt-get update -y && apt-get install</pre> Install the CylancePROTECT Desktop driver DEB packages with the following commands: <pre>dpkg -i cylance-protect-open-driver_xx_amd64.deb dpkg -i cylance-protect-driver_xx_amd64.deb</pre> |

8. Restart the service with the following command: `systemctl start cylancesvc`.

Upgrade the Linux agent manually

Before you begin:

- Review the [CylancePROTECT Desktop requirements](#).
- Download the latest CylancePROTECT Desktop installation files from the management console. Click **Settings > Deployments**. From the **Product** drop-down list, select **CylancePROTECT**, and set the target operating system, the agent version, and the file type. Click **Download**.
- Verify that you have root permissions.

To manually upgrade the agent on a Linux device, run the following commands based on the Linux distribution in the specified order. Use the files extracted from the .tgz file to determine the value of `<version>`.

| Linux distribution | Commands |
|--|---|
| <ul style="list-style-type: none"> Red Hat Enterprise Linux or CentOS Amazon Linux Oracle SUSE Linux Enterprise Server | <p>a. Upgrade the agent:</p> <pre>rpm -Uvh CylancePROTECT.<version>.rpm</pre> <p>b. Upgrade the agent UI*:</p> <pre>rpm -Uvh CylancePROTECTUI.<version>.rpm</pre> <p>* For devices running SUSE Linux Enterprise Server, you might need to install the Gnome 3 library (libgtk-3-0) prior to the agent UI installation. If necessary, use the following command: <code>zypper install libgtk-3-0</code></p> |

| Linux distribution | Commands |
|--|---|
| <ul style="list-style-type: none"> • Ubuntu • Debian | <p>a. Install the agent:</p> <pre>dpkg -i cylance-protect.<version>.deb</pre> <p>b. Install the agent UI:</p> <pre>dpkg -i cylance-protect-ui.<version>.deb</pre> |

Linux commands for the agent

To display list of Linux commands for the CylancePROTECT Desktop agent, use the following:

```
/opt/cylance/desktop/cylance -h
```

Example usage of commands: `cylance <option>`

| Option | Description |
|---------------------------|--|
| -r, --register=<token> | Register the agent with the console using the provided token |
| -s, --status | Check for agent updates |
| -b, --start-bg-scan | Start the background threat detection scan |
| -B, --stop-bg-scan | Stop the background threat detection scan |
| -d, --scan-dir=<dir> | Scan a directory |
| -l, --getloglevel | Retrieve the current logging level |
| -L, --setloglevel=<level> | Set the logging level to specify the level of information gathered in debug logs |
| -P, --getpolicytime | Retrieve the policy update time |
| -p, --checkpolicy | Check for policy updates |
| -t, --threats | Display a list of threats |
| -q, --quarantine=<id> | Quarantine a file by specifying a hash ID |
| -w, --waive=<id> | Waive a file by specifying a hash ID |
| -v, --version | Display the version of this tool |
| -h, --help | Display a list of commands |

Troubleshooting Linux agent installations

The table below outlines the actions you can take to troubleshoot Linux agent installations.

| Task or error | Action |
|--|--|
| Start or stop the agent service | <p>Use the following commands to start or stop the Cylance service on a Linux device:</p> <ul style="list-style-type: none"> To start the Cylance service: <pre>systemctl start cylancesvc</pre> To stop the Cylance service: <pre>systemctl stop cylancesvc</pre> |
| Verify whether kernel drivers are loaded | <p>To verify whether the kernel drivers are loaded, enter the following command:</p> <pre>lsmod grep CyProtectDrv</pre> <p>If the kernel modules are loaded, the command should output something similar to the following:</p> <pre>CyProtectDrv 210706 0CyProtectDrvOpen 16384 1 CyProtectDrv</pre> <p>If the kernel modules are not loaded, no output is returned.</p> |
| Load and unload the kernel drivers | <p>On CylancePROTECT Desktop Linux agent 2.1.1590 and later, there are two drivers that are loaded and unloaded together: <code>CyProtectDrv</code> and <code>CyProtectDrvOpen</code>. On earlier versions of the agent, only the <code>CyProtectDrv</code> driver is loaded.</p> <p>To load the kernel drivers, enter one of the following commands:</p> <ul style="list-style-type: none"> For SUSE Linux distributions: <pre>modprobe --allow-unsupported cyprotect</pre> <p>If you don't want to keep using the <code>--allow-unsupported</code> flag, edit <code>/etc/modprobe.d/10-unsupported-modules.conf</code> and change <code>'allow_unsupported_modules'</code> to <code>'1'</code>.</p> For all other Linux distributions: <pre>modprobe cyprotect</pre> |
| Start the Linux UI manually | <p>If the agent UI did not launch automatically after installation, see Start the UI manually for more information.</p> |
| Error: Multilib version problems found | <p>If the "Error: Multilib version problems found" occurs when installing a package on a device, see Error: Multilib version problems found for more information.</p> |

Start the UI manually

The agent UI might not launch automatically after the installation (for example, on CentOS, Ubuntu and SUSE devices). To launch it manually, you can restart the GNOME Shell Extension, or log out and then log back in.

The GNOME Tweak Tool must be installed before you restart the GNOME Shell Extension. Ubuntu may not include the GNOME Tweak Tool by default.

1. If you need to install the GNOME Tweak Tool, run the following commands:

```
add-apt-repository universe
apt install gnome-tweak-tool
```

2. To restart the GNOME Shell Extension, press `Alt+F2`, type 'r' in the dialog box, then press the `ENTER` key. If the CylanceUI icon does not appear, manually enable the GNOME Shell Extension from the Tweak Tool. To launch the GNOME Tweak Tool, type 'gnome-tweaks' in a terminal. In the GNOME Tweak Tool, go to the **Extensions** tab and enable the CylanceUI.

Error: Multilib version problems found

If the "Error: Multilib version problems found" occurs when installing a package on a device running Red Hat Enterprise Linux or CentOS, it typically means that the corresponding 64-bit library must be installed or upgraded, along with the 32-bit library. The `multilib` version checking is simply pointing out that there is a problem.

For example, if the error is related to the `sqlite` library:

- You have an upgrade for `sqlite` that is missing a dependency that another package requires. `Yum` tries to resolve this by installing an older version of `sqlite` of the different architecture. If you exclude the the other architecture, `yum` displays the root cause of the problem, such as any missing package dependencies. To display an error message with the root cause of the problem, you can try attempting the upgrade again with `--exclude sqlite.otherarch`.
- You have multiple architectures of `sqlite` installed, but `yum` can only see an upgrade for one of those architectures. If you don't need both architectures, you can remove the `sqlite` that is missing the architecture update and see if the error is resolved.
- You have duplicate versions of `sqlite` installed already. You can use "yum check" to show these errors.
- To install or upgrade the matching `sqlite` library, use the following command:

```
yum install sqlite.i686 sqlite
```

If the error is related to the `dbus-libs`, `openssl`, or `libgcc` libraries, replace the `sqlite` with the appropriate library in the command.

Require users to provide a password to remove the CylancePROTECT Desktop and CylanceOPTICS agents

You can require users to provide a password to uninstall the CylancePROTECT Desktop agent for Windows and macOS, the CylanceOPTICS agent for Windows version 3.1 or later, and the CylanceOPTICS agent for macOS version 3.3 or later. Using this feature for the CylanceOPTICS agent for macOS also requires CylancePROTECT Desktop version 3.1 or later.

1. In the management console, on the menu bar, click **Settings > Application**.
2. Select the **Require Password to Uninstall Agent** check box.
3. Specify a password.
4. Click **Save**.

Setting up CylanceOPTICS

| Step | Action |
|------|---|
| 1 | Review the software requirements . |
| 2 | Install the CylanceOPTICS agent on devices. |
| 3 | Enable and configure CylanceOPTICS. |
| 4 | Manage updates for the CylancePROTECT Desktop and CylanceOPTICS agents. |

Install the CylanceOPTICS agent on devices

To enable a device for CylanceOPTICS, you must install the CylanceOPTICS agent on the device. You download the CylanceOPTICS agent installer from the management console, then run it on devices using your organization's preferred method. For example, you can have IT administrators pre-install the agent on devices before providing them to users, or you can push the installation using a trusted software distribution process.

Before you begin:

- Review the [CylanceOPTICS software requirements](#).
- You must install the CylancePROTECT Desktop agent on devices before you install the CylanceOPTICS agent.
- If you want to install the CylanceOPTICS agent on macOS Big Sur (11.x) or later devices, see [Configuration requirements for macOS 11.x and later](#).
- If you want to use a supported RMM solution to install the CylanceOPTICS agent on devices, see [Using RMM solutions to install the Cylance agents on devices](#).

1. In the management console, on the menu bar, click **Settings > Deployments**.
2. In the **Product** drop-down list, click **CylanceOPTICS**.
3. Select the OS, version, and format.

Note:

- For macOS devices, it is a best practice to use the .pkg file. The .dmg file is a disk image of the .pkg file that can be used when a disk image must be mounted for installation.
 - Before you deploy the agent to macOS devices, see [KB article 66578: Allowing Cylance kernel extensions to address "Driver Failed To Connect"](#).
 - For Oracle Linux Server UEK 8 and Oracle Linux Server 8 devices, use the Oracle 8 installation file (requires CylanceOPTICS agent 3.2 or later).
4. Click **Download**.
 5. Using your organization's preferred software distribution method, deploy and run the installation file on devices.

If you want to install the CylanceOPTICS agent on Windows or macOS devices using OS commands, or if you are installing on Linux, see [OS commands for the CylanceOPTICS agent](#).

After you finish:

- [Enable and configure CylanceOPTICS](#) in a device policy and assign the policy to one or more zones.
- For more information about managing upgrades of the CylanceOPTICS agent, see [Manage updates for the CylancePROTECT Desktop and CylanceOPTICS agents](#).

Configuration requirements for macOS 11.x and later

To install CylanceOPTICS agent version 3.0 or later on devices with macOS Big Sur (11.x) or later, note the following configuration requirements. The requirements depend on whether devices are managed by an MDM solution (for example, Jamf Pro).

MDM managed devices

The information below uses Jamf Pro as the MDM solution, but it is applicable to other MDM solutions.

| Requirement | Steps |
|---|---|
| Enable full disk access for CylanceOPTICS. | <p>Create a configuration profile and configure the following privacy preferences:</p> <ul style="list-style-type: none">• Identifier: com.cylance.Optics• Identifier Type: Bundle ID• Code Requirement:<pre>identifier "com.cylance.Optics" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] / * exists */ and certificate leaf[subject.OU] = "6ENJ69K633"</pre>• SystemPolicyAllFiles service: Allow |
| Enable the CylanceOPTICS system extension. | <p>Create a configuration profile and configure the following privacy preferences:</p> <ul style="list-style-type: none">• Display Name: Cylance Endpoint Security Optics System Extension• System Extension Types: Allowed System Extensions• Team Identifier: 6ENJ69K633• Allowed System Extensions: com.cylance.CyOpticsESF.extension |
| Enable the CylanceOPTICS system extension full disk access. | <p>Create a configuration profile and configure the following privacy preferences:</p> <ul style="list-style-type: none">• Identifier: com.cylance.CyOpticsESF.extension• Identifier Type: Bundle ID• Code Requirement:<pre>anchor apple generic and identifier "com.cylance.CyOpticsESF.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] / * exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "6ENJ69K633")</pre>• SystemPolicyAllFiles service: Allow |

| Requirement | Steps |
|---|---|
| Enable the CylanceOPTICS network extension. | <p>Create a configuration profile and configure the following content filter settings:</p> <ul style="list-style-type: none"> Filter Name: com.cylance.CyOpticsESF.extension Identifier: com.cylance.CyOpticsESF.extension Socket Filter Bundle Identifier: com.cylance.CyOpticsESF.extension Socket Filter Designated Requirement: <pre> anchor apple generic and identifier "com.cylance.CyOpticsESF.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] / * exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "6ENJ69K633") </pre> <ul style="list-style-type: none"> Network Filter Bundle Identifier: com.cylance.CyOpticsESF.extension Network Filter Designated Requirement: <pre> anchor apple generic and identifier "com.cylance.CyOpticsESF.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] / * exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "6ENJ69K633") </pre> |
| Restart after installation. | After you complete the configuration steps above and install the CylanceOPTICS agent, restart the device. |

Devices that are not MDM managed

After you install the CylanceOPTICS agent:

1. Restart the device.
2. Go to the Security & Privacy settings and approve CyOpticsESFLoader.
3. When you are prompted, allow the CylanceOPTICS network filter.
4. If System Integrity Protection (SIP) is enabled on the device, on the Privacy tab, click Full Disk Access and verify that CyOpticsESFLoader is selected. If CyOpticsESFLoader is not in the list, click +, navigate to /Library/Application Support/Cylance/Optics, and select CyOptics.
5. Restart the device again.

To verify that the system extension is loaded:

1. Run `$ systemextensionsctl list` and confirm that the output includes `com.cylance.CyOpticsESF.extension`.
2. Run `$ ps aux | grep -i extension | grep -i Cylance` and confirm that the output includes `com.cylance.CyOpticsESF.extension.systemextension`.

OS commands for the CylanceOPTICS agent

The CylanceOPTICS agent installer supports the following OS commands.

Windows

| Actions | Commands |
|---|---|
| Specify the installation directory. | <code>INSTALLFOLDER=<path></code> |
| Specify the directory for the local CylanceOPTICS data store. | <code>OPTICSRROOTDATAFOLDER=<path></code> |
| Perform a silent installation with no user action required. | <p>For the .exe package, use any of the following:</p> <ul style="list-style-type: none">• <code>-q</code>• <code>-quiet</code>• <code>-s</code>• <code>-silent</code> <p>For the .msi package, use either of the following:</p> <ul style="list-style-type: none">• <code>/q</code>• <code>/quiet</code> |
| Create an installation log file. | <p>For the .exe package, use either of the following:</p> <ul style="list-style-type: none">• <code>-l <path_for_log></code>• <code>-log <path_for_log></code> <p>For the .msi package, use either of the following:</p> <ul style="list-style-type: none">• <code>/l <path_for_log></code>• <code>/log <path_for_log></code> |
| Disable proxy bypass for the CylanceOPTICS agent (.msi package only). | <p>Use this option if you want the CylanceOPTICS agent to always use a specified proxy connection to the CylanceOPTICS cloud services. This is optional in most environments but required if you are using CylanceHYBRID.</p> <p>Before you execute the installer with the command below, create the ProxyServer registry key on the device. See Configuring a proxy for the CylancePROTECT Desktop and Cylance OPTICS agents. If you are using CylanceHYBRID, see the Windows setup instructions in the CylanceHYBRID Administration Guide and create the ProxyServer registry key with the required value for CylanceHYBRID.</p> <p>After you create the ProxyServer registry key on the device, use the following command when installing the agent: <code>HYBRID=True</code></p> <p>The installer creates the DisableProxyBypass registry key on the device with the value set to True. For more information, see Proxy options for the CylanceOPTICS agent. If the command is set to <code>False</code>, the installer does not create the registry key.</p> |

| Actions | Commands |
|------------------------------------|---|
| Uninstall the CylanceOPTICS agent. | <p>"<CylanceOPTICS_program_directory>\CyOpticsUninstaller.exe"</p> <p>For example: "C:\Program Files\Cylance\Optics\CyOpticsUninstaller.exe"</p> <p>To perform a silent uninstall that doesn't require user interaction, add the following commands: <code>--use_cli -t v20</code></p> <p>If you configured the CylanceOPTICS agent to require an uninstall password, add the following command: <code>--password <password></code></p> <p>For example: "C:\Program Files\Cylance\Optics\CyOpticsUninstaller.exe" <code>--use_cli -t v20 --password samplepass</code></p> |

macOS

| Action | Commands |
|--|--|
| Install the CylanceOPTICS agent. | <code>sudo installer -pkg CylanceOPTICS.pkg -target /</code> |
| Install the CylanceOPTICS agent and create an installation log file. | <code>sudo installer -verboseR -dumplog -pkg CylanceOPTICS.pkg -target /</code> |
| Disable proxy bypass for the CylanceOPTICS agent | <p>Use this option if you want the CylanceOPTICS agent to always use a specified proxy connection to the CylanceOPTICS cloud services. This is optional in most environments, but required if you are using CylanceHYBRID.</p> <p>Before you install the CylanceOPTICS agent, follow the instructions in Cylance Endpoint Security proxy requirements to configure proxy bypass for macOS devices.</p> |
| Start the CylanceOPTICS service. | <code>sudo launchctl load /Library/LaunchDaemons/com.cylance.cyoaptics_service.plist</code> |
| Stop the CylanceOPTICS service. | <code>sudo launchctl unload /Library/LaunchDaemons/com.cylance.cyoaptics_service.plist</code> |
| Uninstall the CylanceOPTICS agent. | <code>sudo /Applications/Cylance/Optics/Uninstall\CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS</code> |
| Uninstall the CylanceOPTICS agent with no UI. | <p><code>sudo /Applications/Cylance/Optics/Uninstall\CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS --noui</code></p> <p>If you want to use this command, additional actions are required on macOS 11.x devices. For more information, see the troubleshooting section in the Cylance Endpoint Security Administration content.</p> |

Linux

| Action | Commands |
|--|---|
| Install the CylanceOPTICS agent on RHEL/CentOS, SUSE, or Amazon Linux 2. | <code>yum install CylanceOPTICS-<version>.rpm</code> , where <i><version></i> is the version of the .rpm file. |
| Install the CylanceOPTICS agent on Ubuntu. | <code>dpkg -i cylance-optics-<version>_amd64.deb</code> , where <i><version></i> is the version of the .deb file. |
| Start the CylanceOPTICS service. | <code>systemctl start cyoptics.service</code> |
| Stop the CylanceOPTICS service. | <code>systemctl stop cyoptics.service</code> |
| Uninstall the CylanceOPTICS agent on RHEL/CentOS, SUSE, or Amazon Linux 2. | <code>rpm -e CylanceOPTICS</code> |
| Uninstall the CylanceOPTICS agent on Ubuntu. | <code>dpkg -P cylance-optics</code> |

Enable and configure CylanceOPTICS

When you enable CylanceOPTICS in a device policy and assign that policy to devices and zones, the CylanceOPTICS agent on each device collects events and stores data in the CylanceOPTICS database. The agent does not collect data until you enable CylanceOPTICS.

Before you begin: Verify that the CylancePROTECT Desktop application control feature is not enabled. Application control is designed for fixed function devices that do not change after setup (for example, point-of-sales machines). If application control is enabled, the CylanceOPTICS agent will not function as expected.

1. In the management console, on the menu bar, click **Policies > Device Policy**.
2. Create a new policy or click an existing policy.
3. On the **CylanceOPTICS Settings** tab, enable **CylanceOPTICS**.
4. If you want to enable the automatic upload of threat-related focus data from the CylanceOPTICS database to the console, enable **Auto-upload focus data for threats**. If you do not select this option, you must use the console to request focus data for devices.
5. If you want to enable the automatic upload of memory-related focus data from the CylanceOPTICS database to the console, enable **Auto-upload focus data for memory protection**.
If you do not select this option, you must use the console to request focus data for devices.
6. In the **Max storage size** field, specify the maximum amount of storage, in MB, that the CylanceOPTICS agent can access on the device. The default value is 1000 MB.

7. In the **Configurable sensors** section, select the [optional CylanceOPTICS sensors](#) that you want to enable. Note that the optional sensors are supported for 64-bit operating systems only.
8. If you want to associate a detection rule set with the device policy, in the **Detection rule set** drop-down list, click a rule set.
9. If you want to allow the CylanceOPTICS agent to provide OS notifications to the user on Windows or macOS devices, enable **Desktop notifications**.
10. Click **Save**.

After you finish:

- Assign the policy to devices or zones.
- If you want to prevent users from being able to stop the services for the CylanceOPTICS agent for Windows (CylanceOPTICS 3.1 or later with CylancePROTECT Desktop 3.0 or later) and macOS (CylanceOPTICS 3.3 or later with CylancePROTECT Desktop 3.1 or later), in the device policy, on the **Agent Settings** tab, enable **Prevent service shutdown from device**. When this setting is enabled, a macOS user can only stop the service if the Self Protection Level in the device properties is set to Local Admin (Assets > Devices > click the device). Windows users cannot stop the agent service as long as this setting is enabled.
- If you want users to have to provide a password to uninstall the CylancePROTECT Desktop agent, the CylanceOPTICS agent for Windows version 3.1 or later, and the CylanceOPTICS agent for macOS version 3.3 or later, in **Settings > Application**, turn on **Require Password to Uninstall Agent**. Using this feature for the CylanceOPTICS agent for macOS also requires CylancePROTECT Desktop version 3.1 or later.

CylanceOPTICS sensors

The following sensors are enabled by default in the CylanceOPTICS agent when you turn on CylanceOPTICS in a device policy. You cannot disable these sensors. For more information about the optional sensors that you can enable, see [CylanceOPTICS optional sensors](#).

For more information about the events, artifacts, and event types associated with both the default and optional sensors, see [Data structures that CylanceOPTICS uses to identify threats](#).

| Sensor | Platform | Description | Event types |
|---------|---------------------------|--|--|
| Device | macOS Linux | Collects relevant device information | Mount |
| File | Windows macOS Linux | Collects information about file operations | <ul style="list-style-type: none"> • Create • Delete • Overwrite • Rename • Write |
| Memory | macOS Linux | Collects information about memory operations | <ul style="list-style-type: none"> • Mmap • MProtect |
| Network | Windows macOS Linux | Collects information about network connections | Connect |

| Sensor | Platform | Description | Event types |
|----------|---------------------------|--|--|
| Process | Windows macOS Linux | Collects information about process operations | Supported event types differ by platform. See the Process section of Data structures that CylanceOPTICS uses to identify threats . <ul style="list-style-type: none"> Abnormal Exit Exit Forced Exit PTrace Start Suspend Unknown Linux Process Event |
| Registry | Windows | Collects information about registry operations | <ul style="list-style-type: none"> KeyCreated KeyDeleting ValueChanging ValueDeleting |

CylanceOPTICS optional sensors

You can enable any of the following CylanceOPTICS sensors to collect additional data beyond standard process, file, network, and registry events. Enabling optional sensors can impact performance and resource usage on devices, as well as the amount of data stored in the CylanceOPTICS database. BlackBerry recommends enabling optional sensors on a small number of devices initially to assess the impact.

The optional sensors are supported for Windows 64-bit operating systems only, unless otherwise noted.

| Sensor | Description | Best practices | Notes |
|-------------------------------|--|---|---|
| Advanced Scripting Visibility | <p>The CylanceOPTICS agent records commands, arguments, scripts, and content from JScript, PowerShell (console and integrated scripting environment), VBScript, and VBA macro script execution.</p> <p>Signal to noise ratio: High</p> <p>Potential data retention and performance impact: Low to moderate</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> Desktops Laptops Servers <p>Not recommended for Microsoft Exchange and email servers.</p> | <ul style="list-style-type: none"> Tools provided by Microsoft or other third-party solutions may rely heavily on PowerShell to conduct operations. To allow for increased data retention, BlackBerry recommends that you configure detection exceptions for trusted tools that make heavy use of PowerShell. |

| Sensor | Description | Best practices | Notes |
|-------------------------|--|---|---|
| Advanced WMI Visibility | <p>The CylanceOPTICS agent records additional WMI attributes and parameters.</p> <p>Signal to noise ratio: High</p> <p>Potential data retention and performance impact: Low</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> • Desktops • Laptops • Servers | <ul style="list-style-type: none"> • Some Windows background and maintenance processes use WMI to schedule tasks or execute commands, which can result in bursts of high WMI activity. • BlackBerry recommends analyzing your environment's WMI usage before you enable this sensor. |
| API Sensor | <p>The CylanceOPTICS agent monitors an identified set of Windows API calls.</p> <p>Signal to noise ratio: Moderate</p> <p>Potential data retention and performance impact: Enabling this sensor may impact a device's CPU performance</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> • Desktops • Laptops • Servers | <ul style="list-style-type: none"> • Supported on x86 or x64 Windows operating systems. • Requires the CylancePROTECT Desktop agent version 3.0.1003 or later. • Requires the CylanceOPTICS agent version 3.2 or later. |
| COM Object Visibility | <p>The CylanceOPTICS agent monitors COM interface and API calls to detect malicious behaviors such as scheduled task creation.</p> <p>Signal to noise ratio: High</p> <p>Potential data retention and performance impact: Enabling this sensor may impact CPU performance.</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> • Desktops • Laptops <p>Not recommended for servers.</p> | <ul style="list-style-type: none"> • Requires CylancePROTECT Desktop agent version 3.2 or later. • Requires the CylanceOPTICS agent version 3.3 or later. |
| Cryptojacking Detection | <p>The CylanceOPTICS agent processes Intel CPU activity using hardware registers for potential cryptomining and cryptohacking activity.</p> <p>Signal to noise ratio: Moderate</p> <p>Potential data retention and performance impact: Low</p> | <p>Supported for:</p> <ul style="list-style-type: none"> • Windows 10 x64 • Intel Gen 6 to 10 | <p>Note: BlackBerry recommends disabling this sensor, as we are currently investigating stability issues that this sensor can cause with the device OS.</p> <ul style="list-style-type: none"> • Not supported for virtual machines. • Not supported for Intel Gen 11 or later processors. BlackBerry does not recommend enabling this sensor for Gen 11 or later. |

| Sensor | Description | Best practices | Notes |
|--------------------------------------|--|---|---|
| DNS Visibility | <p>The CylanceOPTICS agent records DNS requests, responses, and associated data fields such as Domain Name, Resolved Addresses, and Record Type.</p> <p>Signal to noise ratio: Moderate</p> <p>Potential data retention and performance impact: Moderate</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> Desktops Laptops <p>Not recommended for DNS servers.</p> | <ul style="list-style-type: none"> Note that this sensor can gather a significant amount of data, but can also provide visibility into data that other tools have difficulty recording. To allow for increased data retention, BlackBerry recommends that you configure detection exceptions for trusted tools that make heavy use of cloud-based services. |
| Enhanced File Read Visibility | <p>The CylanceOPTICS agent monitors file reads within an identified set of directories.</p> <p>Signal to noise ratio: Moderate</p> <p>Potential data retention and performance impact: Low</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> Desktops Laptops Servers | <ul style="list-style-type: none"> Some third-party security tools may use the Windows APIs that this sensor collects data from. In some cases, CylanceOPTICS might record irrelevant or trusted data. To allow for increased data retention and a higher signal to noise ratio, BlackBerry recommends that you configure detection exceptions for trusted security tools. |
| Enhanced Portable Executable Parsing | <p>The CylanceOPTICS agent records data fields associated with portable executable files, such as file version, import functions, and packer types.</p> <p>Signal to noise ratio: Moderate</p> <p>Potential data retention and performance impact: Low</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> Desktops Laptops Servers | <ul style="list-style-type: none"> The data gathered by this sensor is passed into the Context Analysis Engine to aid with advanced executable file analysis and is not stored in the CylanceOPTICS database. Enabling this sensor will have little to no impact on CylanceOPTICS data retention. If you add and enable a detection rule that analyzes string resources, the CylanceOPTICS agent might consume significant CPU and memory resources. |

| Sensor | Description | Best practices | Notes |
|---|---|--|--|
| Enhanced Process and Hooking Visibility | <p>The CylanceOPTICS agent records process information from the Win32 API and Kernel Audit messages to detect forms of process hooking and injection.</p> <p>Signal to noise ratio: Moderate</p> <p>Potential data retention and performance impact: Low</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> • Desktops • Laptops • Servers | <ul style="list-style-type: none"> • Some third-party security tools may use the Windows APIs that this sensor collects data from. In some cases, CylanceOPTICS might record irrelevant or trusted data. • To allow for increased data retention and a higher signal to noise ratio, BlackBerry recommends that you configure detection exceptions for trusted security tools. |
| HTTP Visibility | <p>The CylanceOPTICS agent tracks Windows HTTP transactions, including Event Tracing for Windows, WinINet APIs, and WinHTTP APIs.</p> <p>Signal to noise ratio: High</p> <p>Potential data retention and performance impact: Enabling this sensor may impact CPU performance.</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> • Desktops • Laptops <p>Not recommended for servers.</p> | <ul style="list-style-type: none"> • Requires CylancePROTECT Desktop agent version 3.2 or later. • Requires the CylanceOPTICS agent version 3.3 or later. |
| Module Load Visibility | <p>The CylanceOPTICS agent monitors module loads.</p> <p>Signal to noise ratio: High</p> <p>Potential data retention and performance impact: Enabling this sensor may impact CPU performance.</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> • Desktops • Laptops • Servers | <ul style="list-style-type: none"> • Requires CylancePROTECT Desktop agent version 3.2 or later. • Requires the CylanceOPTICS agent version 3.3 or later. |
| Private Network Address Visibility | <p>The CylanceOPTICS agent records network connections within the RFC 1918 and RFC 4193 address spaces.</p> <p>Signal to noise ratio: Low</p> <p>Potential data retention and performance impact: Low</p> | <p>Recommended for desktops.</p> <p>Not recommended for:</p> <ul style="list-style-type: none"> • DNS servers • Low or under resourced systems • Systems that use RDP or other remote access software | <ul style="list-style-type: none"> • This sensor gathers a significant amount of data and can impact the length of time that data is stored in the CylanceOPTICS database. • BlackBerry recommends that you enable this sensor only in environments where full visibility into private network address communication is a requirement. |

| Sensor | Description | Best practices | Notes |
|-----------------------------------|---|---|---|
| Windows Advanced Audit Visibility | <p>The CylanceOPTICS agent monitors additional Windows event types and categories.</p> <p>Signal to noise ratio: Moderate</p> <p>Potential data retention and performance impact: Low</p> | — | <p>This sensor enables monitoring of the following event IDs:</p> <ul style="list-style-type: none"> • 4769 kerberos ticket request • 4662 operation on active directory object • 4624 successful logon • 4702 scheduled task creation |
| Windows Event Log Visibility | <p>The CylanceOPTICS agent records Windows security events and their associated attributes.</p> <p>Signal to noise ratio: Moderate</p> <p>Potential data retention and performance impact: Moderate</p> | <p>Recommended for:</p> <ul style="list-style-type: none"> • Desktops • Laptops • Servers <p>Not recommended for:</p> <ul style="list-style-type: none"> • Domain controllers • Microsoft Exchange and email servers | <ul style="list-style-type: none"> • The Windows event logs that this sensor collects data from will be generated frequently during normal system usage. • To reduce duplicate data and to allow for increased data retention, determine if your organization already has tools in place that collect data from Windows event logs. |

Data structures that CylanceOPTICS uses to identify threats

Events, artifacts, and facets are the three primary data structures that CylanceOPTICS uses to analyze, record, and investigate activities that occur on devices. CylanceOPTICS features rely on these data structures, including InstaQuery, focus data, and the Context Analysis Engine (CAE).

This section provides more information about how CylanceOPTICS interprets and interacts with activities on devices, to help you better understand and make use of detections, queries, and focus data.

Data sources by OS

The CylanceOPTICS agent uses the following data sources:

| OS | Data sources |
|---------|---|
| Windows | <ul style="list-style-type: none"> • CyOpticsDrv kernel driver • Event tracking • Security audit log |
| macOS | CyOpticsDrvOSX kernel driver |
| Linux | ZeroMQ |

For information about the types of network traffic that CylanceOPTICS excludes by default, see [KB65604](#).

Events

Events are the components that result in an observable change or action on a device. Events consist of two primary artifacts: the instigating artifact that initiates an action, and the target artifact that is acted on.

The following tables provide details about the types of events that CylanceOPTICS can detect and interact with.

Event: Any

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Process, User
- Platform: Windows, macOS, Linux

| Event type | Description |
|------------|--|
| Any | All events record the process that generated them and the user that is associated with the action. |

Event: Application

- Device policy option to enable: Advanced WMI Visibility
- Artifact type: WMI trace
- Platform: Windows

| Event type | Description |
|--------------------------------|--------------------------------------|
| Create Filter-Consumer Binding | A process used WMI persistence. |
| Create Temporary Consumer | A process subscribed to WMI events. |
| Execute Operation | A process performed a WMI operation. |

- Device policy option to enable: Enhanced Process and Hooking Visibility
- Artifact type: File
- Platform: Windows

| Event type | Description |
|---------------------|---|
| CBT | The SetWindowsHookEx API installed a hook to receive notifications that are useful to a CBT application. |
| DebugProc | The SetWindowsHookEx API installed a hook to debug other hook procedures. |
| Get Async Key State | A process called the Win32 GetAsyncKeyState API. |
| JournalPlayback | The SetWindowsHookEx API installed a hook to monitor messages previously recorded by a WH_JOURNALRECORD hook procedure. |
| JournalRecord | The SetWindowsHookEx API installed a hook to monitor input messages posted to the system message queue. |

| Event type | Description |
|----------------------------|---|
| Keyboard | The SetWindowsHookEx API installed a hook to monitor keystroke messages. |
| LowLevel Keyboard | The SetWindowsHookEx API installed a hook to monitor low-level keyboard input events. |
| LowLevel Mouse | The SetWindowsHookEx API installed a hook to monitor low-level mouse input events. |
| Message | The SetWindowsHookEx API installed a hook to monitor messages posted to a message queue. |
| Mouse | The SetWindowsHookEx API installed a hook to monitor mouse messages. |
| Register Raw Input Devices | A process called the Win32 RegisterRawInputDevices API. |
| Set Windows Event Hook | A process called the Win32 SetWinEventHook API. |
| Set Windows Hook | The SetWindowsHookEx API installed an unlisted hook type value. |
| ShellProc | The SetWindowsHookEx API installed a hook to receive notifications that are useful to shell applications. |
| SysMsg | The SetWindowsHookEx API installed a hook to monitor messages that are generated as a result of an input event in a dialog box, message box, or scroll bar. |
| WindowProc | The SetWindowsHookEx API installed a hook to monitor Windows procedure messages. |

- Device policy option to enable: API Sensor
- Artifact type: API Call
- Platform: Windows

| Event type | Description |
|------------|---|
| Function | A noteworthy function call has been made. |

- Device policy option to enable: Module Load Visibility
- Artifact type: File
- Platform: Windows

| Event type | Description |
|------------|---------------------------------|
| Load | An application loaded a module. |

- Device policy option to enable: COM Object Visibility
- Platform: Windows

| Event type | Description |
|------------|---------------------------|
| Created | A COM object was created. |

Event: Device

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: File
- Platform: macOS, Linux

| Event type | Description |
|------------|--|
| Mount | The device is connected to a machine or folders are mounted to specific network locations. |

Event: File

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: File
- Platform: Windows, macOS, Linux

| Event type | Description |
|------------|-------------------------|
| Create | A file was created. |
| Delete | A file was deleted. |
| Overwrite | A file was overwritten. |
| Rename | A file was renamed. |
| Write | A file was modified. |

- Device policy option to enable: Enhanced File Read Visibility
- Artifact type: File
- Platform: Windows

| Event type | Description |
|------------|--------------------|
| Open | A file was opened. |

Event: Memory

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Process
- Platform: macOS, Linux

| Event type | Description |
|------------|--|
| Mmap | A region of memory was mapped for a specific purpose, typically allocated for a process. |

| Event type | Description |
|------------|---|
| MProtect | The metadata was changed for a region of memory, typically to change its status (for example, to make it executable). |

Event: Network

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Network
- Platform: Windows, macOS, Linux

| Event type | Description |
|------------|--|
| Connect | A network connection was opened. By default, local traffic is not collected. |

- Device policy option to enable: Private Network Address Visibility
- Artifact type: Network
- Platform: Windows

| Event type | Description |
|------------|---------------------------------------|
| Connect | Connect events include local traffic. |

- Device policy option to enable: DNS Visibility
- Artifact type: DNS request
- Platform: Windows, Linux

| Event type | Description |
|------------|---|
| Request | A process made a network DNS request that was not cached. |
| Response | A process received a DNS response. |

- Device policy option to enable: HTTP Visibility
- Artifact type: HTTP
- Platform: Windows

| Event type | Description |
|------------|--|
| Get | Windows used WinINet or WinHTTP to make an HTTP request. |
| Post | Windows used WinINet or WinHTTP to send data. |

Event: Process

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Process

| Event type | Platform | Description |
|-----------------------------|---------------------------|---|
| Abnormal Exit | macOS Linux | Monitored by the preselect sensor, a process exited without completing (for example, an exception caused a process to exit). |
| Exit | Windows macOS Linux | A process exited. |
| Forced Exit | macOS Linux | Monitored by the preselect sensor, a process was forced to exit by another process. |
| PTrace | macOS Linux | This is a Unix system tool that allows one process to monitor and control another process. |
| Start | Windows macOS Linux | A process started. |
| Suspend | Linux | Monitored by the preselect sensor, a process was suspended. |
| Unknown Linux Process Event | macOS Linux | Monitored by the preselect sensor, an unknown event occurred with the process as a target. This can be a sign of malicious software masking its activity. |

- Device policy option to enable: Enhanced Process and Hooking Visibility
- Artifact type: Process
- Platform: Windows

| Event type | Description |
|------------------|---|
| SetThreadContext | A process called the SetThreadContext API. |
| Terminate | An instigating process terminated another target process. |

Event: Registry

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Registry, File (if the registry key references a specific file)
- Platform: Windows

| Event type | Description |
|---------------|--|
| KeyCreated | A registry key was created. |
| KeyDeleting | A registry key was deleted. |
| ValueChanging | The value of a registry key was changed. |

| Event type | Description |
|---------------|-----------------------------------|
| ValueDeleting | A registry key value was deleted. |

Event: Scripting

- Device policy option to enable: Advanced Scripting Visibility
- Artifact type: Powershell Trace
- Platform: Windows

| Event type | Description |
|---------------------|--|
| Execute Command | Windows PowerShell executed a command. The parameters are unknown. |
| Execute Script | Windows PowerShell executed a script. |
| Execute ScriptBlock | Windows PowerShell executed a script block. |
| Invoke Command | Windows PowerShell invoked a command with bound parameters. |
| Prevent Script | An AMSI ScanBuffer result indicated that a script was detected or blocked by an administrator. |

Event: User

- Device policy option to enable: Advanced Scripting Visibility
- Artifact type: Windows Event
- Platform: Windows

| Event type | Description |
|--------------------------|--|
| Batch Logoff | The following Windows event ID occurred: 4634 (type 4). |
| Batch Logon | The following Windows event ID occurred: 4624 (type 4). |
| CachedInteractive Logoff | The following Windows event ID occurred: 4634 (type 11). |
| CachedInteractive Logon | The following Windows event ID occurred: 4624 (type 11). |
| Interactive Logoff | The following Windows event ID occurred: 4634 (type 2). |
| Interactive Logon | The following Windows event ID occurred: 4624 (type 2). |
| Network Logoff | The following Windows event ID occurred: 4634 (type 3). |
| Network Logon | The following Windows event ID occurred: 4624 (type 3). |
| NetworkClearText Logoff | The following Windows event ID occurred: 4634 (type 8). |

| Event type | Description |
|--------------------------|--|
| NetworkClearText Logon | The following Windows event ID occurred: 4624 (type 8). |
| NewCredentials Logoff | The following Windows event ID occurred: 4634 (type 9). |
| NewCredentials Logon | The following Windows event ID occurred: 4624 (type 9). |
| RemoteInteractive Logoff | The following Windows event ID occurred: 4634 (type 10). |
| RemoteInteractive Logon | The following Windows event ID occurred: 4624 (type 10). |
| Service Logoff | The following Windows event ID occurred: 4634 (type 5). |
| Service Logon | The following Windows event ID occurred: 4624 (type 5). |
| Unlock Logoff | The following Windows event ID occurred: 4634 (type 7). |
| Unlock Logon | The following Windows event ID occurred: 4624 (type 7). |
| User Logoff | The following Windows event ID occurred: 4634 (unlisted type value). |
| User Logon | The following Windows event ID occurred: 4624 (unlisted type value). |

Artifacts and facets

Artifacts are complex pieces of information that CylanceOPTICS can use. The Context Analysis Engine (CAE) can identify artifacts on devices and use them to trigger automatic incident response and remediation actions. InstaQueries use artifacts as the foundation of a query.

Facets are the attributes of an artifact that can be used to identify the traits of an artifact that is associated with an event. Facets are correlated and combined during analysis to identify potentially malicious activity. For example, a file named "explorer.exe" may not be inherently suspicious, but if the file is not signed by Microsoft, and resides in a temporary directory, it may be identified as suspicious in some environments.

CylanceOPTICS uses the following artifacts and facets:

| Artifact | Facets |
|----------|---|
| API Call | <ul style="list-style-type: none"> • Function • DLL • Parameters |

| Artifact | Facets |
|------------------|---|
| DNS | <ul style="list-style-type: none"> • Connection • IsRecursionDesired • IsUnsolicitedResponse • Opcode • RequestId • Resolution • ResponseOriginatedFromThisDevice • Questions |
| Event | <ul style="list-style-type: none"> • Occurrence time • Registration time |
| File | <ul style="list-style-type: none"> • Executable file record (binaries only) • File creation time (reported by OS) • File path • File signature (binaries only) • File size • Last modified time (reported by OS) • md5 hash (binaries only) • Recent write location • sha256 hash (binaries only) • Suspected file type • User |
| Network | <ul style="list-style-type: none"> • Local address • Local port • Protocol • Remote address • Remote port |
| PowerShell trace | <ul style="list-style-type: none"> • EventId • Payload • PayloadAnalysis • ScriptBlockText • ScriptBlockTextAnalysis |
| Process | <ul style="list-style-type: none"> • Command line • File the executable was run from • Parent process • Process ID • Start time • User |
| Registry | <ul style="list-style-type: none"> • If the value references a file on the system • Registry path • Value |

| Artifact | Facets |
|---------------|--|
| Users | <ul style="list-style-type: none"> • Domain • OS-specific identifier (for example, SID) • Username <p>User artifacts can contain any of the following values; however, the data is not available on most devices:</p> <ul style="list-style-type: none"> • AccountType • BadPasswordCount • Comment • CountryCode • FullName • HasPasswordExpired • HomeDirectory • IsAccountDisabled • IsLocalAccount • IsLockedOut • IsPasswordRequired • LanguageCodePage • LogonServer • PasswordAge • PasswordDoesNotExpire • ProfilePath • ScriptPath • UserPrivilege • Workstations |
| Windows event | <ul style="list-style-type: none"> • Class • Event ID • ObjectServer • PrivilegeList • Process ID • Process Name • Provider Name • Service • SubjectDomainName • SubjectLogonId • SubjectUserName • SubjectUserSid |
| WMI trace | <ul style="list-style-type: none"> • ConsumerText • ConsumerTextAnalysis • EventId • Namespace • Operation • OperationAnalysis • OriginatingMachineName |

Registry keys and values

CylanceOPTICS monitors common persistence, process startup, and privilege escalation keys and values as well as the values shown in [KB 66266](#).

To learn more about how CylanceOPTICS monitors persistence points in the registry, see [KB 66357](#).

Managing updates for the CylancePROTECT Desktop and CylanceOPTICS agents

You can use update rules to manage updates of the CylancePROTECT Desktop and CylanceOPTICS agents on devices. Update rules allow you to configure Cylance Endpoint Security to automatically push updates to a specific version or the latest available version, or you can turn off automatic updates so that you can manage the software distribution using your organization's preferred method. Zones are associated with update rules, so that devices and users that are part of those zones receive updates accordingly (also known as zone-based updating). By default, the Test, Pilot, and Production update rules are available but you can also add additional update rules to manage agent updates based on your organization's needs.

The agent version on the device is always updated to the version that is specified in the update rule. You can use update rules to install an earlier version of an agent, even if the device is already using a newer version.

If the Linux driver on a device was previously updated manually on a device, the driver is not automatically updated as part of the agent update. This is to prevent the automated system from overwriting an action taken by an administrator.

Note: Automatic updates are not currently supported for the CylanceOPTICS agent for Linux.

When you are testing agent updates, consider the following:

- BlackBerry recommends that you test agent update rules using update rules and zones that were created for testing purposes (for example, using the Test and Pilot update rules) before using other update rules that you added for production deployment. When testing updates, consider using devices that are reserved for testing and evaluation purposes.
- Create zones for testing agent updates and add devices that are reserved for testing to them. Associate the zones that you created with the Test and Pilot update rules. For more information about creating zones, see [Setting up zones to manage CylancePROTECT Desktop and CylanceOPTICS](#).
- Make sure that all test devices are in a zone that you are testing. The Production update rule applies to all devices that are not in a zone with another update rule associated.
- If memory protection, script control, and/or device control are enabled in the device policy, a reboot of the device following the agent installation or upgrade is recommended, but not strictly required. A reboot will ensure that any new policy settings have taken full effect.

How update rules work with zones

- Devices are associated with zones either by zone rules or by manual assignment.
- Devices can be associated with multiple zones.
- Zones are assigned to update rules. Devices that are assigned to those zones will follow the update rules.
- Update rules are not specific to an operating system (OS) platform, but you can create zones to manage the updates of devices with specific OS platforms. If the agent version that is specified in the update rule is not available for a platform, the device receives the update as soon as it becomes available for the platform.
- Update rules are ranked. If a device is associated with multiple zones that are assigned different update rules, the highest-ranked update rule that specifies an update to the agent (auto-update or a specific version) takes effect. If a device is in at least one zone with an update rule that specifies an update, the agent on the device will be updated accordingly. The Production update rule has the lowest rank and applies to devices that aren't in any zone with an update rule, and devices in zones where none of the rules have specified an update to the agent.

Examples of update rules

The following examples illustrate update rules that are assigned zones that were created specifically for zone-based updates.

| Update rule example | Assigned zones |
|-----------------------------|---|
| Windows Server - Test | <ul style="list-style-type: none">Windows Server - US Test update zoneWindows Server - Europe Test update zone |
| Windows Server - Pilot | <ul style="list-style-type: none">Windows Server - US Pilot update zoneWindows Server - Europe Pilot update zone |
| Windows Server - Production | <ul style="list-style-type: none">Windows Server - US Production update zoneWindows Server - Europe Production update zone |

Manage updates for the CylancePROTECT Desktop and CylanceOPTICS agents

Before you begin: You need to create zones with devices reserved for testing agent updates. You will associate these zones with the Test and Pilot update rules. You can add your own update rules for testing or for production deployment. For more information about creating zones, see [Setting up zones to manage CylancePROTECT Desktop and CylanceOPTICS](#).

1. In the management console, on the menu bar, click **Settings > Update**.
2. If necessary, create an update rule. For example, you can create a rule for testing agent updates.
 - a) Click **Add New Rule**.
 - b) Type a name for the rule.
 - c) Click **Submit**.
3. Click an update rule. For example, click **Test**.
4. Expand **Zones** and select the zones that you want to assign to this update rule.
5. Expand **Agent** and select an update option.

Note: If you do not want to update the agent version on a device, use the **Do not update** setting. You must also make sure that the device is not in another zone with another update rule (including the Production rule) that specifies an update to the agent (auto-update or a specific version). If a device is in a zone with an update rule that specifies an update, it will be updated. If a device is associated with multiple update rules that specifies an update, the agent will be updated according to the rule with the highest rank.

6. Select the **Auto-Update Linux Driver** check box to allow the agent to automatically update to the latest driver to support the latest Linux kernel. The Auto-update Linux Driver feature requires CylancePROTECT Desktop agent version 3.1.1000 or later and the agent driver version 3.1.1000 or later.
7. Expand **CylanceOPTICS** and select an update option.
 - You can select Auto-Update only if you configured the CylancePROTECT Desktop agent to use Auto-Update.
 - Automatic updates are not currently supported for the CylanceOPTICS agent for Linux.
8. Repeat steps 2 to 7 for the **Pilot** update rule, or a rule that you created for pilot testing.
9. Repeat steps 2 to 7 for the **Production** update rule, or a rule that you created for production. You don't assign zones to the default **Production** update rule because it applies to all devices that are not in a zone with an update rule.

If the CylancePROTECT Desktop agent is set to Auto-Update in the Production update rule, the Test and Pilot rules are not available. Update rules that you create are not affected by the configuration of the Production update rule.

10. Click **Save**.

After you finish:

- If you added update rules, click the arrows next to the rules to set the ranking. Rules at the top of the list take priority over rules lower on the list. The Test, Pilot, and Production rules are always at the bottom of the list and you cannot change their ranking. The Production update rule is applied to devices that aren't in any zone with an update rule, and devices in zones where none of the rules have a specified an update to the agent.
- To trigger an update of the CylancePROTECT Desktop agent on a device before the hourly interval, on the device, right-click the CylancePROTECT Desktop icon in the system tray and click **Check for Updates**, restart the Cylance service, or run the following command from the Cylance directory:

```
CylanceUI.exe-update
```

- If memory protection, script control, and/or device control are enabled in the device policy, a reboot of the device following the agent installation or upgrade is recommended, but not strictly required. A reboot will ensure that any new policy settings have taken full effect.

Best practices for deploying CylancePROTECT Desktop on Windows virtual machines

You can use CylancePROTECT Desktop to protect both physical and virtual machines. This section details the best practices for deploying the CylancePROTECT Desktop agent on Windows based virtual desktop infrastructure (VDI) workstations.

CylancePROTECT Desktop works well as a guest OS component because it is not IOPS or memory intensive on a per-guest basis. The preparation and deployment of the CylancePROTECT Desktop agent in a virtual environment is similar to deployment on a physical computer. The deployment steps and best practices in this section will ensure that the agent performs efficiently in a virtual environment with fewer allocated resources and will help you to produce a gold image with no [unsafe](#) or [abnormal](#) files. After the gold image is thoroughly vetted, you can clone production VDI images from it.

Requirements and considerations for using CylancePROTECT Desktop on virtual machines

| Item | Requirements or considerations |
|--|---|
| Supported enterprise virtualization technologies | <ul style="list-style-type: none">• Microsoft Hyper-V• Windows 11 Enterprise multi-session• Windows 10 Enterprise multi-session• Citrix XenDesktop• Citrix VDI (validated with CylancePROTECT Desktop 3.2.x and CylanceOPTICS 3.3.x)• VMware Horizon/View• VMware Workstation• VMware Fusion |

| Item | Requirements or considerations |
|---|--|
| Non-persistent virtual machines | <p>A non-persistent VM is deleted when the session ends and is replaced with the same gold image. When a new VM is created, the CylancePROTECT Desktop agent registers the VM with the management console, resulting in duplicate devices registered for what should be the same endpoint (older registrations are treated as offline duplicate device records that never come back online).</p> <p>Use one of the following installation parameters when you install the CylancePROTECT Desktop agent on the gold image to prevent the duplicate registration of the same VM device:</p> <ul style="list-style-type: none"> • VDI=<X>: The value of <X> is a counter that determines when the agent starts identifying the virtual machine using VDI fingerprinting instead of the default agent fingerprinting mechanism. Duplicate devices are not registered when the agent uses VDI fingerprinting. <p>For example, you install the agent on a gold image using the parameter VDI=2. You use the gold image to create a parent image. You then use the parent image to create a workstation image. The agent will start to use VDI fingerprinting for the workstation image because the counter of 2 has been met by the gold image and the parent image.</p> <ul style="list-style-type: none"> • AD=1: This parameter works the same as VDI=<X>, except there is no counter to define when the agent starts to use VDI fingerprinting. The agent will use VDI fingerprinting on the gold image and for any images that you create from the gold image. This parameter is not supported for the .exe format of the unified CylancePROTECT Desktop and CylanceOPTICS installer. |
| Memory protection and script control features | <p>Consider the following before you enable memory protection and script control features in a VDI environment:</p> <ul style="list-style-type: none"> • Both features use process injection to identify and block unwanted or unauthorized code. Plug-ins, tools, or DLLs in virtualized environments may cause adverse effects, so you should test memory protection and script control options before you deploy them to production workstations. • It is a best practice to test memory protection options in alert only mode and make more stringent device policy changes from there. If the system becomes unstable, you can turn off memory protection. • If system conflicts or instabilities occur, as a failsafe option, you can enable compatibility mode for memory protection. • See KB 83016 to review known incompatibilities for memory protection and script control for CylancePROTECT Desktop 1580 and later. |
| Option to disable the agent UI | <p>You have the option to disable the CylancePROTECT Desktop agent UI to conserve overall system resources. For more information, see Windows installation parameters.</p> |
| Known issues | <p>To review the issues reported when running the CylancePROTECT Desktop agent in a virtual environment, see VDI Trending Issues.</p> |

Deploy CylancePROTECT Desktop on virtual machines

Before you begin: Review the [Requirements and considerations for using CylancePROTECT Desktop on virtual machines](#).

1. [Create a device policy](#) that you will use to prepare the VDI gold image. Configure the following options in the policy:

| Device policy category | Options |
|------------------------|--|
| File Actions | Turn on Auto Quarantine with Execution Control for unsafe and abnormal file types |
| Protection Settings | <ul style="list-style-type: none">• Turn on Background Threat Detection (Run Once)• Turn on Watch for New Files |

2. Prepare the VDI gold image.
 - a) [Install the CylancePROTECT Desktop agent](#) on the gold image. For example, use the following installation command and parameters:

```
msiexec /i CylancePROTECTSetup_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> VDI=1  
LAUNCHAPP=1
```

- b) Apply the device policy that you created in step 1 to the gold image.
Allow the background threat detection scan to complete. This can take several hours, depending on the size of the disk and the activity on the image as it is being scanned.
 - c) [Review the results of the background threat detection scan](#) and, if necessary, add binaries detected on the gold image to the [CylancePROTECT Desktop quarantine or safe lists](#).
3. On the gold image, clear the Fingerprint Values from the registry.
 - a) Stop the CylanceSvc service. Visit support.blackberry.com and read [KB 107236](#).
 - b) Using the Local Administrator account, take ownership of the registry key and add full control permissions to the following registry: HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop
 - c) Back up or export the registry shown above.
 - d) Remove the following registry keys: FP, FPMask, and FPVersion.
 4. Create the gold image.
 5. [Create a device policy](#) that is intended for production VDI workstations. BlackBerry recommends the following options in the policy, in addition to the options that you want to enable for your production workstations:

| Device policy category | Options |
|------------------------|---|
| File Actions | <ul style="list-style-type: none">• Turn on Auto Quarantine with Execution Control for unsafe and abnormal file types• Turn on Auto Upload |
| Protection Settings | <ul style="list-style-type: none">• Turn on Watch for New Files• Turn off Background Threat Detection |

6. Deploy and clone the gold image to production workstations. Each cloned image must have a unique UUID or ID that is different than the gold image.
7. Apply the device policy from step 5 to the production workstations.

After you finish: For the cloned devices, configure [zone-based agent updates](#) to **Do Not Update** or to a specific version of the agent. Updates should be managed on the gold image. See [Update CylancePROTECT Desktop on cloned devices](#).

Update CylancePROTECT Desktop on cloned devices

Before you begin: [Deploy CylancePROTECT Desktop on virtual machines](#).

1. On the gold image, [update the CylancePROTECT Desktop agent](#).
2. If any additional updates or files are applied to the gold image, apply the VDI preparation device policy to the gold image and allow the background threat detection scan to complete.
3. [Review the results of the background threat detection scan](#) and, if necessary, add binaries detected on the gold image to the [CylancePROTECT Desktop quarantine or safe lists](#).
4. Apply the production device policy to the gold image.
5. Reseal the gold image.
6. Verify that the agent update is propagated to the cloned devices.

Using RMM solutions to install the Cylance agents on devices

Cylance Endpoint Security supports using the Datto and Kaseya VSA 10 Remote Monitoring and Management (RMM) solutions to install or remove the CylancePROTECT Desktop and CylanceOPTICS agents.

Your organization must use the Multi-Tenant Console to support installing or removing agents with Kaseya VSA 10.

Use Datto RMM to install or remove the Cylance agents

Follow the steps below to use the Datto RMM solution to install the CylancePROTECT Desktop or CylanceOPTICS agent on devices, or to remove the agent from devices. Using Datto RMM to install or remove agents on Linux devices is not currently supported. After you install an agent using Datto, you can [configure automatic updates in the management console](#).

Before you begin:

- Verify that devices meet the requirements to install the [CylancePROTECT Desktop agent](#) or the [CylanceOPTICS agent](#).
 - Note that you must install the CylancePROTECT Desktop agent on devices before you install the CylanceOPTICS agent.
 - If you want to use Datto to install the agents, record the installation token from the Cylance console.
 - If you want to use Datto to remove an agent from devices, and you configured the agents to require an uninstall password, you must have the uninstall password.
1. In Datto, navigate to the site that you want to use.
 2. In the site settings, navigate to the Variables section and add the following site variables. For more information about site variables, see the [Datto RMM documentation](#):

| Name | Value |
|---|--|
| install_token | Copy and paste the CylancePROTECT Desktop installation token from the Cylance console. |
| protect_uninstall_key optics_uninstall_key | If you configured the CylancePROTECT Desktop and CylanceOPTICS agents to require an uninstall password, specify the password for both site variables. Both agents use the same uninstall password. For more information, see the Require users to provide a password to remove the CylancePROTECT Desktop and CylanceOPTICS agents . |

3. Save the changes that you made to the site.
4. Navigate to the ComStore, search for the following components, and add them to the Datto Component Library:
 - **CylancePROTECT Deploy [Win]**
 - **CylancePROTECT Deploy [Mac]**
 - **CylanceOPTICS Deploy [Win]**
 - **CylanceOPTICS Deploy [Mac]**
5. Create a job to deploy the appropriate component configuration to devices.
 - a) Set the action to **Install** or **Uninstall**.

- b) Set the target to specific devices, sites, or site groups.
- c) Set the Execution to **Run as system account**.

Use Kaseya VSA 10 to install or remove the Cylance agents

You can follow the steps below to use Kaseya VSA 10 to install the CylancePROTECT Desktop or CylanceOPTICS agent on Windows or macOS devices, or to remove the agent from devices. Note that this method requires use of the Multi-Tenant Console. Kaseya VSA 10 does not support deployments to Linux devices.

Before you begin:

- Verify that devices meet the requirements to install the [CylancePROTECT Desktop agent](#) or the [CylanceOPTICS agent](#).
 - Note that you must install the CylancePROTECT Desktop agent on devices before you install the CylanceOPTICS agent.
 - Log in to [BlackBerry myAccount](#) and navigate to the software downloads section (Product Resources > Software Downloads > Cylance Tools) to download a package of Kaseya scripts and workflows for the Cylance agents (Cylance_Kaseya_<version>.zip). Extract the contents of the .zip file.
 - In the Multi-Tenant Console:
 - [Enable custom application integration](#).
 - [Create a partner application to obtain an application ID and application secret](#).
 - Record the tenant ID and installation token for each target tenant.
1. In Kaseya VSA 10, create a Custom Field with the following variables. For all variables, disable expiration. For more information about creating a Custom Field, see [Kaseya VSA 10: Custom fields](#).

| Name | Context | Variable Type | Description |
|-------------------------|---|---------------|---|
| Cylance_Application_Id | Global (Read Only) | text | Specify the application ID. |
| Cylance_Application_Key | Global (Read Only) | text | Specify the application secret. |
| Cylance_Tenant_ID | Any of: <ul style="list-style-type: none"> • Global • Organization • Site • Agent Group | text | Specify the tenant ID from the Multi-Tenant Console. |
| Cylance_Region | Global (Read Only) | text | Specify the appropriate region: <ul style="list-style-type: none"> • United States = us (default) • Asia Pacific SE/Australia = au • European Union = eu • Asia Pacific NE/Japan = jp • South America/Sao Paulo = sp |

| Name | Context | Variable Type | Description |
|------------------------|---|---------------|---|
| Cylance_Install_Token | Any of: <ul style="list-style-type: none"> Global Organization Site Agent Group | text | Specify the installation token from the Multi-Tenant Console. |
| Cylance_Uninstall_Key | Any of: <ul style="list-style-type: none"> Global Organization Site Agent Group | text | If you configured the CylancePROTECT Desktop and CylanceOPTICS agents to require a user to enter a password to uninstall , specify the uninstall password from the Cylance console. |
| Cylance_Download_Token | Any of: <ul style="list-style-type: none"> Organization Site Agent Group | text | A workflow-only variable to pass a download token from one script to another. Leave the value blank. |
| Cylance_Product_Type | Any of: <ul style="list-style-type: none"> Organization Site Agent Group System | text | Specify one of the following values to select the agent that you want to install or remove: <ul style="list-style-type: none"> protect optics The default value is protect. |

2. Navigate to **Automation > Scripts**.
3. Create a folder named **Cylance**.
4. In the **Cylance** folder, create the following scripts with the specified inputs and outputs. The inputs map to the variables that you created in step 1. Copy and paste the body of each script from the **Cylance_Kaseya_<version>** package that you downloaded.

| Script name | Inputs | Outputs |
|----------------------------|--|--|
| Cylance_Is_Installed | c_product_type | c_is_installed Type: Number Default value: 0 |
| Cylance_Get_Download_Token | c_app_id c_app_key c_region c_tenant_id c_product_type | download_token Type: Text Default value: -1 |

| Script name | Inputs | Outputs |
|-----------------------|----------------------|----------------------------------|
| Cylance_Get_Installer | c_download_token | post_action_check |
| | c_install_token | Type: Number |
| | c_region | Default value: 0 |
| | c_product_type | |
| Cylance_Uninstall | c_product_type | post_action_check |
| | c_uninstall_passcode | Type: Number Default value: 0 |

5. In **Automation > Workflows**, use **Actions > Import Workflow** to import the following workflows (.wfl) from the scripts folder of the **Cylance_Kaseya_<version>** package. You must import the workflows in the following order:
 - a. Cylance_Windows_Install.wfl
 - b. Cylance_MacOS_Install.wfl
 - c. Cylance_Install_Workflow.wfl
 - d. Cylance_Uninstall_Workflow.wfl
6. Set the status of each imported workflow to **Active**.
7. Validate the following for each workflow using the workflow condition type. If the values do not resolve to those specified below, manually reset to the expected outcome.

| Workflow | Script or Custom Field variable | Expected value |
|--------------------------------|---|-----------------------|
| Cylance_Windows_Install.wfl | Script: Cylance_Is_Installed | c_is_installed = 0 |
| | Script: Cylance_Get_Download_Token | download_token ≠ -1 |
| Cylance_MacOS_Install.wfl | Script: Cylance_Is_Installed | c_is_installed = 0 |
| | Script: Cylance_Get_Download_Token | download_token ≠ -1 |
| Cylance_Install_Workflow.wfl | Custom Field variable: Cylance_Download_Token | ≠ -1 |
| | Script: Cylance_Get_Installer | post_action_check = 0 |
| Cylance_Uninstall_Workflow.wfl | Script: Cylance_Is_Installed | c_is_installed = 0 |

After you finish: Assign the Custom Field values to an endpoint (Organization, Site, or Agent Group), setting the value of Cylance_Product_Type to “protect” or “optics”, and run the appropriate workflow to install or remove the CylancePROTECT Desktop or CylanceOPTICS agent. It is a best practice to test the installation or removal on a small number of devices first.

Installing the BlackBerry Connectivity Node

The BlackBerry Connectivity Node allows you to create a secure connection between Cylance Endpoint Security and an on-premises Microsoft Active Directory or LDAP directory. Cylance Endpoint Security can synchronize devices, users, and groups from Active Directory. Users created through directory synchronization can be enabled for the CylancePROTECT Mobile app, CylanceGATEWAY, and CylanceAVERT.

You can install one or more instances of the BlackBerry Connectivity Node to provide redundancy. Each instance must be installed on a dedicated computer. If you have more than one BlackBerry Connectivity Node, you must upgrade them all to the same software release. After you upgrade the first instance, directory services are disabled until all instances are upgraded to the same version.

You can configure one or more directory connections, but if you have multiple instances of the BlackBerry Connectivity Node, all of the directory connections must be configured identically in every instance. If one directory connection is missing or incorrectly configured, that BlackBerry Connectivity Node will appear as disabled in the management console.

You don't need to install the BlackBerry Connectivity Node to synchronize with Microsoft Entra ID Active Directory. For more information, see "[Configure Cylance Endpoint Security to synchronize with Entra Active Directory](#)."

To install the BlackBerry Connectivity Node, perform the following actions.

| Step | Action |
|------|--|
| 1 | Review the requirements . |
| 2 | Set an environment variable for the Java location. |
| 3 | Download the installation and activation files for the BlackBerry Connectivity Node. |
| 4 | Install and configure the BlackBerry Connectivity Node. |
| 5 | If your environment has multiple instances of the BlackBerry Connectivity Node, Copy directory connection configurations . |
| 6 | Configure proxy settings for a BlackBerry Connectivity Node instance (Optional). |

Set an environment variable for the Java location

You must install a JRE 17 implementation on the servers where you will install the BlackBerry Connectivity Node, and the environment variable must point to the Java home location.

When you begin the installation, the BlackBerry Connectivity Node verifies that it can find Java. If it can't find Java, the setup application will stop on the requirements panel and you must set an environment variable for the Java location and ensure that the Java bin folder is included in the Path system variable. Note that you must close down the installer at this time and restart it only after the environment variable has been created or updated.

Before you begin: Verify that you have installed JRE 17 on the server where you will be installing the BlackBerry Connectivity Node.

1. Open the **Windows Advanced system settings** dialog box.
2. Click **Environment Variables**.
3. Under the **System variables** list, click **New**.
4. In the **Variable name** field, type `BB_JAVA_HOME`.
5. In the **Variable value** field, type the path to the JRE folder and click **OK**.
6. In the **System variables** list, select **Path** and click **Edit**.
7. If the Path doesn't include the Java bin folder, click **New** and add `%BB_JAVA_HOME%\bin` to the Path.
8. Move the `%BB_JAVA_HOME%\bin` entry high enough in the list that it won't be superseded by another entry and click **OK**.

After you finish: [Download the installation and activation files for the BlackBerry Connectivity Node.](#)

Download the installation and activation files for the BlackBerry Connectivity Node

Before you begin: [Set an environment variable for the Java location.](#)

1. In the management console, on the menu bar, click **Settings > Directory Connections**.
2. Click the **Connectivity Node** tab.
3. Click **Add Connectivity Node**.
4. On the software download page, click **Download**.
5. Select **BlackBerry Connectivity Node for UES**.
6. Click **Download**.
7. Extract the BlackBerry Connectivity Node installation files to the computer.

If you install more than one instance of the BlackBerry Connectivity Node, do not copy used installation files between computers. You must re-extract the installation files on each computer.

8. In the management console, click **Download Activation File**.
9. Save the activation file (.txt).

The activation file is valid for 60 minutes. If you wait longer than 60 minutes before you use the activation file, you must download a new activation file. Only the latest activation file is valid.

After you finish: [Install and configure the BlackBerry Connectivity Node.](#)


Install and configure the BlackBerry Connectivity Node

Before you begin: [Download the installation and activation files for the BlackBerry Connectivity Node.](#)

1. Open the BlackBerry Connectivity Node installation file (.exe) that you downloaded from the management console.
If a Windows message appears and requests permission to make changes to the computer, click **Yes**.
2. Choose your language. Click **OK**.
3. Click **Next**.
4. Select your country or region. Read and accept the license agreement. Click **Next**.
5. The installation program verifies that your computer meets the installation requirements. Click **Next**.

6. To change the installation file path, click ... and navigate to the file path that you want to use. If you receive a message asking you to create the installation and logs folder locations, click **Yes**. Click **Next**.
7. In the **Service account** dialog box, type the password for the service account. Click **Install**.
8. When the installation completes, click **Next**.
The address of the BlackBerry Connectivity Node console is displayed (<http://localhost:8088>). Click the link and save the site in your browser.
9. Select your language. Click **Next**.
10. When you activate the BlackBerry Connectivity Node, it sends data over port 443 (HTTPS) to the BlackBerry Infrastructure (for example na.bbsecure.com or eu.bbsecure.com). After it is activated, the BlackBerry Connectivity Node uses port 3101 (TCP) for all other outbound connections through the BlackBerry Infrastructure. Do any of the following:
 - If you want to use a proxy setting other than the default port 443 to connect to the BlackBerry Infrastructure (<region>.bbsecure.com) to activate the BlackBerry Connectivity Node, click the "here" link to configure the proxy settings and enter the information for the enrollment proxy. This link is only available on the "Name your BlackBerry Connectivity Node" screen. If you do not configure the proxy settings from this screen and click **Next**, you can configure the proxy settings from the top right corner of the screen by clicking **Settings > Proxy** before it is activated.
Note: The proxy must be able to access port 443 to the BlackBerry Infrastructure. You cannot change the enrollment proxy setting after you activate the BlackBerry Connectivity Node.
 - Configure other proxy settings. For more information about the available proxy options, see [Configure proxy settings for a BlackBerry Connectivity Node instance](#).
11. In the **Friendly name** field, type a name for the BlackBerry Connectivity Node. Click **Next**.
12. Click **Browse**. Select the activation file that you downloaded from the management console.
13. Click **Activate**.
If you want to add a BlackBerry Connectivity Node instance to an existing server group when you activate it, your organization's firewall must allow connections from that server over port 443 through the BlackBerry Infrastructure (for example na.bbsecure.com or eu.bbsecure.com) to activate the BlackBerry Connectivity Node and to the same bbsecure.com region as the main BlackBerry Connectivity Node instance.
14. Click **+** and select the type of company directory that you want to configure.
15. Link your directory to the BlackBerry Connectivity Node by following the appropriate task:
 - [Connect to Microsoft Active Directory](#)
 - [Connect to an LDAP directory](#)

After you finish:

- To install a second BlackBerry Connectivity Node instance for redundancy, download another set of installation and activation files and repeat this task on a different computer. This should be done after the first instance has been activated.
- You can configure one or more directory connections, but if you have multiple BlackBerry Connectivity Nodes, all of the directory connections must be configured identically. If one directory connection is missing or incorrectly configured, that BlackBerry Connectivity Node will appear as disabled in the management console. You can make this task easier by [copying directory connection configurations](#) from one BlackBerry Connectivity Node to another.
- To change the directory settings that you configured, in the BlackBerry Connectivity Node console (<http://localhost:8088>), click **General settings > Company directory**. Click  for the directory connection.
- [Configure BlackBerry Connectivity Node logging](#).
- You can remove directory connections from a BlackBerry Connectivity Node as long as you have no users or groups associated with it. If you remove a connection from a BlackBerry Connectivity Node, you can re-add the connection using the same name as the deleted connection.

Copy directory connection configurations

If your environment has multiple instances of the BlackBerry Connectivity Node, the directory connections must be configured identically on all nodes. To help make this task easier, you can export the directory connection configuration from one BlackBerry Connectivity Node and import it to another.

Note: Before you can import company directory configurations to a BlackBerry Connectivity Node, you must remove any existing company directory connections from that node.

Before you begin: [Copy directory connection configurations](#).

1. In the BlackBerry Connectivity Node that you want to copy the configuration from, in the **Company directory connection** screen, click **Export the directory connections in .txt file**.
A .txt file containing information about the company directory connections is downloaded to your computer. Note that the exported (.txt file) will not include any passwords, and they will need to be re-entered before importing it into any other BlackBerry Connectivity Node.
2. On the BlackBerry Connectivity Node that you want to copy the configuration to, on the **Company directory connection** screen, browse to the .txt file you downloaded.
3. Click **Import connections**.

The company directory connections are added to the BlackBerry Connectivity Node.

Configure proxy settings for a BlackBerry Connectivity Node instance

You can configure the components of the BlackBerry Connectivity Node to send data through a TCP proxy server (transparent or SOCKS v5) before it reaches the BlackBerry Infrastructure.

1. On the computer that hosts the BlackBerry Connectivity Node, open the BlackBerry Connectivity Node console from the Start menu or open a browser and navigate to <http://localhost:8088>.
2. Click **General settings > Proxy**.
3. Perform any of the following tasks:

| Task | Steps |
|---|--|
| Send data through a SOCKS v5 proxy server (no authentication) to the BlackBerry Infrastructure. | <ol style="list-style-type: none">a. Select the Proxy server option.b. Select the Enable SOCKS v5 check box.c. Click +.d. Type the IP address or host name of the SOCKS v5 proxy server. Click Add.e. Repeat steps 3 and 4 for each SOCKS v5 proxy server that you want to configure.f. In the Port field, type the port number.g. Click Save. |
| Send data through a transparent proxy server to the BlackBerry Infrastructure. | <ul style="list-style-type: none">• In the BlackBerry Connectivity Node fields, type the FQDN or IP address and port number of the proxy server. |

4. Click **Save**.

Linking to your company directory

You can configure Cylance Endpoint Security to synchronize with your company directory to simplify adding and managing users and groups. Connecting Cylance Endpoint Security to a company directory allows you to create user accounts by searching for and importing user data from the company directory. Users created through directory synchronization can be enabled for the CylancePROTECT Mobile app, CylanceGATEWAY, and CylanceAVERT.

You can link to a company directory in two ways:

- If you want to synchronize with Microsoft Entra ID, you can configure Cylance Endpoint Security to connect with it.
- If you want to synchronize with an on-premises Microsoft Active Directory or LDAP directory, you must first [install the BlackBerry Connectivity Node](#) to create a secure connection between Cylance Endpoint Security and your directory.

To link Cylance Endpoint Security to your company directory, perform the following actions:

| Step | Action |
|------|---|
| 1 | If you want to link to an on-premises company directory, install a BlackBerry Connectivity Node . |
| 2 | Depending on the type of directory you want to connect to, configure Cylance Endpoint Security to synchronize with Entra , or connect to a Microsoft Active Directory or LDAP directory . |
| 3 | Add a directory group. |
| 4 | Configure onboarding and offboarding. |
| 5 | Configure directory synchronization schedules. |

Configure Cylance Endpoint Security to synchronize with Entra Active Directory


To configure Cylance Endpoint Security to synchronize with Entra Active Directory, you must configure both Entra and Cylance Endpoint Security to make the connection.

1. Log in to the [Azure portal](#).
2. Create a new app registration for Entra Active Directory and assign the appropriate settings and permissions.
 - a) Add a name for the app.
 - b) Specify the account types can use the application or access the API.
 - c) Select **Web** as the redirect URI type and set the URI as `http://localhost`.
 - d) Set the following application permissions:
 - Group.Read.All (Application)

- User.Read (Delegated)
 - User.Read.All (Application)
- e) Grant Admin consent to the application.
3. Record the name you assigned to the app and the Application (client) ID.
 4. Create a new client secret and record the information in the Value column of the secret.

Important: The Value is available only when you create it. You cannot access it after you leave the page. If you do not record the value, you must create a new one. This is used as the Client secret in the management console.
 5. In the management console, on the menu bar, click **Settings > Directory Connections**.
 6. Click **Add New Connection**.
 7. Type a **Name** for the directory connection and the **Domain** for your Entra Active Directory.
 8. In the **Client ID** field, type the application ID generated by the Entra app registration.
 9. In the **Client secret** field, type the client secret value that was generated by the Entra app registration in step 4.
 10. Click **Add**.

Update the Microsoft Entra ID Active Directory connection credentials

You must update the client credentials in the management console when your client secret has expired or has been changed in the [Azure portal](#). If your client secret has expired or has been changed, the Directory connections screen displays an  beside the directory connection that is affected. You can choose to update only the client secret, or you can update both the client ID and the client secret.

Before you begin:

- Verify that you have recorded the name that you assigned to the app in [Configure Cylance Endpoint Security to synchronize with Entra Active Directory](#).
 - Verify that you have a valid client secret and recorded the information in the Value column of the secret. Optionally, you can create both a new client ID and client secret.
1. In the management console, on the menu bar, click **Settings > Directory Connections**.
 2. Click the Microsoft Entra ID Active Directory connection that you want to update.
 3. Click the **Connections Settings** tab.
 4. Click **Update client credentials**. Choose to update only the client secret, or update both the client ID and the client secret. Complete one of the following:
 - Update client secret only: Enter the client secret value that you recorded in the [Azure portal](#).
 - Update client ID and client secret: Enter the new client ID and client secret value that you recorded in the [Azure portal](#).
 5. Click **Submit**.
 6. Click **Save**. If the save fails, both the client ID and the client secret will revert to the previous values.

Connect to Microsoft Active Directory

Before you begin: Install at least one instance of the [BlackBerry Connectivity Node](#).

1. In the BlackBerry Connectivity Node console (<http://localhost:8088>), click **General settings > Company directory**.
2. Click **+**.
3. Select **Microsoft Active Directory**.

4. In the **Connection name** field, type a name for this company directory connection.
5. In the **Username** field, type the username of the Microsoft Active Directory account.
6. In the **Domain** field, type the FQDN of the domain that hosts Microsoft Active Directory. For example, domain.example.com.
7. In the **Password** field, type the password of the Microsoft Active Directory account.
8. In the **Domain controller discovery** drop-down list, click one of the following:
 - If you want to use automatic discovery, click **Automatic**.
 - If you want to specify the domain controller computer, click **Select from list below**. Click **+** and type the FQDN of the computer. Repeat this step to add more computers.
9. In the **Global catalog search base** field, type the search base that you want to access (for example, OU=Users,DC=example,DC=com). To search the entire Global Catalog, leave the field blank.
10. In the **Global catalog discovery** drop-down list, click one of the following:
 - If you want to use automatic catalog discovery, click **Automatic**.
 - If you want to specify the catalog computer, click **Select from list below**. Click **+** and type the FQDN of the computer. If necessary, repeat this step to specify more computers.
11. If you want to enable support for linked Microsoft Exchange mailboxes, in the **Support for linked Microsoft Exchange mailboxes** drop-down list, click **Yes**. To configure the Microsoft Active Directory account for each forest that you want to access, in the **List of account forests** section, click **+**. Specify the forest name, user domain name (the user can belong to any domain in the account forest), username, and password.
12. To synchronize more user details from your company directory, select the **Synchronize additional user details** check box. The additional details include company name and office phone.
13. Click **Save**.

After you finish:

- If you want to configure automatic onboarding for Cylance Endpoint Security, see [Configure onboarding and offboarding](#).
- If you want to add a directory synchronization schedule, see [Configure directory synchronization schedules](#).
- If you have more than one instance of the BlackBerry Connectivity Node, you can [copy directory connection configurations](#) from one instance into the others.

Connect to an LDAP directory

Before you begin: To connect to an on-premises LDAP directory, you must first install at least one instance of the [BlackBerry Connectivity Node](#).

1. In the BlackBerry Connectivity Node console (http://localhost:8088), click **General settings > Company directory**.
2. Click **+**.
3. Select **LDAP**.
4. In the **Connection name** field, type a name for this company directory connection.
5. In the **LDAP server discovery** drop-down list, click one of the following: If you want to use automatic discovery, click **Automatic**.
 - If you want to use automatic discovery, click **Automatic** then in the **DNS domain name** field, type the DNS domain name.
 - If you want to specify the LDAP computer, click **Select server from list below**. Click **+** and type the FQDN of the computer. Repeat this step to add more computers.

6. In the **Enable SSL** drop-down list, select whether you want to enable SSL authentication for LDAP traffic. If you click **Yes**, click **Browse** and select the SSL certificate for the LDAP computer.
7. In the **LDAP port** field, type the port number of the LDAP computer.
8. In the **Authorization required** drop-down list, select whether authentication is required with the LDAP computer. If you click **Yes**, type the username and password of the LDAP account. The username must be in DN format (for example, CN=Megan Ball,OU=Sales,DC=example,DC=com).
9. In the **Search base** field, type the search base that you want to access (for example, OU=Users,DC=example,DC=com).
10. In the **LDAP user search filter** field, type the filter that you want to use for LDAP users. For example: (&(objectCategory=person)(objectclass=user)). If you want to restrict searching to all members of a single group for the entire Cylance Endpoint Security tenant, you can use the following example: (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)).
11. In the **LDAP user search scope** drop-down list, click one of the following: If you want user searches to apply to all levels below the base DN, click **All levels**. If you want to limit user searches to one level below the base DN, click **One level**.
12. In the **Unique identifier** field, type the attribute for each user's unique identifier (for example, uid). The attribute must be immutable and globally unique for every user.
13. In the **First name** field, type the attribute for each user's first name (for example, givenName).
14. In the **Last name** field, type the attribute for each user's last name (for example, sn).
15. In the **Login attribute** field, type the attribute for each user's login attribute (for example, cn).
16. In the **Email address** field, type the attribute for each user's email (for example, mail).
17. In the **Display name** field, type the attribute for each user's display name (for example, displayName).
18. To synchronize more user details from your company directory, select the **Synchronize additional user details** check box. The additional details include company name and office phone.
19. To enable directory-linked groups, select the **Enable directory-linked groups** check box.
Specify the following information:
 - In the **Group search base** field, type the value to use as the base DN for group information searches.
 - In the **LDAP group search filter** field, type the LDAP search filter that is required to find group objects in your company directory.
 - In the **Group Unique Identifier** field, type the attribute for each group's unique identifier. This attribute must be immutable and globally unique.
 - In the **Group Display name** field, type the attribute for each group's display name.
 - In the **Group Membership attribute** field, type the name of the attribute for group membership. The attribute values must be in DN format.
 - In the **Test Group Name** field, type an existing group name for validating the group attributes specified.
20. Click **Save**.

After you finish:

- If you want to configure automatic onboarding for Cylance Endpoint Security, see [Configure onboarding and offboarding](#).
- If you want to add a directory synchronization schedule, see [Configure directory synchronization schedules](#).
- If you have more than one instance of the BlackBerry Connectivity Node, you can [copy directory connection configurations](#) from one instance into the others.

Configure onboarding and offboarding

Onboarding allows you to automatically add user accounts to Cylance Endpoint Security based on user membership in a company directory group. Directory groups and user accounts are added to CylanceGATEWAY during the synchronization process.

If you enable onboarding, you can also choose to configure offboarding. When a user is disabled in the directory or removed from all company directory groups in the onboarding directory groups, Cylance Endpoint Security deletes the user account and stops allowing network connections from the user's devices.

You can use offboarding protection to delay the deletion of user accounts to avoid unexpected deletions because of directory replication latency. Offboarding protection delays offboarding actions for two hours after the next synchronization cycle.

Before you begin: Depending on the type of directory that you want to connect to, [configure Cylance Endpoint Security to synchronize with Azure Active Directory](#), or connect to a [Microsoft Active Directory](#) or [LDAP directory](#).

1. In the management console, on the menu bar, click **Settings > Directory Connections**.
2. In the **Directory Connection** list, click the connection that you want to configure onboarding for.
3. On the **Sync settings** tab, select **Directory onboarding**.
4. In the **Sync** field, type the maximum number of changes you want to allow for each synchronization process.
By default, there is no limit. If the number of changes to be synchronized exceeds the limit you set, the synchronization process stops. Changes include users added to groups, users removed from groups, users to be onboarded, and users to be offboarded.
5. In the **Nesting level** field, type the number of nested levels to synchronize for company directory groups. By default, there is no limit.
6. To force the synchronization of directory groups, select **Force synchronization**.
If this option is selected, when a group is removed from your company directory, the links to that group are removed from onboarding directory groups and directory-linked groups. If not selected, if a company directory group is not found, the synchronization process is canceled.
7. To delete a user account from Cylance Endpoint Security when a user is removed from all linked groups in the directory, select **Delete user when the user is removed from all onboarding directory groups**. The first time that a synchronization cycle occurs after a user account is removed from all linked directory groups, the user account is deleted from Cylance Endpoint Security.
8. To prevent user accounts or device data from being deleted from Cylance Endpoint Security unexpectedly, select **Offboarding protection**.
Offboarding protection means that users will not be deleted from Cylance Endpoint Security until two hours after the next synchronization cycle.
9. Click **Save**.

Configure directory synchronization schedules

You can add a schedule to automatically synchronize Cylance Endpoint Security with your organization's company directory.


Before you begin: [Connect to Microsoft Active Directory](#) or [Connect to an LDAP directory](#).

1. In the management console, on the menu bar, click **Settings > Directory Connections**.
2. In the **Directory Connection** list, click the connection that you want to set a sync schedule for.
3. On the **Sync schedule** tab, click **Add Schedule**.
4. In the **Sync type** drop-down list, select one of the following options:

- **All users and groups:** This is the default setting. If you choose this option and onboarding is enabled, users are onboarded and offboarded and linked to the appropriate directory linked groups during the synchronization. Users who are not onboarded or offboarded but change directory groups, and users with changes to their attributes are synchronized.
 - **Onboarding groups:** If you choose this option and onboarding is enabled, users are onboarded and offboarded and linked to the appropriate directory linked groups during the synchronization, and users with changes to their attributes are synchronized. Users who are not onboarded or offboarded but change directory groups are not synchronized.
 - **Directory linked groups:** If you choose this option, users are not onboarded and offboarded during the synchronization. Users with changes to their directory groups are linked appropriately. Users with changes to their attributes are synchronized.
 - **User attributes:** If you choose this option, users are not onboarded and offboarded during the synchronization. Users with changes to their directory groups are not synchronized. Users with changes to their attributes are synchronized.
5. In the **Recurrence** drop-down list, select one of the following options:
 - **Interval:** This is the default setting. If you choose this option, you can specify the number of minutes between synchronizations and the hours and days during which synchronization can occur.
 - **Once a day:** If you choose this option, you can specify the days of the week and the time of day when synchronization occurs.
 - **No recurrence:** If you choose this option, you can specify a day and time within the next week for one synchronization.
 6. Specify appropriate day and time details for the schedule.
 7. Click **Submit**.
 8. Click **Save**.

Synchronize with your company directory

You can synchronize Cylance Endpoint Security with your directory connections at any time.

1. In the management console, on the menu bar, click **Settings > Directory Connections**.
2. In the **Directory Connection** list, click  for the connection that you want to synchronize.

Adding users and devices

You must add user accounts in the management console so that you can enable the following Cylance Endpoint Security services for those users:

- Services available in the CylancePROTECT Mobile app: CylancePROTECT Mobile and CylanceGATEWAY Mobile
- CylanceGATEWAY Desktop

You can use any of the following methods to add users:

- [Link to your company directory](#) and enable onboarding to add users automatically when Cylance Endpoint Security synchronizes with the directory. You can configure the directory synchronization schedules to synchronize Cylance Endpoint Security with your organization's company directory. By default, all users and groups are synchronized at 30-minute intervals daily.
- [Link to your company directory](#) and add directory users individually. You can use this option if you do not want to enable onboarding.
- Add individual users as BlackBerry Online Account users.

You do not need to add user accounts to enable other Cylance Endpoint Security services such as [CylancePROTECT Desktop](#) and [CylanceOPTICS](#). After the agents are installed on devices, you can view and manage those devices and associated data in the management console.

Add CylancePROTECT Mobile app and CylanceGATEWAY users

Before you begin: If you want to add users from your company directory, follow the instructions in [Linking to your company directory](#). If you enable onboarding, directory groups and user accounts are added to the management console during the synchronization process. Follow the steps below if you want to add directory users individually without onboarding, or if you want to add individual users as BlackBerry Online Account users.

1. In the management console, on the menu bar, click **Assets > Users**.
2. Click **Add Users**.
3. Do any of the following:

| Task | Steps |
|---------------------------------------|--|
| Add a directory user. | <ol style="list-style-type: none">a. Type the name of the user and click the matching result from the drop-down list.b. Optionally, if you have already added user groups, add the user to one or more groups. |
| Add a BlackBerry Online Account user. | <ol style="list-style-type: none">a. Click in the search field and click Add a new user manually. If you have not configured a directory connection, skip to the next step.b. Specify the user's name and email address.c. Optionally, if you have already added user groups, add the user to one or more groups.d. Direct the user to the BlackBerry Online Account password reset to enter their email and set a password. The user will use this password to activate the CylancePROTECT Mobile app. Users can also access the password reset link from the CylancePROTECT Mobile app when they activate the app. |

4. Click **Save**. If you want to add another user, click **Save and New** and repeat the previous step.

After you finish:

- To add users to a group, in **Assets > User Groups**, select the group and add users to it from the **Users** tab. If you enabled onboarding, group membership is synchronized from the directory.
- To enable CylancePROTECT Mobile for users that you added, follow the instructions in [Setting up CylancePROTECT Mobile](#).
- To enable CylanceGATEWAY for users that you added, follow the instructions in [Setting up CylanceGATEWAY](#).
- [Assign policies to administrators, users, and groups](#).

Adding user groups

You can create groups for users who are enabled for the CylancePROTECT Mobile app and for CylanceGATEWAY users. A user group is a collection of related users who share common properties. Administering users as a group is more efficient than administering individual users because properties can be added, changed, or removed for all members of the group at the same time. When you assign policies to user groups, the policies apply to all members of the group.

You can assign policies to a group from the group settings page or from the [policy page](#). If a user belongs to two or more groups that are assigned different policies, the [highest ranked](#) of the assigned policies is applied to the user.

You can create two types of user groups:

- Directory groups link to groups in your company directory. The membership of the group synchronizes with the membership list in the directory. For more information, see [Configure onboarding and offboarding](#).
- Local groups are created and maintained in the management console. You can assign any local user or directory user to a local group.

Add a directory group

If you have linked to one or more company directories and [configured onboarding](#), directory groups can be automatically added to Cylance Endpoint Security. You can also add a directory group if it has not been added through onboarding.

1. In the management console, on the menu bar, click **Assets > User Groups**.
2. Click **Add Group > Directory group**.
3. Start typing the name of a group as it appears in the directory.
4. Select the group name when it appears in the search results.
5. If you want the group and any nested groups to be enabled for onboarding, select **Nested directory groups**.
6. To assign a policy to the group, click **+** and select the type of policy that you want to add.
7. Select the policy and click **Save**.

Add a local group

1. In the management console, on the menu bar, click **Assets > User Groups**.
2. Click **Add Group > Local group**.
3. Type a name and description for the group.
4. To assign a policy to the group, click **+** and select the type of policy you want to add.
5. Select the policy and click **Save**.
6. When you've finished assigning policies, click **Save**.
7. To add users to the group, on the **User Groups** page, click the group name, then click **Users**.

8. Click **Add user**.
9. Start typing a name to search for the user you want to add.
10. Select one or more names from the search results.
11. Click **Save**.

You can also add and remove individual users from groups on the [user page](#).

Assign policies to administrators, users, and groups

You can assign user policies to any number of groups, administrators, and users, but each administrator and user can have only one user policy of each type assigned to them. A policy assigned directly to a user or administrator takes precedence over policies assigned to groups that the user or administrator belongs to. If no policy is assigned directly to an administrator or user and the administrator or user belongs to two or more groups that are assigned different policies of the same type, the [highest ranked](#) of the assigned policies is applied to the administrator and user.


Each log in to the management console is evaluated against the policies that are assigned to administrators and users, in order, until a policy that is assigned matches. If no policy is assigned to the administrator or user directly, or through a group that they are a member of, the default policy is applied and they can only sign in to the Cylance console using their Cylance password. The enhanced authentication policies are applied to administrators and users in the following order:

- User policy app exceptions
- User policy
- Tenant app policy
- Default policy

Before you begin: Create one or more of the following policy types:

- [Enrollment policy](#)
- [CylancePROTECT Mobile policy](#)
- [CylanceGATEWAY service policy](#)
- [Authentication policy](#)

1. On the menu bar, click **Policies > User Policy**.
2. Select the tab for the policy type that you want to assign.
3. Click the name of the policy that you want to assign.
4. Click **Assigned Users and Groups**.
5. Click **Add user or group**.
6. Click the **User** tab.
7. Start typing a name to search for the user. By default, a maximum of 50 search results are returned. Refine your search when more than 50 search results are returned.

Administrator accounts are displayed with an  icon in the user list. In some scenarios, you might see two user accounts for one user, an administrator account and an Active Directory user account.

8. Select one or more names from the search results. Click **Add**.

You can also assign policies to a user on the [user configuration page](#).

9. Click the **User Group** tab.
10. Start typing a name to search for the group that you want to add. By default, a maximum of 50 search results are returned. Refine your search when more than 50 search results are returned.
11. Select one or more names from the search results. Click **Add**.


You can also assign policies to a group on the [group settings page](#).

12. To unassign the policy from a user or group, select the users and groups that you want to unassign the policy for and click **Remove**.

Rank policies

You can [assign policies](#) to individual users and to user groups. If you assign a policy to an individual user, it takes precedence over policies assigned to groups that the user belongs to. If no policy is assigned directly to a user and the user belongs to two or more groups that are assigned different policies, the highest ranked of the assigned policies is applied to the user.

Before you rank policies you should decide on a strategy based on your objectives and which groups you assign policies to. For example, you may want network access control policies that apply to specific departmental groups to be ranked highest and more restrictive policies to be ranked below them, or you may want your most restrictive policy to be ranked highest.

1. On the menu bar, click **Policies > User Policy**.
2. Select the tab for the policy type that you want to assign.
3. Click **Rank**.
4. To change the order of a policy in the list, drag  for the policy to a new position in the list.
5. Click **Save**.

Setting up CylancePROTECT Mobile

| Step | Action |
|------|--|
| 1 | Review the software requirements and network requirements for the CylancePROTECT Mobile app. |
| 2 | If you want to add CylancePROTECT Mobile users to Cylance Endpoint Security from your company directory, link to your company directory . |
| 3 | Add CylancePROTECT Mobile app users. Optionally, add groups to manage users . |
| 4 | Create a CylancePROTECT Mobile policy. |
| 5 | Create an enrollment policy. |
| 6 | Device users install and activate the CylancePROTECT Mobile app. For instructions, see the Cylance Endpoint Security User Guide . |
| 7 | Optionally, integrate Cylance Endpoint Security with Microsoft Intune to report device risk levels to Intune so that Intune can execute the desired mitigation actions on devices. |

Cylance Endpoint Security also supports using Microsoft Intune app protection policies to allow or restrict access to specific Microsoft apps based on the device threat level reported by CylancePROTECT Mobile. Enabling this functionality requires a different series of deployment steps. To configure this feature, see [Use Intune app protection policies with CylancePROTECT Mobile](#).

Create a CylancePROTECT Mobile policy

You create and assign a CylancePROTECT Mobile policy to users and groups to enable the service and control which features you want to use.

You can configure risk assessment settings in the policy to map the alerts that are detected by the CylancePROTECT Mobile app to risk levels (for example, you can specify that compromised devices should be treated as high risk). The risk levels of the alerts are used to determine a mobile device's overall risk level. You can view the device risk level in the management console (Assets > Mobile Devices and in the device details). Note that there is no default configuration of the risk assessment settings.

If you [integrate Cylance Endpoint Security with Microsoft Intune](#), Cylance Endpoint Security will periodically send the overall risk level of a mobile device to Intune. You can use Intune to configure mitigation actions for device risk levels.

Before you begin: [Add CylancePROTECT Mobile app and CylanceGATEWAY users](#).

1. In the management console, on the menu bar, click **Policies > User Policy**.
2. On the **Protect Mobile** tab, click **Add Policy**.

3. Type a name and description for the policy.
4. In the **Notifications** section, you can specify the count and interval of the notifications that the CylancePROTECT Mobile app provides to the user when it detects a threat. You specify the type of notification (device, email, or no notification) in the **Device Settings** section (step 6).
5. In the **Data privacy** section, if you want to obfuscate certain pieces of information when the CylancePROTECT Mobile app reports a threat so that the information cannot be stored and displayed in the management console in plain text, turn on **Data privacy**, then select the fields that you want to obfuscate.
6. In the **Device Settings** section, click **Android** or **iOS** and turn on the features that you want to use. For more information about the CylancePROTECT Mobile features, see [Key features of CylancePROTECT Mobile](#). Note that sideload detection is not supported for iOS 17.5 and later.
 - a) For each feature that you enable, select the appropriate check box to enable or disable device notifications and email notifications. If you turn off device and email notifications, the user must open the CylancePROTECT Mobile app to view alerts.
 - b) If you enable any of the following features, complete these additional steps:

| Feature | Platform | Additional steps |
|---|----------------|---|
| Malicious apps | Android | <ol style="list-style-type: none"> a. To exempt apps on the safe list from malware scanning, turn on Always allow apps in the safe app list. b. To automatically block apps on the unsafe list, turn on Always block apps in the restricted app list. c. If you want to scan system apps that are preinstalled in the system partition on the device, turn on Scan system apps. d. If you want to enable the upload of apps to the CylancePROTECT Mobile services over a Wi-Fi connection, turn on Upload app packages for safety check over a Wi-Fi connection. Specify, in MB, the maximum size of an app that can be uploaded over Wi-Fi, and the maximum size of all apps that can be uploaded in a month (30 days). If either maximum is exceeded, the upload does not occur and an error is added to the device log. e. If you want to enable the upload of apps to the CylancePROTECT Mobile services over a mobile network, turn on Upload app packages for safety check over a mobile network connection. Specify, in MB, the maximum size of an app that can be uploaded over a mobile network, and the maximum size of all apps that can be uploaded in a month (30 days). If either maximum is exceeded, the upload does not occur and an error is added to the device log. |
| Unsupported device model | Android iOS | Click Edit and select the device models that you want to restrict. |
| Unsupported OS | Android iOS | Add the available OS versions to the supported and unsupported lists based on your organization's security standards. |
| SafetyNet or Play Integrity attestation failure | Android | If you want to enable Compatibility Test Suite matching for the CylancePROTECT Mobile app, turn on Enable CTS profile matching . |

| Feature | Platform | Additional steps |
|------------------------------|----------------|--|
| Hardware attestation failure | Android | <ol style="list-style-type: none"> In the Minimum security level required drop-down list, click the appropriate level. For more information, see SecurityLevel on the Android Developers site. If you want to enforce a minimum security patch level on devices, turn on Security patch level. Add the appropriate device models and specify the security patch date. |
| Insecure Wi-Fi | Android | Add the available Wi-Fi access algorithms to the safe and unsafe lists based on your organization's security standards. |
| Unsafe message | Android iOS | <ol style="list-style-type: none"> In the Scanning option drop-down list, select one of the following: <ul style="list-style-type: none"> If you want to send messages to the CylancePROTECT Mobile services to determine if they are safe, click Cloud scanning. If you want to use only the local machine learning models of the CylancePROTECT Mobile app to identify unsafe URLs, click On-device scanning. If you want to disable URL scanning, click No scanning. For Android devices, in the Start scanning offset field, specify, in hours, the age of text messages that are eligible for scanning. If you specify 0, only new messages are eligible for scanning. |

- If you want to configure risk assessment settings for CylancePROTECT Mobile alerts, do the following:
 - In the **Risk Assessment** section, click **Add Detections**.
 - Drag and drop the detections to the risk level that you want to apply to them. For information about the detections, see [Key features of CylancePROTECT Mobile](#).

- Click **Save**.

After you finish:

- [Assign the policy to users and groups](#).
- If necessary, [rank policies](#).
- [Create and assign an enrollment policy to users](#). After users are assigned an enrollment policy, they receive an email with instructions to download and activate the CylancePROTECT Mobile app. For more information, see the [Cylance Endpoint Security User Guide](#).
 - Instruct users to enable JavaScript in their default mobile browser (the CylancePROTECT Mobile app supports Google Chrome, Samsung Internet, and Safari). This is required to activate the CylancePROTECT Mobile app.
 - Instruct Android users to allow background activity for the CylancePROTECT Mobile app after it is installed.

Integrating Cylance Endpoint Security with Microsoft Intune to respond to mobile threats

You can connect Cylance Endpoint Security to Microsoft Intune so that Cylance Endpoint Security can report the risk level of devices to Intune. The device risk level is calculated based on the detection of mobile threats by the

CylancePROTECT Mobile app on Intune managed devices. Intune can execute mitigation actions based on the device risk level.


When you connect Cylance Endpoint Security to Intune, you create app configuration policies that define the device types and Intune groups that the integration applies to. CylancePROTECT Mobile policies map events detected by the CylancePROTECT Mobile app to the risk level of your choosing (high, medium, or low). When the CylancePROTECT Mobile app on an Intune managed device detects a threat (for example, a malicious app or sideloaded app), the risk level that is mapped to that threat is factored into an overall risk level that Cylance Endpoint Security calculates for the device. Cylance Endpoint Security reports the device risk level to Intune, and Intune carries out the mitigation actions that have been configured for that risk level.

Note that all Intune managed devices that you want to use this feature must be included in an app configuration policy in the Cylance console. This feature requires the CylancePROTECT Mobile app version 2.0.1.1099 or later.

Cylance Endpoint Security also supports using Microsoft Intune app protection policies to allow or restrict access to specific Microsoft apps based on the device threat level reported by CylancePROTECT Mobile. To enable this functionality, see [Use Intune app protection policies with CylancePROTECT Mobile](#).

Connect Cylance Endpoint Security to Intune

Before you begin: The Cylance Endpoint Security administrator account that you use to connect to Intune must have an [Intune license](#).

1. In the management console, on the menu bar, click **Settings > Connectors**.
2. Click **Add Connection > Microsoft Intune**.
3. Specify your Entra tenant ID. Click **Next**.
4. Specify your administrator credentials for Entra.
Follow the prompts for administrator consent. If required, coordinate with your organization's Intune administrator to grant consent for the CylancePROTECT Mobile MTD connector in the Microsoft Intune admin center.
5. On the **App Configuration Policies** screen, turn on the OS platforms that you want the Intune integration to apply to and complete the following steps for each platform. Note that all Intune managed devices that you want to use this feature must be included in an app configuration policy. If you want to create app configuration policies later, click **Cancel**.
 - a) Optionally, change the name of the policy. Do not change the target app.
 - b) If you want the policy to apply to all groups from the Intune instance, turn on **All groups**.
 - c) If you want the policy to apply to specific groups from the Intune instance, click . Search for and select groups and click **Add**.
6. Click **Save**. If you added an app configuration policy for Android, follow any administrator consent prompts that display.

The app configuration policies that you create are visible in the Intune admin center.

After you finish:

- If you haven't done so yet, configure the risk assessment settings in the CylancePROTECT Mobile policy that is assigned to users to map threats detected by the CylancePROTECT Mobile app to the desired risk levels.
- In the Intune admin center, edit the CylancePROTECT Mobile MTD connector and turn on the compliance policy options to connect Android and iOS devices to CylancePROTECT.

Use Intune app protection policies with CylancePROTECT Mobile

You can use Microsoft Intune app protection policies with CylancePROTECT Mobile to allow or restrict access to specific Microsoft apps based on the device threat level reported by CylancePROTECT Mobile.

1. Review the [software requirements](#) and [network requirements](#) for the CylancePROTECT Mobile app.
2. [Link Cylance Endpoint Security to your company directory.](#)
3. [Add Intune users to Cylance Endpoint Security as CylancePROTECT Mobile users.](#)
4. [Create a CylancePROTECT Mobile policy and assign it to users.](#) Configure the risk assessment settings in the policy to map alerts to device risk levels.
5. [Create an enrollment policy and assign it to users.](#)

Users will receive an email with instructions to download and activate the CylancePROTECT Mobile app. Instruct users to ignore the email for now, they will download and activate the app in step 10. Instruct users to keep the email as they will need the QR code to activate the CylancePROTECT Mobile app.
6. [Connect Cylance Endpoint Security to Intune.](#)
7. In the Intune admin center:
 - a) Edit the CylancePROTECT Mobile MTD connector and turn on the app protection policy options to connect Android and iOS devices to CylancePROTECT.
 - b) Create and configure app protection policies for Android and iOS devices to specify how you want CylancePROTECT Mobile to allow or restrict access to specific apps based on the reported risk level.
 - c) Assign the app protection policies to user groups.
8. Deploy the Microsoft apps that you want to protect using the Intune app protection policy. After a protected Microsoft app is installed, users are prompted to install the Microsoft Authenticator app (iOS) or Intune Company portal app (Android) and register the device.
9. Instruct users to launch a protected Microsoft app and to follow the "Get Access" prompt to install and activate the CylancePROTECT Mobile app. Instruct users to use the QR code they received in step 5.

If Android users do not receive the prompt to install the CylancePROTECT Mobile app, instruct them to close and reopen the protected Microsoft app.

When a user opens a protected Microsoft app, they receive a notification if access to the app is restricted due to the device's current risk level.

Setting up CylanceGATEWAY

Note: If CylanceGATEWAY is not enabled for your tenant the menu options to configure it are not displayed in the management console. If a user with insufficient permissions logs in to the management console a no permissions error message is displayed when selecting a menu option. For more information about the error message, see [support.blackberry.com/ community](https://support.blackberry.com/community) to read article 98223.

DNS resolution of IPv6 addresses is not supported. IPv6 addresses will not be returned to the CylanceGATEWAY agent.

| Step | Action |
|------|--|
| 1 | Install and set up the BlackBerry Connectivity Node and at least one CylanceGATEWAY Connector . |
| 2 | Specify the addresses that are part of your private network. |
| 3 | Specify your private DNS settings and suffixes. |
| 4 | Review the existing CylanceGATEWAY network services or define your own to make creating access control list (ACL) rules on tenants easier (optional). |
| 5 | Configure ACL rules on tenants to manage which Internet and private network destinations CylanceGATEWAY allows and blocks access to. |
| 6 | Configuring network protection to specify the threats that CylanceGATEWAY detects and how it responds. |
| 7 | Add users for CylanceGATEWAY. |
| 8 | Configure Gateway service options to specify OS-specific options. |
| 9 | Configure enrollment policies to allow users to activate the CylancePROTECT Mobile app or CylanceGATEWAY agent on their devices. |
| 10 | Assign policies to administrators, users, and groups . Users must be assigned an enrollment policy and Gateway Service policy before they can activate the CylanceGATEWAY agent. |

| Step | Action |
|------|---|
| 11 | <p>Device users install and activate the CylancePROTECT Mobile app on iOS, Android, and Chromebook devices and the CylanceGATEWAY agent on Windows and macOS devices. Optionally, you can perform a silent installation or upgrade of the CylanceGATEWAY agent.</p> <p>You can download the agents from the BlackBerry web site. For more information on the CylancePROTECT Mobile app and CylanceGATEWAY agent, see the Cylance Endpoint Security User Guide.</p> <p>Optionally, you can integrate Cylance Endpoint Security with BlackBerry UEM or Microsoft Intune to verify whether iOS and Android devices are managed by UEM or Intune before they can use CylanceGATEWAY. For more information, see Connecting Cylance Endpoint Security to MDM solutions to verify whether devices are managed.</p> |
| 12 | <p>Bring your own IP addresses (BYOIP) to provide larger dedicated IP addresses to control traffic in ways, such as using your organization's own IP address for sourcing IP pinning and allowing a single IP address range or CIDR address instead of several non-continuous IP addresses. (Optional)</p> |

Defining your private network

To use CylanceGATEWAY to control access to your private networks, you need to define your private networks. When you define your private networks, you can configure CylanceGATEWAY to apply the most restrictive privilege and micro-segmentation when users access your network resources. CylanceGATEWAY supports access to more than one private network (for example, segments, data centers, and VPCs) both in on-premises and cloud environments. CylanceGATEWAY blocks users from connecting to any location in your private network unless the user is assigned an [access control list \(ACL\) rule](#) that allows the connection.

You define your private networks by adding a connector group for each private network that you want users to be able to access resources on. If your CylanceGATEWAY service was enabled before July 2023 and included one or more CylanceGATEWAY Connectors, all of your existing connectors have moved to the "Default Connector Group". You can rename the default connector group or add additional groups and assign the connectors as required.

Each tenant supports a maximum of eight connector groups.

Connector groups consist of the following:

- The IP addresses, IP address ranges, and CIDR notation that you specify for each group. CylanceGATEWAY Connectors recognize these addresses as a part of one of your private networks.
- The health check URL. This is unique to the group and is used by each CylanceGATEWAY Connector in the group to confirm connectivity to your private network.
- The IP restrictions that you may specify to have Gateway accept connections only from connectors at the specified IP addresses.

To establish a secure tunnel between users' devices and your private networks, you must install one or more CylanceGATEWAY Connectors and assign them to a group.

Each connector group supports a maximum of eight CylanceGATEWAY Connectors.

You can also specify the addresses of your private DNS servers and the private DNS suffixes used for searches. The DNS settings apply to all group connectors in your environment and must be added to one group.

In environments that contain multiple groups with similar destination IP addresses or address ranges, data flow is directed, in order, to the connector groups listed until the IP address is matched to a connector group. The

connector group that includes the matching IP address is then used to route the connection to the destination to access resources.

Setting up the CylanceGATEWAY Connector

The CylanceGATEWAY Connector is a virtual appliance that you must install if you want to use CylanceGATEWAY to establish a secure tunnel between users' devices and your private networks. The CylanceGATEWAY Connector must be deployed and enrolled in part of network that has full access to addresses that you define when you [Specify your private network](#). If you don't install a CylanceGATEWAY Connector, you can use CylanceGATEWAY only to block access to public Internet destinations and secure access to cloud applications using source IP pinning.

It is a best practice to install more than one CylanceGATEWAY Connector. Installing multiple instances provides load balancing to access separate segments or private clouds within your [Defining your private network](#). When your network has multiple instances of the CylanceGATEWAY Connector installed and configured, client connections are distributed evenly across all healthy CylanceGATEWAY Connectors that are assigned to the same connector group, providing redundancy in the event that one instance may become unavailable or when troubleshooting issues.

Each tenant supports a maximum of eight connector groups.

Each connector group supports a maximum of eight CylanceGATEWAY Connectors.

BlackBerry recommends that you specify a health check URL in each connector group to regularly monitor the status of each CylanceGATEWAY Connector. If you do not specify a health check URL, CylanceGATEWAY cannot confirm whether you have connectivity to your private network, and the Health check status column (Private Network > Gateway Connectors) for a connector will not display the DNS and HTTP information. For more information, see [Manage CylanceGATEWAY Connectors](#).

Contact your BlackBerry sales representative, if you plan to install CylanceGATEWAY in an environment that requires different packaging.

To set up a CylanceGATEWAY Connector, perform the following actions.

| Step | Action |
|------|--|
| 1 | Review the Requirements: CylanceGATEWAY Connector . |
| 2 | <p>Install the CylanceGATEWAY Connector to your environment. The CylanceGATEWAY Connector is supported in the following environments. To see a walkthrough of how to install the CylanceGATEWAY Connector in your environment, see the Install the CylanceGATEWAY Connector workflow for your environment.</p> <ul style="list-style-type: none">• vSphere environment• ESXi environment• Microsoft Entra ID environment• Hyper-V environment• AWS environment |
| 3 | Configure the CylanceGATEWAY Connector in the VM environment (optional). |
| 4 | Access the CylanceGATEWAY Connector using OpenSSH (optional). |

| Step | Action |
|------|---|
| 5 | Configure your firewall for the CylanceGATEWAY Connector. |
| 6 | Enroll the CylanceGATEWAY Connector with the BlackBerry Infrastructure. |
| 7 | Configure the CylanceGATEWAY Connector (optional). |
| 8 | Managing CylanceGATEWAY Connectors to set options and check connector status. |

Install the CylanceGATEWAY Connector to a vSphere environment

You can configure the CylanceGATEWAY Connector with a static IP. If you want to make changes to the CylanceGATEWAY Connector network configuration after it is installed, you can edit the VM's vApp options and restart the CylanceGATEWAY Connector for the changes to take affect. For instructions on how to edit the OVF details, see the [VMWare documentation to read 'Edit OVF Details for a Virtual Machine'](#).

Before you begin: Make sure you have permissions to deploy an OVF template into a vSphere environment.

1. Download the CylanceGATEWAY Connector OVA file (cylance-gateway-connector-*<version>*.ova) from [myAccount](#).
2. Log in to the vSphere environment.
3. Right-click on the cluster where you want to install the CylanceGATEWAY Connector and select **Deploy OVF template**.
4. On the **Select an OVF template** screen, click **Local file**.
5. Click **Upload Files** and navigate to the cylance-gateway-connector.ova file.
6. Click **Next**.
7. On the **Select a name and folder** screen, type a name for the virtual machine and click **Next**.
The default name is cylance-gateway-connector.
8. On the **Select a computer resource** screen, select a location for the virtual machine and click **Next**.
9. After the compatibility checks are complete, click **Next**.
10. On the **Review details** screen, review the setup information and click **Next**.
11. On the **Select storage** screen, for **Virtual disk format**, select **Thin Provision** and click **Next**.
12. On the **Select networks** screen, configure the **Destination Network** for this CylanceGATEWAY Connector.
Set the **Source Network** to NAT.
13. Click **Next**.
14. On the **Customize template** screen, specify additional virtual machine properties (optional).

Note: IP addresses must be entered as IPv4 addresses in dot-decimal notation.

- By default, the **Use DHCP** option is enabled and the connector uses automatically assigned IP addresses. If you want to configure the connector with a static IP address, you must clear the Use DHCP check box and provide the IP addresses for the following settings:

- In the **IP address / Prefix Length** field, enter the IP address and prefix that can be assigned to devices (for example, 192.0.2.100/24). If you add multiple IP addresses, separate each IP address and prefix with a comma (,).
- In the **Gateway** field, enter the IP address for the network gateway (for example, 192.0.2.1).
- In the **DNS** field, specify the IP address for the DNS servers that you want to use (for example, 192.0.2.120). If you add multiple DNS servers, separate the addresses with a comma (,).

15. On the **Ready to complete** screen, review the configuration settings and click **Finish**.

After you finish: After you install the connector, you can verify that the OVA file is installed correctly in the virtual environment. For instructions, see [Configure the CylanceGATEWAY Connector in the VM environment](#).

Install the CylanceGATEWAY Connector to an ESXi environment

You can configure the CylanceGATEWAY Connector's network interface to use DHCP or configure a static IP only when you install the CylanceGATEWAY Connector. If you want to make changes to the configuration, you must uninstall and then install the CylanceGATEWAY Connector with the new network interface configuration.

Before you begin: Make sure you have permissions to deploy an OVF template into an ESXi environment.

1. Download the CylanceGATEWAY Connector OVA file (cylance-gateway-connector-*<version>*.ova) from [myAccount](#).
2. Log in to the ESXi environment.
3. In the **Navigator** panel, select **Virtual Machines**.
4. Click the **Create/Register VM** button
5. On the **New Virtual Machine** screen, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
6. Type a name for the virtual machine
7. Navigate to the cylance-gateway-connector-*<version>*.ova file. Drag and drop the file in the dialog box.
8. Click **Next**.
9. On the **Select storage** screen, select **Standard** and a datastore, then click **Next**.
10. On the **Deployment options** screen, for **Disk provisioning**, select **Thin**.
11. On the **Additional settings** screen, expand Options to specify additional VMWare properties (optional).

Note: IP addresses must be entered as IPv4 addresses in dot-decimal notation.

- By default, the **Use DHCP** is enabled and the connector uses automatically assigned IP addresses. If you want to configure the connector with a static IP address, you must clear the Use DHCP check box and provide the IP addresses for the following settings:
- In the **IP address / Prefix Length** field, specify the IP address and prefix that can be assigned to devices (for example, 192.0.2.100/24). To use multiple IP addresses, separate the IP addresses with a comma (,).
- In the **Gateway** field, enter the address for the network gateway (for example, 192.0.2.1)
- In the **DNS** field, specify the IP address for the DNS servers that you want to use (for example, 192.0.2.120). To use multiple DNS servers, separate the addresses with a comma (,).

12. Click **Next**.

13. On the **Ready to complete** screen, review the configuration settings and click **Finish**.

After you finish: After you install the connector, you can verify that the OVA file is installed correctly in the virtual environment. For instructions, see [Configure the CylanceGATEWAY Connector in the VM environment](#).

Prerequisites to install CylanceGATEWAY Connector to a Microsoft Entra ID environment

- Make sure the DNS is enabled in your Entra private network and can be accessed by your connector VM.

- Optionally, make sure that your private network environment has a proxy server for outbound HTTP and HTTPs traffic.
- Make sure that the services you want to make available through CylanceGATEWAY can be accessed by the CylanceGATEWAY Connector on your private network.
- Make sure you can deploy a VHD template into a Entra environment.

Install the CylanceGATEWAY Connector to a Microsoft Entra ID environment

When you install the connector, you upload the VHD file as a blob in the Microsoft Entra ID portal. You use the blob to create an image that is used by the connector VM. For information on configuring your Entra environment, visit [Azure portal documentation - Azure portal | Microsoft Docs](#).

Before you begin: Review [Prerequisites to install CylanceGATEWAY Connector to a Microsoft Entra ID environment](#).

1. Download the CylanceGATEWAY Connector VHD file (cylance-gateway-connector-fixed-<version>.vhd) from [myAccount](#).
2. Log in to the Microsoft Entra ID management portal at <https://portal.azure.com>.
3. Upload the VHD file as a blob.
 - a) In the **Azure services** section, click **Storage accounts**. If you do not have a storage account, create one.
 - b) Click your storage account.
 - c) In the left column, in the **Data storage** section, click **Containers**. If you do not have a container, create one.
 - d) Click your container.
 - e) Click **Upload**.
 - f) In the **Upload blob** screen, navigate to the downloaded cylance-gateway-connector-fixed-<version>.vhd file.
 - g) Expand **Advanced** and set the **Blob type** drop-down list to **Page blob**.
 - h) Click **Upload**.
4. Create an image from the uploaded blob.
 - a) In the management portal, in the left column, click the portal menu > **All Services**.
 - b) In the **Filter services** field, type `images`.
 - c) Click **Images**, make sure the image uses the resource type **Microsoft.Compute/images**.
 - d) Click **Create**.
 - e) Complete the required fields for your environment. In the **OS disk** section, specify the following settings:
 - OS Type: Linux
 - VM Generation: Gen 1
 - Storage blob: Navigate to the blob that you created in step 3.
 - f) Click the **Tags** tab and add tags as required (optional).
 - g) Click **Review + create**.
 - h) Click **Create**.
 - i) Click **Go to resource**. The Create a virtual machine screen opens.
5. Create a connector VM.
 - a) On the **Basics** tab, complete the required fields for your environment. Specify the following settings:
 - Image: Select the image that you created in step 4.
 - Size: Select a size with that includes 2 vCPUs and a minimum of 4.5 GB memory.
 - Authentication type: Select **Password**.
 - Username: Enter any value. The connector VM image disregards this field.
 - Password and Confirm password: Enter any value. The connector VM image disregards these fields.
 - b) Click the **Disks** tab.

- c) On the **Disks** page, in the **OS disk type** drop-down list, select **Standard HDD**. The connector VM does not require low latency disk access.
- d) Click the **Networking** tab. Complete the required fields for your environment. Make sure that the connector image uses your private network. The connector does not support Entra's Accelerated Networking feature. If you enable this setting, the connector VM might not function as expected.
- e) Click the **Management** tab. The image doesn't support "Login with Azure AD". If you enable this setting, the connector VM might not function as expected.
- f) Click the **Advanced** tab. Configure as required for your environment. The connector doesn't support setting "Custom data" or "User data". The "Custom data" or "User data" settings can be configured as required by your environment, but they are disregarded by the connector VM. BlackBerry does not recommend installing additional VM applications on the VM that is running the connector VM.
- g) Click the **Tags** tab. Configure tags as required for your environment.
- h) Click the **Review + create** tab. Review your configuration.
- i) Click **Create**.

Note: A timeout error message might display when the VM resource is created. If necessary, refresh the screen.

Install the CylanceGATEWAY Connector to a Hyper-V environment

Before you begin: Make sure you have permissions to deploy the VHD file and create a connector image.

1. Download the CylanceGATEWAY Connector VHD file (cylance-gateway-connector-dynamic<version>.vhd) from [myAccount](#).
2. Run the Hyper-V Manager as an administrator.
3. In the Hyper-V Manager menu, click **Action > New > Virtual Machine**. Click **Next**.
4. On the **Specify Name and Location** screen, specify a name for the VM. Click **Next**.
5. On the **Specify Generation** screen, select **Generation 1**. Click **Next**.
6. On the **Assign Memory** screen, click **Next**.
7. On the **Configure Networking** screen, select the appropriate connection. Click **Next**.
8. On the **Connect Virtual Hard Disk** screen, select **Use an existing virtual hard disk**.
9. Navigate to the cylance-gateway-connector-dynamics-<version>.vhd file that you downloaded in step 1.
10. On the **Assign memory** screen, make sure that the connector has a minimum of 5 GB of memory. Click **Next**.
11. On the **Completing the New Virtual Machine Wizard** screen, review the configuration settings and click **Finish**.
12. Start the connector.

After you finish: After you install the connector, you can verify that the VHD file is installed correctly in the virtual environment. For instructions, see [Configure the CylanceGATEWAY Connector in the VM environment](#).

Install the CylanceGATEWAY Connector to an AWS environment

You install the CylanceGATEWAY Connector using the AMI in the AWS Marketplace.

1. Sign in to the AWS management console at <https://aws.amazon.com/console>.
2. To create the CylanceGATEWAY Connector instance. Perform the following actions:
 - a. Open the **EC2** service.
 - b. In the left column, under **Instances**, click **Instances**.
 - c. Click **Launch instances**.
 - d. On the **Launch an instance** screen, type a name for the CylanceGATEWAY Connector instance.
 - e. In the **Amazon Machine Image (AMI)** section, click **Browse more AMIs**.

- f. On the **Choose an Amazon Machine Image (AMI)** screen, click the **AWS Marketplace AMIs** tab.
- g. In the **Selected AMI** search field, type `CylanceGATEWAY`. Press **Enter**.
- h. Select an instance type according to your organization's requirements.
Note: BlackBerry recommends that you select an instance type of c6in or c5n for production environments.
- i. Select a key pair to securely connect to your connector instance through OpenSSH.
- j. In the **Network settings** section, click **Edit** and specify the following settings:
 1. Click the **VPC** drop-down and select your private network.
 2. Optionally, click the **Auto-assign public IP** and select **Enable**. You must assign a public IP address to the CylanceGATEWAY Connector only if you do not have a way to access the connector's web interface using the private network that it is installed on.
 3. Select or create a security group according to your organization's requirements. The security group must have port 22 (SSH), port 80 (HTTP), and port 443 (HTTPS) access to the CylanceGATEWAY Connector from the network that the enrollment is being completed from.
- k. Click **Launch instance**.

After you finish: [Enroll the CylanceGATEWAY Connector with the BlackBerry Infrastructure](#)

Configure the CylanceGATEWAY Connector in the VM environment

Note: The AWS CylanceGATEWAY Connector AMI does not support access to the EC2 serial console. Do not complete this task if you are installing the connector to your AWS environment. See [Configure your firewall for the CylanceGATEWAY Connector](#) to continue with the CylanceGATEWAY Connector setup.

The CylanceGATEWAY Connector is a minimal installation of the Ubuntu operating system, which can operate without a user logging in. You need to log in only if you want to update the default settings or verify that the OVA or VHD deployed correctly.

1. Do one of the following to open the console in your environment.

| Environment | Steps |
|--------------------|---|
| vSphere | <ol style="list-style-type: none"> a. Log in to your environment. b. Click the host name of the CylanceGATEWAY Connector. c. Click Launch Remote or Launch Web Console. |
| ESXi | <ol style="list-style-type: none"> a. Log in to your environment. b. Click the host name of the CylanceGATEWAY Connector. c. Click Console. |
| Microsoft Entra ID | <ol style="list-style-type: none"> a. Sign in to the Microsoft Entra ID management portal at https://portal.azure.com. b. Click Virtual machines. c. In the left column, in the Support + troubleshooting section, click Serial console. |
| Hyper-V | <ol style="list-style-type: none"> a. Open the Hyper-V Manager. b. Right-click the connector that you want to access > Connect. |

2. At the UNIX prompt, type the administrator username and press **Enter**.
The default username is **admin**.
3. Type the administrator password.
The default password is **admin**.

4. Complete any of the following actions:

| Task | Environment | Steps |
|--|-----------------|---|
| Verify the network interface configuration. | vSphere ESXi | Type <code>sudo /var/lib/cylance-gateway/scripts/configure-network --ovfenv --check</code> . Press Enter . If you are prompted, enter the administrator password. |
| Change the keyboard layout in the connector. | All | By default, Ubuntu only supports US keyboard layouts. a. To select a new keyboard layout, type <code>sudo dpkg-reconfigure keyboard-configuration</code> . Press Enter . b. If you are prompted, enter the administrator password. c. Follow the onscreen prompts. |

Access the CylanceGATEWAY Connector using OpenSSH

Note: OpenSSH is enabled in the AWS CylanceGATEWAY Connector AMI by default. Do not complete this task if you are installing the connector to your AWS environment. See [Configure your firewall for the CylanceGATEWAY Connector](#) to continue with the CylanceGATEWAY Connector setup.

OpenSSH is preinstalled on the connector image and allows you to access the CylanceGATEWAY Connector and perform system operations and maintenance using the SSH protocol. By default, the OpenSSH service is disabled. You must enable the OpenSSH service and generate the host keys each time that you access a CylanceGATEWAY Connector instance using OpenSSH. In Microsoft Entra ID environments, incoming TCP traffic must be allowed.

Before you begin: Verify that port 22 (SSH), port 80 (HTTP), and port 443 (HTTPS) are open and that the security group has access to the CylanceGATEWAY Connector from the network that the enrollment is being connected from.

1. Do one of the following to open the console in your environment.

| Environment | Description |
|-------------|--|
| vSphere | a. Log in to your environment. b. Click the host name of the CylanceGATEWAY Connector. c. Click Launch Remote Console or Launch Web Console . |
| ESXi | a. Log in to your environment. b. Click the host name of the CylanceGATEWAY Connector. c. Click Console . |

| Environment | Description |
|--------------------|---|
| Microsoft Entra ID | <ol style="list-style-type: none"> Sign in to the Microsoft Entra ID management portal at https://portal.azure.com. Click Virtual machines. Click the connector that you created in Install the CylanceGATEWAY Connector to a Microsoft Entra ID environment, step 5. In the left menu, in the Support + troubleshooting section, click Serial console. In the left column, click Boot diagnostics. Click the Settings tab. Select Enable with custom storage account. In the Diagnostics storage account, drop-down list, select the storage account that you created in Install the CylanceGATEWAY Connector to a Microsoft Entra ID environment, step 3. Click Save. On the connector screen, in the left menu, in the Support + troubleshooting section, click Serial console. |
| Hyper-V | <ol style="list-style-type: none"> Open the Hyper-V Manager. Right-click the connector that you want to access > Connect. |

- At the UNIX prompt, type the administrator username and press **Enter**. The default username is admin.
- Type the administrator password. The default password is admin.
- Generate the host keys for the OpenSSH service. Type `sudo dpkg-reconfigure openssh-server`. Press **Enter**.
- If you are prompted, enter the administrator password.
- Enable the OpenSSH service. Type `sudo systemctl --system enable ssh`. Press **Enter**.
Note: This command does not start the service.
- Start the OpenSSH service. Type `sudo systemctl --system start ssh`. Press **Enter**.
- You can complete any of the following actions (optional):

| Task | Steps |
|--|---|
| Disable the OpenSSH service from starting during the system startup. | Type <code>sudo systemctl --system disable ssh</code> . This command does not stop the service. |
| Stop the OpenSSH service. | Type <code>sudo systemctl --system stop ssh</code> . Press Enter . |
| Verify if the OpenSSH service is enabled. | Type <code>sudo systemctl --system is-enabled ssh</code> . |
| Verify if the OpenSSH service is running. | Type <code>sudo systemctl --system is-active ssh</code> . |

| Task | Steps |
|--|--|
| Obtain the status of the OpenSSH service | Type <code>sudo systemctl --system status ssh</code> . |

9. Exit the console.
10. Optionally, in a Microsoft Entra ID environment, you can disable the Boot diagnostics settings for the connector VM that you configured in step 1.

Configure your firewall for the CylanceGATEWAY Connector

The CylanceGATEWAY Connector runs inside your private network, behind your firewall, and has a private IP address. It connects to the CylanceGATEWAY cloud service with HTTPS and UDP. The CylanceGATEWAY Connector must be able to connect to CylanceGATEWAY through your firewall (via NAT).

The CylanceGATEWAY Connector must be able to use DNS to resolve public CylanceGATEWAY FQDNs to Internet IP addresses. The CylanceGATEWAY Connector uses [your private DNS servers](#) to do this.

The CylanceGATEWAY agent communicates over secure websockets (WSS) with the management console and must be able to establish this connection directly. To allow the CylanceGATEWAY agent to activate and periodically authenticate, you must allow access to the appropriate domains (for example, [idp.blackberry.com](#) and the domain for your region). If your environment uses an authentication proxy, you must allow the traffic on the proxy server.

For more information about FQDNs, ports, IP address ranges and other firewall requirements, visit [support.blackberry.com/community](#) to read article 79017. For more information on network requirements for Cylance Endpoint Security, see [Cylance Endpoint Security network requirements](#).

Enroll the CylanceGATEWAY Connector with the BlackBerry Infrastructure

After you install the CylanceGATEWAY Connector and configure its firewall, you must connect it to the BlackBerry Infrastructure.

1. In a web browser, navigate to the IP address of your CylanceGATEWAY Connector.
2. To accept the self-signed certificate and proceed to the HTTPS service, click **Proceed to the HTTPs service**.
3. At the prompt, enter the default administrator username and password and click **Sign In**.
The default username is admin. The default password is blackberry.
4. The first time that you log in to the CylanceGATEWAY Connector web interface, you must change the default administrator password for the CylanceGATEWAY Connector. This does not change the password for the CylanceGATEWAY Connector in the ESXi, vSphere, the Microsoft Entra ID portal, the AWS console, or Hyper-V Manager console.
5. Log in again to the CylanceGATEWAY Connector web interface using the new password.
6. On the **BlackBerry Solution License Agreement** screen, review the license agreement and click **I Agree**.
7. To authorize the CylanceGATEWAY Connector to the BlackBerry Infrastructure for your organization, you must enroll the connector.
 - a) Review and agree to the privacy notice. Select the **I agree to the BlackBerry Privacy Notice** check box.
 - b) In the **URL** field, type the URL for the connector to access the management console.
To get the URL, in the management console, click **Settings > Network > Private Network** and on the **Gateway Connectors** tab, click **Add Connectors**.
 - c) In the **Proxy URL** field, enter the URL for the proxy server. When you enter the proxy URL on this screen, the **Proxy URL** field on the Settings page is populated with the same URL and vice versa.
8. Click **Enroll this Connector**. The management console opens.

9. Log in to the management console as an administrator.
10. In the **Connector name** field, type a name for the connector.
11. In the **Connector group** drop-down list, select a connector group that you want to assign it to.
12. Click **Authorize**.

The connector, its version, and the connector group that it is assigned to appears in the list of CylanceGATEWAY Connectors. The **Status** column shows whether or not the private network, its DNS, and health checks are functioning normally. For information on statuses that might be displayed, see [Managing CylanceGATEWAY Connectors](#)

After you finish: If the CylanceGATEWAY Connector is enrolled, but its tunnel is not connected to the BlackBerry Infrastructure, you can initiate a connectivity test to verify whether the UDP packets that are sent from your private network have been received by the BlackBerry Infrastructure and UDP packets that are sent from the BlackBerry Infrastructure are received by your private network. At the login prompt of your environment (for example, vSphere). Type `/var/lib/cylance-gateway/bin/udp-connectivity-test`. Press **Enter**. You can run this command in any shell (for example, csh and bash). For more information about the connectivity results, see [UDP connectivity test responses](#).

View details for an enrolled CylanceGATEWAY Connector

You can view the CylanceGATEWAY Connector details after it is enrolled in the CylanceGATEWAY Connector web interface. If your network has multiple instances of the CylanceGATEWAY Connector, you must access the web interface for each instance. You can view the status of all the connectors in your environment in the management console.

- When the connector is enrolled with the BlackBerry Infrastructure, you can view the following information. You can then click the **Manage this connector** to open the Cylance Endpoint Security management console and manage the CylanceGATEWAY Connectors:
 - CylanceGATEWAY Connector identifiers that are used by the BlackBerry Infrastructure to identify the instance
 - Current status and registration information of the instance
 - Number of tunnels that are connected to the BlackBerry Infrastructure by the CylanceGATEWAY Connector
- You can download the log files. The log files are downloaded to your Downloads folder in a zip file and can contain multiple CylanceGATEWAY Connector log files. Click **Download logs**. Extract the logs to review them or send the zip file to BlackBerry Support to help troubleshoot potential issues. The log files for each instance can also be downloaded from the management console from the Connector information pane on the CylanceGATEWAY Connectors page.
- [You can configure the CylanceGATEWAY Connector.](#)

Configure the CylanceGATEWAY Connector

You can complete various tasks in the CylanceGATEWAY Connector web interface. If your network has multiple instances of the CylanceGATEWAY Connector installed and configured, the tasks must be completed on each CylanceGATEWAY Connector instance in your environment as necessary. You can view the status of all the connectors in your environment on the Gateway Connectors page in the management console. You can view the status of each CylanceGATEWAY Connector in the web browser. For more information, see [View details for an enrolled CylanceGATEWAY Connector](#)

Before you begin: Verify that you have one or more CylanceGATEWAY Connector instances deployed.

1. In a web browser, navigate to the IP address of your CylanceGATEWAY Connector.
2. Enter your credentials and click **Sign in**.
3. Complete any of the following tasks:

| Tasks | Steps |
|----------------|--|
| Edit settings. | <p>You can specify one or more of the following settings (optional).</p> <ol style="list-style-type: none"> Click Settings. Complete one or more of the following settings: <ul style="list-style-type: none"> Generate a new self-signed TLS certificate: You can regenerate the TLS certificate at any time. By default, the certificate is valid for one year. The web interface displays the certificate expiry day and time, the serial number, and host that is bound to the certificate. Each time that you generate a new TLS certificate, you are prompted to accept the new certificate. HTTP/S Proxy configuration: If your environment is configured with an unauthenticated proxy server that is used for Internet-destined HTTP and HTTPS requests, you can enter the URL of the proxy. When the proxy URL is added, HTTPS requests to the BlackBerry Infrastructure made by the CylanceGATEWAY Connector will use the proxy. Tunnel traffic will not use the proxy. Maximum Transfer Unit (MTU) configuration: By default, the CylanceGATEWAY Connector automatically detects the MTU of your network. In some instances, you might need to specify the MTU value that the CylanceGATEWAY Connector can use. BlackBerry recommends that you use automatic detection. <p>Note: If you specify the MTU and want to use automatic detection, you must restart the CylanceGATEWAY Connector from within the vSphere, Hyper-V, Microsoft Entra ID, AWS, or ESXi environment.</p> <ul style="list-style-type: none"> Network Time Protocol (NTP) configuration: By default, the CylanceGATEWAY Connector uses Ubuntu's ntp.ubuntu.com server for time synchronization. You can specify a custom NTP server. Advanced Package Tool (APT) configuration: By default, the CylanceGATEWAY Connector uses Ubuntu's repository hosts, archive.ubuntu.com and security.ubuntu.com. For more information, visit support.blackberry.com/community and read article 79017. You can specify a custom package repository that the CylanceGATEWAY Connector uses. Note that security updates are applied automatically, and you must restart the CylanceGATEWAY Connector in the management console for updates to take affect. Complete one of the following: <ul style="list-style-type: none"> Click Update settings to save the changes on the Settings screen. Click Restore default settings to restore all of the default settings. You must enter your credentials for the changes to take affect. Network connectivity might be interrupted (for example, if you specify an MTU the CylanceGATEWAY Connector must be restarted). Click Factory Reset to erase all CylanceGATEWAY Connector configurations, including the self-signed TLS certificate. The CylanceGATEWAY Connector must be restarted and will result in a network connectivity interruption. |

| Tasks | Steps |
|--------------------------------|---|
| Change administrator password. | <p>You can change the administrator password for the CylanceGATEWAY Connector password at any time. This does not change the administrator password that is used for CylanceGATEWAY Connector access in the vSphere, Hyper-V, Microsoft Entra ID, AWS, or ESXi environment. Each time that you change the password, you are prompted to log in again using the new password.</p> <ol style="list-style-type: none"> Click Change admin password. Enter the current administrator password. Enter and confirm your new password. Click Change password. When prompted, click Log in now. You will also be automatically redirected to the login prompt after a short wait. Enter your administrator username and new password and click Sign in. |


Managing CylanceGATEWAY Connectors

After you've registered CylanceGATEWAY Connectors, you can specify a health check URL and restrict IP addresses for your connectors. If a health check URL is not specified, the DNS and HTTP information is not displayed in the health check status for a connector. For the CylanceGATEWAY Connectors, you can perform the following:


| Screen | Actions |
|---------------------------------------|--|
| On the Gateway Connectors list screen | <ul style="list-style-type: none"> View the number of connections that are active. View the connector group that the CylanceGATEWAY Connector is a part of. View additional health check metadata for each connector instance. View the version of each connector instance. View the status of your connectors. Reload the CylanceGATEWAY Connectors information. Download the log files of each connector instance. Disable a connector to prevent new connections from being routed through the connector. Active network connections are not interrupted. |
| On the Connector info page | <ul style="list-style-type: none"> View the connector group that the CylanceGATEWAY Connector is a part of. Edit the Private URL field for a connector and open the URL in a separate page. Assign the connector to a different connector group. Disable a connector to prevent new connections from being routed through the connector. Active network connections are not interrupted. View the version of the connector. View the connection status of the connector. Download the log files for the connector. View the Public Key View the connection history of the connector. The connection history time is in UTC. |

Restricting source IP addresses provides additional security to ensure that only CylanceGATEWAY Connectors with the IP addresses you specify can connect to your private network. If you restrict source IP addresses, your CylanceGATEWAY Connectors should have a fixed IP address, either by setting a static IP address for the





CylanceGATEWAY Connector when it is deployed in a [vSphere environment](#) or [ESXi environment](#), or creating a DHCP IP reservation on your network.

Depending on the number of active CylanceGATEWAY users in your environment, a component of the BlackBerry Infrastructure that is responsible for managing incoming tunnels from the connector might scale the resources that are allocated to your organization. Each CylanceGATEWAY Connector establishes a tunnel to this component and has a health check performed on it. The health check status and Status columns indicate the state of those tunnels from the connector to the component that is responsible for managing them. For example, if the Health Check column status displays X/2, this means that two of the components are allocated to your organization at that time. If the column displays 2/2, the connector has successfully established two tunnels to the component. If you see 0/2 or 1/2 that means the connector has either not established a tunnel or has established 1 out of the 2 tunnels that are required. If the status is , some but not all of your users are able to access resources on your private network.

The health check URL can be any URL within your private networks that you want CylanceGATEWAY users to be able to connect to. CylanceGATEWAY periodically sends an HTTP or HTTPS GET request, including a DNS lookup, through each CylanceGATEWAY Connector tunnel to this URL. The Health check status expands to display Tunnel, DNS, and HTTP connection status for each connector. A status of 2/2 indicates that everything is working correctly. A status of 0/0 indicates that the status check of a new connection is still pending.


The Status column displays the enrollment status of the CylanceGATEWAY Connector with the BlackBerry Infrastructure. The  indicates that the CylanceGATEWAY Connector has successfully completed the enrollment process and has established a connection to the BlackBerry Infrastructure. The status column displays the connection state and might include a security message (for example, if the connector requires a restart to apply an update).

| Column | Description |
|---------------------|---|
| Health check status | <p>This is the overall status of the CylanceGATEWAY Connector and includes the following information:</p> <ul style="list-style-type: none">• Tunnel: This is the status of the CylanceGATEWAY Connector connection to the BlackBerry Infrastructure. If the status indicates a connection issue, contact your BlackBerry support representative.• DNS: This is the status of the DNS query made from the CylanceGATEWAY Connector to your specified DNS server. If the status indicates an issue, verify that you've correctly specified your private DNS server.• HTTP: This is the status of the HTTP query made to the CylanceGATEWAY Connector for the health check URL. If the status indicates an issue, verify that the health check URL can be reached from the CylanceGATEWAY Connector and that you have specified a DNS forward lookup zone. |

| Column | Description |
|--------|--|
| Status | <p>This is the overall status of the CylanceGATEWAY Connector connection to the BlackBerry Infrastructure, including the health check status.</p> <ul style="list-style-type: none"> : The connector has not completed the enrollment process. This status is displayed only the first-time connector is enrolled. : The connector has completed the enrollment process and is establishing a connection to the BlackBerry Infrastructure. : The connector has completed the enrollment process, but not all of the connections to the BlackBerry Infrastructure have been established. If this status is displayed, read the associated security message and verify that a health check URL has been specified in the connector group. : The connector enrollment process has not completed or there is an error in establishing all the connections to the BlackBerry Infrastructure. The following error messages might be displayed: <ul style="list-style-type: none"> Failed to register due to storage error: Verify that you have sufficient disk space to register the CylanceGATEWAY Connector. Failure: View the full health check status for the connector, including the Tunnel, DNS, and HTTP information. For example, if DNS displays "Fail", verify that your DNS settings are accurate. |

Manage CylanceGATEWAY Connectors

Complete this task for each connector group.

1. In the management console, on the menu bar, click **Settings > Network**.
2. Click the **Private Network** tab.
3. Click **Connector Groups**. Click a connector group.
4. Click **Health Check**.
5. Specify a URL within your private network that the CylanceGATEWAY Connector can access to verify that CylanceGATEWAY can connect to the URL.
The health check URL must contain an FQDN that your private DNS server can resolve. The FQDN must resolve to an IP address that is within the IP space defined for your private network.
6. To specify allowed IP addresses for your CylanceGATEWAY Connectors, click **Source IP Restriction**.
7. Click **Add**.
8. Click **Save**.
9. To view additional information about a CylanceGATEWAY Connector and to download the connector log files or enter a custom FQDN or IP address in the private URL, click the name of the CylanceGATEWAY Connector.
Note: If you enter a custom FQDN or IP address, the FQDN or IP address is not validated.
10. To reload the CylanceGATEWAY Connectors information, click .

Update a CylanceGATEWAY Connector

You can check whether an update for the CylanceGATEWAY Connector or update for the virtual machine OS is available.

Before you begin: Verify the version of the CylanceGATEWAY Connector that is installed in the Cylance Endpoint Security management console in Settings > Network > Private Network > Gateway Connectors.

1. Check *myAccount* or the [Cylance Endpoint Security Release Notes](#) to see whether a new version of the CylanceGATEWAY Connector software is available and perform one of the following actions:
 - If new CylanceGATEWAY Connector software is available, complete step 2 for your environment.
 - If no new CylanceGATEWAY Connector software update is available, check for a Linux OS update.
2. Complete one of the following tasks:

| Environment | Steps |
|--|--|
| Update the CylanceGATEWAY Connector version 2.9 or later. | <p>Use the DEB file to update the connector instance and to retain your configurations.</p> <ol style="list-style-type: none"> a. In <i>myAccount</i> download the DEB version of the connector. b. Copy the DEB package to the connector that you want to upgrade. If SSH is enabled, you can use SCP to copy the DEB package from any host with SSH access to the connector. For instructions, see Access the CylanceGATEWAY Connector using OpenSSH. Otherwise, you can use SCP on the connector to copy the DEB package from any SSH-enabled host that can be reached by the connector. c. In the Unix console, type <code>sudo apt install <path>/cylance-gateway-connector-<version>.deb</code>. For example, <code>sudo apt install /home/admin/cylance-gateway-connector-2.10.0.938.deb</code> d. Press Enter. |
| Update the CylanceGATEWAY Connector version 2.8 or earlier or perform a complete reinstallation. | Create a new instance of the connector for your environment. For instructions, see Setting up the CylanceGATEWAY Connector . |

3. For any CylanceGATEWAY Connector showing **Reboot required to apply OS updates and security fixes** in the **Status** column, restart the virtual machine to finish installing the OS update.

After you finish: If the CylanceGATEWAY Connector is enrolled, but its tunnel is not connected to the BlackBerry Infrastructure, you can initiate a connectivity test to verify whether the UDP packets that are sent from your private network have been received by the BlackBerry Infrastructure and UDP packets that are sent from the BlackBerry Infrastructure are received by your private network. At the login prompt of your environment (for example, vSphere), type `/var/lib/cylance-gateway/bin/udp-connectivity-test`. Press **Enter**. You can run this command in any shell (for example, `csh` and `bash`). For more information about the connectivity results, see [UDP connectivity test responses](#).

UDP connectivity test responses

The following examples show the outputs that might be displayed when you verify the UDP path between the CylanceGATEWAY Connector and the BlackBerry Infrastructure.

In the following examples,

- "Endpoint" is the IP address and port of the `udp-connectivity-test` that is being tested.
- "Client Address:Port" is the external IP address and port of the CylanceGATEWAY Connector as seen by the BlackBerry Infrastructure.

- "Server" is the BlackBerry Infrastructure.

Example: UDP traffic is successfully sent and received

In this example, the UDP traffic is successfully sent and receive between the connector in your private network and the BlackBerry Infrastructure.

```
Initiating discovery request
Starting connectivity test using endpoint=<IP address>:<port>
Sent hello message with id='62f6bf9e-741c-4f22-9907-2725789aa318' to <IP
address>:<port>
Waiting for server hello
Received server hello with id='62f6bf9e-741c-4f22-9907-2725789aa318' from <IP
address>:<port>
Sent ack message with id='62f6bf9e-741c-4f22-9907-2725789aa318' to <IP
address>:<port>
Report:
  Client Address:Port = <IP address>:<port>
  Packet Size       = 1500
  Fragmented       = false
  RTT               = 3ms
```

Example: The outbound UDP traffic is blocked.

In this example, the UDP connectivity test client was able to send the client hello, but the BlackBerry Infrastructure did not receive the response within the timeout period.

```
Initiating discovery request
Starting connectivity test using endpoint=<IP address>:<port>
Sent hello message with id='2dca5fcf-3f9a-46c3-a158-911a851f94a7' to <IP
address>:<port>
Waiting for server hello
Error: Timeout on receiving server hello
Getting test report from server
Error: The server did not receive our hello message.  Is outbound UDP blocked?
Starting connectivity test using endpoint=<IP address>:<port>
Sent hello message with id='40fe1e15-b2c0-4607-9880-7be08ec505ac' to <IP
address>:<port>
Waiting for server hello
Error: Timeout on receiving server hello
Getting test report from server
Error: The server did not receive our hello message.  Is outbound UDP blocked?
Error: No endpoints to test
```

Example: The inbound UDP traffic is blocked.

In this example, the UDP connectivity test client sent the UDP connectivity test client hello and the BlackBerry Infrastructure received it and replied, but the test client did not receive the response within the timeout period.

```
Initiating discovery request
Starting connectivity test using endpoint=<IP address>:<port>
Sent hello message with id='973e0d45-71f0-427b-be08-9e5f16d03349' to <IP
address>:<port>
Waiting for server hello
Error: Timeout on receiving server hello
```

```

Getting test report from server
Error: The server sent a response that was not received.  Is inbound UDP blocked?
Starting connectivity test using endpoint=99.83.155.194:58255
Sent hello message with id='2fc6d3f8-43c2-4707-bc77-e85168c2596e' to <IP
address>:<port>
Waiting for server hello
Error: Timeout on receiving server hello
Getting test report from server
Error: The server sent a response that was not received.  Is inbound UDP blocked?
Error: No endpoints to test

```





Specify your private network

Before you begin:

- Ensure that you have a list of the IP addresses or IP address ranges for all destinations that you want to define as part of your private network. You can get this information from your network administrator.
- You cannot setup private network access if you do not install a CylanceGATEWAY Connector. Ensure that you installed one or more CylanceGATEWAY Connectors in a part of every network that has full access to addresses that you specify here. For instructions on installing a CylanceGATEWAY Connector, see [Setting up the CylanceGATEWAY Connector](#).
- You can create a maximum of eight connector groups. You can add a maximum of eight CylanceGATEWAY Connectors instances to each connector group.

1. On the menu bar, click **Settings > Network**.
2. Click the **Private Network** tab.
3. Click **Connector Groups**.
4. Click **Add Connector group**.
5. Type a name and description. The connector name can be between 3 and 250 characters. The description can be between 3 and 500 characters.
6. On the **Network Routing** tab, click **Add Address**.
7. Type one or more IP addresses, IP ranges, or CIDRs and click **Add**.
If your environment requires all network traffic to be redirected to your on-premises infrastructure, type 0.0.0.0/0. BlackBerry recommends that you redirect only traffic that is destined to resources on your private network and then configure your environment to use CylanceGATEWAY cloud services for traffic to Internet destinations.



Note: When you specify 0.0.0.0/0 for your network routing, all non-DNS traffic (for example, HTTP traffic) routes through the CylanceGATEWAY Connector. Traffic to resources that are not part of your private network require the DNS query to be sent to public DNS servers, and not your private DNS server, before the connection is established and traffic is routed through the CylanceGATEWAY Connector.

8. To add an optional description for the IP addresses, IP ranges, and CIDRs defined in step 7, complete the following steps for each entry in the connector group:
 - a) Click  next to an address.
 - b) Type a description for each private network (for example, North network).
 - c) Click **Save**.
9. To remove an address, click  next to the address.
10. To change the order of the connector group list, click the **Order** button, and then drag  for the connector group to the appropriate location in the list.
11. To delete a connector group, remove or reassign all of the assigned CylanceGATEWAY Connectors from the connector group. Click .

Specify your private DNS




You can provide the settings for your private DNS to help CylanceGATEWAY route traffic within your private network. You can specify the IP addresses of your DNS servers, the domain names delegated to your DNS servers for forward lookups, and the CIDRs delegated to your DNS servers for reverse lookups. The DNS Server IP addresses are shared by all of connector groups and must be included in a connector group. You can get this information from your network administrator.

1. On the menu bar, click **Settings > Network**.
2. Click the **Private Network** tab.
3. Click **DNS**.
4. To specify a DNS server, perform the following actions:
 - a) Click **DNS Servers**.
 - b) Click **Add DNS Server**.
 - c) Type the IP address for your DNS server and click **Add**.
5. To specify a domain for forward lookups, perform the following actions. You can specify a maximum of 100 forward lookup zones.
 - a) Click **Forward Lookup Zone**.
 - b) Click **Add Forward Zone**.
 - c) Type a domain name and click **Add**.

If you do not specify a forward lookup zone, the [CylanceGATEWAY Connector health check](#) will fail. If you enable split tunneling and do not specify a forward lookup zone, all DNS queries will go through the tunnel.
6. To specify a CIDR for reverse lookups, perform the following actions:
 - a) Click **Reverse Lookup Zone**.
 - b) Click **Add Reverse Zone**.
 - c) Type a CIDR and click **Add**.
7. To edit an address or domain name, click .
8. To remove an address or domain name, click .

Specify your DNS suffixes

You can specify up to 32 suffixes that your private DNS appends to searches for unqualified names. You can get this information from your network administrator. If you specify more than one suffix, you can rank them.

1. On the menu bar, click **Settings > Network**.
2. Click the **Client DNS** tab.
3. Turn on **DNS search domain (or suffix)**.
4. Click **Add DNS Suffix**.
5. Type the DNS suffix name and click **Add**.
6. Repeat steps 4 and 5 for each suffix that you want to add.
7. To edit a suffix, click .
8. To remove a suffix, click .
9. To change the order of the list, drag  for the suffix to the appropriate location in the list.
10. Click **Save**.

Specify private CylanceGATEWAY agent IP ranges

CylanceGATEWAY allocates tunnel private IP addresses to CylanceGATEWAY agents from a private IP range that is configured system-wide and is the same for each tenant. You may want to specify an endpoint tunnel private IP

range that does not overlap the tenant's private network range to CylanceGATEWAY agents. Providing a private IP range might prevent potential conflicts such as when an agent attempts to access a private network service that has the same IP address that is assigned to the agent. The agent IP range must be in a IPv4 CIDR format and unique within your private network to prevent issues with routing to other endpoints in your network. By default, the range is 10.10.0.0/16. Suffixes must be less than 17.



Warning: If you change the agent IP range, the associated agents and CylanceGATEWAY Connectors might disconnect and reconnect. If you access the Gateway Connectors screen (Settings > Network > Private Network) during the disconnect and reconnect, one of the following messages might be displayed. Click ↺.

- Registration could not be completed: 500
- Failure. Reboot required to apply OS updates and security fixes

1. On the menu bar, click **Settings > Network**.
2. Click the **Private Network** tab.
3. Click **Agent IP Range**.
4. Enter the CIDR.
5. Click **Save**.

Bring your own IP addresses (BYOIP)

You can add dedicated IP addresses in an IPv4 CIDR /24 range to CylanceGATEWAY that are used to manage network egress traffic.

You can use the dedicated IP addresses to do the following:

- Use your organization's own IP addresses for source IP pinning.
- Avoid issues where some websites block AWS IP ranges.
- Reflect the GeoIP information for the addresses.
- Allow a single CIDR instead of several non-continuous IPs.

To add dedicated IP addresses to CylanceGATEWAY, you submit a request to BlackBerry Technical Support Services. For instructions, visit <https://support.blackberry.com/community> to read article 100189.

Network Address Translation with CylanceGATEWAY

By default, CylanceGATEWAY applies Network Address Translation (NAT) to traffic flow to your private network. NAT is also applied to your endpoints (for example, devices) when users access the Internet and SaaS apps. After NAT is applied, the real IP address is concealed and all inbound connections to a specific endpoint are prevented. NAT is not applied to flows that do not use the CylanceGATEWAY tunnel (for example, Safe Mode).

Note: Inbound connections to endpoints are prevented by CylanceGATEWAY (for example, you cannot establish a connection to endpoints using remote IT tools, such as Remote Desktop Connection).

NAT is applied to traffic that flows through the CylanceGATEWAY Connector to your private network. The connector provides additional information on UDP and TCP flows that are displayed on the Network Events screen (CylanceGATEWAY > Events). You can identify the private source IP and private source port of an event that has been blocked or identified as a potentially malicious. For more information, see the following:

- [Viewing the Event Details page](#)
- [Data flow: Accessing an application or content server on your private network](#)

NAT is applied by CylanceGATEWAY to traffic that flows through the tunnel to access Internet destinations and cloud-based SaaS applications. You can filter the events based on the Gateway tunnel IP address that was used by users to access the external destinations. For more information, see the following:

- [Viewing the Event Details page](#)
- [Data flow: Accessing a cloud-based application or Internet destination](#)

Define network services

A network service is a group of addresses (FQDNs or IP addresses) that you can use to simplify setting up [access control list \(ACL\) rules](#). When you create ACL rules, you can specify a network service instead of specifying each individual address. BlackBerry maintains and regularly updates network services for many common SaaS applications to simplify the process for you. You can define additional network services for both public and private applications. You can nest existing network services. When you nest network services, the destinations of each added network service are referenced, and you have access to all of the contained destinations. If a change is made to one of the combined network services, it is automatically reflected immediately. You can perform a search of the network services that you have added. For more information on searching, see [Searching ACL rules and Network Services](#).

1. In the management console, on the menu bar, click **Settings > Network**.
2. Click the **Network Services** tab.
3. Click **Add**.
4. Type a name and description for the network service.
5. Optionally, click **Network Services** and select one or more network services.
6. Optionally, click **Address**. Type an IP address, FQDN, or wildcard domain for the destination. Click **+** to add additional addresses. The following address formats are supported:
 - IP Address range: 172.16.10.0 - 172.16.10.255
 - Single address: 172.16.10.2
 - IP Address range: 172.16.10.0 - 172.16.10.255
 - CIDR: 172.16.10.0/24
 - FQDN: domain.example.com
 - Domain with wildcard: *.example.com
7. Click **Protocol** and select a protocol to use for the connection attempt and specify a single port or range of ports to use. Click **+** to add additional protocol and ports.
8. Repeat steps 6 and 7 to add additional addresses and ports.
9. Click **Add**.
10. To edit a network service, click the field that you want to edit and make the changes. You cannot edit services that are defined by BlackBerry.
11. To remove a network service, click **X** beside the service, address or port. To remove an address and port row, click **X** beside the appropriate destination address and port row. You cannot delete services that are defined by BlackBerry.

After you finish: You can search the network services list to view the information. Click **Q** and select one or more predefined scopes, a condition, and specify the criteria. Click the network service that you want to view the settings for. Click **X** to reset the search.

Controlling network access

You define the network resources that devices enrolled with CylanceGATEWAY can connect to using the access control list (ACL). The ACL defines allowed and blocked destinations on private and public networks. The ACL applies only to users that are assigned a Gateway Service policy.

The ACL applies to all CylanceGATEWAY users in the tenant. Each network access attempt by a device is evaluated against the rules, in order, for each connection phase (DNS lookup, connection establishment, and TLS handshake) until a rule that matches the attempt is found. The rule must match on all specified properties including destination or destination categories, specified users or groups, and the risk level determined for the destination. The first matching rule determines whether the access attempt is blocked or allowed to continue to the next phase. An access attempt that is allowed through all of its phases can be fully established. If a network access attempt does not match any rule in the ACL, access is blocked. The ACL supports a maximum of 1000 rules.

Applying ACL rules

ACL rules apply to all CylanceGATEWAY users in the tenant. ACL rules evaluate each network access attempt in the order that they are displayed in the management console, from the top down. The default rule will always be evaluated last, and if none of the previous rules match will block access to all resources. The Default rule cannot be disabled or modified

When you create the ACL rules, BlackBerry recommends that you create your ACL rules and make sure that they are displayed in the in following order:

1. Block access to Internet content that contains CylanceGATEWAY specified categories
2. Block access to non-categorized services based on your organization's requirements
3. Allow access to organization-wide services in the private network
4. Allow access to all public Internet destinations
5. Default

The following table provides examples of rules and their necessary settings:

| Rule | Description |
|--|---|
| Allow users to access public Internet destinations | <p>This rule will allow users to access any destination that your organization considers to be the public internet. Users will not be able to access the specified RFC1918 addresses.</p> <p>To create this rule, you can specify the following settings:</p> <ul style="list-style-type: none">• In the Action section,<ul style="list-style-type: none">• The Action drop-down list displays Allow.• Check access attempts against Network Protection check box is selected. This setting allows the rule to pass the ACL, but also allows for further inspection by Gateway.• In the Destination section,<ul style="list-style-type: none">• The Target dropdown list displays Does not match.• In the Addresses and Ports, Address field, enter the RFC1918 network ranges. |

| Rule | Description |
|---|--|
| Allow users to access the private network | <p>This rule will allow user to access network services within your private network.</p> <p>For users to access the private network, the following prerequisites must be met:</p> <ul style="list-style-type: none"> • Ensure that the CylanceGATEWAY Connector is installed in the network to allow traffic to reach your private network. For instructions on how to install the CylanceGATEWAY Connector in your environment, see Setting up the CylanceGATEWAY Connector. • Ensure that you have defined a network service containing the private network resources that you want users to access. For information on how to define network services, see Define network services. <p>You can specify the following settings:</p> <ul style="list-style-type: none"> • In the Action section: <ul style="list-style-type: none"> • The Action drop-down list displays Allow. • Optionally, clear the Check access attempts against Network Protection check box. No further inspection will be performed by Gateway. • In the Destination section: <ul style="list-style-type: none"> • The Target drop-down list displays Matches any. • In the Network services field, select the network service that you want users to access. |

ACL parameters

The ACL is an ordered list of rules that defines what happens when a CylanceGATEWAY user attempts to access a destination on the Internet or your private network. Each rule includes several parameters that can specify destinations, users, and other factors that a rule can match with and the action to take when a rule matches. If a network access attempt does not match any ACL rules, access is blocked.

When you add or edit ACL rules, the updates are added to a list of draft rules until you commit them. Each administrator has their own draft rule list. If an administrator commits a rule update, all other administrators with a draft rule list will be notified to delete or update their draft rule list before continuing.

Each rule can include the following parameters:

| Item | Description |
|----------------------------|--|
| General information | |
| Name | This is a name for the rule. |
| Description | This is a brief description of the purpose for the rule. |
| Enabled | This setting specifies that the rule is part of the ACL. You can turn off this option to disable the rule without deleting it. |
| Action | |

| Item | Description |
|---|---|
| Action | This setting specifies whether to allow or block access if the attempt matches the rule. If allowed to continue, the access attempt may be evaluated again during the next phases of the attempt. |
| Check addresses against network protection | If the rule Action allows access, this setting specifies whether CylanceGATEWAY still blocks the connection if it detects a potential network threat . You should keep this option selected unless specified users need to connect to potentially malicious destinations. |
| Display a blocked notification message on devices | If the rule Action blocks access, this setting specifies a notification message that displays on the device when an access attempt is blocked. |
| Traffic Privacy | This setting specifies whether the network access attempts are displayed in the Network Events screen (CylanceGATEWAY > Events). You may want to enable Traffic Privacy for liability or privacy reasons. When this setting is enabled, network access attempts are not displayed in the Network Events screen. If your environment sends events to a SIEM solution or syslog server and the connection attempt matches a rule with traffic privacy, the events are not sent to the SIEM solution or syslog server. |
| Content logging | This setting specifies whether the Network Events > Events Details page should include originally plain-text, unencrypted HTTP connection data. HTTP flows are not decrypted. When this setting is enabled, a summary of the request and response details of an event are included in the Events Details page. You can view all of the HTTP transactions within an event. The Events Details page includes the first three HTTP events of the total number of events. You can view all the events and the details that are associated with each one. If you create a rule that includes both Traffic Privacy and Content logging, traffic privacy takes precedence. |
| Ignore port | This setting specifies whether the destination port of the access control attempt should be evaluated or ignored as part of this rule. |
| Destinations | |
| Target | <p>Targets can be defined by a network service, a set of addresses, a set of addresses with defined protocols and ports, or only defined protocols and ports. You can select one of the following options:</p> <ul style="list-style-type: none"> • Not applicable: The rule does not include destinations. For example, the rule specifies only categories, or you may want to create a rule that allows all access attempts for specific users unless the connection is blocked by network protection. • Matches any: The rule applies if the destination matches any target specified in the rule. • Does not match: The rule applies if the destination does not match any target specified in the rule. |
| Network services | You can select one or more network services . |

| Item | Description |
|------------|---|
| Address | <p>This setting specifies the IP addresses, FQDNs, or wildcard domains for the destination address. IP addresses can be in IPv4 or IPv6 format and can be represented by a single IP, an IP range, or CIDR notation. For example, the following address formats are supported:</p> <ul style="list-style-type: none"> • Single IP address: 172.16.10.2 • IP Address range: 172.16.10.0 - 172.16.10.255 • CIDR: 172.16.10.0/24 • FQDN: domain.example.com • Domain with wildcard: *.example.com <p>In some cases, for example when you target a FQDN destination that is behind a content delivery network (CDN) or a website with a frequently changing IP address, if you add a rule to allow connections to the FQDN and add a second rule which blocks connections to IP addresses that resolve to the same destination, the connection might be blocked. Consider the scenario where your environment includes the following two rules:</p> <ol style="list-style-type: none"> 1. Allow access to the FQDN example.com. 2. Block an IP address which resolves to example.com. <p>If the connection to the destination is an https request, users might be blocked from accessing example.com by rule 2, unless the IP addresses are added to the allowed rule. BlackBerry recommends that you add the destination's FQDN and IP addresses to rule 1 to allow access.</p> |
| Protocol | <p>This setting specifies whether the rule matches connection attempts using TCP, UDP, or both. If you do not select an option, the default is both TCP and UDP on all ports.</p> |
| Port | <p>This setting specifies the ports used for the destination. You can specify a single port or a range.</p> |
| Category | <p>A category defines the type of content available on a site. CylanceGATEWAY makes a best effort based on available information to determine the category of destination sites. You can select one of the following options:</p> <ul style="list-style-type: none"> • Not applicable: The rule does not include categories. • Matches any: The rule applies if the destination matches any category specified in the rule. If you select this option, a list of categories that you select from is displayed. • Does not match: The rule applies if the destination does not match any category specified in the rule. If you select this option, a list of categories that you select from is displayed. <p>For more information on the available categories that can be specified, see Destination content categories</p> |
| Conditions | |

| Item | Description |
|-----------------|--|
| User properties | <p>This setting specifies users, user groups, or operating systems to include in the rule. You can specify any number of users, user groups, and operating systems or a combination of each. When you click the User properties drop-down, select the user property that you want to specify the condition for. You can select one of the following options:</p> <ul style="list-style-type: none"> • Not applicable: The rule applies to all users, groups, and operating systems. • Matches any: The rule applies only to the users, groups, and operating systems you add to the rule. If you select this option, a field to add user properties is displayed. • Does not match: The rule applies only to users, groups, and operating systems that are not listed in the rule. If you select this option, a field to add user properties is displayed. <p>When you begin typing a name or user group, a list will display a matching list of user names. When you specify the operating system, you must select it from the list. You can select from the following OS options:</p> <ul style="list-style-type: none"> • Android • iOS • macOS • Windows <p>You can add rows to specify any number of users, groups, and operating systems.</p> |
| Risk | <p>This setting specifies the acceptable risk level of the device as it is configured in the CylancePROTECT Mobile policy.</p> <ul style="list-style-type: none"> • Not applicable: The risk level is not a condition for access. • Matches any: The device must be within the range of acceptable risk levels to allow the connection. If you select this option, you can select the acceptable risk levels. The default risk level is Secure (no risk). |

Destination content categories

These categories control the type of content that users can access on an available site. You can select an entire category or a subcategory that you want to match.

Adult

Adult themed content. Possible options:

| | | |
|-----------------------|-----------------------|---------------------------------|
| • Adult | • Obscene Language | • Sex Toys |
| • Alcohol and Tobacco | • Nudity | • Swimsuit and Intimate Apparel |
| • Dating | • Obscene Language | • Weapons |
| • Gambling | • Personal and Dating | |
| • Nudity | • Porn | |

Bandwidth

Sites that may affect the speed of data transfer in your network. Possible options:

- | | | |
|--|--|---|
| <ul style="list-style-type: none"> • Application Software Download • Download Sites • Internet Communications and Telephony • Media Sharing • Online Storage and Backup • Parked Domains | <ul style="list-style-type: none"> • Parked Domains • Peer-to-Peer • Personal Network Storage and Backup • Photo Galleries • Shareware and Freeware • Spam | <ul style="list-style-type: none"> • Streaming Media • Surveillance • Video Hosting • VVOIP |
|--|--|---|

Computer and Information Technology

Computer and IT themed content. Possible options:

- | | | |
|--|--|--|
| <ul style="list-style-type: none"> • Computer and Internet Information • Content Delivery Networks • Dialer Sites • DoH • Email • Information Technology • Internet • Internet Portals | <ul style="list-style-type: none"> • Online Services • Remote Access • Remote Control • Search Engines • Technology and Computing • Update Sites • URL Redirector • URL Shortner | <ul style="list-style-type: none"> • VPN Sites • Web Applications • Web Collaboration • Web Hosting • Web Infrastructure • Web-based Email |
|--|--|--|

General Interest - Business

Business themed content. Possible options:

- | | | |
|--|---|--|
| <ul style="list-style-type: none"> • Banking • Bitcoin • Business • Business and Economy | <ul style="list-style-type: none"> • Business Applications • Financial Services • Non-Profit Organizations | <ul style="list-style-type: none"> • Online Payment • Professional Organizations • Stock Advice and Tools |
|--|---|--|

General Interest - Personal

Personal interest themed content. Possible options:

- | | | |
|--|--|--|
| <ul style="list-style-type: none"> • Accommodation • Advice • Advocacy • Arts and Culture • Astrology • Auctions Blogs and Forums • Blogs and Wikis • Cartoons • Celebrity • Cooking • Cult • Education and Reference • Educational Institutions • Entertainment • Entertainment and Arts • Fashion and Beauty • Food and Drink • Games • General Organizations • Health and Medicine • Home and Garden | <ul style="list-style-type: none"> • Humor and Satire • Hunting and Fishing • Institutions • Internet Auctions • Internet Shopping • Job Search • Kids • Lifestyle • Mobile Communications • Mobile Phone • Motor Vehicles • Music • News • Occult • Opinion • Pay to Surf • Personal • Personal Sites and Blogs • Pharmacy • Philosophy and Political Advocacy • Political | <ul style="list-style-type: none"> • Press • Professional Association • Professional Networking • Public Information • Real Estate • Recreation and Hobbies • Reference and Research • Religion and Philosophy • Restaurants and Food • Sect • Shopping • Social Networking • Society • Sports • Suggested • Tabloids • Training and Tools • Translation • Travel |
|--|--|--|

Government

Government themed content. Possible options:

- | | |
|---|---|
| <ul style="list-style-type: none"> • Government • Government Business | <ul style="list-style-type: none"> • Legal • Military |
|---|---|

Potentially Liable

Potentially liable themed content. Possible options:

- | | | |
|--|--|--|
| <ul style="list-style-type: none"> • Cheating Exam • Copyright Infringement • Crime • Cryptojacking • Dangerous Material • Drugs | <ul style="list-style-type: none"> • Extremism • Fraud • Hate and Discrimination • Illegal • Marijuana • Narcotics | <ul style="list-style-type: none"> • Proxy Avoidance and Anonymizers • Questionable • Suicide • Violence |
|--|--|--|

Productivity

Content themed sites that might affect productivity. Possible options:

- | | | |
|---|---|---|
| <ul style="list-style-type: none"> • Advertisements and Analytics • Chat and IM • Insufficient Content | <ul style="list-style-type: none"> • Marketing and Advertising • Productivity Application | <ul style="list-style-type: none"> • Web Advertisements • Web and Email Marketing |
|---|---|---|

Security Risk

Sites that are not malicious but share information that might be a security risk (for example, content that teaches about spyware). Possible options:

- | | | |
|--|---|---|
| <ul style="list-style-type: none">• Bot Networks• Command and Control• Compromised Websites• DDoS• DNS Tunneling• Dynamic DNS | <ul style="list-style-type: none">• Grey Sites• Hacking• Malware• Mixed Content• Phishing• Potentially Harmful | <ul style="list-style-type: none">• Potentially Unwanted Software• Spyware• Suspicious Website• Unauthorized Marketplace• Warez |
|--|---|---|

Unknown

Site content that may or may not be malicious. Possible options:

- | | |
|--|--|
| <ul style="list-style-type: none">• Miscellaneous• New Domain | <ul style="list-style-type: none">• Not resolved• Unknown |
|--|--|

Evaluate the risk level of a network destination

You can use the management console to evaluate the risk level and identify the category and subcategory of a network destination as it would be analyzed and determined by the CylanceGATEWAY cloud services. This feature gives you insight into how CylanceGATEWAY would classify the destination when the agent attempts to access it. This can help you create and update your [access control list \(ACL\) rules](#) to allow or block a destination. Destinations that are not evaluated as malicious will return only the category and subcategory.



Before you begin: You must have the Administrator role to access this feature in the console.



1. In the management console, on the menu bar, click **Protection > Threat Analysis > Network Threats**.
2. In the text field, type the destination IP address, FQDN, or URL.
3. Click **Analyze**.

Configure the access control list

CylanceGATEWAY evaluates existing connections to a destination every five minutes. On evaluation, CylanceGATEWAY reapplies the ACL rules, and the established connection might be disconnected, if required. This can occur if, for example, the users' risk level has changed, or the destination reputation has been updated since the connection was established.

Before you begin: Ensure that you have defined your private network according to your organization's needs. For instructions, see [Define your private network](#).

1. In the management console, on the menu bar, click **Settings > Network**.
2. Click the **Access Control List** tab.
3. If you see a notification that a draft set of rules is in progress, click the **Draft Rules** tab.
If you do not have a draft set of rules in progress, any update you make creates a draft set of rules.
4. Perform any of the following actions:
 - To search for a rule or drafted rule, click  and select one or more predefined scopes, a condition, and specify the criteria. Click the rule that you want to view the settings for. Click  to reset the search. For more information on searching, see [Searching ACL rules and Network Services](#).
 - To add a new rule to the end of the list, click **Add Rule**.

- To add a new rule above or below an existing rule, click ... in the row for the existing rule and select **Add rule above** or **Add rule below**.
 - To copy a rule and add it above or below an existing rule, click ... in the row for the existing rule and select **Copy rule above** or **Copy rule below**.
 - To edit an existing rule, click the name of the rule.
 - To disable a rule, click  in the row for the rule.
 - To enable a rule, click  in the row for the rule.
 - To delete a rule, click ... in the row for the rule and select **Delete rule**.
 - To change the order of the rules, click **Order** and use the arrows to move rules up or down in the list.
 - To add a rule to allow traffic to a blocked malicious destination in the event that users require access (for example, users that perform threat research), click **Add rule** with the following settings. This rule must be ordered before other rules that allow access to a destination.
 - Action: Allow
 - Check access attempts against Network Protection check box: Clear the check box.
 - Target: Matches any. Add the destination address.
 - Users or groups: Matches any. Add the users or groups that require access to the destination.
5. If you chose to add or edit a rule, specify the [ACL rule parameters](#) and click **Save**.
6. Click **Commit rules** to apply your changes to the ACL.
- You can also leave the page and return to the draft rules later. When you commit a draft ACL, all other administrators with a draft rule list are prompted to discard their out-of-date draft.

Configuring network protection

You can configure how CylanceGATEWAY detects and reacts to threats in various ways. When you configure your [access control list \(ACL\) rules](#) to allow access to destinations, CylanceGATEWAY can still block the user from accessing the destination if a potential threat is identified. You can also control the information that can be displayed in the Network Events screen and Alerts view and what is sent to the SIEM solution or syslog server, if configured. To enable the additional network protection, ensure that each ACL rule also has the "Check addresses against Network Protection" parameter selected. This setting is enabled by default.

- **Signature detection:** You can use signature detection to enable deep network threat detection using the network connection's signatures. When signature detection is enabled, CylanceGATEWAY automatically blocks connections where threats are detected if the ACL rule matches the destination and checks the network protection. When signature detection is disabled, threats are logged but the connection is not blocked. For more information on a list of detections and their actions, see [viewing network activity](#). Signature detection is enabled by default.
- **Destination protection:** You can use destination reputation to block potentially malicious IP addresses and FQDNs that match the risk level that you specify (low, medium, or high). When enabled, the default risk level is high. CylanceGATEWAY logs and automatically blocks connections to the destinations that match the set risk level when the destination matches the ACL rule and checks the network protection. When destination protection is disabled, threats are logged but the connection is not blocked. For more information on a list of detections and their actions, see [viewing network activity](#). Destination reputation is enabled by default.

Risk levels use a combination of machine learning (ML) models and static IP reputation database to determine if a destination might contain potential threats.

- **ML models:** The ML models assign a confidence level to destinations that your users might access. ML models continuously learn whether a destination might contain potential threats.
- **IP reputation databases:** The IP reputation database provides a confidence level to IP addresses from open and commercial IP reputation feeds. CylanceGATEWAY references the reputation feeds to determine

the risk level of an IP address. CylanceGATEWAY considers the number of vendors that have convicted a specific destination and the dependability of the sources before it assigns a risk level (for example, if the majority of sources and IP reputation engines identify a destination to contain potential threats, CylanceGATEWAY will assign the destination a risk level of high. For more information on the risk levels, see [Destination reputation risk threshold](#).

CylanceGATEWAY automatically applies the Dynamic Risk category and a subcategory to IP Reputation detections that have been identified to possibly contain malicious threats using a combination of ML models and IP Reputation database. The databases continuously change to add or remove destination entries. You can view additional metadata and details for network events categorized as Dynamic Risk on the Network Events screen. The Dynamic Risk category includes the following subcategories:

- | | | |
|-----------------------|-----------------------|-------------------------------------|
| • Beacon | • Malware | • Suspicious Website |
| • Command and control | • Phishing | • Domain Generation Algorithm (DGA) |
| • DNS Tunneling | • Potentially Harmful | |

Destination reputation risk threshold

You can specify whether CylanceGATEWAY should block network access to potentially malicious destinations based on the minimum threshold that you set.

| Item | Description |
|--------|--|
| High | This risk category indicates that there is a greater than 80% confidence that the destination is harmful or malicious. |
| Medium | This risk category indicates a 60-80% confidence that the destination might be a cyber threat. |
| Low | This risk category indicates a 50-60% confidence that the destination is suspicious or contain potential threats. |

Configure network protection settings

You can specify the detections that you want to enable and display on the Network Events screen, as well as the information that is sent to the SIEM solution or syslog server. You can also configure CylanceGATEWAY to display a message to users whenever CylanceGATEWAY blocks a connection to a potentially malicious destination. For information on the available risk levels, see [Destination reputation risk threshold](#). When you configure network protection settings, CylanceGATEWAY will generate alerts that are displayed in the Alerts view. For more information, see [Managing alerts across Cylance Endpoint Security services](#).

Before you begin: Verify that "Check access attempts against Network Protection" is selected for each ACL rule. For more information on ACLs, see [Controlling network access](#).

1. On the menu bar, click **Settings > Network**.
2. Click the **Network Protection** tab.
3. Do any of the following:

| Task | Steps |
|--|---|
| Specify the detections that you want to enable and whether to notify users when they are blocked due to detections. | <ol style="list-style-type: none"> Click the Protect tab. If you want users to see a message when CylanceGATEWAY blocks a connection, select Display a blocked notification message on devices. In the Message field, type the message that you want to display to users. To turn on signature detection, select Enable signature detection. When enabled, alerts are generated for blocked signature detections and display in the Alerts view. When disabled, alerts are not generated. For more information, see Managing alerts across Cylance Endpoint Security services. To turn on destination reputation, select Enable destination reputation and select the minimum risk level of potentially malicious IP addresses and FQDNs to block. When enabled, alerts are generated and displayed in the Alerts view based on the risk level that you have set. For example, if you select the risk level of "Medium and higher", alerts that are medium or high risk will display in the Alerts view. When disabled, alerts that CylanceGATEWAY considers high risk will be generated and displayed in the Alerts view by default. |
| <p>Specify and control the detections to display in the Network Events screen.</p> <p>Note: If you enable Traffic privacy and the network access attempts match the ACL rule, the network access attempts are not displayed in the Network Events screen.</p> | <ol style="list-style-type: none"> Click the Report tab. To display the signature detections for network events that are allowed, enable Display allowed signature detection events. By default, signature detections that are blocked automatically are displayed in the Network Events screen. To display destination reputation detections for network events that are allowed, enable Display allowed destination reputation events and select the minimum risk level of potentially malicious IP addresses to display. If this option is disabled, signature events will be captured as normal allowed traffic. To display DNS tunneling detections, enable Display DNS tunneling detections and select the minimum risk level of potential threats based on analysis of the DNS traffic from the client to the DNS server. By default, the risk level is Medium. To display Zero Day detections, enable Display Zero Day detections and select the minimum risk level of newly identified malicious destinations that have not been identified previously. By default, the risk level is Medium. |

| Task | Steps |
|---|---|
| Specify and control the detections to display in the Alerts view and to send to the SIEM solution or syslog server, if configured. Note: If you enable Traffic privacy and the network access attempts match the ACL rule, the network access attempts are not sent to the SIEM solution or syslog server, if configured. | <ol style="list-style-type: none"> Click the Share tab. To send allowed or blocked network events and alerts that have signature detections, enable Share signature detection events. When enabled, the blocked signature detections are displayed in the Alerts view and sent to the SIEM solution or syslog server, by default. Optionally, select Allowed events to send allowed events. To send network events and alerts that have destination reputation detections and were allowed based on the minimum risk level that you set or blocked, enable Share destination reputation events. When enabled, destination reputation events that are blocked are displayed in the Alerts view and sent to the SIEM solution or syslog server, by default. Optionally, select Allowed events to send allowed events. To send network events and alerts that have DNS tunneling detections based on the minimum risk level that you set, select Share DNS tunneling detections. By default, the risk level is Medium. To send network events and alerts that have Zero Day detections based on the minimum risk level that you set, select Share Zero Day detections. By default, the risk level is Medium. To send network events that are blocked by ACL rules, enable Share blocked ACL events. Blocked and allowed ACL events are not displayed in the Alerts view. |

4. Click **Save**.

Searching ACL rules and Network Services

You can search the ACL rules and Network Services that you have added to CylanceGATEWAY. CylanceGATEWAY provides predefined scopes and conditions for your search criteria.

A search looks at the criteria that you specify for a scope and condition in the search field to return the search results. For example, if you search the ACL rules for a rule that includes 'IT' in the name (for example, Scope = Name, Condition = Contains, and the Search criteria = IT), all of the rules that include the specified 'IT' in the rule name are returned.

Note: You can perform a search of the committed ACL rules or perform a search of the drafted ACL rules. A search does not span the committed and draft ACL rules.

In advanced searches, when multiple scopes and search criteria are specified, the search engine uses an AND operator between the search criteria. All search results will contain all of the criteria that is specified. For example, if you perform a search of the network services for a service with the name 'example' and a FQDN of example.com (for example, Scope = Name, Condition = Contains, Search criteria = Example and Scope = FQDN, Condition = Contains, Search criteria = example.com), all of the rules that include both criteria are returned.

The search is not case-sensitive. For example, searching for Example or example, produces the same results.

Using source IP pinning

CylanceGATEWAY allows you to obtain dedicated IP addresses that you can use for source IP pinning. Many SaaS applications allow source IP pinning as a way to limit access only to connections from a specific range of trusted IP addresses. Your organization may already use this method to limit access to a SaaS application tenant

to the IP address used by devices connected to your organization's network. For users working remotely, this means you can secure access between your users and cloud-based applications using source IP pinning without requiring them to use your organization's VPN, which can reduce the traffic on your network and improve connections for users.

If you have enabled source IP pinning for CylanceGATEWAY, the Source IP Pinning network settings display the IP addresses that BlackBerry has allocated for use only by your organization.

To obtain dedicated IP addresses, visit support.blackberry.com/community to read article 96499.

To view your allocated IP addresses, on the menu bar, click **Settings > Network**, and then select the **Source IP Pinning** tab.

Configuring the Gateway service options

You configure Gateway Service policies to specify OS-specific options that control how apps can or cannot use the tunnel, specify whether users can access destinations with poor reputations, and have users verify their identity before they can establish a tunnel.

Gateway Service policy parameters


If you are configuring CylanceGATEWAY on devices that are activated with an EMM solution such as BlackBerry UEM, you can also [specify options in your EMM solution](#) that control how CylanceGATEWAY works on devices.

| Item | Description |
|--|---|
| General information | |
| Name | This is a name for the rule. |
| Description | This is a brief description of the purpose for the rule. |
| Agent Configuration | |
| Allow Gateway to run only if the device is managed by BlackBerry UEM or Microsoft Intune | <p>This setting specifies that iOS, Android, or Chromebook devices must be managed by BlackBerry UEM or Microsoft Intune before users can use CylanceGATEWAY.</p> <p>This feature requires one of the following:</p> <ul style="list-style-type: none">• BlackBerry UEM: The BlackBerry UEM connector is added to the Cylance Endpoint Security tenant and apps are sent from BlackBerry UEM.• Intune: The Microsoft Intune connector is added to the Cylance Endpoint Security tenant and you create app configuration policies that define the device types and Intune user groups that the integration applies to. <p>For more information, see Connecting Cylance Endpoint Security to MDM solutions to verify whether devices are managed</p> |
| Allow Gateway to run only if the device is managed by Microsoft Intune | <p>This setting specifies that Windows devices must be managed by Microsoft Intune and is Entra ID joined before users can use CylanceGATEWAY. For more information, see Connecting Cylance Endpoint Security to MDM solutions to verify whether devices are managed and complete the Intune tasks.</p> <p>This feature is supported on CylanceGATEWAY agent for Windows version 2.10 or later.</p> |

| Item | Description |
|---|--|
| Allow Gateway to establish tunnels only on MDM managed devices where Gateway is configured as the managed VPN | <p>You can require that a device be enrolled in Mobile Device Management (MDM) for your organization with CylanceGATEWAY configured as a VPN provider before CylanceGATEWAY Work Mode will create a tunnel on that device.</p> <p>This feature is supported on the following devices:</p> <ul style="list-style-type: none"> • CylanceGATEWAY agent for macOS 2.7 or later • CylancePROTECT Mobile app for iOS 2.14 or later |
| Allow Gateway to run only if CylancePROTECT Desktop is also activated on the device | <p>This setting requires that users have CylancePROTECT Desktop installed and activated from the same tenant. This feature is supported on the following devices:</p> <ul style="list-style-type: none"> • Windows devices that are running CylanceGATEWAY for Windows • macOS devices that are running CylancePROTECT Desktop 3.0 or later and CylanceGATEWAY for macOS 2.0.17 or later. If you enable this feature for devices that are running a version of CylancePROTECT Desktop earlier than 3.0, the tunnel may not function as expected. |

| Item | Description |
|-----------|--|
| Safe Mode | <p data-bbox="493 268 1458 554">You can enable Safe Mode for your users. With Safe Mode, CylanceGATEWAY blocks apps and users from accessing potentially malicious destinations and enforces an acceptable use policy (AUP) by intercepting DNS requests. The CylanceGATEWAY cloud services evaluate each DNS query against the configured ACL rules and network protection settings (for example DNS Tunneling and Zero Day Detections such as DGA, Phishing, and Malware), and then instructs the agent to allow or block the request in real time. If allowed, the DNS request completes normally over the bearer network. Otherwise, the CylanceGATEWAY agent overrides the normal response to prevent access.</p> <p data-bbox="493 573 1463 730">When enabled, Safe Mode automatically takes effect when Work Mode is disabled. When enabled for Windows devices, the agent is minimized in the system tray when it launches. Enabling Safe Mode does not prevent users from opening the agent and enabling or disabling Work Mode (if the users' policy allows such operations).</p> <p data-bbox="493 749 1446 808">Safe Mode events appear in the CylanceGATEWAY Events screen and Alerts view and are sent to the SIEM solution or syslog server, if configured.</p> <p data-bbox="493 827 1438 953">Note: When enabled, Safe Mode will protect all DNS traffic that does not use the CylanceGATEWAY tunnel (for example, allow Gateway to establish tunnels only on MDM managed devices where Gateway is configured as the managed VPN, per-app tunnel, split tunneling).</p> <p data-bbox="493 972 1084 999">This feature is supported on the following devices:</p> <ul data-bbox="493 1018 1114 1083" style="list-style-type: none"> • CylanceGATEWAY agent for Windows 2.8 or later. • CylanceGATEWAY agent for macOS 2.7 or later. <p data-bbox="493 1102 1463 1194">Note: This feature is not supported in environments that use secure DNS with DoT (DNS-over-TLS) and DoH (DNS-over-HTTPS) protocols. DNS queries sent using DoT or DoH cannot be viewed by CylanceGATEWAY.</p> <p data-bbox="493 1213 1430 1530">Safe Mode and CylanceGATEWAY agent for macOS: On macOS, the CylanceGATEWAY agent uses a system extension to implement Safe Mode. If you add the "P7E3XMAM8G:com.blackberry.big3.gatewayfilter" system extension to an allowed list, it can load automatically without user interaction when the CylanceGATEWAY agent is activated. Otherwise, instruct your users to allow the CylanceGATEWAY system extension when they are prompted during activation. For information on how to add a system extension to an allowed list, see your macOS documentation. For more instructions on how to activate the CylanceGATEWAY agent to use Safe Mode, see Activate Safe Mode in the CylanceGATEWAY agent in the user guide.</p> <p data-bbox="493 1549 1458 1766">Safe Mode and third-party VPNs: If your environment is configured to use Safe Mode and a third-party VPN, you must review and, if necessary, adjust the VPN DNS settings to ensure that the DNS settings only route the DNS queries for traffic that is defined to use the VPN tunnel. If you enable Safe Mode and the VPN DNS settings are not reviewed, the VPN may not work as expected. By default, the configuration for many VPNs is to route all DNS traffic through the VPN tunnel when active.</p> |

| Item | Description |
|---|---|
| Enforce the "Start CylanceGATEWAY when I sign in" setting | <p>This setting specifies whether to force the CylanceGATEWAY agent on macOS or Windows devices to start automatically when users log in. This policy setting overrides the "Start CylanceGATEWAY when I sign in" setting in the agent.</p> <p>BlackBerry recommends that you enable this option in the Gateway Service policy.</p> <p>This feature is supported on the following devices:</p> <ul style="list-style-type: none"> • CylanceGATEWAY agent for macOS 2.7 or later • CylanceGATEWAY agent for Windows 2.7 or later |
| Automatically start CylanceGATEWAY when user signs in | <p>This setting starts the CylanceGATEWAY agent automatically when users sign in to the device, but users can still stop the agent manually. When you enable both this setting and "Enable Work Mode Automatically" for Windows devices, the agent is minimized in the system tray when it launches.</p> <p>This setting is only valid if the "Enforce the Start CylanceGATEWAY when I sign in" setting is enabled.</p> |
| Enforce the 'Enable Work Mode Automatically' setting | <p>This setting specifies whether to force the CylanceGATEWAY agent on macOS or Windows devices to enable Work Mode automatically when the agent starts. This policy setting overrides the "Enable Work Mode Automatically" setting in the agent.</p> <p>This feature is supported on the following devices:</p> <ul style="list-style-type: none"> • CylanceGATEWAY agent for macOS 2.7 or later. • CylanceGATEWAY agent for Windows 2.7 or later |
| Enable Work Mode Automatically | <p>This setting enables Work Mode automatically when the CylanceGATEWAY agent starts, but users can still manually enable and disable Work Mode after the agent starts. When you enable both this setting and "Automatically start CylanceGATEWAY when user signs in" for Windows devices, the agent is minimized in the system tray when it launches.</p> <p>This setting is only valid if the "Enforce the Enable Work Mode Automatically setting" is enabled.</p> |
| Tunnel Use | |

| Item | Description |
|------------------------------|---|
| Per-app tunnel | <p>This setting specifies which apps can send data through the tunnel to the CylanceGATEWAY cloud services. You can configure per-app tunnel with either an Allowed apps or Restricted apps list. For example, if you select the Allowed apps option and specify apps that can use the tunnel, and then change the option to Restricted apps, the listed apps cannot use the tunnel.</p> <p>Possible options:</p> <ul style="list-style-type: none"> • Select Allowed apps to specify the apps that use the tunnel. No other apps can use the tunnel. System apps and Windows DNS always use the tunnel. If you select this option, any set ACL rules or network access control policies are applied. For more information on ACL rules and network access control policies, see Controlling network access. • Select Restricted apps to specify the apps that cannot use the tunnel. All other apps can use the tunnel. • Click  and enter the full path or include a wildcard in the path for desktop apps or add the Windows Package Family Name (PFN) for store apps. You can specify a combined maximum of 200 app paths or PFNs. <p>When you include a wildcard in the path, consider the following:</p> <ul style="list-style-type: none"> • You can include only one wildcard per path. The supported format is <code>*</code> (for example, <code>%ProgramFiles%\Folder_Name*Application_Name.exe</code>) • Wildcards are not supported in the following instances: <ul style="list-style-type: none"> • Used in place of environment variables • Used in place of root directories in the path • Used for partial directory names (for example, <code>"C:\Win*\notepad.exe"</code>) • Used in executable names (for example, <code>"C:\Windows*.exe"</code>) <p>Wildcards are supported on Windows devices that are running CylanceGATEWAY agent for Windows 2.7 or later.</p> <p>This feature is supported on the following devices:</p> <ul style="list-style-type: none"> • CylanceGATEWAY for Windows 2.0.0.13 or later. • Android or Chromebook device users that are running the CylancePROTECT Mobile app. |
| Force apps to use the tunnel | <p>This setting requires all non-loopback connections to use the tunnel. If you select this option and have split tunneling enabled, all traffic will use the tunnel. On Windows devices, if you select this option and have split tunneling enabled, connections that don't use the tunnel may not function as expected. This feature is supported on the following devices:</p> <ul style="list-style-type: none"> • Unmanaged macOS devices that are running macOS 10.15 or later and CylanceGATEWAY for macOS 2.0.17 or later. • Unmanaged iOS devices that are running iOS 14.0 or later and CylancePROTECT Mobile app 2.4.0.1731 or later. • Windows devices that are running CylanceGATEWAY for Windows |

| Item | Description |
|---|---|
| Allow apps to use the local network | <p>This setting allows the apps that are forced to use the tunnel to reach local network destinations. This feature is supported on the following devices:</p> <ul style="list-style-type: none"> • Unmanaged macOS devices that are running macOS 10.15 or later and CylanceGATEWAY for macOS 2.0.17 or later. • Unmanaged iOS devices that are running iOS 14.2 or later and CylancePROTECT Mobile app 2.4.0.1731 or later. • Windows devices that are running CylanceGATEWAY for Windows 2.5 or later. <p>This setting is only valid if "Force apps to use the tunnel" is enabled.</p> |
| Block network traffic from restricted apps | <p>This setting prevents all non-loopback network connections from apps that cannot use the tunnel. If you do not select this setting, the restricted apps can use the default network connection. This feature is supported on devices that are running the CylanceGATEWAY for Windows agent.</p> |
| Allow other Windows users to use the tunnel | <p>This setting allows all users that use the same Windows device to use the tunnel. If you select this option, any per-app tunnel criteria applies. If you do not select this option, apps run by other Windows users are treated as restricted apps.</p> |
| Allow incoming connections | <p>This setting allows incoming TCP connections and UDP flows from non-tunnel, non-loopback interfaces. CylanceGATEWAY never routes incoming connections through the tunnel. This feature is supported on devices that are running the CylanceGATEWAY for Windows agent.</p> |
| Tunnel reauthentication | |
| Tunnel reauthentication | <p>This setting specifies how frequently users must authenticate before they establish a tunnel.</p> <p>When you enable this feature, BlackBerry recommends that you set the "Allow authentication reuse" option to specify the period after which users need to authenticate again.</p> <p>This feature is supported on the following devices:</p> <ul style="list-style-type: none"> • CylanceGATEWAY for macOS 2.5 or later. • CylanceGATEWAY for Windows 2.5 or later. |
| Allow authentication reuse | <p>When enabled, this setting specifies a reuse period after which users who have authenticated and established a tunnel are required to authenticate again. The reuse period can be set between 5 minutes and 365 days from their last authentication. For example, if you set the reset period to 10 days, users must authenticate again 10 days after their first authentication before they can establish a tunnel. By default, this setting is disabled.</p> <p>Note: If you do not enable the Allow authentication reuse and specify a reuse period, users must authenticate each time they establish a tunnel.</p> <p>This setting is only valid if "Tunnel reauthentication" is enabled.</p> |

| Item | Description |
|------------------------|---|
| Grace period | <p>This setting allows users to reconnect to the tunnel without authenticating if the connection to the tunnel is established within 2 minutes of the connection being disconnected. By default, this option is enabled when you turn on tunnel reauthentication.</p> <p>This setting is only valid if "Tunnel reauthentication" is enabled.</p> |
| Split tunneling | |
| Split tunneling | <p>This setting allows traffic to public destinations to bypass CylanceGATEWAY. You can specify whether the destination must use the tunnel or cannot use the tunnel using the following options:</p> <ul style="list-style-type: none"> Inclusive: You can type the CIDRs and FQDNs for destinations that must route through the tunnel. For enhanced user experience, the management console periodically refreshes the FQDN to IP address resolution. <p>Note: FQDN addresses do not support wildcards.</p> <ul style="list-style-type: none"> Exclusive: You can type the CIDRs for destinations that you do not want to use the tunnel. You can use this option when you only have a few destinations that you want to exclude from using the tunnel, all other network traffic will use the tunnel. FQDNs are not supported. <p>Important: If you have configured both options, only the option that is selected and displayed is applied to the network traffic, but all settings are retained to allow you to easily change between the options.</p> <p>If you enable split tunneling, connections to allowed public destinations bypass the tunnel and the CylanceGATEWAY cloud services unless you specify that connections to the destination must use the tunnel. If you enable split tunneling and do not enable split DNS, all DNS queries are evaluated against the configured ACL rules and network access controls are applied before traffic is routed to the public destination. If you are using source IP pinning, all destinations configured for source IP pinning must use the tunnel.</p> <p>If you make changes to tunneling settings or incoming connections, users must disable and then enable Work Mode in the CylanceGATEWAY agent installed on Windows and macOS devices or in the CylancePROTECT Mobile app on iOS, Android, and 64-bit Chromebook devices for the changes to take effect.</p> |
| Split DNS | <p>When enabled, this setting allows DNS lookups for the domains that are listed in the Private Network > DNS > Forward Lookup Zone configuration to be completed through the tunnel where network access controls are applied. All other DNS lookups are completed using local DNS. If you enabled Safe Mode, DNS traffic that does not use the Gateway tunnel is protected by Safe Mode. Split DNS is disabled by default.</p> <p>Android and 64-bit Chromebook devices do not support split DNS tunneling and will use the tunnel where access controls are applied.</p> <p>This setting is only valid if "Split Tunneling" is enabled.</p> |

Configure Gateway service options

1. On the menu bar, click **Policies > User Policy**.

2. Click the **Gateway Service** tab.
3. Click **Add Policy**.
4. Specify the [Gateway Service policy parameters](#).
5. Click **Add**.
6. If you made changes to the tunneling settings or incoming connections, make sure that users disable and then enable work mode in the CylanceGATEWAY agent installed on Windows and macOS devices or in the CylancePROTECT Mobile app on iOS, Android and Chromebook devices for the changes to take effect.

After you finish:

- [Assign the policy to users and groups](#)
- If necessary, [rank the policies](#)

Specifying how devices activated with an EMM solution use the CylanceGATEWAY tunnel

CylanceGATEWAY is a cloud-native, artificial intelligence (AI) assisted zero trust network access (ZTNA) solution. When CylanceGATEWAY is enabled on a device, the device recognizes CylanceGATEWAY as a VPN provider that establishes a zero trust network access profile. If you have activated devices using BlackBerry UEM or another EMM solution, the VPN options you set in your EMM solution can affect how CylanceGATEWAY works on the device.

For iOS devices, you can use your BlackBerry UEM or another EMM solution to set up per-app VPN to designate which apps send data through the CylanceGATEWAY tunnel. Devices must be activated to allow VPN management and app management. For more information, see the following:

- [Specify which apps use CylanceGATEWAY on iOS devices](#)
- [Specify which apps use CylanceGATEWAY on iOS devices in a Microsoft Intune environment](#)

For Android devices, you can use BlackBerry UEM or another EMM solution to force CylanceGATEWAY to always be enabled and to prevent users from changing the VPN configuration in the work profile. For more information, see the following:

- [Specify CylanceGATEWAY options on Android Enterprise devices](#)
- [Specify CylanceGATEWAY options on Android Enterprise devices in your Microsoft Intune environment](#)

Specify which apps use CylanceGATEWAY on iOS devices

For iOS devices, if your organization manages devices using an EMM solution that supports configuring per-app VPN, you can configure devices to recognize CylanceGATEWAY as a VPN provider and configure per-app VPN to specify which apps send data through the CylanceGATEWAY tunnel.

To set up per-app tunnel options, you must have permissions for VPN management and app management on iOS devices activated using your EMM solution. To specify which apps use the CylanceGATEWAY tunnel in BlackBerry UEM perform the following steps:

1. In the UEM management console, [add the apps](#) that you want to send data through CylanceGATEWAY to UEM and assign them to users.

Only apps that are assigned to users use the CylanceGATEWAY tunnel. Do not assign the default browser or the CylancePROTECT Mobile app to users or the device will be unable to establish a tunnel with CylanceGATEWAY.

For devices with the "User privacy" and "User privacy - User enrollment" activation types, only assigned [internal apps](#) and apps licensed through the [Apple Volume Purchase Program](#) use the tunnel.

2. Create an [activation profile](#) that assigns one of the following [activation types](#):
 - MDM controls
 - User privacy - User enrollment

- User privacy with VPN management and app management enabled

3. Create a [VPN profile](#) and include the following [settings](#):

| Setting | Description |
|-------------------------------------|---|
| Connection type | Custom |
| VPN bundle ID | com.blackberry.protect |
| Server | This setting specifies the FQDN or IP address of a VPN server. The value must be 127.0.0.1. |
| Authentication type | Password |
| Password | Leave this field blank |
| Enable per-app VPN | Selected |
| Domain settings | Specify the domains that can establish a connection through the CylanceGATEWAY tunnel. If you specify a domain, assigned apps use the tunnel only for connections to the specified domain. You can specify domains for Safari, Calendar, Contacts, Mail, and domains listed in the apple-app-site-association file . You can also specify domains that never use the tunnel. For devices with the "User privacy" and "User privacy - User enrollment" activation types, if you specify a domain that is not a child of the root domain specified in the Server field, the device ignores the entire VPN profile, not just the invalid domain. |
| Allow apps to connect automatically | Select this option to specify that the app can start the connection automatically. Note: Connections through the CylanceGATEWAY tunnel can start only if CylanceGATEWAY is enabled in the CylancePROTECT Mobile app on the device. |
| Traffic tunneling | IP layer |

4. Assign profiles to users and instruct them to activate devices.

Specify which apps use CylanceGATEWAY on iOS devices in a Microsoft Intune environment

You can configure iOS devices to recognize CylanceGATEWAY as a VPN provider and configure per-app VPN to specify which apps send data through the CylanceGATEWAY tunnel. In Microsoft Intune, you can configure settings that affect CylanceGATEWAY.

To set up per-app tunnel options, you must have permissions for VPN management and app management on iOS devices that are activated using Intune. To specify which apps use the CylanceGATEWAY tunnel in Intune, perform the following steps:

1. In the Microsoft Intune admin center, [add the apps](#) that you want to send through CylanceGATEWAY to Intune and assign them to users.

Only apps that are assigned to users use the CylanceGATEWAY tunnel. Do not assign the default browser or the CylancePROTECT Mobile app to users or the device will be unable to establish a tunnel with CylanceGATEWAY.

2. Create a [VPN profile](#) and include the following settings. For more information on the iOS and iPadOS settings, see [Add VPN settings on iOS and iPadOS devices](#).

| Setting | Description |
|-----------------------|--|
| Connection type | Custom VPN |
| VPN server address | The value must be 127.0.0.1. This value is not used by CylanceGATEWAY. |
| Authentication Method | Username & Password |
| Split tunneling | Disable |
| VPN identifier | For iOS devices, enter com.blackberry.protect For macOS devices, enter com.blackberry.big |
| | <ul style="list-style-type: none"> • Key: <i>key</i> • Value: <i>value</i> <p>Microsoft Intune requires one custom attribute. CylanceGATEWAY does not use this setting. You can enter any attribute.</p> |
| Automatic VPN | Per-app VPN |
| Provider Type | Packet-tunnel |
| Safari URLs | <p>Specify the domains that can establish a connection through the CylanceGATEWAY tunnel. Intune does not support wildcards in domains, they are implied. For example, if you enter "org", implies "*.org".</p> <p>Note: Connections through the CylanceGATEWAY tunnel can start only if CylanceGATEWAY is enabled in the CylancePROTECT Mobile app on the device.</p> <p>If you specify blackberry.com as a managed Safari VPN, newly activate CylancePROTECT Mobile apps will be prevented from activating.</p> |

3. If necessary, have users activate the CylancePROTECT Mobile app.

Specify CylanceGATEWAY options on Android Enterprise devices

For Android devices, you can specify which apps send data through the CylanceGATEWAY tunnel using the [CylanceGATEWAY service policy](#). If your organization manages Android Enterprise devices using an EMM solution such as BlackBerry UEM, you can configure settings in your EMM provider that affect CylanceGATEWAY.

You can use the IT policy in BlackBerry UEM to specify whether CylanceGATEWAY is always enabled on devices and whether users can change VPN configurations in the work profile on the device. For more information on UEM IT policy rules, download the [UEM IT Policy Reference](#).

1. In the UEM management console, create or edit an [IT policy](#).
2. Perform one of the following actions:
 - a) To force CylanceGATEWAY to always be enabled, set the following IT policy rules for the Android work profile.

| IT policy rule | Description |
|---|--|
| Force always-on VPN | Selected |
| Use BlackBerry Secure Connect Plus for VPN connection | Not selected |
| VPN app package ID | com.blackberry.protect |
| Force work apps to only use VPN | Not selected. If this option is selected, the CylancePROTECT Mobile app can't be activated on the device. |
| Work apps exempt from VPN | <p>If the "Force work apps to only use VPN" rule is selected,</p> <ul style="list-style-type: none"> • you must enter <code>com.android.chrome</code> to allow the Chrome browser to access the network and activate the CylancePROTECT Mobile app on the device before the VPN is connected. This rule applies to devices running Android OS 10.0.0 or later. • If you enter <code>com.android.protect</code>, the CylancePROTECT Mobile app can access the network without using the VPN only when the VPN is not connected. |

- b) To allow devices to send data through the CylanceGATEWAY tunnel if **Force always-on VPN** is not selected, select **Allow user-configured VPN in workspace**.

If neither **Force always-on VPN** nor **Allow user-configured VPN in workspace** is selected, the device will not allow work apps to send data through the tunnel.

3. Assign the IT policy to users.

Specify CylanceGATEWAY options on Chromebook devices

For 64-bit Chromebook devices, you can specify which apps send data through the CylanceGATEWAY tunnel using the [CylanceGATEWAY service policy](#). If your organization manages Chrome OS Enterprise devices using a Google domain, you can force CylanceGATEWAY to always be enabled and prevent users from changing the VPN configuration in the CylancePROTECT Mobile app. For instructions, visit <https://support.google.com/> and read "Set up virtual private networks (Android VPN app)". You can also extend the management of Chromebook Enterprise devices to your EMM provider such as BlackBerry UEM. For more information, see [Extending the management of Chrome OS devices to BlackBerry UEM](#).

Specify CylanceGATEWAY options on Android Enterprise devices in your Microsoft Intune environment

For Android devices, you can specify which apps send data through the CylanceGATEWAY tunnel using the Gateway policy. In Microsoft Intune, you can configure settings that affect CylanceGATEWAY.

You can use the configuration profile to specify whether CylanceGATEWAY is always enabled on devices and whether users can change VPN configurations in the profile on the device. For more information on the configuration profile settings, see [Android Enterprise device settings to configure VPN](#).

1. In the Microsoft Intune admin center, create a [configuration profile](#). Set the following settings:
 - Platform: Android Enterprise
 - Profile type: Device restrictions
2. Set the following rules for the configuration profile.

| Setting | Description |
|---------------|---|
| Always-on VPN | Enable |
| VPN Client | Custom |
| Package ID | com.blackberry.protect |
| LockDown mode | Not configured. If this option is selected, the CylancePROTECT Mobile app might not activate. |

3. Assign the configuration profile to users.
4. Assign the CylancePROTECT Mobile app to users.

Connecting Cylance Endpoint Security to MDM solutions to verify whether devices are managed

You can connect Cylance Endpoint Security to BlackBerry UEM or Microsoft Intune so that Cylance Endpoint Security can verify whether iOS and Android devices are managed. Cylance Endpoint Security can also verify whether Windows devices are Intune managed.

After you establish the connection to UEM, you configure the iOS and Android devices, users, and groups that the integration applies to. For UEM, you ensure users are activated with a supported activation type and manage the distribution of the CylancePROTECT Mobile app using the user and group management features available in the UEM management console.

Note that all BlackBerry UEM managed devices that you want to use this feature must have the CylancePROTECT Mobile app deployed from the BlackBerry UEM instance.

For Intune integration, when you connect Cylance Endpoint Security to Intune, you create app configuration policies that define the device types and Intune user groups that the integration applies to. Note that all Intune managed devices that you want to use this feature must be included in an app configuration policy in the Cylance console through Assests > User Groups.

In the Cylance console, you create and assign the Gateway Service policy that allows Gateway to run only if the device is managed by BlackBerry UEM or Intune. When the user tries to access a network destination on an MDM-managed device, if the destination is allowed the network traffic is sent through the secure tunnel.

To connect Cylance Endpoint Security to BlackBerry UEM, perform the following actions.

| Step | Action |
|------|--|
| 1 | Review the prerequisites . |
| 2 | Link to your company directory. <ul style="list-style-type: none"> • In Cylance Endpoint Security, see Linking to your company directory. • In BlackBerry UEM, see Connecting to your company directories. |

| Step | Action |
|------|--|
| 3 | Install and configure the BlackBerry Connectivity Node. <ul style="list-style-type: none"> • In Cylance Endpoint Security, see Installing or upgrading the BlackBerry Connectivity Node. • In BlackBerry UEM, see Install a BlackBerry Connectivity Node instance. |
| 4 | Add a BlackBerry UEM connector. |
| 5 | Use BlackBerry UEM to install the CylancePROTECT Mobile app on devices. |

To connect Cylance Endpoint Security to Intune, perform the following actions:

| Step | Action |
|------|--|
| 1 | Review the prerequisites . |
| 2 | Connect Cylance Endpoint Security to Intune. |

Prerequisites: Verifying that devices are MDM managed

BlackBerry UEM

- BlackBerry UEM Cloud or UEM on-premises version 12.15 or later is supported.
- Make sure that you have a valid BlackBerry UEM SRP ID and Authentication key for your BlackBerry UEM Cloud and BlackBerry UEM instances. You can view the SRP IDs and authentication keys for your UEM instances in your *myAccount*, under Organization > Services > UEM.
- Your organization's Cylance Endpoint Security tenant and UEM domain must have the same organization ID.
- For BlackBerry UEM on-premises environments, you must allow connections from BlackBerry UEM Connector. If you do not allow connections from the BlackBerry UEM Connector, when you try to save your tenant information, the error message "The UEM connection request is invalid" displays and you cannot save the information. For instructions on how to enable the BlackBerry UEM connector, visit support.blackberry.com/community to read article 97480. By default, this is enabled in BlackBerry UEM Cloud environments.
- Users' accounts must use the same Active Directory or Entra ID accounts on the Cylance console.
- Cylance Endpoint Security supports a connection to one UEM domain.
- You must [Use BlackBerry UEM to install the CylancePROTECT Mobile app on devices](#). The app must be distributed from UEM because it requires app configurations that are not present if users download and install the app from the App Store or Google Play.
- For iOS devices prerequisites, see [Prerequisites: Verifying that iOS devices are managed by UEM](#).
- For Android devices prerequisites, see [Prerequisites: Verifying that Android devices are managed by UEM](#).

Microsoft Intune

- The Cylance Endpoint Security administrator account that you use to connect to Intune must have an [Intune license](#).
- Cylance Endpoint Security supports a connection to one Intune instance.

- All Intune-managed devices that you want to use this feature must be included in an app configuration policy in the Cylance console. For more information, see [Connect Cylance Endpoint Security to Intune](#).
- For iOS and Android devices, the user account must use the same Active Directory or Entra ID account on the Cylance console.
- For Windows devices, user accounts must be Entra ID joined and from the same directory in the same domain for Windows Intune endpoints. Visit learn.microsoft.com to find more information about Entra joined devices.

Prerequisites: Verifying that iOS devices are managed by UEM

The iOS devices must be activated using one of the following activation types*:

- MDM Controls
- User Privacy
- User Privacy - User enrollment

If your users are activated with the User privacy activation type, complete one of the following tasks:

| Task | Steps |
|---|--|
| Use Cylance Endpoint Security to manage the per-app VPN | <ol style="list-style-type: none"> 1. In the user privacy activation type, clear the Allow VPN Management checkbox and select the Allow app management checkbox. 2. In the Cylance Endpoint Security console, configure the Gateway Service options. |
| Use UEM to manage the per-app VPN | <ol style="list-style-type: none"> 1. In the user privacy activation profile, select the Allow VPN Management and Allow app management checkboxes. 2. Create a custom VPN profile. In the VPN bundle ID field, enter the CylancePROTECT Mobile bundle id, <code>com.blackberry.protect</code>. 3. In the Cylance Endpoint Security console, configure the Gateway Service options. |

* If you want to deactivate a device from the UEM instance, use the "Delete only work data" command to delete work data (for example, the IT policy, profiles, apps, and certificates) that is on the device. If you select the "Remove device" command, the device is removed from your UEM instance, but data and profiles are not removed and the device may continue to receive email and other work data. BlackBerry recommends that you use the "Remove device" command only if a device is irretrievably lost or damaged and is not expected to contact the server again. For more information on commands that you can send to devices, see [Commands for iOS devices](#) in the BlackBerry UEM content.

Prerequisites: Verifying that Android devices are managed by UEM

The Android devices must be activated using one of the following activation types:

- Work and personal - user privacy (Android Enterprise with work profile)
- Work space only (Android Enterprise fully managed device)
- Work and personal - full control (Android Enterprise fully managed device with work profile)
- Work space only (Samsung Knox)
- Work and personal - full control (Samsung Knox)
- Work and personal - user privacy (Samsung Knox)

Add a BlackBerry UEM connector

By default, the Connectors page will display the name, connection type, and connection status for the BlackBerry UEM connector that is currently used in your environment. Your Cylance Endpoint Security tenant supports a connection to one UEM domain.

Before you begin: Review the [prerequisites for BlackBerry UEM connector](#).

1. In the management console, on the menu bar, click **Settings > Connectors**.
2. Click **Add Connector** and select **BlackBerry UEM** from the drop-down list.
3. On the **Tenant Information** screen, enter the BlackBerry UEM tenant SRP ID and Authentication key.
4. Click **Save**.

Use BlackBerry UEM to install the CylancePROTECT Mobile app on devices

You can use UEM to install the CylancePROTECT Mobile app on devices. The app must be distributed from UEM because it requires app configurations that are not present if users download and install the app from the [BlackBerry web site](#), App Store, or Google Play.

Note:

Consider the following feature limitations when you use UEM to install the CylancePROTECT Mobile app on devices:

- For devices with the Android Enterprise user privacy or full control activation types, SMS message scanning is not supported.
- For devices with any Android Enterprise activation type, screen lock detection is not supported.

Before you begin: Review the [Prerequisites: Verifying that devices are MDM managed](#).

1. Follow the instructions in the UEM Administration content to add the CylancePROTECT Mobile app to the app list:
 - [Add an iOS app to the app list](#)
 - [Add an Android app to the app list](#)

Specify the following app configuration settings:

| OS | App configuration settings |
|---------|--|
| iOS | <ul style="list-style-type: none">• App configuration name: <i>name</i>• Key: uemperimeterid• Value: %perimeterid% |
| Android | <p>Name: <i>name</i></p> <p>The following settings are prepopulated:</p> <ul style="list-style-type: none">• User Id: userid• UEM Perimeter Id: %perimeterid% |

2. [Assign the CylancePROTECT Mobile app to users or groups.](#)
3. [Set the disposition of the CylancePROTECT Mobile app to Required.](#)

After you finish:

- Instruct users to activate the CylancePROTECT Mobile app using the information they received in their activation email. Cylance Endpoint Security will send the activation email after you [assign an enrollment policy](#).

- Follow the instructions for [Connecting Cylance Endpoint Security to MDM solutions to verify whether devices are managed](#).

Connect Cylance Endpoint Security to Intune

Before you begin:

The Cylance Endpoint Security administrator account that you use to connect to Intune must have an [Intune license](#).

1. In the management console, on the menu bar, click **Settings > Connectors**.
2. Click **Add Connector** and select **Microsoft Intune** from the drop-down list.
3. Specify your Entra tenant ID. Click **Next**.
4. Specify your administrator credentials for Entra.
5. On the **App Configuration Policies** screen, turn on the OS platforms that you want the Intune integration to apply to and complete the following steps for each platform. Note that all Intune managed devices that you want to use this feature must be included in an app configuration policy. If you want to create app configuration policies later, click **Cancel**.
 - a) Optionally, change the name of the policy. Do not change the target app.
 - b) If you want the policy to apply to all groups from the Intune instance, turn on **All groups**.
 - c) If you want the policy to apply to specific groups from the Intune instance, click **+**. Search for and select groups and click **Add**.
6. Click **Save**. If you added an app configuration policy for Android, follow any administrator consent prompts that display.

The app configuration policies that you create are visible in the Intune admin center.

After you finish: Complete the following tasks only for Intune managed iOS and Android devices.

- Instruct your organization's Intune administrator to edit the CylancePROTECT Mobile MTD connector in the Intune admin center and turn on the following options. To enable the connector, complete the following steps:
 1. Log in to the [Intune admin center](#).
 2. Click **Tenant administration > Connectors and tokens**.
 3. In the **Cross platform** section, click **Mobile Threat Defense**.
 4. Click **Add**.
 5. In the **Select the Mobile Threat Defense connector to setup** dropdown, select **CylancePROTECT Mobile**.
 6. Click **Create**.
- If you want to add app configuration policies at a later time, or if you want to add additional policies, in **Settings > Connectors**, click **Generate App Configuration** for the Intune connection.
- If you also want to connect Cylance Endpoint Security to Intune to manage risk levels of devices, see [Integrating Cylance Endpoint Security with Microsoft Intune to respond to mobile threats](#).

Installing the CylanceGATEWAY agent

The CylanceGATEWAY agent protects users' Windows 10, Windows 11, and macOS devices by allowing you to block connections to Internet destinations that you don't want devices to reach, even when the device isn't connected to your network. BlackBerry maintains an ever-growing list of unsafe Internet destinations that it can block endpoints from connecting to. If your organization also wants to block users from visiting specific sites that don't meet your acceptable use standards, you can create policies to specify additional destinations that all users or specific users or groups cannot access.

The CylanceGATEWAY agent is installed on user's devices, allowing them to access network resources safely and protect their device from suspicious and potentially malicious network activity. When the CylanceGATEWAY agent is installed and Work Mode is enabled, CylanceGATEWAY establishes secure connections between the user's device and your organization's network and the public Internet, analyzes your network activity, and applies network access policies that you manage. When you enable Safe Mode for macOS and Windows devices, CylanceGATEWAY extends the tenant ACL rules and endpoint protection for devices when Work Mode is not enabled to ensure that devices are always protected for network traffic that does not use the tunnel.

When you deploy a new installation of the CylanceGATEWAY agent, users' devices must be restarted, and users must manually complete the installation process and [enable Work Mode](#) or [activate Safe Mode](#). When you deploy an upgrade of the CylanceGATEWAY agent, users' devices must be restarted for the upgrade to complete. During the upgrade, the CylanceGATEWAY agent retains all of the configurations. No additional action is required by users.

When the CylanceGATEWAY agent installation is controlled by enterprise device management tools (for example, Microsoft System Center Configuration Manager (SCCM) or another deployment tool), you can include the customDomain parameters to minimize user interaction when the agent is activated. You can obtain the custom domain name from the "Custom Domain Name" field in Settings > Application. You can supply the parameters for Windows devices from the command line and for macOS devices using a managed app configuration or MCX app preferences. You can also direct users to manually download and install the CylanceGATEWAY agent to [enable Work Mode](#) or [activate Safe Mode](#).

- For macOS devices, include the following value to specify the custom domain name to be used when users activate CylanceGATEWAY agent 2.9 or later:

```
<dict>
  <key>customDomain</key>
  <string>Your_custom_domain_name</string>
</dict>
```

- For Windows devices, include the following command to specify the custom domain name to be used when users activate CylanceGATEWAY agent 2.9 or later:

```
CylanceGATEWAY-<version>.exe /v "CUSTOM_DOMAIN=<your_custom_domain_name>"
```

To specify the custom domain name for a silent installation, see [Perform a silent installation and upgrade of the CylanceGATEWAY agent](#).

Perform a silent installation and upgrade of the CylanceGATEWAY agent

You can deploy the CylanceGATEWAY agent to users. If the deployment is for a new installation, users must restart their device and manually complete the installation process and [enable Work Mode](#) or [activate Safe Mode](#). For new deployments, you can specify the custom domain name that you obtain the "Custom Domain Name" field in Settings > Application. If the deployment is an upgrade, users must restart their devices for the upgrade to complete. The CylanceGATEWAY agent configurations are retained, and no additional action is required by users.

Before you begin: Download a copy of the CylanceGATEWAY agent for Windows from [the BlackBerry website](#) and save it to a location on your computer.

1. Open a command prompt and run as administrator.
2. Navigate to the location where you saved the CylanceGATEWAY agents. Complete one of the following tasks. In this example, we will use CylanceGATEWAY agent version 2.7.0.19.
 - To perform a silent installation or upgrade without restarting the users' devices, type
`.\CylanceGATEWAY-2.7.0.19.exe /s /v" REBOOT=Suppress /qn"`
 - To perform a silent installation or upgrade and immediately restart the users' devices, type
`.\CylanceGATEWAY-2.7.0.19.exe /s /v" /qn"`
 - To perform a silent installation or upgrade and create an installation log file called GWInstall, type

```
.\CylanceGATEWAY-2.7.0.19.exe /s /v" REBOOT=Suppress /qn /l*v .\GWInstall.log"
```

- To perform a new installation and specify the custom domain name, type

```
.\CylanceGATEWAY-<2.9.x.x>.exe /s /v" CUSTOM_DOMAIN=<your_custom_domain_name> /qn"
```

This feature requires CylanceGATEWAY agent for Windows 2.9 or later.

3. If necessary, direct your users to restart their devices and follow the onscreen prompts.

Enrolling CylancePROTECT Mobile and CylanceGATEWAY users

You assign an enrollment policy to users to allow them to activate the CylancePROTECT Mobile app on mobile devices and CylanceGATEWAY agent on Windows and macOS devices.

The enrollment policy includes separate settings for mobile and desktop devices. You can specify the supported device types and the text for email messages to be sent to users to provide activation instructions and a password or QR Code required to begin the activation process. You can specify the number of days that the activation password or QR Code is valid under **Settings > Activation**. The setting applies to all enrollment policies.

Users must have the following policies assigned to them before they can activate the CylancePROTECT Mobile app or the CylanceGATEWAY agent.

| User type | Required policies |
|---|---|
| CylancePROTECT Mobile app user without CylanceGATEWAY support | <ul style="list-style-type: none">• Enrollment policy• CylancePROTECT Mobile policy |
| CylancePROTECT Mobile app user with only CylanceGATEWAY support | <ul style="list-style-type: none">• Enrollment policy• Gateway Service policy |
| CylancePROTECT Mobile app user with both CylancePROTECT Mobile and CylanceGATEWAY support | <ul style="list-style-type: none">• Enrollment policy• CylancePROTECT Mobile policy• Gateway Service policy |
| Desktop user with CylanceGATEWAY agent | <ul style="list-style-type: none">• Enrollment policy• Gateway Service policy |

Note: The CylanceGATEWAY agent communicates over HTTPS with the management console and must be able to establish this connection directly. You must configure your organization's network to allow connections to the appropriate domains. For example, to allow the CylanceGATEWAY agent to activate and periodically authenticate, you must allow access to idp.blackberry.com and the domain for your region. If your environment uses an authentication proxy, you must allow the traffic on the proxy server. If the appropriate domains are not allowed, the CylanceGATEWAY agent will not be able to open the browser to complete the authentication process. For more information on the domains that must be allowed for CylanceGATEWAY, visit support.blackberry.com/community to read article 79017. For information on the network requirements for Cylance Endpoint Security, see [Cylance Endpoint Security network requirements](#).

Create an enrollment policy

1. In the management console, on the menu bar, click **Policies > User Policy**.
2. Click the **Enrollment** tab.
3. Click **Add Policy**.
4. Type a name and description for the policy.
5. To set enrollment options for mobile device users with the CylancePROTECT Mobile app, perform the following actions:
 - a) Click **Mobile**.
 - b) To limit the device types that the user can enroll, under **Allowed Platforms**, turn off **iOS** or **Android**.

- c) Under **UES Mobile Welcome email**, review the subject for the email message sent to users and update it if necessary.
 - d) Update the body of the message as necessary to provide information specific to your organization.
You can use [variables](#) in the email message.
6. To set enrollment options for the CylanceGATEWAY agent on Windows and macOS devices, perform the following actions:
- a) Click **Gateway Desktop**.
 - b) To limit the device types that the user can enroll, under **Allowed Platforms**, turn off **Windows** or **macOS**.
 - c) Under **Welcome email**, review the subject for the email message that is sent to users and update it if necessary.
 - d) Update the body of the message as necessary to provide information specific to your organization.
You can use [variables](#) in the email message. Users must enter the {{CustomDomain}} value in the Custom Domain field on the first sign-in page. You can use the variable to insert the value or find it in **Settings > Application** in the **Company** field.
7. Click **Add**.

After you finish: [Assign the policy to users and groups](#).

Supported enrollment email variables

You can use the following variables in the text of the email message specified by the enrollment policy:

| Variable | Description |
|------------------------------|---|
| {{UserDisplayName}} | User display name as it appears on the User page or in the directory the user was onboarded from. |
| {{FullUserName}} | Full user name as it appears on the User page or in the directory the user was onboarded from. |
| {{UserName}} | User name as it appears on the User page or in the directory the user was onboarded from. |
| {{UserEmailAddress}} | User email address as it appears on the User page or in the directory the user was onboarded from. |
| {{CustomDomain}} | Your organization's Cylance Endpoint Security company domain name. This value is displayed under Settings > Application in the Company field. |
| {{EnrollmentQRCode}} | QR code generated by Cylance Endpoint Security to simplify activating the CylancePROTECT Mobile app on mobile devices. This variable can be used only in the email message sent to mobile device users. |
| {{EnrollmentPasscode}} | Activation password generated by Cylance Endpoint Security |
| {{EnrollmentPasscodeExpiry}} | The date the activation password and QR code expire. You can set the number of days that the activation password or QR code is valid under Settings > Activation . |

Setting up CylanceAVERT

| Item | Description |
|------|--|
| 1 | Review the software requirements |
| 2 | Define sensitive content |
| 3 | Install CylanceAVERT |
| 4 | Create information protection policies |
| 5 | Assign policies to administrators, users, and groups |

Installing the CylanceAVERT agent

You can download and install CylanceAVERT from the Downloads page in the [BlackBerry myAccount portal](#).

You can install CylanceAVERT in silent mode through SCCM or JAMF for the user. To do so, you will need to include the `IAgreetoBBSLA=true` command line parameter to accept the end-user license agreement (EULA). The EULA will not be displayed to the user. After you install CylanceAVERT in silent mode, you must reboot the system.

Note: Prior to installing CylanceAVERT in silent mode, you must read the [BlackBerry Solution License Agreement](#), including the [BlackBerry Privacy Notice](#). You may install the application only if you accept the terms and conditions of the BlackBerry Solution License Agreement in the manner indicated above. **If you do not accept the terms and conditions of the BlackBerry Solution License Agreement, do not install or use CylanceAVERT.**

After the CylanceAVERT agent is installed, the user can get security notifications for potential unauthorized sharing of sensitive company data when sending emails, transferring files through USB, and uploading files to a website.

If a user that is not added to Cylance Endpoint Security logs into a desktop that has CylanceAVERT installed, the user will be automatically added to Cylance Endpoint Security with all policies applied to them. This requires an Active Directory or BlackBerry Connectivity Node directory connection. If you are using a BlackBerry Connectivity Node directory connection for user management, you must use BlackBerry Connectivity Node version 2.12.1 or later. For more information, see [Installing the BlackBerry Connectivity Node](#) and [Linking to your company directory](#) in the Cylance Endpoint Security Setup Guide.

Note: If a user quits the CylanceAVERT app from the Windows application tray, they will not receive a Windows notification when an exfiltration event occurs.

Install CylanceAVERT

CylanceAVERT requires CylancePROTECT Desktop version 3.1 or later.

Note: CylanceAVERT cannot be installed on a computer with CylancePERSONA.

1. On the device, double-click the CylanceAVERT agent installer.
2. Follow the installation steps.

After you finish:

- To verify that the CylanceAVERT agent is installed, check the following:
 - The CylanceAVERT icon appears in the system tray.
 - The CylanceAVERT user appears in the Users list on the Assets page in the console.
 - In Windows Task Manager, check that the CylanceAVERT process is running.
- To uninstall the agent, use the Windows Settings.

Note: After CylanceAVERT is installed, the browser plugin will prevent uploading any files to unsecured (non-SSL) websites. BlackBerry recommends that you don't attempt to upload files to non-SSL websites.

Define sensitive content using information protection settings

With the information protection settings, you can specify the data types that CylanceAVERT will look for in sensitive files, the evidence that is collected, the email and browser domains that you want to consider as trusted, and the email addresses that you want to send notifications of an exfiltration event to.

Manage evidence collection

You can customize how data exfiltration events are collected in CylanceAVERT. Data collection settings allow you to configure the evidence that you want to be collected during a data exfiltration event for auditing purposes. By configuring data collection settings, you can make decisions such as including file snippets of the exfiltration event, saving full copies of the files involved in the exfiltration event, managing uploads to the evidence locker, selecting times for file uploads, and specifying the length of time data evidence should be retained.

1. In the management console, on the menu bar, click **Settings > Information Protection**.
2. Click the **Data Collection** tab.
3. Perform any of the following to configure information protection settings:

| Item | Steps |
|--------------------------|--|
| File Snippets | Click the Generate File Snippets toggle to turn on or off file snippet collection. When Generate File Snippets is turned on, a file snippet of the data exfiltration event will be saved in the events details. By default, Generate File Snippets is set to off. |
| Evidence File Collection | <ul style="list-style-type: none">• Click the Enable evidence file collection toggle to turn on or off evidence file collection. By default, Enable evidence file collection is set to off. When Enable evidence file collection is turned on, a full copy of the files involved in a data exfiltration event will be saved in the event details. See Viewing CylanceAVERT event details for more information.• Click the Disk space text field and enter a value to specify the maximum amount of free disk space that you can allocate to caching evidence files on remote devices or evidence locker. By default, Disk space is set to 10%. |

| Item | Steps |
|-------------------------|---|
| File Upload | Click the File Upload Method drop-down menu and select a method. By selecting Direct , devices on your network will be able to upload files directly to your evidence locker. If direct access to your evidence locker is blocked (for example, by your firewall), BlackBerry will upload the files through its cloud by selecting BlackBerry Proxy Service . By default, Direct is selected. |
| Evidence File Retention | Click the Data retention drop-down menu and select the length of time you would like evidence files to be stored in your evidence locker. The values for the length of time that evidence files can be stored is 30, 60, or 90 days. By default, Data retention is set to 30 days. |

Add allowed and trusted domains

You specify domains so that you can list browser and email addresses that you trust to safely upload files to. After you add domains, you will need to enable them to be used in the information protection policies. When you specify an allowed domain for a policy, that domain will not trigger any policy violations when it is scanned for sensitive file uploads if the domain has been validated against an added certificate and become a trusted domain. If you don't specify any domains in the information protection settings or add any domains for use in your policies, all domains will be treated as untrusted.

Note:

- All USB device domains are considered as untrusted.
- After you specify an allowed domain, any subdomains will also be considered as allowed as long as their trusted certificates are added.

Before you begin: Verify that you have upload a trusted certificate. For a domain to be considered as trusted, a trusted certificate must be uploaded. If a trusted certificate is not uploaded and the allowed domain is used in a policy, it will still trigger an exfiltration event. For more information, see [Verify domains using trusted certificates](#).

1. In the management console, on the menu bar, click **Settings > Information Protection**.
2. Click the **Allowed Domains** tab.
3. To add a new browser domain, click the **Add New Domain** button.
4. In the **Add allowed domain** dialog box, type a name and description for the domain in the text fields. Wildcard characters are not supported in the domain name field.
5. Optionally, turn on the ability to use this domain in a policy.
6. Click **Verify** to check if this domain uses an existing trusted certificate. If you have not uploaded a certificate, add the certificate now. For instructions, see [Verify domains using trusted certificates](#).
7. Click **Add**.
8. If you would like to add a new email domain, type the domain in the **Allowed Email Domains** section and use a comma to separate it from the previously entered domains.

After you finish:

To delete an allowed domain, in the **Allowed Domains** list, click the check box beside the domain that you want to delete and click **Delete**.

Use templates to group data types

You can use templates to group sensitive data types for your organization to use in a policy.



1. From the management console, on the menu bar, click **Settings > Information Protection**.

2. Click the **Templates** tab.
3. To add a predefined template, click **Add Predefined**, select the predefined templates from the list and click **Add**.
4. To create a custom template, click **Create Custom**.
5. From the **Add new template** page, in the **General Information** section, enter the Template name and select the region from the drop-down list.
6. In the **Region** drop-down menu, select the region the template will be used for. For example, if you are creating a template with Canadian Health card and Canadian Sin number data types, select Canada as the region.
7. In the **Information type** drop-down menu, select the type of information that matches your template. Values are custom, financial, health, and personal data.
8. In the **Conditions Builder** section, select the data type from the drop-down list and specify the number of minimum occurrences required to trigger the policy violation. To add another data type to the group, click **Add Item**.
 - To add another data type to the group, click **Add Item**.
 - To add another condition group, click **Add Group**.
9. Click **Save**.

After you finish:


After your template is added, you can add it to an information protection policy. See [Managing information protection policies](#) for more information.

To remove a template, in the **Actions** column beside the template that you want to remove, do the following:

- To remove a predefined template, click . At the confirmation dialog, click **Remove**.
- To delete a custom template, click . At the confirmation dialog, click **Delete**.

When a template is removed from your list, it will no longer be available for use in an information protection policy.

To edit a custom template, click on the template in the list, and edit the information in the fields. You cannot edit a predefined template. Refer to steps 4-7 for more information.

To copy a template, click  in the actions column of the template you want to copy.

Specify sensitive data types

Data types represent the sensitive data that CylanceAVERT will scan for. You can set data types in the information protection settings and customize them to fit your organization's needs. The search methods available for data types are keywords or regular expressions.

1. In the management console, on the menu bar, click **Settings > Information Protection**.
2. Click the **Data Types** tab.
3. Click **Add Custom Data Type**.

Note: You can also add predefined data types to your list, which will allow the data type to be used in an information protection policy. To add a predefined data type to a list, click **Add Predefined Data Type**, select the predefined data types that you want to add to your list, and click **Add**.

4. On the **Add custom data type** page, add a name and description for the new data type.
5. In the **Region** drop-down list, select the region the data type will be used for. For example, if you are going to check for a Canadian drivers license number, select Canada as the region.
6. In the **Information type** drop-down menu, select the type of information that matches your data type. Values are custom, financial, health, and personal data.

7. In the **Search method** drop-down menu, select the search method that you want to use. Values are keywords, expression, or keyword dictionary. A keyword dictionary is a text file that specifies multiple keywords. To create a keyword dictionary, you must create a text file with each keyword written on a new line.

8. Do any of the following:

- If you selected **Keywords** as your search method, enter the keywords that you want to scan for in the **Keywords** field. You can use commas to separate multiple keywords.
 - Select **Exact match** if you want to consider the file as sensitive if the keywords are exact matches. If this is selected, keywords will not be matched if they are part of a larger text string. For example, if you specify "confidential" as a keyword, "confidentiality" will not produce a match.
 - Select **Enforce case sensitivity** if you want to consider the file as sensitive if the case of the keywords are exact matches. If this is selected, text case is enforced. For example, if you specify "confidential" as a keyword, "CONFIDENTIAL" will not produce a match.
- If you selected **Regular Expression (Regex)** as your search method, enter the regular expression that you want to scan for in the **Regex** field.

Note: If you are using a regex, note the following:


- The regex must conform to the .NET expression language.
- You can validate the regex using popular tools such as [Regex101](#) or [Regex Storm](#).
- If you selected **Keyword Dictionary**, do the following:
 - Select **Exact match** if you want to consider the file as sensitive if the keywords are exact matches. If this is selected, keywords will not be matched if they are part of a larger text string. For example, if you specify "confidential" as a keyword in your keyword dictionary, "confidentiality" will not produce a match.
 - Select **Enforce case sensitivity** if you want to consider the file as sensitive if the case of the keywords are exact matches. If this is selected, text case is enforced. For example, if you specify "confidential" as a keyword in your keyword dictionary, "CONFIDENTIAL" will not produce a match.
 - Click **Upload Keyword Dictionary** and select your keyword dictionary. You can only upload one keyword dictionary file per data type.


Note: The following are limitations for a keyword dictionary:

- The combined size of all keyword dictionaries on a tenant cannot exceed 1.5 MB.
- A single keyword in the keyword dictionary cannot exceed 1024 characters.
- The maximum number of keyword dictionary data entities on a tenant is 1000.

9. Click **Create**.

After you finish:

- A custom data type can be deleted. To delete a custom data type, click  in the **actions** column. On the confirmation pop-up, click **Delete**.

Note: You will receive a **Data type in use** pop-up if the data type is used in a policy and you will not be able to delete it until it is removed.
- A predefined data type can be removed from your list but not deleted. To remove a predefined data type from your list click  in the **Actions** column. On the confirmation pop-up, click **Remove**. You can re-add a predefined data type to your list by clicking **Add Predefined Data Type** and selecting the data type from the list.

Note: You will receive a **Data type in use** pop-up if the data type is used in a policy and you will not be able to delete it until it is removed.
- An existing keyword dictionary file can be downloaded. If an updated keyword dictionary is uploaded, the endpoint will be rescanned and the policies will be evaluated. Currently, existing events will remain evaluated from the previous datatype.

Verify domains using trusted certificates

Trusted certificates allow you to verify the allowed browser domains that were added in the information protection settings. If a trusted certificate is missing and the allowed domain is used in a policy, it will trigger an exfiltration event. For more information on allowed domains, see [Add allowed and trusted domains](#).

1. In the management console, on the menu bar, click **Settings > Information Protection**.
2. Click the **Trusted Certificates** tab.
3. Click **Add Certificate**.
4. Upload a root or intermediate certificate file (.pem). Click **Browse Files** to search for a local .pem file on your device, then click **Add**.

Send notifications to specified email addresses

You can specify email addresses to send notifications to when a data exfiltration event occurs or when the evidence locker is reaching storage capacity. Only Cylance Endpoint Security administrators can see events details, but any user can receive notifications.

1. In the management console, on the menu bar, click **Settings > Information Protection**.
2. Click the **Notifications** tab.
3. Turn on **Enable Information Protection Event Notifications** to enable sending email notifications for CylanceAVERT events to specified email recipients.
4. In the **Email recipients** text field, type the email addresses that you want to receive CylanceAVERT Event notifications. You can use a comma to separate multiple email address entries.
5. Turn on **Enable Evidence Locker Storage Notifications** to enable sending email notifications for evidence locker storage capacity to specified email recipients.
6. In the **Email recipients** text field, type the email addresses that you want to receive evidence locker storage capacity notifications. You can use a comma to separate multiple email address entries.

Managing information protection policies

Information protection policies allow you to create organizational or regulatory policies that are triggered when specified conditions are met. You can add conditions using a template or through the conditions builder. Information protection policies are cumulative and not ranked like other Cylance Endpoint Security policies. If the user is unknown or had no policies assigned, all policies will be applied to the user.

Information protection policies can either be regulatory or organizational. Depending on the policy type, different reconciliation logic will be applied.

- When a user is assigned multiple regulatory policy types, policies will be consolidated for the user and the most restrictive rules and remediation actions will be applied.
- When a user is assigned multiple organizational policy types, policies will be consolidated for the user and the least restrictive rules and remediation actions will be applied.

Note: At least one information protection policy is required. If you try to delete the information protection policies, you will receive an error stating that one policy is required.

Best practices for policy consolidation

CylanceAVERT has two policy compliance types that can be used in an information protection policy.

Regulatory compliance refers to a finite set of sensitive data that is used to protect sensitive information related to industry or government regulations. Regulatory data is data that does not change over time. The pre-defined data types in the [CylanceAVERT settings](#) are all regulatory and are provided to you by BlackBerry to accelerate

and simplify product setup. You can create your own regulatory data types and templates for use in a policy that encapsulates all of the regulatory data that your organization requires. For example, instead of using the BlackBerry provided template, you can create a Canada Health regulatory policy, that combines a Canadian SIN number, PHIN, health service number, Driver's license, bank account number, and passport number in a single policy. CylanceAVERT will use regular expression or keyword matching to determine if a file contains relevant regulatory information as stated in the policy.

Organizational compliance refers to a set of infinite data where the content and the people who can access the data changes from organization to organization is constantly changing based on organizational situations. As a result, organizational compliance should be used to protect sensitive data that contains information on company IP or other information relevant to your organization.

There is a possibility that multiple policies can apply to the same sensitive file, where the policies will conflict in their remediation action that they will take when a sensitive file is discovered. In this case, CylanceAVERT will apply remediation reconciliation for these policies.


When policy collisions occur, CylanceAVERT will automatically apply reconciliation. The reconciliation action will differ if the file violates a regulatory policy, an organizational policy, or both. If a file is classified as only organizational, the least restrictive remediation action is taken. If a file is classified as regulatory and/or organizational, the most restrictive action is taken. For example, if a file is subject to an organizational policy that determines the file is sensitive if it contains 2 occurrences of the word "confidential", and a second organizational policy that determines sensitivity based on 3 occurrences of the word, the file will be determined as sensitive for 3 occurrences (least restrictive). However, if one or both of these policies were regulatory, then the file would be sensitive with 2 occurrences (most restrictive).

Create an information protection policy

1. In the management console, on the menu bar, click **Policies > User Policy**.
2. Click the **Information Protection** tab.
3. Click **Add Policy**.
4. In the **General Information** section, fill in the following:
 - In the **Policy name** field, type in a name for your policy.
 - In the **Description** field, type in a description for your policy.
 - In the **Policy type** drop-down menu, select the type of policy you are creating. Possible values for policy type are regulatory or organizational.
 - A regulatory policy type refers to the finite set of sensitive data defined by a regulation that does not necessarily change over time (for example, PCI, HIPAA, etc.).
 - An organizational policy type refers to company proprietary data where the audience for who can access the data can be constantly changing. As a result, organizational data should be classified data elements (for example, the file type, keywords, the file creator, the file creator's role, etc.).
5. In the **Conditions** section, configure the conditions that will trigger a policy violation by using one of the following:

| Condition | Description |
|---------------------------------|--|
| Add conditions using a template | <p>a. Click Add From Template.</p> <p>b. Click the checkbox for the templates that you want to add to your policy.</p> <p>Note: You can filter the list of templates using the search bar.</p> |

| Condition | Description |
|---|--|
| Add conditions using the conditions builder | <p>Note: The conditions builder is comprised of And and Or statement groups. You need to use a combination of these statement groups to determine when a policy will be triggered.</p> <p>a. In the And conditions section, select the conditions from the drop-down list, then specify the minimum number of occurrences required to trigger the condition from the numeric drop-down menu.</p> <ul style="list-style-type: none"> • If you would like to add another item to your current statement group, click Add Item. • If you would like to add another statement group, click Add Group. • If you would like to delete a statement group, click Delete Group. <p>b. In the Or conditions section, select the conditions from the drop-down list, then specify the minimum number of occurrences required to trigger the condition from the numeric drop-down menu.</p> |

6. In the **Allowed Domains** section, click  then select the browser domain you want to allow for you policy from the list.
7. In the **Allowed Email Domains** section, select which email recipients specified in the information protection settings should be allowed for your policy.
8. In the **Actions** section, from the drop-down lists, select the action to take for Web browser, USB, and email exfiltration events. Select from the following actions:
 - **Report:** This option reports the data exfiltration or policy violation to the Cylance Endpoint Security console that can be viewed on the Avert Events (Avert > Events) page, creates an alert in the Alerts view, and sends the events to the SIEM solution or syslog server, if configured. In addition, an email is sent to the email recipients that are specified in the Notifications (Settings > Information protection) screen.
 - **Report and notify:** This option reports the data exfiltration or policy violation to the Cylance Endpoint Security console and displays the data exfiltration or policy violation badge and notification in the taskbar of the endpoint for the user.
 - **Report, notify and warn:** This option reports the data exfiltration or policy violation to the Cylance Endpoint Security console, displays a badge and notification in the taskbar, and adds a Windows notification in the endpoint and a popup warning to the user before the data exfiltration or policy violation occurs. For example, if a user uses Microsoft Outlook, the CylanceAVERT agent will intercept the email and display an alert in the email editor as well as a warning to the user before the sensitive data is sent.

9. Click **Add**.

Note: If a user has policies assigned to them, and then has all of those policies removed, the user will be deleted from CylanceAVERT.

After you finish:

Do any of the following:

- You can assign a policy to users and user groups. See [View CylanceAVERT user details](#) for more information.
- To delete an information protection policy, select the checkbox beside the policy in the list, then click **Delete**.
- To edit an information protection policy, click on the policy in the list, make a change to the policy, then click **Save**.

Connecting Cylance Endpoint Security to external services

Cylance Endpoint Security supports various connectors that allow you to integrate data and functionality with third-party services and other BlackBerry products. One Cylance Endpoint Security tenant can connect to multiple external services.

Cylance Endpoint Security supports the following connectors:

| Connector | Description |
|------------------|---|
| BlackBerry UEM | <p>The BlackBerry UEM connector allows CylanceGATEWAY to verify whether Android and iOS devices are managed by UEM.</p> <p>For more information, see Connecting Cylance Endpoint Security to MDM solutions to verify whether devices are managed.</p> |
| Microsoft Intune | <p>The Microsoft Intune connector allows Cylance Endpoint Security to report the risk level of your organizations mobile devices to Intune. The device risk level is calculated based on the detection of mobile threats by the CylancePROTECT Mobile app on Intune managed devices. Intune can execute mitigation actions based on the device risk level.</p> <p>For more information, see Integrating Cylance Endpoint Security with Microsoft Intune to respond to mobile threats.</p> |
| Okta | <p>The Okta connector allows you to collect login authentication and access information from Okta services and view the associated information in the Alerts view in the Cylance console.</p> <p>For more information, see Integrating Cylance Endpoint Security with Okta.</p> |
| Mimecast | <p>The Mimecast connector allows you to integrate email attachment risk score data from Mimecast services and view the associated information in the Alerts view in the Cylance console.</p> <p>For more information, see Integrating Cylance Endpoint Security with Mimecast.</p> |

Integrating Cylance Endpoint Security with Okta

You can add an Okta connection to your Cylance console to view Okta alerts in the Alerts view. The Alerts view allows administrators to view Okta authorization and access alerts from one unified interface. The Okta connector uses the Okta events API to display event telemetry in the Alerts view. The Okta user anomaly events that are aggregated in the Alerts view include suspicious user login attempts and blocked security request events. By aggregating Okta events into these categories, you will have greater visibility into login attempts by third parties, erroneous logins by users, and login attempts from suspicious source IP addresses.

The Alerts view aggregates requests from banned IP addresses across your company's user base to provide insight into possible patterns or campaigns. The surfaced data can also contain information on the source device of the access attempt, allowing you to determine if the request was made by a human or machine.

For more information about configuring Okta to generate alerts that can be viewed in the Alerts view, see the following resources:

- [Okta Help Center: Configure a password policy](#)
- [Okta Help Center: Blocklist network zones](#)

For more information about the Alerts view, see [Managing alerts across Cylance Endpoint Security services](#) in the Administration content.

Prerequisites for adding an Okta connector

Before you can configure a Okta connection for Cylance Endpoint Security, you must complete some tasks using the Okta service.

| Step | Item | Description |
|------|------------------------------|--|
| 1 | Document the Okta base URL | <p>You must document the Okta base URL for your environment to use it during configuration of the Okta connector. The Okta base URL will be the production URL of your Okta server.</p> <p>For more information on locating your Okta base URL, see Find your Okta Domain in the Okta documentation.</p> |
| 2 | Create an Okta administrator | <p>You must create an Okta administrator to use the Okta API. BlackBerry recommends creating a dedicated user that is linked to the API token in step 3. This step is recommended because it aids in auditing workflows and is the best practice to ensure that other Okta users do not have tokens that are created and used for security operation workflows.</p> <p>For more information on creating an Okta administrator, see Create an admin role assignment using an admin in the Okta documentation.</p> |
| 3 | Create an Okta API token | <p>You must create an Okta API token to authenticate requests to the Okta API.</p> <p>For more information on creating an Okta API token, see API token management in the Okta documentation.</p> |

After you complete these steps, follow the instructions in [Add and configure an Okta connector](#).

Add and configure an Okta connector

Before you begin: Review the [Prerequisites for adding an Okta connector](#).

1. In the management console, on the menu bar, click **Settings > Connectors**.
2. Click **Add Connector > Okta**.
3. In the **General Information** section, type a name for the connector.
4. In the **Okta Configuration** section, specify the Okta service API URL, the Okta API token, and the polling frequency.

Note: BlackBerry recommends leaving the polling frequency at its default value unless you have a specific rate limit requirement for your organization.

5. Click **Test Connection**.

6. Click **Save**.

After you finish: View and manage alerts in the Alerts view. See [Managing alerts across Cylance Endpoint Security services](#) in the Administration content.

Integrating Cylance Endpoint Security with Mimecast

You can add a Mimecast connection to your Cylance console. Mimecast attachment protection analyzes all email attachments that your users receive and can handle the attachment based on the policy that you configure.

The Alerts view allows administrators to view Mimecast attachment risk information from one unified interface. Mimecast surfaces the attachment risk telemetry that is provided by the Mimecast Attachment Protection Service. The action that Mimecast applies to the file attachment is displayed in the response column of the Alerts view. If Mimecast categorizes an alert as malicious, the alert will be categorized as high priority in the Alerts view. If Mimecast categorizes an alert as unsafe or unknown, the alert will be categorized as medium priority. Any alerts that are deemed low priority by Mimecast will not display in the Alerts view.

The Alerts view uses the attachment hash to group alerts, meaning that a similar alert across multiple users in your organization can be grouped for the same threat. You can use the Detection Details link to access the Mimecast Attachment Protection dashboard to investigate and remediate threats.

For more information about the Alerts view, see [Managing alerts across Cylance Endpoint Security services](#) in the Administration content.

Prerequisites for adding a Mimecast connector

Before you can configure a Mimecast connection for Cylance Endpoint Security, you must complete some tasks using the Mimecast Service.

| Step | Task | Details |
|------|------------------------------|---|
| 1 | Create a Mimecast account | Administrators must create a new account for all service users. For more information, see Creating/Editing Mimecast Users in the Mimecast documentation. |
| 2 | Add an API application | Specify the details and settings of your API application. When configuring the API application, verify that "Service Application" is selected. This is required to ensure that API keys do not expire. If this option is not selected, the Mimecast connector will lose connectivity when the key expires. For information on how to add an API application in Mimecast, see Adding an API application in the Managing API Applications guide from Mimecast. |
| 3 | Create user association keys | You must create user association keys to connect Mimecast to Cylance Endpoint Security. For information on how to create user association keys, see Creating User Association Keys in the Managing API Applications guide from Mimecast. |

| Step | Task | Details |
|------|--|---|
| 4 | Inform users of the Mimecast configuration | It is recommended that you notify your users of the Mimecast configuration. You can download the preconfigured email templates available from Mimecast . |
| 5 | Configure attachment protection definitions and policies | Configure the attachment protection definitions and policies that Mimecast will use when an insecure email is discovered. For more information, see Attachment Protect Configuration in the Mimecast documentation. |
| 6 | Enable and configure notifications | Ensure that you have enabled and configured notifications for all API users for notification data so that it is available in the Alerts view. For more information, see Attachment Protect Configuration in the Mimecast documentation. |
| 7 | Enable directory services | Ensure that you have enabled Mimecast Directory Services so that the Mimecast user information (email address) is correlated with your user data that is stored in your Entra or Active Directory service. This configuration also enables correlation with your devices and the device data that is associated with the users in your directory services. For more information on enabling directory services, see Directory Synchronization in the Mimecast documentation. |

After you complete these steps, follow the instructions in [Add and configure a Mimecast connector](#).

Add and configure a Mimecast connector

Before you begin: Review the [Prerequisites for adding a Mimecast connector](#).

1. In the management console, on the menu bar, click **Settings > Connectors**.
2. Click **Add Connector > Mimecast**.
3. In the **General Information** section, type a name for the connector.
4. In the **Mimecast Configuration** section, specify the required information, specify a polling frequency, and select a base URL.
For more information on Mimecast key generation, see [Managing API Applications](#) in the Mimecast documentation.
5. Click the toggle control to enable polling.
6. Click **Test Connection**.
7. Click **Save**.

After you finish: View and manage alerts in the Alerts view. See [Managing alerts across Cylance Endpoint Security services](#) in the Administration content.

Legal notice

© 2025 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, EMBLEM Design, ATHOC, and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada