Cylance Endpoint Security

Setup-Anleitung

Contents

Cylance Endpoint Security-Anforderungen

Lesen Sie diesen Abschnitt, um mit der Einrichtung von Cylance Endpoint Security zu beginnen. Überprüfen Sie, ob die Umgebung Ihres Unternehmens die Anforderungen der Funktionen und Komponenten der Lösung erfüllt.

Anforderungen: Cylance-Konsole

Element	Anforderungen
Unterstützte Browser	Aktuelle Version von: • Google Chrome (empfohlen) • Microsoft Edge • Mozilla Firefox **Hinweis:** Wenn Sie Firefox für den Zugriff auf die Verwaltungskonsole verwenden, sollten Sie nicht den privaten Browsermodus verwenden, „Cookies und Website-Daten beim Beenden von Firefox löschen“ nicht aktivieren und Service Worker nicht deaktivieren. Diese Konfigurationen können dazu führen, dass einige Bildschirme der Konsole nicht wie erwartet geladen werden.
Unterstützte Sprachen	Stellen Sie Ihren Browser auf eine der folgenden unterstützten Sprachen ein: • Deutsch • Französisch • Deutsch • Italienisch • Japanisch • Koreanisch • Portugiesisch • Spanisch

Anforderungen: CylancePROTECT Desktop

Informationen zu den Betriebssystemen, die von den einzelnen CylancePROTECT Desktop-Agenten unterstützt werden, finden Sie in der Kompatibilitätsmatrix für Cylance Endpoint Security. Informationen zum Anzeigen von Support-Zeitplänen für alle BlackBerry-Produkte finden Sie im Referenzleitfaden zum Lebenszyklus der BlackBerry Enterprise-Software.

In den folgenden Tabellen werden die unterstützten Betriebssysteme aufgeführt, für die zusätzliche Anforderungen oder Überlegungen gelten. Beachten Sie, dass diese Tabellen keine umfassende Liste der unterstützten Betriebssysteme sind. Wenn ein Betriebssystem nicht in den Tabellen aufgeführt ist, bedeutet dies, dass keine zusätzlichen Anforderungen oder Überlegungen bestehen.

Windows Betriebssystem

Unterstütztes Betriebssystem	Anforderungen
Alle unterstützten Windows-Betriebssystemversionen	• .NET Framework 4.6.2 oder höher • TLS 1.2 • Informationen zu Anforderungen an virtuelle Maschinen, Bereitstellungsrichtlinien und Best Practices finden Sie unter Anhang: Best Practices für die Bereitstellung von CylancePROTECT Desktop auf virtuellen Maschinen unter Windows. • CylancePROTECT Desktop unterstützt das Scannen nicht hydratisierter Dateien von Microsoft OneDrive nicht. • Stellen Sie sicher, dass die neuesten Windows-Sicherheitsupdates auf den Geräten installiert wurden, bevor Sie den CylancePROTECT Desktop-Agent installieren oder aktualisieren.
Windows 11 (64 Bit)	• Dateisysteme, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, werden nicht unterstützt. • Windows 11-Multi-Sitzung wird derzeit nicht unterstützt.
Windows 10 (32 Bit, 64 Bit)	• Dateisysteme, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, werden nicht unterstützt. • Windows 10-Multi-Sitzung wird derzeit nicht unterstützt. • Windows 10 (v1809, Update von Oktober 2018): Unified Write Filter (UWF) wird nicht unterstützt. Deaktivieren Sie UWF, bevor Sie den Agent installieren. • Windows 10 (v1709, Fall Creators Update): siehe KB 65647. • Windows 10 Anniversary (v1607, Anniversary-Update): Es wird empfohlen, das Windows-Subsystem für Linux zu deaktivieren.
Windows 7 (32 Bit, 64 Bit)	• Embedded Standard 7 und Embedded POSReady 7 werden unterstützt. • Installieren Sie die für den Agent erforderlichen Stammzertifikate.

Windows Server 2022 (64 Bit)	• Standard-, Data Center- und Core-Editionen werden unterstützt.
	• Für Data Center-Editionen unterstützt der Agent Folgendes nicht:
	  • Hyper-V Server Role für Shielded Virtual Machines
	  • Host Guardian Hyper-V-Support
	  • Softwaredefinierte Netzwerke
	  • Storage Spaces Direct
	• Storage Server 2022 wird nicht unterstützt.

Windows Server 2019 (64 Bit)	• Standard-, Data Center- und Core-Editionen werden unterstützt.
	• Für Data Center-Editionen unterstützt der Agent Folgendes nicht:
	  • Hyper-V Server Role für Shielded Virtual Machines
	  • Host Guardian Hyper-V-Support
	  • Softwaredefinierte Netzwerke
	  • Storage Spaces Direct
	• Storage Server 2019 wird nicht unterstützt.

Unterstütztes Betriebssystem	Anforderungen
Windows Server 2016 (64 Bit)	• Standard-, Data Center-, Essentials- und Server Core-Editionen werden unterstützt. • Nano Server und Storage Server werden nicht unterstützt.
Windows Server 2012 und 2012 R2 (64 Bit)	• Standard-, Data Center-, Essentials-, Server Core-, Embedded- und Foundation-Editionen werden unterstützt. • Minimal Server Interface und Storage Server werden nicht unterstützt.

macOS

Unterstütztes Betriebssystem	Anforderungen

Alle unterstützten macOS-Versionen	• TLS 1.2
	• Stellen Sie sicher, dass die folgenden Stammzertifikate installiert sind: Wenn sie fehlen, wird der Agent möglicherweise nicht gestartet oder das Gerät kann möglicherweise nicht mit der Verwaltungskonsole kommunizieren. Weitere Informationen finden Sie in KB 66608.
	  • VeriSign Class 3 Public Primary Certification Authority - G5
	  • Thawte Primary Root CA
	  • DigiCert Global Root
	• Informationen zu Anforderungen an virtuelle Maschinen, Bereitstellungsrichtlinien und Best Practices finden Sie unter Anhang: Best Practices für die Bereitstellung von CylancePROTECT Desktop auf virtuellen Maschinen unter Windows.
	• Datenträgerformate, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, werden nicht unterstützt.

macOS Sonoma (14)	• Siehe KB 66578. • Aktivieren Sie den vollen Datenträgerzugriff. Wenn der volle Datenträgerzugriff nicht aktiviert ist, kann CylancePROTECT Desktop durch Benutzerdatenschutz gesicherte Dateien nicht verarbeiten. Weitere Informationen finden Sie unter KB 66427. • Siehe Fehlerbehebung bei macOS-Installationen. • Folgende Speicherschutzverletzungen werden unterstützt: Remote-Speicherzuweisung, Remote-Speicherzuordnung, Remote-Schreibzugriff auf Speicher, Remote-Aufhebung der Speicherzuordnung. Weitere Speicherschutzverletzungen werden für Sonoma nicht unterstützt.

Unterstütztes Betriebssystem	Anforderungen
macOS Monterey (12)	• Siehe KB 66578. • Aktivieren Sie den vollen Datenträgerzugriff. Wenn der volle Datenträgerzugriff nicht aktiviert ist, kann CylancePROTECT Desktop durch Benutzerdatenschutz gesicherte Dateien nicht verarbeiten. Weitere Informationen finden Sie unter KB66427. • Siehe Fehlerbehebung bei macOS-Installationen. • Folgende Speicherschutzverletzungen werden unterstützt: Remote-Speicherzuweisung, Remote-Speicherzuordnung, Remote-Schreibzugriff auf Speicher, Remote-Aufhebung der Speicherzuordnung. Weitere Speicherschutzverletzungen werden für Monterey nicht unterstützt.
macOS Big Sur (11)	• Siehe KB 66578. • Aktivieren Sie den vollen Datenträgerzugriff. Wenn der volle Datenträgerzugriff nicht aktiviert ist, kann CylancePROTECT Desktop durch Benutzerdatenschutz gesicherte Dateien nicht verarbeiten. Weitere Informationen finden Sie unter KB 66427. • Siehe Fehlerbehebung bei macOS-Installationen. • Folgende Speicherschutzverletzungen werden unterstützt: Remote-Speicherzuweisung, Remote-Speicherzuordnung, Remote-Schreibzugriff auf Speicher, Remote-Aufhebung der Speicherzuordnung. Weitere Speicherschutzverletzungen werden für Big Sur nicht unterstützt.

Linux Betriebssystem

Unterstütztes Betriebssystem	Anforderungen

Alle unterstützten Linux-Betriebssystemversionen	• Erfordert eine Internetverbindung. Wenn das Gerät diese Anforderung nicht erfüllt, erwägen Sie stattdessen die CylanceON-PREM-Lösung.
	• Siehe Tabelle „Unterstützte Linux-Kernel“.
	• TLS 1.2
	• Erforderliche Pakete:
	  • `bzip2(x86-64)`
	  • `dbus-libs` (Für RHEL/CentOS 7.x oder 8.x ist Version 1.10.24 oder höher erforderlich.)
	  • `glibc`
	  • `gtk3` (für RHEL/CentOS)
	  • `libgcc`
	  • `openssl` (Für RHEL/CentOS 6.x)
	  • `openssl-libs` (Für RHEL/CentOS 7.x)
	  • `sqlite`
	• Stammzertifikate:
	  • VeriSign Class 3 Public Primary Certification Authority - G5
	  • Thawte Primary Root CA
	  • DigiCert Global Root
	• Für den 2.1.1590-Agenten unterstützte GNOME-Versionen:
	  • 3.28
	  • 3.20
	  • 3.14
	  • 3.10
	  • 3.8
	• Virtuelle Maschinen werden unterstützt.

Ubuntu 22.04 LTS (64 Bit) Ubuntu 20.04 LTS (64 Bit) Ubuntu 20,04 (64 Bit) Ubuntu 18,04 (64 Bit)	• Ubuntu-spezifische Azure-Kernels werden nicht unterstützt. • Verwenden Sie das CylancePROTECT Desktop Secure Boot CA-Zertifikat zur Unterstützung von UEFI Secure Boot. Weitere Informationen finden Sie in 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)	• Verwenden Sie das CylancePROTECT Desktop Secure Boot CA-Zertifikat zur Unterstützung von UEFI Secure Boot. Weitere Informationen finden Sie in KB 73487. • FIPS wird unterstützt Anweisungen zum Aktivieren von FIPS finden Sie in der Red Hat-Dokumentation zu Ihrem Betriebssystem.

Verwenden von CylancePROTECT Desktop mit anderer Antivirensoftware

Wenn auf Geräten mit CylancePROTECT Desktop eine Antivirensoftware von Drittanbietern installiert ist, müssen Sie möglicherweise einige zusätzliche Konfigurationen vornehmen, um sicherzustellen, dass diese Produkte

die Funktionalität von CylancePROTECT Desktop nicht beeinträchtigen. Weitere Informationen finden Sie in KB 66448.

Hardwareanforderungen

Hardwarekomponente	Anforderungen
Prozessor (CPU)	Mindestens zwei Prozessorkerne: • Unterstützt den SSE2-Befehlssatz • Unterstützt den x86_64-Befehlssatz • Unterstützt Apple Silicon-Prozessoren einschließlich M1, M2 und M3; erfordert Rosetta • Unterstützt nicht den ARM-Befehlssatz für Windows und Linux
Arbeitsspeicher (RAM)	2 GB
Speicherplatz (Festplatte)	• 600 MB • Die Speicherplatznutzung kann sich je nach den aktivierten Funktionen erhöhen (z. B. Einstellung der Protokollebene auf „Ausführlich“).

Für den CylancePROTECT Desktop-Agenten für Windows erforderliche Stammzertifikate

Bei einigen Versionen von Windows erfordert der CylancePROTECT Desktop-Agent die folgenden Stammzertifikate (siehe Anforderungen: CylancePROTECT Desktop). Wenn Stammzertifikate fehlen, wird der Agent möglicherweise nicht gestartet oder das Gerät kann möglicherweise nicht mit der Verwaltungskonsole kommunizieren. Weitere Informationen zu fehlenden Stammzertifikaten finden Sie in KB66608.

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

Weitere Informationen finden Sie unter:

- Thawte Root Certificates
- PKI Repository - Microsoft PKI Services
- DigiCert Roots and Intermediates
- DigiCert Trusted Root Authority Certificates
- GlobalSign Root Certificates
- How to Download & Install Sectigo Intermediate Certificates - RSA
- Obtain the VeriSign Class 3 Public Primary Certification Authority - G5 root certificate

Anforderungen: CylanceOPTICS

Agenten

Agent	Anforderungen

CylancePROTECT Desktop-Agent	• Sie müssen den CylancePROTECT Desktop-Agenten auf einem Gerät installieren, bevor Sie den CylanceOPTICS-Agenten installieren. Der CylanceOPTICS-Agent benötigt den CylancePROTECT Desktop-Agenten, um seine Aufgabe zu erfüllen.
	• BlackBerry empfiehlt die Installation der neuesten verfügbaren Version des CylancePROTECT Desktop-Agenten, um von den neuesten Funktionen und Korrekturen zu profitieren.
	• Für den CylanceOPTICS-Agenten der Version 3.3 ist 3.1.x die mindestens erforderliche Version des CylancePROTECT Desktop-Agenten. Wenn Sie die neuen Windows-Sensoren verwenden möchten, die in CylanceOPTICS 3.3 eingeführt wurden, ist 3.2.x die erforderliche Mindestversion des CylancePROTECT Desktop-Agenten für Windows.
	• Die Versionen 3.2 und 3.1 des CylanceOPTICS-Agenten erfordern die folgenden Mindestversionen des CylancePROTECT Desktop-Agenten:
	  • Windows: 2.1.1578.x
	  • macOS: 3.0.1000.x
	  • Linux: 2.1.1590.x
	• Prüfen Sie die Desktop-Kompatibilitätsmatrix von CylancePROTECT und die Desktopanforderungen von CylancePROTECT, um sicherzustellen, dass Sie einen unterstützten CylancePROTECT Desktop-Agenten installieren und alle anderen Anforderungen erfüllen.

Agent	Anforderungen
CylanceOPTICS-Agent	• BlackBerry empfiehlt die Installation der neuesten verfügbaren Version des CylanceOPTICS-Agenten auf jedem Gerät. • CylanceOPTICS-Agent Version 3.0 oder höher ist für die Unterstützung der automatischen Speicherung erfasster Daten in der CylanceOPTICS-Cloud-Datenbank erforderlich. Frühere Versionen des Agenten speichern CylanceOPTICS-Daten in einer lokalen Datenbank auf dem Gerät. • In CylanceOPTICS-Agent 3.x werden die von den CylanceOPTICS-Sensoren erfassten Daten lokal zwischengespeichert, bevor sie an die Optics-Cloud-Datenbank gesendet werden. Wenn das Gerät offline ist, werden die Daten zwischengespeichert, bis das Gerät eine Verbindung zur Cloud-Datenbank herstellen kann. Es können maximal 1 GB Daten lokal gespeichert werden. Wenn mehr als 1 GB Daten gespeichert werden, bevor sie hochgeladen werden können, werden die Daten mit der niedrigsten Priorität gelöscht, damit Daten mit höherer Priorität zwischengespeichert werden können. • Weitere Informationen zum Upgrade des CylanceOPTICS-Agent 2.x auf 3.x finden Sie in den Versionshinweisen zu Cylance Endpoint Security. • Wenn Sie ein Upgrade von Version 2.x auf Version 3.x vornehmen, wird der gesamte Inhalt der lokalen CylanceOPTICS-Datenbank in Batches in die Cloud-Datenbank hochgeladen. • Nach dem Upgrade auf Version 3.x können Sie kein Downgrade des Agenten auf Version 2.x durchführen. Wenn Sie Version 2.x installieren möchten, müssen Sie Version 3.x deinstallieren und dann Version 2.x installieren.

Betriebssystemunterstützung und zusätzliche Anforderungen

Informationen zu den von CylanceOPTICS unterstützten Betriebssystemen finden Sie in der Cylance Endpoint Security-Kompatibilitätsmatrix Informationen zum Anzeigen von Support-Zeitplänen für alle BlackBerry-Produkte finden Sie im Referenzleitfaden zum Lebenszyklus der BlackBerry Enterprise-Software.

In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt, für die zusätzliche Anforderungen oder Überlegungen gelten. Beachten Sie, dass diese Tabelle keine umfassende Liste der unterstützten Betriebssysteme ist. Wenn ein Betriebssystem nicht in der Tabelle aufgeführt ist, bedeutet dies, dass keine zusätzlichen Anforderungen oder Überlegungen bestehen.

OS	Anforderungen oder Überlegungen
Windows-Betriebssysteme	
Windows 8.1 Windows 7 SP1	Weitere Informationen finden Sie in diesem Microsoft-Artikel zu zusätzlichen Abhängigkeiten für die Unterstützung von .NetCore.
macOS-Betriebssysteme	
macOS Sonoma (14.x) macOS Ventura (13.x) macOS Monterey (12.x) macOS Big Sur (11.x)	• Aktivieren Sie den vollen Datenträgerzugriff. Weitere Informationen finden Sie unter KB 66427. • Siehe Konfigurationsanforderungen für macOS 11.x und höher.

OS	Anforderungen oder Überlegungen
macOS Catalina (10.15)	Aktivieren Sie den vollen Datenträgerzugriff. Weitere Informationen finden Sie unter KB 66427.
Linux-Betriebssysteme	
Alle unterstützten Linux-Systeme	• kernel-headers und kernel-devel sind erforderlich und die Version muss mit dem ausgeführten Kernel übereinstimmen. Während der Installation zeigt der Paket-Manager die erforderlichen Versionen an. Für unterstützte Ubuntu- und Debian-Systeme ist linux-headers das Äquivalent zu kernel-headers. • Eines der folgenden Linux-Sensorpakete ist erforderlich: eBPF, Netlink (mit Unterstützung von Multicast-Netlink-Socket 3.16 oder höher oder deinstalliertem Audit-Daemon) oder Auditdsp (auditd- und auditdsp-Plugins für den Start beim Boot-Vorgang aktiviert). Für optimale Leistung in Verbindung mit dem CylanceOPTICS-Agent wird eBPF empfohlen. Wenn eBPF nicht verfügbar ist, versucht der Agent, Netlink für die nächsthöhere Leistungsstufe zu verwenden. Wenn Netlink nicht verfügbar ist, versucht der Agent, Auditdsp zu verwenden. Die verfügbaren Sensorpakete hängen von der Version Ihres Betriebssystems ab.
RHEL/CentOS 8.x RHEL/CentOS 7.x	• Für RHEL/CentOS 8.x ist ncurses-compat-libs erforderlich, wenn auf den Geräten nicht CylanceOPTICS-Agent Version 3.2.1140-x oder höher ausgeführt wird. • Firewalld muss aktiviert sein und ausgeführt werden, um die Gerätesperrfunktion zu unterstützen. Firewalld ist standardmäßig mit RHEL/CentOS verfügbar.
Amazon Linux 2	• ncurses-compat-libs ist erforderlich, wenn auf den Geräten nicht CylanceOPTICS-Agent Version 3.2.1140-15000 oder höher ausgeführt wird. • Firewalld muss aktiviert sein und ausgeführt werden, um die Gerätesperrfunktion zu unterstützen. Firewalld muss auf Amazon Linux 2 manuell installiert werden.
Oracle Linux Server UEK 8 (64 Bit) Oracle Linux Server 8 (64 Bit) Oracle Linux Server 7 (64 Bit) Oracle Linux Server UEK 7 (64 Bit)	• ncurses-compat-libs ist erforderlich, wenn auf den Geräten nicht CylanceOPTICS-Agent Version 3.2.1140-37000 oder höher ausgeführt wird. • Firewalld muss aktiviert sein und ausgeführt werden, um die Gerätesperrfunktion zu unterstützen. Firewalld ist standardmäßig mit Oracle Linux verfügbar.
Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04	• Ubuntu 20.04 erfordert libtinfo5, wenn auf den Geräten nicht CylanceOPTICS-Agent Version 3.2.1140-x oder höher ausgeführt wird. • Firewalld muss aktiviert sein und ausgeführt werden, um die Gerätesperrfunktion zu unterstützen. Firewalld muss für Ubuntu manuell installiert werden.

OS	Anforderungen oder Überlegungen
SUSE Enterprise Linux 15 SP4 SUSE Enterprise Linux 15 SUSE Enterprise Linux 12	• policycoreutils ist erforderlich. • Für SUSE 15.x ist außerdem kernel-default-devel zur Anpassung an den Kernel erforderlich. libncurses5 ist ebenfalls erforderlich, es sei denn, auf den Geräten wird CylanceOPTICS-Agent Version 3.2.1140-29000 oder höher ausgeführt. • Firewalld muss für die Unterstützung der Gerätesperrfunktion unter SUSE 15.x aktiviert sein und ausgeführt werden. Firewalld ist standardmäßig mit SUSE 15.x verfügbar Für SUSE 12 wird die Gerätesperrfunktion nicht unterstützt.
Debian 11 Debian 10	• Debian 10-Geräte benötigen iptables 1.8.5 oder höher, um die Gerätesperrfunktion zu unterstützen. • Firewalld muss aktiviert sein und ausgeführt werden, um die Gerätesperrfunktion zu unterstützen. Firewalld muss für Debian manuell installiert werden.

Kompatibilität mit anderen EDR-Lösungen

Der CylanceOPTICS-Agent ist nicht mit anderen EDR-Lösungen (Endpoint Detection and Response, Endpunkterkennung und Reaktion) kompatibel, die auf demselben Gerät installiert sind. Entfernen Sie alle EDR-Lösungen von Drittanbietern vom Gerät, bevor Sie den CylanceOPTICS-Agenten installieren und aktivieren.

Hardware

Element	Anforderungen
Prozessor (CPU)	• Im allgemeinen Einsatz nur 1 % zusätzliche CPU-Belastung • Bei hoher, anhaltender Belastung können je nach Belastung zusätzlich 5 % bis 25 % CPU-Bursts erforderlich sein.
Arbeitsspeicher (RAM)	Der Agent benötigt je nach Belastung 0,2 bis 1,0 GB zusätzlichen Speicher.
Speicherplatz (Festplatte)	Mindestens 1 GB • Für CylanceOPTICS-Agent 2.x und früher sind mindestens 1 GB für die lokale Datenbank erforderlich. • Für CylanceOPTICS 3.0 und höher werden mindestens 1 GB für das Caching der CylanceOPTICS-Sensordaten empfohlen, bevor das Gerät die Daten in die CylanceOPTICS-Cloud-Datenbank hochladen kann, wenn es online ist.

Virtuelle Maschinen

CylanceOPTICS wird für virtuelle Maschinen unterstützt. Informationen zu Anforderungen, Bereitstellungsrichtlinien und Best Practices finden Sie unter Anhang: Best Practices für die Bereitstellung von CylancePROTECT Desktop auf virtuellen Maschinen unter Windows. Wenn Sie CylanceOPTICS für eine virtuelle Maschine verwenden, empfiehlt BlackBerry die Deaktivierung des Sensors für die erweiterte WMI-Sichtbarkeit, um die Anzahl der aufgezeichneten Ereignisse zu reduzieren.

Anforderungen: CylancePROTECT Mobile-App

Element	Beschreibung
OS	Weitere Informationen finden Sie in der Kompatibilitätsmatrix für Cylance Endpoint Security.
Unterstützte Gerätebrowser	Aktuelle Version von: • Android: Google Chrome, Samsung Internet, Firefox, Brave • iOS: Safari
Gerätekonfiguration	• Bitten Sie die Benutzer, in ihrem standardmäßigen mobilen Browser JavaScript zu aktivieren. Dies ist erforderlich, um die CylancePROTECT Mobile-App zu aktivieren. • Bitten Sie Android-Benutzer, nach der Installation der CylancePROTECT Mobile-App Hintergrundaktivitäten für diese zuzulassen.

Anforderungen: BlackBerry Connectivity Node

Software

Element	Beschreibung
Java Runtime Environment	JRE 17 (neueste Update-Version, 64 Bit)

Hardware

Komponente	BlackBerry Connectivity Node
Prozessor (CPU)	6 Prozessorkerne, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) oder gleichwertig
Arbeitsspeicher (RAM)	12 GB
Speicherplatz (Festplatte)	64 GB

Zusätzliche BlackBerry Connectivity Node-Anforderungen

- Wählen Sie ein Verzeichniskonto mit Leseberechtigung für jede konfigurierte Verzeichnisverbindung, das der BlackBerry Connectivity Node für den Zugriff auf das Unternehmensverzeichnis verwenden kann.
- Verwenden Sie ein Windows-Konto mit Berechtigungen zum Installieren und Konfigurieren der Software auf dem Computer, der den BlackBerry Connectivity Node hostet.

- Überprüfen Sie, ob die folgenden ausgehenden Ports in der Firewall Ihres Unternehmens geöffnet sind, sodass die BlackBerry Connectivity Node-Komponenten mit der BlackBerry Infrastructure kommunizieren können (<*region*>>.bbsecure.com, z. B. ca.bbsecure.com):
  - 443 (HTTPS) zum Aktivieren des BlackBerry Connectivity Node
  - 3101 (TCP) für alle übrigen ausgehenden Verbindungen
- Installieren Sie die Software auf einer Windows Server-Version, die von Microsoft unterstützt wird.
- Sie können BlackBerry Connectivity Node unter englisch-, französisch-, spanisch-, japanisch- oder deutschsprachigen Versionen des Betriebssystems installieren.

Anforderungen: CylanceGATEWAY Connector

Hardware

Komponente	CylanceGATEWAY Connector
Prozessor (CPU)	Zwei Prozessorkerne
Arbeitsspeicher (RAM)	5 GB
Speicherplatz (Festplatte)	2 GB

AWS

Element	Beschreibung
Instanztyp	BlackBerry empfiehlt eine Instanz des Typs c6in oder c5n für Produktionsumgebungen.

Anforderungen: CylanceGATEWAY-Agenten

Wenn Sie die CylanceGATEWAY-Funktion für Ihre mobilen Benutzer aktiviert haben, kann der Benutzer den Arbeitsmodus über die CylancePROTECT Mobile-App aktivieren. Weitere Informationen zu Anforderungen für CylancePROTECT Mobile finden Sie unter Anforderungen: CylancePROTECT Mobile-App.

Element	Anforderungen
Prozessor (CPU)	• Unterstützt alle Apple-Geräte, einschließlich Apple Silicon-Geräte über Rosetta 2 • Unterstützt alle x64-basierten Prozessoren • Unterstützt keine 32-Bit-Betriebssysteme • Unterstützt keine ARM-Geräte

Element	Anforderungen
OS	Informationen zu den von CylanceGATEWAY-Agent unterstützten Betriebssystemen finden Sie in der Cylance Endpoint Security-Kompatibilitätsmatrix Informationen zum Anzeigen von Support-Zeitplänen für alle BlackBerry-Produkte finden Sie im Referenzleitfaden zum Lebenszyklus der BlackBerry Enterprise-Software.

Anforderungen: CylanceAVERT

Element	Beschreibung
CylanceAVERT-Agent	CylanceAVERT ist ein im Lieferumfang enthaltenes Installationsprogramm, das das CylanceAVERTMicrosoft Outlook Plug-in und die Browsererweiterungen für Chrome, Firefox und Microsoft Edge enthält.
CylancePROTECT Desktop-Agent	CylancePROTECT Desktop-Agent Version 3.1 oder höher.
Microsoft Outlook-Unterstützung	Informationen zu den Betriebssystemen und Microsoft Outlook-Versionen, die von CylanceOPTICS unterstützt werden, finden Sie in der Cylance Endpoint Security-Kompatibilitätsmatrix. Informationen zum Anzeigen von Support-Zeitplänen für alle BlackBerry-Produkte finden Sie im Referenzleitfaden zum Lebenszyklus der BlackBerry Enterprise-Software.
.NET	• Microsoft .NET 4.6.2 oder höher • .NET Standard 2.0 oder höher
Microsoft Visual C++	Microsoft Visual C++ 2017 Redistributable oder höher

Cylance Endpoint Security-Netzwerkanforderungen

Cylance Endpoint Security-Agenten

Port 443 (HTTPS) muss geöffnet sein, damit die Cylance Endpoint Security-Desktop-Agenten mit der Verwaltungskonsole kommunizieren können.

Die Agenten kommunizieren über sichere WebSockets (WSS) und müssen diese Verbindung direkt herstellen können. Konfigurieren Sie das Netzwerk Ihres Unternehmens so, dass Verbindungen zu den folgenden Domänen zugelassen werden.

Hinweis:

- Die Verwaltungskonsole wird von AWS gehostet und hat keine festen IP-Adressen. Sie können HTTPS-Datenverkehr auf *.cylance.com zulassen. Für den Host cylance-optics-files-use1.s3.amazonaws.com (und ähnliche Hosts für andere Regionen) wird empfohlen, diesen spezifischen Host zuzulassen. Es wird nicht empfohlen, *.amazonaws.com zuzulassen, da dadurch das Netzwerk für andere Hosts geöffnet werden kann.

- Beachten Sie, dass die Domain api2.cylance.com veraltet ist, jedoch zur Unterstützung älterer CylancePROTECT Desktop-Agenten offen gehalten wird. api2.cylance.com leitet zum Zweck der Bedrohungsanalyse und Risikobewertung an dasselbe Ziel wie api.cylance.com weiter.

Element	Beschreibung
Nordamerika	Erforderlich für die Anmeldung an der Cylance-Konsole: • login.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com
	Erforderlich für CylancePROTECT Desktop: • data.cylance.com • protect.cylance.com • update.cylance.com • api.cylance.com • download.cylance.com • venueapi.cylance.com
	Erforderlich für CylanceOPTICS: • cylance-optics-files-use1.s3.amazonaws.com • opticspolicy.cylance.com • content.cylance.com • rrws-use1.cylance.com • collector.cylance.com • scalar-api-use1.cylance.com • cement.cylance.com
	Erforderlich für CylanceGATEWAY-Agent: • idp.blackberry.com • quip.webapps.blackberry.com • us1.cs.blackberry.com Erforderlich für CylanceGATEWAY Connector: deb.nodesource.com Erforderlich für CylanceGATEWAY-Agent und für CylanceGATEWAY Connector: us1.bg.blackberry.com Weitere Informationen finden Sie unter KB79017.
Asien-Pazifik Nordost	Erforderlich für die Anmeldung an der Cylance-Konsole: • login-apne1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com

Element	Beschreibung
	Erforderlich für CylancePROTECT Desktop: • data-apne1.cylance.com • protect-apne1.cylance.com • update-apne1.cylance.com • api.cylance.com • download.cylance.com • venueapi-apne1.cylance.com
	Erforderlich für CylanceOPTICS: • 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
	Erforderlich für CylanceGATEWAY-Agent: • idp.blackberry.com • quip.webapps.blackberry.com • jp1.cs.blackberry.com Erforderlich für CylanceGATEWAY Connector: deb.nodesource.com Erforderlich für CylanceGATEWAY-Agent und für CylanceGATEWAY Connector: jp1.bg.blackberry.com Weitere Informationen finden Sie unter KB79017.
Asien-Pazifik Südost	Erforderlich für die Anmeldung an der Cylance-Konsole: • login-au.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com
	Erforderlich für CylancePROTECT Desktop: • data-au.cylance.com • protect-au.cylance.com • update-au.cylance.com • api.cylance.com • download.cylance.com • venueapi-au.cylance.com

Element	Beschreibung
	Erforderlich für CylanceOPTICS: • 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
	Erforderlich für CylanceGATEWAY-Agent: • idp.blackberry.com • quip.webapps.blackberry.com • au1.cs.blackberry.com Erforderlich für CylanceGATEWAY Connector: deb.nodesource.com Erforderlich für CylanceGATEWAY-Agent und für CylanceGATEWAY Connector: au1.bg.blackberry.com Weitere Informationen finden Sie unter KB79017.
Mitteleuropa	Erforderlich für die Anmeldung an der Cylance-Konsole: • login-euc1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com
	Erforderlich für CylancePROTECT Desktop: • data-euc1.cylance.com • protect-euc1.cylance.com • update-euc1.cylance.com • api.cylance.com • download.cylance.com • venueapi-euc1.cylance.com
	Erforderlich für CylanceOPTICS: • 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

Element	Beschreibung
	Erforderlich für CylanceGATEWAY-Agent: • idp.blackberry.com • quip.webapps.blackberry.com • eu1.cs.blackberry.com Erforderlich für CylanceGATEWAY Connector: deb.nodesource.com Erforderlich für CylanceGATEWAY-Agent und für CylanceGATEWAY Connector: eu1.bg.blackberry.com Weitere Informationen finden Sie unter KB79017.
Südamerika	Erforderlich für die Anmeldung an der Cylance-Konsole: • login-sae1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com
	Erforderlich für CylancePROTECT Desktop: • data-sae1.cylance.com • protect-sae1.cylance.com • update-sae1.cylance.com • api.cylance.com • download.cylance.com • venueapi-sae1.cylance.com
	Erforderlich für CylanceOPTICS: • 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
	Erforderlich für CylanceGATEWAY-Agent: • idp.blackberry.com • quip.webapps.blackberry.com • br1.cs.blackberry.com Erforderlich für CylanceGATEWAY Connector: deb.nodesource.com Erforderlich für CylanceGATEWAY-Agent und für CylanceGATEWAY Connector: br1.bg.blackberry.com Weitere Informationen finden Sie unter KB79017.

Element	Beschreibung
GovCloud	Erforderlich für die Anmeldung an der Cylance-Konsole: • login.us.cylance.com • idp.blackberry.com • idp.cs.cylance.com
	Erforderlich für CylancePROTECT Desktop: • 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
	Erforderlich für CylanceOPTICS: • 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

Die CylancePROTECT Mobile-App erfordert eine sichere, direkte Verbindung zu den folgenden URLs, um mit den CylancePROTECT Mobile-Cloud-Diensten zu kommunizieren. Wenn Geräte mit dem Wi-Fi-Netzwerk Ihres Unternehmens verbunden sind, muss Ihre Netzwerkkonfiguration folgende Verbindungen zulassen:

- CylancePROTECT Mobile-Cloud-Dienste:
  - 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
- Gateway für allgemeine Dienste:
  - 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-Anforderungen

Konfigurieren eines Proxys für die CylancePROTECT Desktop- und CylanceOPTICS-Agenten

- Wenn Sie sowohl den CylancePROTECT Desktop-Agenten als auch den CylanceOPTICS-Agenten auf einem Gerät so konfigurieren möchten, dass ein Proxyserver für die ausgehende Kommunikation mit BlackBerry-Servern verwendet wird, navigieren Sie im Registrierungs-Editor zu HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop und erstellen Sie den String-Wert REG_SZ:
  - Wertname = ProxyServer
  - Wertdaten = *<proxyIP:port>* (z. B. http://123.45.67.89:8080)
- Der Proxy muss nicht autorisierte Anfragen akzeptieren. Die SSL-Prüfung wird nicht unterstützt und muss für den gesamten Agentendatenverkehr umgangen werden (*.cylance.com).

Proxyoptionen für den CylanceOPTICS-Agent

- Der CylanceOPTICS-Agent ist Proxy-fähig und fragt das .NET-Framework ab, um die verfügbaren Proxy-Einstellungen zu identifizieren und zu verwenden. Wenn Sie den ProxyServer-Wert in der Registrierung konfiguriert haben, verwendet der CylanceOPTICS-Agent den angegebenen Proxy. Der CylanceOPTICS-Agent versucht zuerst, als lokales System und dann als aktuell angemeldeter Benutzer zu kommunizieren.
- Wenn Sie den CylanceOPTICS-Agent so konfigurieren, dass er einen Proxy verwendet, der Agent aber nicht mit den Cloud-Diensten kommunizieren kann, versucht der Agent, den Proxy zu umgehen, um eine direkte Verbindung herzustellen. Auf Windows- und macOS-Geräten können Sie diese Proxy-Umgehung deaktivieren. Gehen Sie wie folgt vor, bevor Sie den CylanceOPTICS-Agenten installieren:

Plattform	Schritte
Windows	Erstellen Sie in HKLM\SOFTWARE\Cylance\Optics\ den String-Wert REG_SZ: • Wertname = DisableProxyBypass • Wertdaten = True

macOS	• Fügen Sie unter /Library/Application Support/Cylance/Desktop/registry/LocalMachine/Software/Cylance/Desktop/ folgende Elemente zur Datei „values.xml“ hinzu:
	`<value name=“ProxyServer” type=“string”>http://proxy_server_IP:port</value>`
	• Erstellen Sie unter /Library/Application Support/Cylance/Optics/Configuration eine Datei „ExternalConfig.xml“ mit folgenden Elementen:
	`<?xml version=“1.0” encoding=“utf-8”?><EnforceProxyServer>true</EnforceProxyServer>`

- Wenn von CylanceOPTICS ein Erkennungsereignis erstellt wird, das eine signierte Datei als Artefakt beinhaltet, verwendet es einen Befehl der Windows-API, um die Signatur oder das Zertifikat zu validieren. Der Befehl sendet eine Validierungsanforderung an einen OCSP-Server. Die OCSP-Serveradresse wird durch Windows bestimmt. Wenn Ihr Proxyserver versucht, externen Datenverkehr an einen OCSP-Server zu senden, aktualisieren Sie die Proxyeinstellungen auf den Geräten, um Verbindungen mit dem OCSP-Server zu ermöglichen.

Linux: Konfigurieren der CylancePROTECT Desktop- und CylanceOPTICS-Agenten zur Verwendung eines Proxyservers

Verwenden Sie bei unterstützten Versionen von RHEL, CentOS, Ubuntu, Amazon, Linux 2 und SUSE 15 die folgenden Befehle, um die Agenten so zu konfigurieren, dass sie einen nicht authentifizierten oder authentifizierten Proxy verwenden. Diese Befehle können vor der Installation der Agenten verwendet werden. Mit den folgenden Befehlen konfigurieren Sie einen Proxy für den CylancePROTECT Desktop-Agent. So legen Sie einen Proxy für den CylanceOPTICS-Agenten fest:

- Ersetzen Sie alle Instanzen von „cylancesvc“ durch „cyoptics“.
- Duplizieren Sie alle „http_proxy“-Zeilen und ersetzen Sie „http_proxy“ durch „https_proxy“. In den meisten Fällen verwendet https_proxy denselben Wert wie http_proxy, da HTTPS-Datenverkehr über TCP Connect getunnelt wird. Wenn Ihr Unternehmen jedoch einen HTTPS-Terminierungs-Proxyserver verwendet, geben Sie den entsprechenden Wert für https_proxy an.

Nicht authentifizierter 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
```

Authentifizierter 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
```

Anmelden an der Verwaltungskonsole

Nach der Aktivierung Ihres Kontos erhalten Sie eine E-Mail mit Ihren Anmeldeinformationen für die Cylance Endpoint Security-Verwaltungskonsole. Klicken Sie auf den Link in der E-Mail, um die Anmeldeseite zu öffnen, oder navigieren Sie zu:

- **Nordamerika:** https://login.cylance.com
- **Asien-Pazifik Nordost:** https://login-apne1.cylance.com
- **Asien-Pazifik Südost:** https://login-au.cylance.com
- **Mitteleuropa:** https://login-euc1.cylance.com
- **Südamerika Ost:** https://login-sae1.cylance.com
- **GovCloud:** https://login.us.cylance.com

Die E-Mail-Adresse dient zur Kontoanmeldung. Nachdem Sie ein Kennwort erstellt haben, können Sie zur Konsole wechseln.

Kennwortanforderungen

Ihr Kennwort muss drei der folgenden Zeichen enthalten:

- Ein Kleinbuchstabe
- Ein Großbuchstabe
- Ein Sonderzeichen (z. B. * # $ %)
- Ein numerisches Zeichen
- Ein Unicode-Zeichen (z. B. ♥✷☆)

Sitzungs-Timeout

Die Sitzung wird eine Stunde nach der letzten erfolgreichen Authentifizierung beendet.

Benutzerdefinierte Authentifizierung

Wichtig: Die benutzerdefinierte Authentifizierung ist veraltet und wird in naher Zukunft entfernt. Wenn Sie eine benutzerdefinierte Authentifizierung für den Zugriff auf Cylance Endpoint Security verwenden, können Sie Ihren externen IDP zu einem Authentifikator migrieren und eine erweiterte Authentifizierung für den Zugriff auf die Cylance-Konsole verwenden. Weitere Informationen zur verbesserten Authentifizierung finden Sie unter Erweiterte Authentifizierungsanmeldung. Eine Anleitung zur Konfiguration Ihres externen IDP als Authentifikator finden Sie unter Migrieren externer IDPs von der älteren benutzerdefinierten Authentifizierung zu einem modernen Authentifikator-Framework.

Verwenden Sie externe Identitätsanbieter (IdP), um sich bei der Verwaltungskonsole anzumelden. Dazu müssen die Einstellungen mit Ihrem IdP konfiguriert werden, um ein X.509-Zertifikat und eine URL zur Überprüfung der IdP-Anmeldung zu erhalten. Für die benutzerdefinierte Authentifizierung wird Microsoft SAML 2.0 verwendet. Diese Funktion ist mit OneLogin, Okta, Microsoft Azure und PingOne kompatibel. Sie bietet auch eine benutzerdefinierte Einstellung und sollte auch mit anderen IdPs funktionieren, die Microsoft SAML 2.0 unterstützen.

Beispiele für die Verwendung der benutzerdefinierten Authentifizierung finden Sie in den folgenden Artikeln.

- Microsoft Azure
- Okta
- OneLogin
- PingOne
- Verwenden von SAML 2.0

Hinweis: Active Directory Federation Services (ADFS) wird von der benutzerdefinierten Authentifizierung nicht unterstützt.

Konfigurieren der benutzerdefinierten Authentifizierung

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Anwendung**.
2. Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Authentifizierung**. Es werden Konfigurationsoptionen angezeigt.
3. Wählen Sie die Optionen aus, die Sie für die Authentifizierung verwenden möchten. Eine Beschreibung der Optionen finden Sie unter Benutzerdefinierte Authentifizierungsbeschreibungen.
4. Klicken Sie auf **Speichern**.

Benutzerdefinierte Authentifizierungsbeschreibungen

Option	Beschreibung
Strong Authentication	Wählen Sie diese Option aus, um Multi-Faktor-Authentifizierungszugriff bereitzustellen.
Einmalige Anmeldung	Wählen Sie diese Option aus, um Zugriff mit einmaliger Anmeldung (Single Sign-On, SSO) bereitzustellen. Die Auswahl von Strong Authentication oder SSO hat keinen Einfluss auf die benutzerdefinierten Authentifizierungseinstellungen, da alle Konfigurationseinstellungen vom Identitätsprovider (IdP) verarbeitet werden.
Kennwortanmeldung zulassen	Wenn Sie diese Option auswählen, können Sie sich direkt bei der Konsole per SSO anmelden. Auf diese Weise können Sie Ihre SSO-Einstellungen testen, ohne von der Konsole gesperrt zu werden. Es wird empfohlen, diese Funktion zu deaktivieren, sobald Sie sich mit SSO erfolgreich bei der Konsole angemeldet haben.
Anbieter	Wählen Sie den Dienstanbieter für die benutzerdefinierte Authentifizierung aus.
X.509-Zertifikat	Geben Sie die X.509-Zertifizierungsinformationen ein.
Anmelde-URL	Geben Sie die URL für die benutzerdefinierte Authentifizierung ein.

Migrieren externer IdPs von der benutzerdefinierten Authentifizierung zu einem Authentifikator

Wenn Sie sich mit einem externen Identitätsanbieter (Identity Provider, IdP), der für die benutzerdefinierte Authentifizierung konfiguriert ist, bei der Verwaltungskonsole anmelden, müssen Sie sich mit den externen IdP-Zugangsdaten über den Link „Oder melden Sie sich mit Ihrem externen Identitätsanbieter an“ anmelden. BlackBerry empfiehlt, dass Sie Ihren externen IdP als Authentifikator konfigurieren und eine Authentifizierungsrichtlinie verwenden, um sich über den Hauptbildschirm mit Ihren IdP-Anmeldeinformationen anzumelden. Wenn Sie Ihren externen IdP als Authentifikator konfigurieren, erhalten Sie mehr Präzision und Flexibilität bei der Authentifizierungskonfiguration.

Um einen externen IdP für die Anmeldung bei der Verwaltungskonsole über den Hauptbildschirm für die Anmeldung zu konfigurieren, gehen Sie wie folgt vor. Weitere Informationen finden Sie unter Migrieren externer IdPs von der benutzerdefinierten Authentifizierung zu einem Authentifikator.

Wenn Sie Ihren vorhandenen IDP vor Dezember 2023 als Authentifikator konfiguriert haben und Benutzern den direkten Zugriff auf die Cylance-Konsole über das IDP-Benutzerportal ermöglichen möchten, siehe Erweiterte Authentifizierungsanmeldung.

Schritt	Aktion
1	Lesen Sie Überlegungen zum Hinzufügen von SAML-Authentifikatoren.
2	Melden Sie sich bei der Cylance-Konsole mit Ihrem externen IdP an.
3	Konfigurieren Sie den externen IdP für die Kommunikation mit Cylance Endpoint Security. • Notieren Sie die Informationen der benutzerdefinierten Authentifizierung. • Konfigurieren Sie den Authentifikator.
4	Verwalten von Authentifizierungsrichtlinien für Mandanten der den Authentifikator verwendet, den Sie erstellt haben. **Hinweis:** Erstellen Sie als Sicherheitsmaßnahme eine Benutzerrichtlinie, die nur das Cylance-Konsolenkennwort beinhaltet, und weisen Sie sie einem Administrator zu.
5	Vergewissern Sie sich, dass das Kontrollkästchen Kennwortanmeldung zulassen (Einstellungen > Anwendung > Benutzerdefinierte Authentifizierung) aktiviert ist. Bei Auswahl dieser Option können Sie sich direkt bei der Konsole anmelden und SSO nutzen. Aktivieren Sie diese Option, um Ihre SSO-Einstellungen zu testen, ohne von der Konsole gesperrt zu werden.
6	Melden Sie sich über die Cylance-Konsole auf dem Hauptbildschirm für die Anmeldung an der Konsole an und testen Sie die Richtlinie für externe IdP-Anmeldeinformationen.
7	(Optional) Deaktivieren Sie die benutzerdefinierte Authentifizierung (Einstellungen > Anwendung).

Erweiterte Authentifizierungsanmeldung

Die Verwaltungskonsole bietet erweiterte Authentifizierungsfunktionen, einschließlich lokaler Multi-Faktor-Authentifizierung und detailliertere Authentifizierungsrichtlinien und Richtlinienzuweisungen. Sie können bei der Konfiguration der Umgebung festlegen, welche Authentifizierungstypen Administratoren bei der Anmeldung an der Cylance-Verwaltungskonsole durchlaufen und Benutzer bei der Aktivierung von Cylance Endpoint Security-Apps oder -Agenten durchlaufen müssen. Standardmäßig greifen Administratoren mithilfe des Konsolenkennworts Cylance auf die Verwaltungskonsole zu, und Benutzer aktivieren mit diesem Kennwort Cylance Endpoint Security-Apps und -Agenten. Für Mandanten, die ab März 2024 erstellt wurden, müssen Administratoren standardmäßig ein einmaliges Kennwort eingeben, um auf die Cylance-Konsole zugreifen zu können, nachdem sie ihr Konsolenkennwort eingerichtet haben.

Sie können Authentifizierungsrichtlinien für Ihren Mandanten erstellen, die die Authentifizierungstypen angeben, die von allen Administratoren und Benutzern auf dem Mandanten durchlaufen werden müssen. Es kann nur eine Mandantenrichtlinie für die Cylance-Konsolenanmeldung, die Cylance Endpoint Security-Apps und Cylance Endpoint Security Desktop-Agenten erstellt werden. Sie können Authentifizierungsrichtlinien für

Benutzer erstellen, die die Authentifizierungstypen angeben, die von Administratoren und Benutzern auf dem Mandanten durchlaufen werden müssen. Die Authentifizierung, die der Mandantenrichtlinie und der Authentifizierungsrichtlinie hinzugefügt wird, muss in der Reihenfolge abgeschlossen werden, in der sie in der Richtlinie angegeben ist. Als Sicherheitsmaßnahme können Sie einen Administrator für den Zugriff auf die Cylance-Konsole mit eigenem Benutzernamen und einem starken Kennwort konfigurieren.

Hinweis: Der aktualisierte Anmeldeablauf ist jetzt die einzige Methode für den Zugriff auf die Cylance-Konsole. Alle Authentifizierungsrichtlinien, die Sie während des Vorschauzeitraums in Ihrer Konsole angewendet haben, sind nun wirksam.

Mit einer der folgenden Aktionen konfigurieren Sie die erweiterte Authentifizierung für die Anmeldung:

Konfigurieren der erweiterten Authentifizierung für die Anmeldung an der Cylance-Konsole

Wenn Ihr Mandant vor März 2024 erstellt wurde, führen Sie diese Schritte aus, um Ihre Benutzer so zu konfigurieren, dass sie sich bei der Cylance-Konsole zusätzlich zum Cylance-Kennwort mit einem Authentifikator (z. B. Einmalkennwort) authentifizieren können. Eine Anleitung zum Hinzufügen des Einmalkennwort-Authentifikators zu Ihrer Mandantenrichtlinie finden Sie unter Hinzufügen der Einmalkennwort-Authentifizierung für Administratoren für den Zugriff auf die Cylance-Konsole.

Schritt	Aktion
1	Melden Sie sich mit Ihrem vorhandenen Benutzernamen und Kennwort bei der Cylance-Konsole an.
2	Fügen Sie einen Authentifikator hinzu (z. B. Einmalkennwort oder Unternehmensauthentifizierung). Standardmäßig sind die folgenden Authentifikatoren für die Verwendung in Ihrer Umgebung konfiguriert: Einmalkennwort, Cylance-Konsolenkennwort und Unternehmensauthentifizierung.
3	Erstellen Sie eine Authentifizierungsrichtlinie, die das Kennwort und den Authentifikator enthält, die Sie erstellt haben (optional). **Hinweis:** Erstellen Sie als Sicherheitsmaßnahme eine Authentifizierungsrichtlinie, die nur das Cylance-Konsolenkennwort beinhaltet, und weisen Sie sie einem Administrator zu.
4	Erstellen Sie eine Mandantenrichtlinie für Administratoren und Benutzer.

Entfernen der Einmalkennwort-Authentifizierung für die Anmeldung an der Cylance-Konsole

Mandanten, die im März 2024 oder später erstellt wurden, müssen jedes Mal ein Einmalkennwort eingeben, nachdem sie das Kennwort der Cylance-Konsole eingegeben haben, bevor sie auf die Konsole zugreifen können. Führen Sie diese Schritte aus, wenn Sie die Einmalkennwort-Anforderung entfernen möchten, mit der sich die Benutzer bei der Konsole authentifizieren müssen. Eine Anleitung zum Entfernen des Einmalkennwort-Authentifikators aus Ihrer Mandantenrichtlinie finden Sie unter Entfernen der Einmalkennwort-Authentifizierung für Administratoren für den Zugriff auf die Cylance-Konsole.

Schritt	Aktion
1	Melden Sie sich mit Ihrem vorhandenen Benutzernamen, dem Kennwort und dem Einmalkennwort bei der Cylance-Konsole an.

Schritt	Aktion
2	Entfernen Sie den Einmalkennwort-Authentifikator aus der Mandantenrichtlinie der Administrationskonsole.
3	Melden Sie sich bei der Cylance-Konsole an, und testen Sie die Kennwortrichtlinie der Cylance-Konsole.

Konfigurieren eines neuen IDP-SAML-Authentifikators für SSO- und IDP-initiierten Zugriff auf die Cylance-Konsole

Führen Sie diese Schritte aus, wenn Sie einen neuen IDP-SAML-Authentifikator konfigurieren möchten, mit dem sich die Benutzer bei der Cylance-Konsole authentifizieren können. Die Benutzer können ihre IDP-Anmeldedaten verwenden, um über die Anmeldeseite auf die Konsole zuzugreifen, oder den IDP-initiierten SSO verwenden, um über das IDP-Benutzerportal auf die Konsole zuzugreifen. Eine Übersicht zur Konfiguration Ihrer IDP-SAML finden Sie unter Konfigurieren von IDP-SAMLs für die erweiterte Authentifizierung und den IDP-initiierten Zugriff auf die Cylance-Konsole. Wählen Sie dort Ihren IDP aus.

Schritt	Aktion
1	Erstellen Sie in der IDP-Umgebung eine neue SAML-Anwendung.
2	Konfigurieren Sie den IDP für die Kommunikation mit Cylance Endpoint Security.
3	Fügen Sie in der Cylance-Konsole einen Authentifikator hinzu.
4	Erstellen Sie eine Authentifizierungsrichtlinie, die das Kennwort und den Authentifikator enthält, die Sie erstellt haben. **Hinweis:** Erstellen Sie als Sicherheitsmaßnahme eine Authentifizierungsrichtlinie, die nur das Cylance-Konsolenkennwort beinhaltet, und weisen Sie sie einem Administrator zu.
5	Aktualisieren Sie in der IDP-Umgebung die SSO-Callback-URL, die Sie in der Cylance-Konsole generiert haben.
6	Melden Sie sich über die Cylance-Konsole auf dem Hauptbildschirm für die Anmeldung an der Konsole an, und testen Sie die Richtlinie für externe IDP-Anmeldeinformationen.
7	(Optional) Deaktivieren Sie die benutzerdefinierte Authentifizierung (Einstellungen > Anwendung).

Aktualisieren eines vorhandenen IDP-SAML-Authentifikators, um den IDP-initiierten Zugriff auf die Cylance-Konsole zu aktivieren

Führen Sie diese Schritte nur aus, wenn Ihr IDP-SAML-Authentifikator vor Dezember 2023 erstellt wurde und Sie den IDP-initiierten SSO für alle Benutzer aktivieren möchten, die über das IDP-Benutzerportal auf die Konsole

zugreifen können. Eine Anleitung finden Sie unter Aktualisieren von IDP- (SAML-)Authentifikatoren, um IDP-initiierten Zugriff auf die Cylance-Konsole zu aktivieren. Wählen Sie dort Ihren IDP.

Schritt	Aktion
1	Melden Sie sich mit Ihrem vorhandenen Benutzernamen und Kennwort bei der Cylance-Konsole an.
2	Generieren Sie im aktuellen SAML-Authentifikator eine neue SSO-Callback-URL.
3	Aktualisieren der aktuellen Authentifizierungs-Policy mit der neu generierten SSO-Callback-URL.
4	Aktualisieren Sie die SAML-Einstellungen in der IDP-Umgebung.

Mit der erweiterten Authentifizierung bei der Cylance Endpoint Security-Verwaltungskonsole anmelden

Sie können Authentifizierungsrichtlinien festlegen, um die Authentifizierungstypen anzugeben, die Administratoren durchlaufen müssen, um sich bei der Cylance Endpoint Security-Verwaltungskonsole anzumelden, und die Benutzer durchlaufen müssen, um Cylance Endpoint Security-Apps oder -Agenten zu aktivieren (z. B. die CylancePROTECT Mobile-App oder den CylanceGATEWAY-Agenten). Vor dem Zugriff auf die Cylance Endpoint Security-Verwaltungskonsole wird kurz ein Übergangsbildschirm angezeigt.

Wenn Sie sich mit einem externen IdP anmelden, der für die benutzerdefinierte Authentifizierung in der Verwaltungskonsole konfiguriert wurde („Einstellungen“ > „Benutzerdefinierte Authentifizierung“), müssen Sie sich weiterhin über den Link „Oder melden Sie sich mit Ihrem externen Identitätsanbieter an“ mit Ihren externen IdP-Zugangsdaten des Drittanbieters anmelden. BlackBerry empfiehlt, dass Sie Ihre externe IdP-Konfiguration als Authentifikator konfigurieren, damit Sie sich mit Ihren IdP-Anmeldedaten über eine Authentifizierungsrichtlinie vom Hauptbildschirm aus anmelden können. Dies bietet mehr Granularität und Flexibilität bei der Authentifizierungskonfiguration. Weitere Informationen zum Konfigurieren Ihres externen IDP als Authentifikator finden Sie unter Migrieren externer IdPs von der benutzerdefinierten Authentifizierung zu einem Authentifikator.

Wenn Sie Ihre externe IDP-Konfiguration vor Dezember 2023 als Authentifikator konfiguriert haben, können Benutzer nicht direkt über ihr externes IDP-Benutzerportal mit Single Sign-on auf die Cylance-Konsole zugreifen. Um diese Funktion zu aktivieren, müssen Sie eine neue Cylance Endpoint Security-Anmeldeanforderung für Single Sign-On generieren. Weitere Informationen zum Aktivieren der IDP-initiierten Anmeldung bei der Cylance-Konsole finden Sie unter Erweiterte Authentifizierungsanmeldung und im Abschnitt Aktualisieren des externen IDP für den SSO-Zugriff auf die Cylance-Konsole.

Bevor Sie beginnen: Erstellen Sie eine Authentifizierungsrichtlinie und weisen Sie sie Administratoren, Benutzern und Gruppen zu, denen Administratoren und Benutzer angehören.

Führen Sie eine der folgenden Aufgaben aus, um auf die Verwaltungskonsole zuzugreifen.

Zugriff	Aufgabe	Schritte
Zentraler Cylance Endpoint Security-Anmeldebildschirm.	Melden Sie sich bei Ihrem Cylance-Konto an.	**a.** Geben Sie Ihre E-Mail-Adresse ein. **b.** Klicken Sie auf **Anmelden**. **c.** Geben Sie das Kennwort ein. **d.** Klicken Sie auf **Anmelden**.

Zugriff	Aufgabe	Schritte
	Melden Sie sich mit Ihrem externen Identitätsanbieter an, der als Authentifikator konfiguriert ist.	**a.** Geben Sie Ihre E-Mail-Adresse ein. **b.** Klicken Sie auf **Anmelden**. **c.** Geben Sie das Kennwort ein. **d.** Klicken Sie auf **Anmelden**.
	Melden Sie sich mit Ihrem externen Identitätsanbieter an.	**a.** Klicken Sie auf **Mit externem Identitätsanbieter anmelden**. **b.** Geben Sie im Browser Ihre E-Mail-Adresse ein. **c.** Klicken Sie auf **Anmelden**. **d.** Geben Sie das Kennwort ein. **e.** Klicken Sie auf **Anmelden**.
Portal für Benutzer eines externen IDP	Single Sign-on mit den Anmeldeinformationen Ihres externen Identitätsanbieters.	**a.** Melden Sie sich bei Ihrem IDP-Benutzerportal an. **b.** Klicken Sie auf die Anwendung, die Ihnen zugewiesen ist.

Generieren einer neuen SSO-Callback-URL

Mithilfe der Kopieroption können Sie Ihre aktuellen Authentifikatorinformationen kopieren und die neue SSO-Callback-URL erstellen. Die Kopieroption entfernt die aktuelle SSO-Callback-URL und generiert eine neue URL, wenn der kopierte Authentifikator gespeichert wird.

Wichtig: Führen Sie diese Aufgabe nur aus, wenn Sie Ihre Umgebung für eine erweiterte Anmeldung konfiguriert haben, Ihr Authentifikator vor Dezember 2023 erstellt wurde und Sie das IDP-initiierte Single Sign-On (SSO) auf der Konsole aktivieren möchten. Um zu überprüfen, ob der Authentifikator vor Dezember 2023 erstellt wurde, öffnen Sie in der Cylance-Konsole den IDP-SAML-Authentifikator (Einstellungen > Authentifizierung).

- Wenn die SSO-Callback-URL das Format https://login.eid.blackberry.com/_/resume/saml20/<*hash*> aufweist, sind keine weiteren Maßnahmen erforderlich.
- Wenn die SSO-Callback-URL „https://idp.blackberry.com/_/resume" lautet, führen Sie die folgenden Schritte aus, um die aktualisierte URL zu generieren.

Bevor Sie beginnen: Der IDP-SAML-Authentifikator wurde vor Dezember 2023 erstellt und verwendet die nicht mehr unterstützte SSO-Callback-URL.

1. Öffnen Sie den Bildschirm „Authentifikatoren" (Einstellungen > Authentifizierung).
2. Klicken Sie auf den aktuellen IDP-SAML-Authentifikator.
3. Klicken Sie auf das Symbol „Kopieren" in der oberen rechten Ecke des Bildschirms.
4. Aktualisieren Sie den Namen des kopierten Authentifikators. Klicken Sie auf **Speichern**.
5. Öffnen Sie den kopierten Authentifikator. Erfassen Sie die **SSO-Callback-URL**.
6. Löschen Sie den vorherigen IDP-Authentifikator.

Wenn Sie fertig sind: Aktualisieren Sie die aktuelle Authentifizierungsrichtlinie mit dem kopierten Authentifikator.

Konfigurieren eines neuen Cylance Endpoint Security-Mandanten

Wenn Sie einen neuen Cylance Endpoint Security-Mandanten erstellen oder einen Mandanten auf den empfohlenen Standardstatus zurücksetzen, enthält der Mandant vorkonfigurierte Zonen und vorkonfigurierte Geräterichtlinien, mit deren Hilfe Sie Ihre Umgebung an die jeweilige Sicherheitssituation anpassen können.

Ein neuer oder auf den empfohlenen Standardzustand zurückgesetzter Mandant enthält drei vorkonfigurierte Zonen: eine für jedes Desktop-Betriebssystem (Windows, macOS und Linux). Diese Zonen sind so konfiguriert, dass neue Desktop-Geräte automatisch der entsprechenden Betriebssystemzone zugewiesen werden. Den vorkonfigurierten Zonen wird die unten beschriebene Phase-1-Geräterichtlinie zugewiesen.

Ein neuer oder zurückgesetzter Mandant enthält drei vorkonfigurierte Geräterichtlinien zur Steuerung der Funktionen von CylancePROTECT Desktop und CylanceOPTICS. Die vollständige Konfiguration jeder vorkonfigurierten Richtlinie finden Sie unter Standardeinstellungen der Konfiguration für einen neuen Cylance Endpoint Security-Mandanten.

Vorkonfigurierte Richtlinie	Beschreibung
Phase 1	Anfangskonfiguration, mit der Geräte Malware-Bedrohungen erkennen können. Erweiterte Richtlinieneinstellungen sind deaktiviert. Verwenden Sie diese Richtlinie zuerst in Ihrer Umgebung, um die Ersterkennung der Geräte zu beobachten und entsprechende Ausnahmen zu konfigurieren. Wenn Sie mit der Leistung und Wirkung dieser Richtlinie vertraut sind, können Sie mit den Geräten zur Phase-2-Richtlinie übergehen.
Phase 2	Diese Geräterichtlinie ermöglicht die Erkennung einer größeren Bandbreite von Bedrohungen einschließlich abnormaler Malware, unsicherer Skripte und Arbeitsspeicher-Exploits. Weisen Sie diese Richtlinie nur wenigen Geräten zu, um die Anzahl und Häufigkeit der Erkennung sowie den erforderlichen Untersuchungsaufwand einschätzen zu können. Dadurch können Sie die Richtlinienkonfiguration verfeinern, bevor Sie sie weiteren Geräten zuweisen. Wenn Sie mit der Leistung dieser Richtlinie vertraut sind, können Sie mit den Geräten zur Phase-3-Richtlinie übergehen.
Phase 3	Diese Geräterichtlinie basiert auf Phase 2 und passt die Einstellungen so an, dass die Geräte auf Bedrohungen achten und gleichzeitig vorbeugende Maßnahmen ergreifen können. Verwenden Sie diese Geräterichtlinie nur nach ausreichenden Tests mit der Phase-2-Richtlinie sowie nur nach der Anpassung der Phase-2-Richtlinie auf diese Richtlinie.

Während Sie die vorkonfigurierten Zonen und Geräterichtlinien testen und auswerten, können Sie die Konfiguration nach Bedarf anpassen, z. B. indem Sie Änderungen an den vorkonfigurierten Optionen vornehmen oder eine Zone bzw. Richtlinie kopieren und ändern, um zu ermitteln, welche Konfiguration am besten zu Ihrer Umgebung passt.

Cylance Endpoint Security bietet außerdem zusätzliche Optionen, mit deren Hilfe Sie einen neuen Mandanten schnell nach den Anforderungen Ihres Unternehmens konfigurieren können. Sie können die Konfiguration eines Mandanten exportieren und in einen neuen Mandanten importieren oder einen Mandanten auf die empfohlenen Standardwerte (siehe Standardeinstellungen der Konfiguration für einen neuen Cylance Endpoint Security-

Mandanten) zurücksetzen. Weitere Informationen finden Sie unter Exportieren, Importieren oder Rücksetzen der Konfiguration eines Cylance Endpoint Security-Mandanten.

Standardeinstellungen der Konfiguration für einen neuen Cylance Endpoint Security-Mandanten

Vorkonfigurierte Zonen

Vorkonfigurierte Zonen	Zugewiesene Geräterichtlinie	Standardzonenregeln
Windows-Zone	Phase 1	Automatische Zonenzuweisung, um alle neuen Windows-Geräte in diese Zone zu verschieben.
Mac-Zone	Phase 1	Automatische Zonenzuweisung, um alle neuen macOS-Geräte in diese Zone zu verschieben.
Linux-Zone	Phase 1	Automatische Zonenzuweisung, um alle neuen Linux-Geräte in diese Zone zu verschieben.

Vorkonfigurierte Geräterichtlinien

Geräterichtlinien-Einstellung	Phase-1-Richtlinie	Phase-2-Richtlinie	Phase-3-Richtlinie
Dateiaktionen			
Automatische Quarantäne mit Ausführungssteuerung: unsicher	Deaktiviert	Aktiviert	Aktiviert
Automatische Quarantäne mit Ausführungssteuerung: anormal	Deaktiviert	Deaktiviert	Aktiviert
Automatische Löschung für Dateien in Quarantäne aktivieren	Deaktiviert	Aktiviert	Aktiviert
Automatisches Hochladen: ausführbar	Aktiviert	Aktiviert	Aktiviert
Speicheraktionen			
Speicherschutz	Deaktiviert	Aktiviert	Aktiviert
Exploit: Stack Pivot	Deaktiviert	Ignorieren	Ignorieren
Exploit: Stackschutz	Deaktiviert	Ignorieren	Ignorieren
Exploit: Codeüberschreibung	Deaktiviert	Ignorieren	Ignorieren

Geräterichtlinien-Einstellung	Phase-1-Richtlinie	Phase-2-Richtlinie	Phase-3-Richtlinie
Exploit: RAM-Scraping	Deaktiviert	Alarm	Sperren
Exploit: schädliche Payload	Deaktiviert	Ignorieren	Ignorieren
Exploit: Systemaufrufüberwachung	Deaktiviert	Ignorieren	Ignorieren
Exploit: direkte Systemaufrufe	Deaktiviert	Ignorieren	Ignorieren
Exploit: System-DLL-Überschreibung	Deaktiviert	Ignorieren	Ignorieren
Exploit: gefährliches COM-Objekt	Deaktiviert	Ignorieren	Ignorieren
Exploit: Injektion über APC	Deaktiviert	Ignorieren	Ignorieren
Exploit: gefährliches VBA-Makro	Deaktiviert	Ignorieren	Ignorieren
Prozessinjektion: Remote-Speicherzuweisung	Deaktiviert	Alarm	Sperren
Prozessinjektion: Remote-Speicherzuordnung	Deaktiviert	Alarm	Sperren
Prozessinjektion: Remote-Schreiben in Speicher	Deaktiviert	Alarm	Sperren
Prozessinjektion: Remote-Schreiben von PE in Speicher	Deaktiviert	Alarm	Sperren
Prozessinjektion: Remote-Codeüberschreibung	Deaktiviert	Ignorieren	Ignorieren
Prozessinjektion: Remote-Aufhebung der Speicherzuordnung	Deaktiviert	Ignorieren	Ignorieren
Prozessinjektion: Remote-Thread-Erstellung	Deaktiviert	Ignorieren	Ignorieren
Prozessinjektion: Remote-APC-Planung	Deaktiviert	Ignorieren	Ignorieren
Prozessinjektion: DYLD-Injektion	Deaktiviert	Ignorieren	Ignorieren
Prozessinjektion: Doppelgänger	Deaktiviert	Ignorieren	Ignorieren
Prozessinjektion: gefährliche Umgebungsvariable	Deaktiviert	Ignorieren	Ignorieren
Eskalation: LSASS-Lesen	Deaktiviert	Alarm	Sperren
Eskalation: Nullzuteilung	Deaktiviert	Alarm	Sperren
Eskalation: Änderungen der Speicherberechtigung in anderen Prozessen	Deaktiviert	Ignorieren	Ignorieren
Eskalation: Änderungen der Speicherberechtigung in untergeordneten Prozessen	Deaktiviert	Ignorieren	Ignorieren

Geräterichtlinien-Einstellung	Phase-1-Richtlinie	Phase-2-Richtlinie	Phase-3-Richtlinie
Eskalation: gestohlenes Systemtoken	Deaktiviert	Ignorieren	Ignorieren
Eskalation: Prozessstart mit geringer Integrität	Deaktiviert	Ignorieren	Ignorieren
Schutzeinstellungen			
Dienstbeendung über Gerät verhindern	Aktiviert	Aktiviert	Aktiviert
Unsichere laufende Prozesse und deren Unterprozesse beenden	Deaktiviert	Deaktiviert	Deaktiviert
Bedrohungserkennung im Hintergrund	Aktiviert	Aktiviert	Aktiviert
Ausführungseinstellung	Wiederkehrend	Wiederkehrend	Wiederkehrend
Tage	10	10	10
Auf neue Dateien überwachen	Aktiviert	Aktiviert	Aktiviert
MB	150	150	150
Bestimmte Ordner ausschließen	Deaktiviert	Deaktiviert	Deaktiviert
Dateiproben kopieren	Deaktiviert	Deaktiviert	Deaktiviert
CylanceOPTICS-Einstellungen			
CylanceOPTICS	Deaktiviert	Deaktiviert	Deaktiviert
CylanceOPTICS-Desktop-Benachrichtigungen aktivieren	Deaktiviert	Deaktiviert	Deaktiviert
Erkennungseinstellungen	Keine	Keine	Keine
Anwendungssteuerung			
Anwendungssteuerung	Deaktiviert	Deaktiviert	Deaktiviert
Agent-Einstellungen			
Automatisches Hochladen von Protokolldateien aktivieren	Deaktiviert	Deaktiviert	Deaktiviert
Desktop-Benachrichtigungen aktivieren	Deaktiviert	Deaktiviert	Deaktiviert
Softwarebestand aktivieren	Aktiviert	Aktiviert	Aktiviert
Skriptsteuerung			

Geräterichtlinien-Einstellung	Phase-1-Richtlinie	Phase-2-Richtlinie	Phase-3-Richtlinie
Skriptsteuerung	Deaktiviert	Aktiviert	Aktiviert
Aktives Skript	Deaktiviert	Alarm	Unsichere blockieren
PowerShell-Skript	Deaktiviert	Alarm	Unsichere blockieren
PowerShell-Konsole	Deaktiviert	Deaktiviert	Deaktiviert
Makros	Deaktiviert	Deaktiviert	Deaktiviert
Python	Deaktiviert	Deaktiviert	Deaktiviert
.NET DLR	Deaktiviert	Deaktiviert	Deaktiviert
XLM-Makros	Deaktiviert	Deaktiviert	Deaktiviert
Erweitert: Alle Skripte bewerten	Deaktiviert	Aktiviert	Aktiviert
Erweitert: Skript in Cloud hochladen	Deaktiviert	Aktiviert	Aktiviert
Erweitert: Benachrichtigung nur bei Ausführung verdächtiger Skripte	Deaktiviert	Aktiviert	Aktiviert
Gerätesteuerung			
Windows-Gerätesteuerung	Aktiviert	Aktiviert	Aktiviert
Android	Vollzugriff	Vollzugriff	Vollzugriff
iOS	Vollzugriff	Vollzugriff	Vollzugriff
Digitalbild	Vollzugriff	Vollzugriff	Vollzugriff
USB CD DVD RW	Vollzugriff	Vollzugriff	Vollzugriff
USB-Laufwerk	Vollzugriff	Vollzugriff	Vollzugriff
VMware USB-Passthrough	Vollzugriff	Vollzugriff	Vollzugriff
Tragbares Windows-Gerät	Vollzugriff	Vollzugriff	Vollzugriff

Exportieren, Importieren oder Rücksetzen der Konfiguration eines Cylance Endpoint Security-Mandanten

Sie können einen neuen Cylance Endpoint Security-Mandanten konfigurieren, indem Sie die Konfiguration eines vorhandenen Mandanten exportieren und in den neuen Mandanten importieren. Sie können auch einen neuen Mandanten zurücksetzen, um die empfohlenen Standardeinstellungen zu verwenden.

Die folgenden Einstellungen sind enthalten, wenn Sie die Konfiguration eines vorhandenen Mandanten exportieren; sie werden geändert, wenn Sie die Mandantenkonfiguration importieren oder zurücksetzen:

- Geräterichtlinien
- Zonenkonfigurationen
- Agent-Update-Einstellungen
- Globale Sicherheits- und Quarantänelisten
- Syslog-Einstellungen

Hinweis: Die Optionen zum Exportieren, Importieren und Zurücksetzen wurden speziell entwickelt, um Ihnen bei der Konfiguration neuer Mandanten- und Testeinstellungen zu helfen, bevor Sie Geräte registrieren. Die Exportfunktion ist nicht für die Erstellung einer Backup-Konfigurationsdatei eines vorhandenen Mandanten vorgesehen. Wenn Sie eine Konfiguration in einen neuen Mandanten importieren oder einen Mandanten zurücksetzen, wird die vorherige Konfiguration der oben aufgeführten Elemente entfernt und kann nicht wiederhergestellt werden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Mandanteneinstellungen**.
2. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Exportieren Sie die Konfiguration des aktuellen Mandanten.	Beachten Sie, dass nur die mit einer gespeicherten Abfrage erstellten Zonen und Zonenregeln in die exportierte Konfiguration aufgenommen werden. Die exportierte Konfigurationsdatei kann nur in derselben Region in einen neuen Mandanten importiert werden. Für Mandanten mit einer anderen Region ist die exportierte Konfigurationsdatei nicht gültig. **a.** Klicken Sie auf **Exportieren**. **b.** Legen Sie einen Namen für die ZIP-Datei fest. **c.** Klicken Sie auf **Exportieren**. **d.** Beachten Sie die folgenden Anweisungen, um die Konfiguration in einen neuen Mandanten zu importieren.
Importieren Sie die aus einem anderen Mandanten exportierten Konfigurationseinstellunge in diesen Mandanten.	Beachten Sie, dass die aktuelle Konfiguration des Mandanten durch den Import einer Mandantenkonfiguration entfernt wird, darunter auch die Zuordnung zwischen Geräten und Geräterichtlinien und Zonen. Nach dem Entfernen kann die Konfiguration nicht wiederhergestellt werden. **a.** Klicken Sie auf **Importieren**. **b.** Navigieren Sie zu der ZIP-Datei, und wählen Sie sie aus. **c.** Geben Sie in das Bestätigungsfeld **Import** ein. **d.** Klicken Sie auf **Importieren**. **e.** Bestätigen Sie den Import. Wenn der Prozess fehlschlägt, werden alle auf den Mandanten angewendeten Änderungen zurückgesetzt.

Aufgabe	Schritte
Setzen Sie einen Mandanten auf die empfohlenen Standardeinstellungen zurück.	Wenn Sie die Mandantenkonfiguration auf die Standardeinstellungen zurücksetzen, wird die aktuelle Konfiguration einschließlich der Zuordnung zwischen Geräten und Geräterichtlinien und Zonen entfernt. Nach dem Entfernen kann die Konfiguration nicht wiederhergestellt werden. **a.** Klicken Sie auf **Zurücksetzen**. **b.** Geben Sie in das Bestätigungsfeld **Zurücksetzen** ein. **c.** Klicken Sie auf **Zurücksetzen**. **d.** Bestätigen Sie die Rücksetzung. Wenn der Prozess fehlschlägt, werden alle auf den Mandanten angewendeten Änderungen zurückgesetzt.

Details zum Import oder Rücksetzen werden in das Prüfprotokoll geschrieben.

Installieren des BlackBerry Connectivity Node

Mit dem BlackBerry Connectivity Node können Sie eine sichere Verbindung zwischen Cylance Endpoint Security und einem lokalen Microsoft Active Directory oder LDAP-Verzeichnis herstellen. Cylance Endpoint Security kann Geräte, Benutzer und Gruppen aus Active Directory synchronisieren. Benutzer, die durch die Verzeichnissynchronisierung erstellt wurden, können für die CylancePROTECT Mobile-App, für CylanceGATEWAY und CylanceAVERT aktiviert werden.

Sie können drei oder mehr Instanzen des BlackBerry Connectivity Node installieren, um Redundanz zu bieten. Jede Instanz muss auf einem dedizierten Computer installiert werden. Wenn Sie über mehr als einen BlackBerry Connectivity Node verfügen, müssen Sie alle auf dieselbe Softwareversion aktualisieren. Nach dem Upgrade der ersten Instanz werden die Verzeichnisdienste deaktiviert, bis alle Instanzen auf dieselbe Version aktualisiert worden sind.

Sie können eine oder mehrere Verzeichnisverbindungen konfigurieren. Wenn Sie jedoch über mehrere Instanzen von BlackBerry Connectivity Node verfügen, müssen alle Verzeichnisverbindungen identisch konfiguriert werden. Wenn eine Verzeichnisverbindung fehlt oder falsch konfiguriert ist, wird dieser BlackBerry Connectivity Node in der Verwaltungskonsole als deaktiviert angezeigt.

Sie müssen den BlackBerry Connectivity Node nicht installieren, um die Synchronisierung mit Microsoft Entra ID Active Directory auszuführen. Weitere Informationen finden Sie unter Konfigurieren von Cylance Endpoint Security für die Synchronisierung mit Entra Active Directory.

Führen Sie die folgenden Schritte aus, um BlackBerry Connectivity Node zu installieren.

Schritt	Aktion
1	Sehen Sie die Anforderungen durch.
2	Einrichtung einer Umgebungsvariable für den Java-Speicherort.
3	Herunterladen der Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node.
4	Installieren und Konfigurieren des BlackBerry Connectivity Node.
5	Wenn in Ihrer Umgebung mehrere Instanzen von BlackBerry Connectivity Node vorhanden sind, Kopieren von Konfigurationen der Verzeichnisverbindungen.
6	Konfigurieren von Proxyeinstellungen für eine BlackBerry Connectivity Node-Instanz (Optional).

Einrichtung einer Umgebungsvariable für den Java-Speicherort

Sie müssen eine JRE 17-Implementierung auf den Servern installieren, auf dem BlackBerry Connectivity Node installiert ist, und die Umgebungsvariable muss auf den Java-Speicherort verweisen.

Wenn Sie mit der Installation beginnen, überprüft BlackBerry Connectivity Node, ob Java auffindbar ist. Wenn sie Java nicht findet, wird die Setup-Anwendung im Anforderungsbereich beendet. Sie müssen dann eine Umgebungsvariable für den Java-Speicherort festlegen und dafür sorgen, dass der bin-Ordner für Java in der Systemvariable des Pfads enthalten ist. Beachten Sie, dass Sie das Installationsprogramm zu diesem Zeitpunkt schließen müssen und es erst neu starten dürfen, nachdem die Umgebungsvariable erstellt oder aktualisiert wurde.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie JRE 17 auf dem Server installiert haben, auf dem Sie BlackBerry Connectivity Node installieren werden.

1. Öffnen Sie das Dialogfeld **Erweiterte Windows-Systemeinstellungen**.
2. Klicken Sie auf **Umgebungsvariablen**.
3. Klicken Sie in der Liste **Systemvariablen** auf **Neu**.
4. Geben Sie `BB_JAVA_HOME` im Feld **Variablenname** ein.
5. Geben Sie in das Feld **Variablenwert** den Pfad zum JRE-Ordner ein und klicken Sie auf **OK**.
6. Wählen Sie in der Liste der **Systemvariablen** die Option **Pfad** aus und klicken Sie auf **Bearbeiten**.
7. Wenn der Pfad nicht den bin-Ordner für Java enthält, klicken Sie auf **Neu**, und ergänzen Sie den Pfad mit `%BB_JAVA_HOME%\bin`.
8. Verschieben Sie den Eintrag %BB_JAVA_HOME%\bin in der Liste so weit nach oben, dass er nicht durch einen anderen Eintrag außer Kraft gesetzt wird, und klicken Sie auf **OK**.

Wenn Sie fertig sind: Herunterladen der Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node.

Herunterladen der Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node

Bevor Sie beginnen: Einrichtung einer Umgebungsvariable für den Java-Speicherort.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Verzeichnisverbindungen**.
2. Klicken Sie auf die Registerkarte **Connectivity Node**.
3. Klicken Sie auf **Connectivity Node hinzufügen**.
4. Klicken Sie auf der Seite für den Softwaredownload auf **Herunterladen**.
5. Wählen Sie **BlackBerry Connectivity Node für UES** aus.
6. Klicken Sie auf **Download**.
7. Extrahieren Sie die BlackBerry Connectivity Node-Installationsdateien auf den Computer.

   Kopieren Sie die verwendeten Installationsdateien nicht zwischen den Computern, wenn Sie mehr als eine Instanz von BlackBerry Connectivity Node installieren. Sie müssen die Installationsdateien auf jedem Computer erneut extrahieren.
8. Klicken Sie in der Verwaltungskonsole auf **Aktivierungsdatei herunterladen**.
9. Speichern Sie die Aktivierungsdatei (.txt).

   Die Aktivierungsdatei ist 60 Minuten lang gültig. Wenn Sie die Aktivierungsdatei nicht innerhalb von 60 Minuten verwenden, müssen Sie eine neue Aktivierungsdatei herunterladen. Nur die letzte Aktivierungsdatei ist gültig.

Wenn Sie fertig sind: Installieren und Konfigurieren des BlackBerry Connectivity Node.

Installieren und Konfigurieren des BlackBerry Connectivity Node

Bevor Sie beginnen: Herunterladen der Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node.

1. Öffnen Sie die BlackBerry Connectivity Node-Installationsdatei (.exe), die Sie über die Verwaltungskonsole heruntergeladen haben.

   Wenn eine Windows-Meldung mit dem Hinweis angezeigt wird, dass eine Erlaubnis für das Vornehmen von Änderungen am Computer benötigt wird, klicken Sie auf **Ja**.
2. Wählen Sie Ihre Sprache aus. Klicken Sie auf **OK**.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie Ihr Land oder Ihre Region aus. Lesen Sie die Lizenzvereinbarung, und stimmen Sie ihr zu. Klicken Sie auf **Weiter**.
5. Das Installationsprogramm überprüft, ob Ihr Computer die Installationsanforderungen erfüllt. Klicken Sie auf **Weiter**.
6. Klicken Sie zum Ändern des Installationsdateipfads auf **...**, und navigieren Sie zum gewünschten Dateipfad. Wenn Ihnen eine Nachricht angezeigt wird, ob Sie die Installations- und Protokollverzeichnis-Speicherorte erstellen möchten, klicken Sie auf **Ja**. Klicken Sie auf **Weiter**.
7. Geben Sie im Dialogfeld **Dienstkonto** das Kennwort für das Dienstkonto ein. Klicken Sie auf **Installieren**.
8. Sobald die Installation abgeschlossen ist, klicken Sie auf **Weiter**.

   Die Adresse der BlackBerry Connectivity Node-Konsole wird angezeigt (http:/localhost:8088). Klicken Sie auf den Link, und speichern Sie die Website in Ihrem Browser.
9. Wählen Sie Ihre Sprache aus. Klicken Sie auf **Weiter**.
10. Wenn Sie den BlackBerry Connectivity Node aktivieren, sendet er Daten über Port 443 (HTTPS) an die BlackBerry Infrastructure (z. B. na.bbsecure.com oder eu.bbsecure.com). Nach der Aktivierung verwendet der BlackBerry Connectivity Node Port 3101 (TCP) für alle ausgehenden Verbindungen über die BlackBerry Infrastructure. Führen Sie eine der folgenden Aktionen aus:

    - Wenn Sie nicht die Standardeinstellung für den Proxy (Port 443) für die Verbindung zur BlackBerry Infrastructure (<*region*>.bbsecure.com) und für die Aktivierung von BlackBerry Connectivity Node verwenden möchten, klicken Sie auf den Link „Hier“ für die Konfiguration der Proxyeinstellungen und geben Sie die Informationen für den Anmeldungsproxy ein. Dieser Link ist nur auf dem Bildschirm „Name für BlackBerry Connectivity Node eingeben“ verfügbar. Wenn Sie die Proxyeinstellungen in diesem Bildschirm nicht konfigurieren und auf **Weiter** klicken, können Sie die Proxyeinstellungen in der oberen rechten Ecke des Bildschirms konfigurieren, indem Sie vor der Aktivierung auf **Einstellungen > Proxy** klicken.

      Hinweis: Der Proxy muss über Port 443 auf die BlackBerry Infrastructure zugreifen können. Die Einstellung für den Anmeldungs-Proxy kann nach der Aktivierung des BlackBerry Connectivity Node nicht mehr geändert werden.
    - Konfigurieren Sie weitere Proxyeinstellungen. Weitere Informationen zu den verfügbaren Proxyoptionen finden Sie unter Konfigurieren von Proxyeinstellungen für eine BlackBerry Connectivity Node -Instanz.
11. Geben Sie im Feld **Anzeigename** einen Namen für den BlackBerry Connectivity Node ein. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Durchsuchen**. Wählen Sie die Aktivierungsdatei aus, die Sie über die Verwaltungskonsole heruntergeladen haben.
13. Klicken Sie auf **Aktivieren**.

    Wenn Sie eine BlackBerry Connectivity Node-Instanz bei der Aktivierung zu einer bestehenden Servergruppe hinzufügen möchten, muss die Firewall Ihres Unternehmens Verbindungen von diesem Server über Port 443 über die BlackBerry Infrastructure (z. B. na.bbsecure.com oder eu.bbsecure.com) zur Aktivierung des

BlackBerry Connectivity Node und zur selben bbsecure.com-Region wie die Hauptinstanz von BlackBerry Connectivity Node zulassen.

14. Klicken sie auf +, und wählen Sie den Typ des zu konfigurierenden Unternehmensverzeichnisses aus.
15. Verknüpfen Sie Ihr Verzeichnis mit BlackBerry Connectivity Node, indem Sie die entsprechende Aufgabe ausführen:
    - Herstellen einer Verbindung mit Microsoft Active Directory
    - Herstellen der Verbindung zu einem LDAP-Verzeichnis

Wenn Sie fertig sind:

- Um eine zweite BlackBerry Connectivity Node-Instanz als Redundanz zu installieren, laden Sie einen weiteren Satz Installations- und Aktivierungsdateien herunter, und wiederholen Sie diese Aufgabe auf einem anderen Computer. Dies sollte durchgeführt werden, nachdem die erste Instanz aktiviert wurde.
- Sie können eine oder mehrere Verzeichnisverbindungen konfigurieren. Wenn Sie jedoch mehrere BlackBerry Connectivity Node s haben, müssen alle Verzeichnisverbindungen identisch konfiguriert werden. Wenn eine Verzeichnisverbindung fehlt oder falsch konfiguriert ist, wird dieser BlackBerry Connectivity Node in der Verwaltungskonsole als deaktiviert angezeigt. Sie können diese Aufgabe durch Kopieren von Konfigurationen der Verzeichnisverbindungen von einem BlackBerry Connectivity Node zu einem anderen vereinfachen.
- Klicken Sie zum Ändern der konfigurierten Verzeichniseinstellungen in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Firmenverzeichnis**. Klicken Sie auf ✎ für die Verzeichnisverbindung.
- Konfigurieren der BlackBerry Connectivity Node-Protokollierung.
- Sie können Verzeichnisverbindungen von BlackBerry Connectivity Node entfernen, solange keine Benutzer oder Gruppen damit verbunden sind. Wenn Sie eine Verbindung von BlackBerry Connectivity Node entfernen, können Sie die Verbindung mit dem gleichen Namen wie die gelöschte Verbindung erneut hinzufügen.

Kopieren von Konfigurationen der Verzeichnisverbindungen

Wenn Ihre Umgebung über mehrere Instanzen von BlackBerry Connectivity Node verfügt, müssen die Verzeichnisverbindungen auf allen Knoten identisch konfiguriert werden. Um diese Aufgabe zu vereinfachen, können Sie die Konfiguration der Verzeichnisverbindung von einer BlackBerry Connectivity Node exportieren und in eine andere importieren.

Hinweis: Bevor Sie Konfigurationen des Unternehmensverzeichnisses in ein BlackBerry Connectivity Node importieren können, müssen Sie alle vorhandenen Unternehmensverzeichnis-Verbindungen von diesem Knoten entfernen.

Bevor Sie beginnen: Kopieren von Konfigurationen der Verzeichnisverbindungen.

1. Klicken Sie auf dem BlackBerry Connectivity Node, von dem Sie die Konfiguration kopieren möchten, auf dem Bildschirm **Unternehmensverzeichnisverbindung** auf **Verzeichnisverbindungen in .txt-Datei exportieren**.

   Eine .txt-Datei mit Informationen über die Unternehmensverzeichnis-Verbindungen wird auf Ihren Computer heruntergeladen.
2. Navigieren Sie auf der BlackBerry Connectivity Node, in die Sie die Konfiguration kopieren möchten, auf dem Bildschirm **Unternehmensverzeichnis-Verbindung** zur heruntergeladenen .txt -Datei.
3. Klicken Sie auf **Verbindungen importieren**.

   Die Unternehmensverzeichnis-Verbindungen werden BlackBerry Connectivity Node hinzugefügt.

Konfigurieren von Proxyeinstellungen für eine BlackBerry Connectivity Node-Instanz

Sie können die Komponenten von BlackBerry Connectivity Node so konfigurieren, dass Daten zuerst über einen TCP-Proxyserver (transparent oder SOCKS v5) gesendet werden, bevor sie die BlackBerry Infrastructure erreichen.

1. Öffnen Sie auf dem Computer, auf dem der BlackBerry Connectivity Node gehostet wird, die BlackBerry Connectivity Node-Konsole über das Startmenü, oder öffnen Sie einen Browser, und navigieren Sie zu http://localhost:8088.
2. Klicken Sie auf **Allgemeine Einstellungen > Proxy**.
3. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Senden von Daten über einen SOCKS v5-Proxyserver (keine Authentifizierung) an die BlackBerry Infrastructure.	**a.** Wählen Sie die Option **Proxy-Server**. **b.** Aktivieren Sie das Kontrollkästchen **SOCKS v5 aktivieren**. **c.** Klicken Sie auf **+**. **d.** Geben Sie die IP-Adresse oder den Hostnamen des SOCKS v5-Proxyservers ein. Klicken Sie auf **Hinzufügen**. **e.** Wiederholen Sie die Schritte 3 bis 4 für jeden zu konfigurierenden SOCKS v5-Proxy-Server. **f.** Geben Sie im Feld **Port** die Portnummer ein. **g.** Klicken Sie auf **Speichern**.
Senden von Daten über einen Proxyserver (transparent) an die BlackBerry Infrastructure.	• Geben Sie in den Feldern **BlackBerry Connectivity Node** den FQDN oder die IP-Adresse und die Portnummer des Proxyservers ein.

4. Klicken Sie auf **Speichern**.

Verknüpfung mit Ihrem Unternehmensverzeichnis

Sie können Cylance Endpoint Security so konfigurieren, dass eine Synchronisierung mit Ihrem Unternehmensverzeichnis durchgeführt wird, um das Hinzufügen und Verwalten von Benutzern und Gruppen zu vereinfachen. Durch das Verbinden von Cylance Endpoint Security mit einem Unternehmensverzeichnis können Sie durch Suchen nach und Importieren von Benutzerdaten aus dem Unternehmensverzeichnis Benutzerkonten erstellen. Benutzer, die durch die Verzeichnissynchronisierung erstellt wurden, können für die CylancePROTECT Mobile-App, für CylanceGATEWAY und CylanceAVERT aktiviert werden.

Die Verbindung mit einem Unternehmensverzeichnis kann auf zwei Arten hergestellt werden:

- Wenn Sie mit Microsoft Entra ID synchronisieren möchten, können Sie Cylance Endpoint Security so konfigurieren, dass eine entsprechende Verbindung hergestellt wird.
- Wenn Sie mit einem lokalen Microsoft Active Directory oder einem LDAP-Verzeichnis synchronisieren möchten, müssen Sie zunächst BlackBerry Connectivity Node installieren, um eine sichere Verbindung zwischen Cylance Endpoint Security und Ihrem Verzeichnis herzustellen.

Führen Sie die folgenden Schritte aus, um Cylance Endpoint Security mit Ihrem Unternehmensverzeichnis zu verknüpfen:

Schritt	Aktion
1	Wenn Sie eine Verknüpfung zu einem lokalen Unternehmensverzeichnis herstellen möchten, installieren Sie BlackBerry Connectivity Node.
2	Je nach Typ des Verzeichnisses, mit dem Sie eine Verbindung herstellen möchten, konfigurieren Sie Cylance Endpoint Security für die Synchronisierung mit Entra, oder stellen Sie eine Verbindung mit einem Microsoft Active Directory oder LDAP-Verzeichnis her.
3	Hinzufügen einer Verzeichnisgruppe.
4	Konfigurieren von Onboarding und Offboarding.
5	Konfigurieren der Zeitpläne für die Verzeichnissynchronisierung.

Konfigurieren von Cylance Endpoint Security für die Synchronisierung mit Entra Active Directory

Um Cylance Endpoint Security für die Synchronisierung mit Entra Active Directory zu konfigurieren, müssen Sie zur Herstellung der Verbindung sowohl Entra als auch Cylance Endpoint Security konfigurieren.

1. Melden Sie sich beim Azure-Portal an.
2. Erstellen Sie eine neue App-Registrierung für Entra Active Directory und weisen Sie die entsprechenden Einstellungen und Berechtigungen zu.
   a) Fügen Sie einen Namen für die App hinzu.
   b) Geben Sie die Kontotypen an, die die Anwendung verwenden bzw. auf die API zugreifen können.

c) Wählen Sie **Web** als Umleitungs-URI-Typ aus und legen Sie als URI `http://localhost` fest.
d) Legen Sie die folgenden Anwendungsberechtigungen fest:
   - Group.Read.All (Anwendung)
   - User.Read (Delegiert)
   - User.Read.All (Anwendung)
e) Gewähren Sie der Anwendung Administratorzustimmung.

3. Notieren Sie den Namen, den Sie der App zugewiesen haben, und die ID der Anwendung (des Clients).
4. Erstellen Sie einen neuen geheimen Zugangsschlüssel, und notieren Sie den Schlüsselwert in der Wertspalte.

   Wichtig: Der Wert ist nur verfügbar, wenn Sie ihn erstellen. Sie können nicht mehr darauf zugreifen, nachdem Sie die Seite verlassen haben. Wenn Sie den Wert nicht notieren, müssen Sie einen neuen erstellen. Er wird als geheimer Client-Schlüssel in der Verwaltungskonsole verwendet.
5. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Verzeichnisverbindungen**.
6. Klicken Sie auf **Neue Verbindung hinzufügen**.
7. Geben Sie einen **Namen** für die Verzeichnisverbindung und die **Domäne** für Entra Active Directory ein.
8. Geben Sie in das Feld **Client-ID** die durch die Entra-App-Registrierung generierte Anwendungs-ID ein.
9. Geben Sie in das Feld **Geheimer Client-Schlüssel** den geheimen Client-Schlüsselwert ein, der während der Registrierung der Entra-App in Schritt 4 generiert wurde.
10. Klicken Sie auf **Hinzufügen**.

Aktualisieren der Anmeldeinformationen für die Verbindung zu Microsoft Entra ID Active Directory

Sie müssen die Client-Anmeldeinformationen in der Verwaltungskonsole aktualisieren, wenn Ihr Client-Schlüssel abgelaufen ist oder im Azure-Portal geändert wurde. Wenn Ihr Client-Schlüssel abgelaufen ist oder geändert wurde, wird auf dem Bildschirm „Verzeichnisverbindungen“  neben der betroffenen Verzeichnisverbindung angezeigt. Sie können entweder nur den Client-Schlüssel aktualisieren oder sowohl die Client-ID als auch den Client-Schlüssel aktualisieren.

Bevor Sie beginnen:

- Überprüfen Sie, ob Sie den der App zugewiesenen Namen unter Konfigurieren von Cylance Endpoint Security für die Synchronisierung mit Entra Active Directory erfasst haben.
- Überprüfen Sie, ob Sie einen gültigen Client-Schlüssel haben und die Informationen in der Wertspalte des Schlüssels erfasst haben. Optional können Sie sowohl eine neue Client-ID als auch einen Client-Schlüssel erstellen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Verzeichnisverbindungen**.
2. Klicken Sie auf die Microsoft Entra ID Active Directory-Verbindung, die Sie aktualisieren möchten.
3. Klicken Sie auf die Registerkarte **Verbindungseinstellungen**.
4. Klicken Sie auf **Client-Anmeldeinformationen aktualisieren**. Wählen Sie, ob nur der Client-Schlüssel oder sowohl die Client-ID als auch der Client-Schlüssel aktualisiert werden sollen. Führen Sie einen der folgenden Schritte aus:
   - Nur Client-Schlüssel aktualisieren: Geben Sie den Client-Schlüsselwert ein, den Sie im Azure-Portal erfasst haben.
   - Client-ID und Client-Schlüssel aktualisieren: Geben Sie die neue Client-ID und den Client-Schlüsselwert ein, den Sie im Azure-Portal erfasst haben.
5. Klicken Sie auf **Senden**.
6. Klicken Sie auf **Speichern**. Wenn der Speichervorgang fehlschlägt, werden sowohl die Client-ID als auch der Client-Schlüssel auf die vorherigen Werte zurückgesetzt.

Herstellen einer Verbindung mit Microsoft Active Directory

Bevor Sie beginnen: Es muss mindestens eine Instanz von BlackBerry Connectivity Node installiert werden.

1. Klicken Sie in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Unternehmensverzeichnis**.
2. Klicken Sie auf +.
3. Wählen Sie **Microsoft Active Directory** aus.
4. Geben Sie im Feld **Verbindungsname** einen Namen für die Unternehmensverzeichnisverbindung ein.
5. Geben Sie im Feld **Benutzername** den Benutzernamen des Microsoft Active Directory-Kontos ein.
6. Geben Sie im Feld **Domäne** den FQDN der Domäne ein, die Microsoft Active Directory hostet. Beispiel: domain.example.com.
7. Geben Sie im Feld **Kennwort** das Kennwort für das Microsoft Active Directory-Konto ein.
8. Klicken Sie in der Dropdown-Liste **Erkennung des Domain Controllers** auf eine der folgenden Optionen:
   - Wenn Sie die automatische Erkennung nutzen möchten, klicken Sie auf **Automatisch**.
   - Wenn Sie den Domain Controller-Computer angeben möchten, klicken Sie auf **Aus der Liste unten auswählen**. Klicken Sie auf + und geben sie den FQDN des Computers ein. Wiederholen Sie diesen Schritt, um weitere Computer hinzuzufügen.
9. Geben Sie im Feld **Suchbasis des globalen Katalogs** die Suchbasis ein, auf die Sie zugreifen möchten (beispielsweise: OU=Users,DC=example,DC=com). Lassen Sie das Feld leer, um den gesamten globalen Katalog zu durchsuchen.
10. Klicken Sie in der Dropdown-Liste **Erkennung des globalen Katalogs** auf eine der folgenden Optionen:
    - Wenn Sie eine automatische Erkennung des Katalogs durchführen möchten, klicken Sie auf **Automatisch**.
    - Wenn Sie den Katalogcomputer angeben möchten, klicken Sie auf **Aus der Liste unten auswählen**. Klicken Sie auf + und geben sie den FQDN des Computers ein. Wiederholen Sie diesen Schritt gegebenenfalls, um weitere Computer anzugeben.
11. Wenn Sie die Unterstützung für verknüpfte Microsoft Exchange-Postfächer aktivieren möchten, klicken Sie in der Dropdown-Liste **Unterstützung für verknüpfte Microsoft Exchange-Postfächer** auf **Ja**. Um das Microsoft Active Directory-Konto für jede Gesamtstruktur zu konfigurieren, auf die Sie zugreifen möchten, klicken Sie im Abschnitt **Auflisten von Kontengesamtstrukturen** auf +. Geben Sie den Namen der Gesamtstruktur, den Namen der Benutzerdomäne (der Benutzer kann einer beliebigen Domäne in der Kontengesamtstruktur angehören) sowie den Benutzernamen und das Kennwort an.
12. Um, weitere Benutzerdetails aus Ihrem Unternehmensverzeichnis zu synchronisieren, aktivieren Sie das Kontrollkästchen **Zusätzliche Benutzerdetails synchronisieren**. Zu den zusätzlichen Details gehören der Name des Unternehmens und die geschäftliche Telefonnummer.
13. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Wenn Sie automatisches Onboarding für Cylance Endpoint Security konfigurieren möchten, siehe Konfigurieren von Onboarding und Offboarding.
- Informationen zum Hinzufügen eines Synchronisierungsplans für Verzeichnisse finden Sie unter Konfigurieren der Zeitpläne für die Verzeichnissynchronisierung.
- Wenn Sie über mehr als eine Instanz von BlackBerry Connectivity Node verfügen, können Sie Verzeichnisverbindungskonfigurationen von einer Instanz in die anderen kopieren.

Herstellen der Verbindung zu einem LDAP-Verzeichnis

Bevor Sie beginnen: Um eine Verbindung zu einem lokalen LDAP-Verzeichnis herzustellen, müssen Sie zunächst mindestens eine Instanz von BlackBerry Connectivity Node installieren.

1. Klicken Sie in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Unternehmensverzeichnis**.
2. Klicken Sie auf +.
3. Wählen Sie **LDAP** aus.
4. Geben Sie im Feld **Verbindungsname** einen Namen für die Unternehmensverzeichnisverbindung ein.
5. Klicken Sie in der Dropdown-Liste **LDAP-Servererkennung** auf eine der folgenden Optionen: Wenn Sie die automatische Erkennung verwenden möchten, klicken Sie auf **Automatisch**.
   - Wenn Sie die automatische Erkennung verwenden möchten, klicken Sie auf **Automatisch** und geben dann in das Feld **DNS-Domänenname** den DNS-Domänennamen ein.
   - Wenn Sie den LDAP-Computer angeben möchten, klicken Sie auf **Server aus der Liste unten auswählen**. Klicken Sie auf + und geben sie den FQDN des Computers ein. Wiederholen Sie diesen Schritt, um weitere Computer hinzuzufügen.
6. Wählen Sie in der Dropdown-Liste **SSL aktivieren** aus, ob Sie die SSL-Authentifizierung für den LDAP-Verkehr aktivieren möchten. Wenn Sie **Ja** auswählen, klicken Sie auf **Durchsuchen**, und wählen Sie das SSL-Zertifikat für den LDAP-Computer aus.
7. Geben Sie in das Feld **LDAP-Port** die Portnummer des LDAP-Computers ein.
8. Wählen Sie in der Dropdown-Liste **Autorisierung erforderlich** aus, ob eine Authentifizierung mit dem LDAP-Computer erforderlich ist. Wenn Sie **Ja** auswählen, geben Sie den Benutzernamen und das Kennwort des LDAP-Kontos ein. Der Benutzername muss im DN-Format angegeben werden (beispielsweise: CN=Megan Ball,OU=Sales,DC=example,DC=com).
9. Geben Sie im Feld **Basissuche** die Basissuche ein, auf die Sie zugreifen möchten (beispielsweise: OU=Users,DC=example,DC=com).
10. Geben Sie im Feld **LDAP-Suchfilter nach Benutzer** den Filter ein, den Sie für LDAP-Benutzer verwenden möchten. Beispiel: (&(objectCategory=person)(objectclass=user)). Wenn Sie die Suche auf alle Mitglieder einer einzelnen Gruppe für den gesamten Cylance Endpoint Security-Mandanten beschränken möchten, können Sie folgendes Beispiel verwenden: (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)).
11. Klicken Sie in der Dropdown-Liste **LDAP-Benutzersuchbereich** auf eine der folgenden Optionen: Wenn Sie möchten, dass Benutzersuchvorgänge auf alle Ebenen unter dem Basis-DN angewendet werden, klicken Sie auf **Alle Ebenen**. Wenn Sie die Benutzersuche auf eine Ebene unter dem Basis-DN beschränken möchten, klicken Sie auf **Eine Ebene**.
12. Geben Sie im Feld **Eindeutige Kennung** das Attribut für die eindeutige Kennung der einzelnen Benutzer ein (beispielsweise: uid). Das Attribut muss für jeden Benutzer unveränderbar und global eindeutig sein.
13. Geben Sie im Feld **Vorname** das Attribut für den Vornamen der einzelnen Benutzer ein (beispielsweise: givenName).
14. Geben Sie im Feld **Nachname** das Attribut für den Nachnamen der einzelnen Benutzer ein (beispielsweise: sn).
15. Geben Sie im Feld **Anmeldeattribute** das Anmeldeattribut der einzelnen Benutzer ein (beispielsweise: cn).
16. Geben Sie im Feld **E-Mail-Adresse** das Attribut für die E-Mail der einzelnen Benutzer ein (beispielsweise: mail).
17. Geben Sie im Feld **Anzeigename** das Attribut für den Anzeigenamen der einzelnen Benutzer ein (beispielsweise displayName).
18. Um, weitere Benutzerdetails aus Ihrem Unternehmensverzeichnis zu synchronisieren, aktivieren Sie das Kontrollkästchen **Zusätzliche Benutzerdetails synchronisieren**. Zu den zusätzlichen Details gehören der Name des Unternehmens und die geschäftliche Telefonnummer.

19. Wenn per Verzeichnis verknüpfte Gruppen aktiviert werden sollen, aktivieren Sie das Kontrollkästchen **Aktivieren von per Verzeichnis verknüpften Gruppen**.

    Geben Sie die folgenden Informationen an:

    - Geben Sie im Feld **Suchbasis für Gruppen** den Wert ein, der als Basis-DN für Gruppeninformationssuchen verwendet werden soll.
    - Geben Sie im Feld **LDAP-Suchfilter für Gruppen** den LDAP-Suchfilter ein, der zum Auffinden von Gruppenobjekten in Ihrem Unternehmensverzeichnis erforderlich ist.
    - Geben Sie im Feld **Eindeutige Kennung der Gruppe** das Attribut für die eindeutige Kennung der einzelnen Gruppen ein. Dieses Attribut muss unveränderbar und global eindeutig sein.
    - Geben Sie in das Feld **Anzeigename der Gruppe** das Attribut für den Anzeigenamen jeder einzelnen Gruppe ein.
    - Geben Sie im Feld **Gruppenmitgliedschaft – Attribut** den Namen des Attributs für die Gruppenmitgliedschaft ein. Die Attributwerte müssen im DN-Format vorliegen.
    - Geben Sie im Feld **Gruppenname testen** einen vorhandenen Gruppennamen ein, um die festgelegten Gruppenattribute zu validieren.

20. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Wenn Sie automatisches Onboarding für Cylance Endpoint Security konfigurieren möchten, siehe Konfigurieren von Onboarding und Offboarding.
- Informationen zum Hinzufügen eines Synchronisierungsplans für Verzeichnisse finden Sie unter Konfigurieren der Zeitpläne für die Verzeichnissynchronisierung.
- Wenn Sie über mehr als eine Instanz von BlackBerry Connectivity Node verfügen, können Sie Verzeichnisverbindungskonfigurationen von einer Instanz in die anderen kopieren.

Konfigurieren von Onboarding und Offboarding

Onboarding bedeutet, dass Benutzerkonten basierend auf der Benutzermitgliedschaft in einer Unternehmensverzeichnisgruppe automatisch zu Cylance Endpoint Security hinzugefügt werden können. Verzeichnisgruppen und Benutzerkonten werden während des Synchronisierungsvorgangs zu CylanceGATEWAY hinzugefügt.

Wenn Sie Onboarding aktivieren, können Sie auch den Offboarding-Vorgang konfigurieren. Wenn ein Benutzer im Verzeichnis deaktiviert oder aus allen Unternehmensverzeichnisgruppen in den Onboarding-Verzeichnisgruppen entfernt wird, löscht Cylance Endpoint Security das Benutzerkonto und von den Geräten des Benutzers ausgehende Netzwerkverbindungen werden nicht mehr zugelassen.

Mithilfe des Offboarding-Schutzes können Sie das Löschen von Benutzerkonten verzögern, damit unerwartete Löschvorgänge vermieden werden, die aufgrund der Verzeichnisreplikationslatenz auftreten können. Der Offboarding-Schutz verzögert Offboarding-Aktionen um zwei Stunden nach dem nächsten Synchronisierungszyklus.

Bevor Sie beginnen: Je nach Verzeichnistyp, zu dem Sie eine Verbindung herstellen möchten, konfigurieren Sie entweder Cylance Endpoint Security für die Synchronisierung mit Azure Active Directory oder stellen Sie eine Verbindung zu einem Microsoft Active Directory oder einem LDAP-Verzeichnis her.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Verzeichnisverbindungen**.
2. Klicken Sie in der Liste **Verzeichnisverbindung** auf die Verbindung, für die Sie das Onboarding konfigurieren möchten.
3. Wählen Sie auf der Registerkarte **Synchronisierungseinstellungen** die Option **Verzeichnis-Onboarding** aus.

4. Geben Sie in das Feld **Synchronisierung** die maximale Anzahl der Änderungen ein, die pro Synchronisierungsprozess zulässig sein sollen.

   Standardmäßig gibt es kein Limit. Falls die Anzahl der zu synchronisierenden Änderungen das von Ihnen festgelegte Limit übersteigt, wird die Synchronisierung gestoppt. Zu den Änderungen gehören Benutzer, die zu Gruppen hinzugefügt wurden, Benutzer, die aus Gruppen entfernt wurden, Onboarding-Benutzer und Offboarding-Benutzer.
5. Geben Sie in das Feld **Verschachtelungsebene** die Anzahl der Verschachtelungsebenen ein, die für Unternehmensverzeichnisgruppen synchronisiert werden sollen. Standardmäßig gibt es kein Limit.
6. Um die Synchronisierung von Verzeichnisgruppen durchzusetzen, wählen Sie **Synchronisierung erzwingen** aus.

   Wenn diese Option aktiviert ist und eine Gruppe aus dem Unternehmensverzeichnis entfernt wird, werden die Verknüpfungen für diese Gruppe aus den Onboarding-Verzeichnisgruppen und den per Verzeichnis verknüpften Gruppen entfernt. Wenn diese Option nicht aktiviert ist und eine Unternehmensverzeichnisgruppe gefunden werden kann, wird der Synchronisierungsvorgang abgebrochen.
7. Um ein Benutzerkonto aus Cylance Endpoint Security zu löschen, wenn ein Benutzer aus allen verknüpften Gruppen im Verzeichnis entfernt wird, aktivieren Sie das Kontrollkästchen **Benutzer löschen, wenn der Benutzer aus allen integrierten Verzeichnisgruppen entfernt wird**. Beim ersten Synchronisierungszyklus, der durchgeführt wird, nachdem ein Benutzerkonto aus allen verknüpften Verzeichnisgruppen entfernt wurde, wird das Benutzerkonto aus Cylance Endpoint Security gelöscht.
8. Um zu verhindern, dass Benutzerkonten oder Gerätedaten unerwartet aus Cylance Endpoint Security gelöscht werden, wählen Sie **Offboarding-Schutz** aus.

   Offboarding-Schutz bedeutet, dass Benutzer erst zwei Stunden nach dem nächsten Synchronisierungszyklus aus Cylance Endpoint Security gelöscht werden.
9. Klicken Sie auf **Speichern**.

Konfigurieren der Zeitpläne für die Verzeichnissynchronisierung

Sie können einen Zeitplan hinzufügen, um Cylance Endpoint Security automatisch mit dem Unternehmensverzeichnis Ihres Unternehmens zu synchronisieren.

Bevor Sie beginnen: Herstellen einer Verbindung mit Microsoft Active Directory oder Herstellen der Verbindung zu einem LDAP-Verzeichnis.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Verzeichnisverbindungen**.
2. Klicken Sie in der Liste **Verzeichnisverbindung** auf die Verbindung, für die Sie einen Synchronisierungszeitplan festlegen möchten.
3. Klicken Sie auf der Registerkarte **Synchronisierungszeitplan** auf **Zeitplan hinzufügen**.
4. Wählen Sie in der Dropdown-Liste **Synchronisierungstyp** eine der folgenden Optionen aus:

   - **Alle Gruppen und Benutzer**: Dies ist die Standardeinstellung. Wenn Sie diese Option wählen und das Onboarding aktiviert ist, erfolgt das Onboarding und Offboarding von Benutzern und die Verknüpfung mit den entsprechenden per Verzeichnis verknüpften Gruppen während der Synchronisierung. Benutzer, für die kein Onboarding oder Offboarding, aber eine Änderung der Verzeichnisgruppen durchgeführt wird, und Benutzer, deren Attribute geändert wurden, werden synchronisiert.
   - **Onboarding-Gruppen**: Wenn Sie diese Option wählen und das Onboarding aktiviert ist, erfolgt das Onboarding und Offboarding von Benutzern und die Verknüpfung mit den entsprechenden per Verzeichnis verknüpften Gruppen während der Synchronisierung, und Benutzer, deren Attribute geändert wurden, werden synchronisiert. Benutzer, für die kein Onboarding oder Offboarding, aber eine Änderung der Verzeichnisgruppen durchgeführt wird, werden nicht synchronisiert.
   - **Per Verzeichnis verknüpfte Gruppen**: Wenn Sie diese Option auswählen, erfolgt das Onboarding und Offboarding von Benutzern nicht während der Synchronisierung. Benutzer, deren Verzeichnisgruppen

geändert wurden, werden entsprechend verknüpft. Benutzer, deren Attribute geändert wurden, werden synchronisiert.
   - **Benutzerattribute**: Wenn Sie diese Option auswählen, erfolgt das Onboarding und Offboarding von Benutzern nicht während der Synchronisierung. Benutzer, deren Verzeichnisgruppen geändert wurden, werden nicht synchronisiert. Benutzer, deren Attribute geändert wurden, werden synchronisiert.
5. Wählen Sie in der Dropdown-Liste **Wiederholung** eine der folgenden Optionen aus:
   - **Intervall**: Dies ist die Standardeinstellung. Wenn Sie diese Option wählen, können Sie die Anzahl der Minuten zwischen den Synchronisierungen und die Stunden und Tage angeben, während denen die Synchronisierung stattfinden kann.
   - **Einmal täglich**: Wenn Sie diese Option wählen, können Sie die Wochentage und die Uhrzeit angeben, an denen bzw. zu der die Synchronisierung erfolgt.
   - **Keine Wiederholung**: Wenn Sie diese Option auswählen, können Sie einen Tag und eine Uhrzeit innerhalb der nächsten Woche für eine einzelne Synchronisierung angeben.
6. Geben Sie die entsprechenden Tages- und Uhrzeitdetails für den Zeitplan an.
7. Klicken Sie auf **Senden**.
8. Klicken Sie auf **Speichern**.

Synchronisieren mit Ihrem Unternehmensverzeichnis

Sie können Cylance Endpoint Security jederzeit mit Ihren Verzeichnisverbindungen synchronisieren.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Verzeichnisverbindungen**.
2. Klicken Sie in der Liste **Verzeichnisverbindung** auf das Symbol ⟳ der Verbindung, die Sie synchronisieren möchten.

Einrichten von Administratoren

Sie können steuern, wie Administratoren auf die Verwaltungskonsole zugreifen und diese verwenden, indem Sie ihnen vordefinierte oder benutzerdefinierte Rollen zuweisen. Mit dieser rollenbasierten Zugriffskontrolle können Sie Administratoren Zugriff auf die für ihre Rolle benötigten Konsolenfunktionen gewähren und die Funktionen einschränken, auf die sie keinen Zugriff haben sollen.

Weitere Informationen zu Rollen und deren Berechtigungen finden Sie unter Berechtigungen für Administratorrollen.

Hinzufügen eines Administrators

Sie können Administratorbenutzer zur Verwaltungskonsole hinzufügen, um diesen Benutzern die Möglichkeit zu geben, Ihre Cylance Endpoint Security-Umgebung zu steuern und zu konfigurieren. Vorhandene und neu hinzugefügte Administratorkonten werden auf der Seite „Benutzer“ (Assets > Benutzer) in der Verwaltungskonsole angezeigt. Sie können die Spalte „Administrator“ hinzufügen, um neben jedem Administratorkonto das Symbol anzuzeigen. Die Bildschirme, die ein Administratorbenutzer in der Verwaltungskonsole anzeigen kann, und die Funktionen, die der Benutzer konfigurieren und ändern kann, hängen von der Rolle ab, die Sie diesem Benutzer zuweisen. Weitere Informationen zu Rollen und deren Berechtigungen finden Sie unter Berechtigungen für Administratorrollen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Administratoren**. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Hinzufügen eines neuen Administrators	**a.** Geben Sie unter **Benutzer hinzufügen** in das Feld **E-Mail eingeben** die E-Mail-Adresse des Benutzers ein. **b.** Klicken Sie in der Dropdown-Liste „Rolle auswählen“ auf eine Rolle. Weitere Informationen zu Rollen und deren entsprechenden Berechtigungen finden Sie unter Verwalten von Rollen. **c.** Wenn Sie einen Zonenmanager oder eine Benutzerrolle ausgewählt haben, klicken Sie in der Dropdown-Liste **Zone auswählen** auf eine Zone. **d.** Klicken Sie auf **Hinzufügen**. Cylance Endpoint Security sendet eine E-Mail mit einem Link zum Erstellen eines Kennworts an den neuen Administratorbenutzer.

Aufgabe	Schritte
Ändern einer Administratorrolle	**a.** Klicken Sie auf einen Administratorbenutzer. **b.** Klicken Sie in der Dropdown-Liste auf eine neue Rolle. **c.** Wenn Sie die Zonenmanager- oder Benutzerrolle ausgewählt haben, gehen Sie wie folgt vor: **1.** Wählen Sie die **Standardzonenrolle** aus, die dem Benutzer beim Erstellen einer neuen Zone zugewiesen werden soll. Der Standardwert ist „Keine“. **2.** Passen Sie die Rolle des Benutzers für jede Zone individuell an. Beachten Sie, dass ein Benutzer, der für mindestens eine Zone als Zonenmanager eingeteilt ist, einige Zonenmanager-Funktionen erbt (z. B. die Möglichkeit, die Liste der Geräterichtlinien anzuzeigen, das Installationsprogramm herunterzuladen und die globale Liste anzuzeigen). Der Benutzer kann jedoch nur Zonenmanager-Funktionen auf Geräten in Zonen, in denen ihm die Zonenmanager-Rolle zugeteilt ist, ausführen. Ebenso kann der Benutzer nur Benutzerfunktionen auf Geräten in Zonen, denen ihm die Benutzerrolle zugeteilt ist, ausführen. **d.** Geben Sie im Popup-Fenster Ihr Kennwort ein. **e.** Klicken Sie auf **Speichern**.

2. Klicken Sie in der Menüleiste auf **Assets > Benutzer**. Führen Sie eine der folgenden Aktionen aus:
   - Um Spalten hinzuzufügen oder zu entfernen, klicken Sie auf ||| und wählen die Spalten aus, die Sie anzeigen möchten.
   - Um Benutzer in auf- oder absteigender Reihenfolge anhand einer Spalte zu sortieren, klicken Sie auf die entsprechende Spalte.
   - Um Benutzer anhand einer Spalte zu filtern, verwenden Sie das Filterfeld und das Symbol für die Spalte.
   - Um nur Administratorkonten anzuzeigen, klicken Sie auf ⏷ und setzen Sie die Option „Administrator“ auf **True**.

Berechtigungen für Administratorrollen

In den folgenden Tabellen sind die Standardberechtigungen für systemdefinierte Rollen innerhalb der Verwaltungskonsole aufgeführt. Berechtigungen, die in Fettdruck dargestellt werden, weisen untergeordnete Berechtigungen auf, die erst nach Auswahl der Hauptberechtigung verfügbar sind.

Die Daten, die von den Zonenmanagern in der Konsole abgerufen werden können, sind auf die von ihnen verwalteten Zonen beschränkt.

Dashboard

Diese Berechtigungen ermöglichen den Zugriff auf die Dashboard-Seite und können nicht deaktiviert werden. Die im Dashboard angezeigten Informationen richten sich nach der Rolle und den Berechtigungen, die der Administratorrolle zugewiesen sind.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Geräteschutz	√	√	√	√

Reaktion auf Endpunkterkennung

Mit diesen Berechtigungen können Sie CylanceOPTICS-Funktionen verwalten.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Erkennung hinzufügen	√	√		√
Erkennungen bearbeiten	√	√		
Erkennungen löschen	√	√		
InstaQuery anzeigen oder erstellen	√	√		√
InstaQuery löschen	√	√		
Erweiterte Abfragen anzeigen oder erstellen	√	√		√
Freigegebene Vorlagen erstellen	√	√		
Freigegebene Vorlagen löschen	√			
Freigegebene Snapshots löschen	√			
Freigegebene Exportabfragen löschen	√			
Geplante Abfragen erstellen	√	√		
Freigegebene geplante Abfragen bearbeiten	√			
Freigegebene geplante Abfragen löschen	√			
Anzeigen oder Erstellen von Fokusdaten	√	√		√
Paketbereitstellung anzeigen	√			√

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Paketbereitstellung erstellen	√			
Paketbereitstellung aktualisieren	√			
Paketbereitstellung löschen	√			
Playbook-Ergebnisse anzeigen	√			√
Playbook-Ergebnisse löschen	√			
Paket anzeigen	√			√
Paket erstellen	√			
Paket löschen	√			
Playbook anzeigen	√			√
Playbook erstellen oder bearbeiten	√			
Playbook löschen	√			
Regelsatz anzeigen*	√			√
Regelsatz bearbeiten*	√			
Regelsatz löschen	√			
Regeln anzeigen	√			√
Benutzerdefinierte Regeln erstellen oder bearbeiten	√			
Benutzerdefinierte Regeln löschen	√			
Ausnahmen anzeigen	√			√
Ausnahmen erstellen oder bearbeiten	√			
Ausnahmen löschen	√			
Sperrkonfiguration anzeigen	√			√

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Sperrkonfiguration erstellen oder bearbeiten	√			
Sperrkonfiguration löschen	√			

*Um einen Regelsatz anzuzeigen, benötigen Sie eine Administratorrolle mit den Berechtigungen „Regelsatz anzeigen“ und „Regelsatz bearbeiten“.

Benutzer und Geräte

Diese Berechtigungen steuern, welche Aktionen für Benutzer und Geräte in der Verwaltungskonsole ausgeführt werden können. Sie müssen über Berechtigungen für die globale Liste verfügen, wenn Sie von diesen Seiten aus eine Bedrohung unter globale Quarantäne stellen oder zur sicheren Liste hinzufügen möchten.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Benutzer und Gruppen anzeigen	√			√
Benutzer und Gruppen erstellen	√			
Benutzer und Gruppen bearbeiten	√			
Benutzer und Gruppen löschen	√			
Mobile Geräte anzeigen	√			√
Mobile Geräte löschen	√			
Geräte anzeigen	√	√	√	√
Geräte bearbeiten	√	√		
Geräte löschen	√			
Hintergrundscan durchführen	√			
CylanceOPTICS-Gerät sperren	√			
CylanceOPTICS-Gerät entsperren	√			
Remote-Antwort ausführen	√			

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Dateidownload zulassen	√			
Geräterichtlinien anzeigen	√	√		√
Geräterichtlinien erstellen	√			
Geräterichtlinien bearbeiten	√			
Geräterichtlinien löschen	√			
Zonen anzeigen	√	√	√	√
Zonen erstellen	√			
Zonen bearbeiten	√	√		
Zonen löschen	√			

Schutz vor Bedrohungen

Diese Berechtigung bietet Zugriff auf die Menüs „Schutz“, „CylancePROTECT Mobile-Warnungen“ und „Schwachstellen“.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Bedrohungsschutz anzeigen	√	√	√	√
Protect Mobile-Ereignisse bearbeiten	√			
Protect Mobile-Richtlinien anzeigen	√			√
Protect Mobile-Richtlinien erstellen	√			
Protect Mobile-Richtlinien bearbeiten	√			
Protect Mobile-Richtlinien löschen	√			

Netzwerk

Mit diesen Berechtigungen können Sie die Einstellungen für den Netzwerkschutz verwalten, einschließlich der Netzwerkzugriffssteuerung, CylanceGATEWAY-Einstellungen sowie CylanceGATEWAY-Warnungen und -Ereignisse.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Gateway-Dienst-Richtlinien anzeigen	√			√
Gateway-Dienst-Richtlinien erstellen	√			
Gateway-Dienst-Richtlinien bearbeiten	√			
Gateway-Dienst-Richtlinien löschen	√			
Netzwerkzugriffskontrollen anzeigen	√			√
Netzwerkzugriffskontrollen bearbeiten	√			
Gateway-Einstellungen anzeigen	√			√
Gateway-Einstellungen erstellen	√			
Gateway-Einstellungen bearbeiten	√			
Gateway-Einstellungen löschen	√			
Gateway-Berichtsereignisse anzeigen	√			√
Anzeigen von Gateway-Warnungen und -Ereignissen	√			√

Avert

Mit diesen Berechtigungen können Sie CylanceAVERT-Funktionen verwalten.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Avert-Einstellungen anzeigen	√			√
Avert-Einstellungen bearbeiten	√			

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Avert-Gerätekennung anzeigen	√			√
Avert-Risikobewertungen anzeigen	√			√
Avert-Geräteereignisse anzeigen	√			√
Avert-Richtlinien anzeigen	√			√
Erstellen von Avert-Richtlinien	√			
Avert-Richtlinien bearbeiten	√			
Avert-Richtlinien löschen	√			
Avert-Zusammenfassung zu vertraulichen Dateien anzeigen	√			
Avert-Dateiinhalt anzeigen	√			
Avert-Dateien löschen	√			

Allgemein

Mit diesen Berechtigungen können Administratoren Einstellungen auf Mandantenebene verwalten, die sich auf mehrere Funktionen in der Cylance Endpoint Security-Lösung auswirken, einschließlich EMM-Anbieter und -Verzeichnisse, Registrierungen für mobile Geräte und CylanceGATEWAY sowie adaptive Risikooptionen und -ereignisse. Bei Verzeichnisverbindungen können nur Microsoft Entra ID Active Directory-Verbindungen (AD) erstellt werden.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
EMM-Verbindungen anzeigen	√			√
EMM-Verbindungen erstellen	√			
EMM-Verbindungen bearbeiten	√			
EMM-Verbindungen löschen	√			
Verzeichnisverbindungen anzeigen	√			√

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Verzeichnisverbindungen erstellen	√			
Verzeichnisverbindungen bearbeiten	√			
Verzeichnisverbindungen löschen	√			
Lokalen Verzeichnis-Connector anzeigen	√			√
Lokalen Verzeichnis-Connector erstellen	√			
Lokalen Verzeichnis-Connector bearbeiten	√			
Lokalen Verzeichnis-Connector löschen	√			
Authentifizierungssteuerungen anzeigen	√			√
Authentifikatoren erstellen	√			
Authentifikatoren bearbeiten	√			
Authentifikatoren löschen	√			
Registrierungsrichtlinien anzeigen	√			√
Registrierungsrichtlinien erstellen	√			
Registrierungsrichtlinien bearbeiten	√			
Registrierungsrichtlinien löschen	√			
Adaptive Risikorichtlinien anzeigen	√			√
Adaptive Risikorichtlinien erstellen	√			

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Adaptive Risikorichtlinien bearbeiten	√			
Adaptive Risikorichtlinien löschen	√			
Adaptive Risikoeinstellungen anzeigen	√			√
Adaptive Risikoeinstellungen erstellen	√			
Adaptive Risikoeinstellungen bearbeiten	√			
Adaptive Risikoeinstellungen löschen	√			
Warnungen anzeigen	√			√
Warnungen bearbeiten	√			
Warnungen löschen	√			

Protokollierung

Mit diesen Berechtigungen können Sie Berichte und das Überwachungsprotokoll anzeigen.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Berichte anzeigen	√			√
Überwachungsprotokoll anzeigen	√			√

Einstellungen

Mit diesen Berechtigungen können Sie die Einstellungen der Verwaltungskonsole verwalten. Benutzerverwaltungsberechtigungen und Rollenverwaltungsberechtigungen sind miteinander verknüpft. Wenn einem Benutzer eine Rolle mit ausgewählten Benutzerverwaltungsberechtigungen zugewiesen wird, hat dieser Benutzer somit auch Zugriff auf die Rollenverwaltungsfunktionalität.

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Anwendung	√	√		√

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Token-Verwaltung	√			
Installationsprogramm-Download	√	√		
Kennwortverwaltung für die Deinstallation	√			
Support-Anmeldung	√			
Syslog/SIEM	√			
Benutzerdefinierte Authentifizierung	√			
Bedrohungsdatenbericht	√			
Benutzerverwaltung	√			
Globale Liste anzeigen	√	√		√
Globale Liste erstellen	√			
Globale Liste bearbeiten	√			
Globale Liste löschen	√			
Agent-Update-Einstellungen anzeigen	√			√
Agent-Update-Einstellungen erstellen	√			
Agent-Update-Einstellungen bearbeiten	√			
Agent-Einstellungen löschen	√			
Zertifikate	√	√		√
Integrationen	√			
Gerätelebenszyklus-Einstellungen anzeigen	√			√
Gerätelebenszyklus-Einstellungen erstellen	√			

Berechtigung	Administrator	Zonenmanager	Benutzer	Nur Lesezugriff
Gerätelebenszyklus-Einstellungen bearbeiten	√			
Gerätelebenszyklus-Einstellungen löschen	√			
Aktivierungseinstellungen anzeigen	√			√
Aktivierungseinstellungen bearbeiten	√			

Verwalten von Rollen

Sie können vordefinierte Rollen verwenden oder benutzerdefinierte Rollen erstellen, um den Administratorzugriff auf Funktionen in der Verwaltungskonsole zu verwalten. Vordefinierte Rollen beinhalten die folgenden Berechtigungen, die nicht geändert werden können. Einige Menüoptionen, Seiten und Funktionen sind je nach den Berechtigungen Ihrer Rolle möglicherweise nicht verfügbar. Wenn ein Benutzer beispielsweise keinen Zugriff auf die Zonenfunktion hat, wird die Menüoption „Zonen“ nicht angezeigt. Das Dashboard ist für alle vordefinierten und kundenspezifischen Rollen verfügbar; die angezeigten Daten spiegeln jedoch nur die Zonen wider, die der angemeldete Benutzer verwalten darf.

Eine umfassende Liste der für die jeweilige Rolle zulässigen Benutzerberechtigungen finden Sie unter Berechtigungen für Administratorrollen. Benutzer, die einer benutzerdefinierten Rolle zugewiesen sind, können keine Benachrichtigungen auf der Seite „Mein Konto“ aktivieren.

Hinzufügen von Rollen

Benutzerdefinierte Rollen sind global gültig und bieten vollen operativen Zugriff auf die zugehörigen Seiten und Aktionen für einen definierten Bereich. Wenn beispielsweise eine benutzerdefinierte Rolle Berechtigungen für die Zonenfunktionen hat, hat jeder der Rolle zugewiesene Benutzer Zugriff auf alle Funktionen, die auf den Seiten „Zonen“ oder „Zonendetails“ verfügbar sind.

Wenn für eine Rolle kein Zugriff ausgewählt ist, wird diese Seite nicht im Menü angezeigt und der Benutzer kann von anderen Stellen in der Konsole nicht zu dieser Seite navigieren. Beispiel: Wenn für eine benutzerdefinierte Rolle „Zulassen“ für Bedrohungen aktiviert, aber für Geräte deaktiviert ist, wird die Seite „Schutz vor Bedrohungen“ im Menü angezeigt, aber die Seite „Geräte“ wird nicht angezeigt. Wenn der Benutzer die Seite „Bedrohungsdetails“ für eine Bedrohung anzeigt, werden die betroffenen Geräte und Zonen angezeigt, aber der Benutzer erhält eine Fehlerseite, wenn er versucht, auf den Link zu klicken, um Details für ein bestimmtes Gerät zu erhalten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Administratoren**.
2. Klicken Sie auf **Rollen**.
3. Klicken Sie auf **Neue Rolle hinzufügen**.
4. Geben Sie einen Namen für die Rolle ein.
5. Klicken Sie neben jeder Funktion, auf die diese Rolle zugreifen können soll, auf das Kontrollkästchen **Zugriff**. Erweitern Sie die Abschnitte, um weitere Optionen anzuzeigen. Weitere Informationen finden Sie im Abschnitt Berechtigungen für Administratorrollen.
6. Klicken Sie auf **Rolle hinzufügen**.

Wenn Sie fertig sind:

- Um eine Rolle zu bearbeiten, klicken Sie auf eine vorhandene Rolle und ändern den Namen oder die Berechtigungen. Der aktualisierte Name bzw. die aktualisierten Berechtigungen werden auf alle Benutzer angewendet, die der vorhandenen Rolle zugewiesen sind.
- Wenn einer vordefinierten oder benutzerdefinierten Rolle Benutzer zugewiesen sind, können Sie auf den Link in der Spalte **Zugewiesene Benutzer** klicken, um die E-Mail für alle Benutzer anzuzeigen, die dieser Rolle zugewiesen sind. Sie können auf die E-Mail klicken, um die Seite „Benutzerdetails“ für diesen Benutzer anzuzeigen.
- Um eine Rolle zu löschen, klicken Sie auf ein Kontrollkästchen neben einer Rolle, der keine Benutzer zugewiesen sind, und klicken Sie dann auf **Entfernen**. Wenn einer Rolle Benutzer zugewiesen sind, können Sie das Kontrollkästchen nicht aktivieren.

Konfigurieren von Grenzwerten für Sitzungs- und Leerlauf-Zeitüberschreitungen

Sie können festlegen, wie lange ein Administrator bei der Verwaltungskonsole angemeldet bleiben kann, bevor er abgemeldet wird, auch wenn die Sitzung aktiv ist. Sie können auch angeben, wie lange eine Sitzung ohne Aktivität bleiben darf, bevor der Administrator von der Konsole abgemeldet wird.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Authentifizierung**.
2. Konfigurieren Sie auf der Registerkarte **Einstellungen** im Abschnitt **Konsolen-Timeout** den Grenzwert für das **Sitzungs-Timeout**.

   Administratoren erhalten einige Minuten vor Erreichen des Grenzwerts für das Konsolen-Timeout eine Countdown-Anzeige, die es ihnen ermöglicht, sich erneut zu authentifizieren, um die Sitzung fortzusetzen. Wenn der Administrator nicht aktiv auf die Aufforderung reagiert, indem er auf **Überprüfen** klickt und sich erneut anmeldet, wird er abgemeldet, wenn das Zeitlimit erreicht ist.
3. Konfigurieren Sie den Grenzwert für **Leerlauf-Timeout**.
4. Klicken Sie auf **Speichern**.

Hinzufügen von Benutzern und Geräten

Sie müssen Benutzerkonten in der Verwaltungskonsole hinzufügen, damit Sie die folgenden Cylance Endpoint Security-Dienste für diese Benutzer aktivieren können:

- In der CylancePROTECT Mobile-App verfügbare Dienste: CylancePROTECT Mobile und CylanceGATEWAY Mobile
- CylanceGATEWAY Desktop

Sie können die folgenden Methoden verwenden, um Benutzer hinzuzufügen:

- Stellen Sie eine Verknüpfung mit Ihrem Unternehmensverzeichnis her und aktivieren Sie das Onboarding, um Benutzer automatisch hinzuzufügen, wenn Cylance Endpoint Security mit dem Verzeichnis synchronisiert. Sie können die Zeitplanung für die Verzeichnissynchronisierung so konfigurieren, dass Cylance Endpoint Security mit dem Unternehmensverzeichnis Ihres Unternehmens synchronisiert wird. Standardmäßig werden alle Benutzer und Gruppen täglich in 30-Minuten-Intervallen synchronisiert.
- Stellen Sie eine Verknüpfung mit Ihrem Unternehmensverzeichnis her und fügen Sie Verzeichnisbenutzer einzeln hinzu. Sie können diese Option verwenden, wenn Sie das Onboarding nicht aktivieren möchten.
- Fügen Sie einzelne Benutzer als BlackBerry Online Account-Benutzer hinzu.

Sie müssen keine Benutzerkonten hinzufügen, um andere Cylance Endpoint Security-Dienste wie CylancePROTECT Desktop und CylanceOPTICS zu aktivieren. Nachdem die Agenten auf Geräten installiert worden sind, können Sie diese Geräte und die zugehörigen Daten in der Verwaltungskonsole anzeigen und verwalten.

Hinzufügen der CylancePROTECT Mobile-App und von CylanceGATEWAY-Benutzern

Bevor Sie beginnen: Wenn Sie Benutzer aus Ihrem Unternehmensverzeichnis hinzufügen möchten, befolgen Sie die Anweisungen unter Verknüpfung mit Ihrem Unternehmensverzeichnis. Wenn Sie „Onboarding“ aktivieren, werden Verzeichnisgruppen und Benutzerkonten während des Synchronisierungsprozesses zur Verwaltungskonsole hinzugefügt. Führen Sie die folgenden Schritte aus, wenn Sie Verzeichnisbenutzer einzeln ohne Onboarding hinzufügen möchten oder einzelne Benutzer als BlackBerry Online Account-Benutzer hinzufügen möchten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Assets > Benutzer**.
2. Klicken Sie auf **Benutzer hinzufügen**.
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Hinzufügen eines Verzeichnisbenutzers	**a.** Geben Sie den Namen des Benutzers ein und klicken Sie in der Dropdown-Liste auf das passende Ergebnis. **b.** Wenn Sie bereits Benutzergruppen hinzugefügt haben, können Sie den Benutzer optional zu einer oder mehreren Gruppen hinzufügen.

Aufgabe	Schritte
Hinzufügen eines BlackBerry Online Account-Benutzers	**a.** Klicken Sie in das Suchfeld und dann auf **Einen neuen Benutzer manuell hinzufügen**. Wenn Sie keine Verzeichnisverbindung konfiguriert haben, springen sie zum nächsten Schritt. **b.** Geben Sie den Namen und die E-Mail-Adresse des Benutzers an. **c.** Wenn Sie bereits Benutzergruppen hinzugefügt haben, können Sie den Benutzer optional zu einer oder mehreren Gruppen hinzufügen. **d.** Weisen Sie den Benutzer an, das Kennwort für das BlackBerry Online-Konto zurückzusetzen, um seine E-Mail-Adresse einzugeben und ein Kennwort festzulegen. Der Benutzer verwendet dieses Kennwort, um die CylancePROTECT Mobile-App zu aktivieren. Benutzer können auch über die CylancePROTECT Mobile-App auf den Link zum Zurücksetzen des Kennworts zugreifen, wenn sie die App aktivieren.

4. Klicken Sie auf **Speichern**. Wenn Sie einen weiteren Benutzer hinzufügen möchten, klicken Sie auf **Speichern und neu** und wiederholen den vorherigen Schritt.

Wenn Sie fertig sind:

- Um Benutzer zu einer Gruppe hinzuzufügen, wählen Sie unter **Assets > Benutzergruppen** die Gruppe aus und fügen über die Registerkarte **Benutzer** die entsprechenden Benutzer hinzu. Wenn Sie Onboarding aktiviert haben, wird die Gruppenmitgliedschaft aus dem Verzeichnis synchronisiert.
- Um CylancePROTECT Mobile für die von Ihnen hinzugefügten Benutzer zu aktivieren, befolgen Sie die Anweisungen unter Einrichten von CylancePROTECT Mobile.
- Um CylanceGATEWAY für die von Ihnen hinzugefügten Benutzer zu aktivieren, befolgen Sie die Anweisungen unter Einrichten von CylanceGATEWAY.
- Zuweisen von Richtlinien zu Administratoren, Benutzern und Gruppen.

Hinzufügen von Benutzergruppen

Sie können Gruppen für Benutzer erstellen, die für die CylancePROTECT Mobile-App und für CylanceGATEWAY-Benutzer aktiviert sind. Eine Benutzergruppe ist eine Zusammenfassung ähnlicher Benutzer, die gemeinsame Eigenschaften haben. Die Administration von Benutzern als Gruppe ist effizienter als die Administration von individuellen Benutzern, da die Eigenschaften für alle Mitglieder der Gruppe gleichzeitig hinzugefügt, geändert oder entfernt werden können. Wenn Sie Benutzergruppen Richtlinien zuweisen, gelten diese Richtlinien für alle Gruppenmitglieder.

Richtlinien können Sie einer Gruppe auf der Seite „Gruppeneinstellungen“ oder auf der Seite Richtlinien zuweisen. Wenn ein Benutzer zu zwei oder mehr Gruppen gehört, denen unterschiedliche Richtlinien zugewiesen sind, wird die Richtlinie mit dem höchsten Rang auf den Benutzer angewendet.

Sie können zwei Arten von Benutzergruppen erstellen:

- Verzeichnisgruppen sind mit Gruppen in Ihrem Unternehmensverzeichnis verknüpft. Die Mitgliedschaft der Gruppe wird mit der Mitgliedschaftsliste im Verzeichnis synchronisiert. Weitere Informationen finden Sie unter Konfigurieren von Onboarding und Offboarding.
- Lokale Gruppen werden in der Verwaltungskonsole erstellt und verwaltet. Sie können einen beliebigen lokalen Benutzer oder Verzeichnisbenutzer einer lokalen Gruppe zuweisen.

Hinzufügen einer Verzeichnisgruppe

Wenn Sie eine Verknüpfung mit einem oder mehreren Unternehmensverzeichnissen hergestellt und das Onboarding konfiguriert haben, können Verzeichnisgruppen automatisch zu Cylance Endpoint Security

hinzugefügt werden. Sie können auch eine Verzeichnisgruppe hinzufügen, wenn sie nicht über das Onboarding hinzugefügt worden ist.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Assets > Benutzergruppen**.
2. Klicken Sie auf **Gruppe hinzufügen > Verzeichnisgruppe**.
3. Geben Sie den Namen einer Gruppe so ein, wie er im Verzeichnis angezeigt wird.
4. Wählen Sie den Gruppennamen aus, wenn er in den Suchergebnissen angezeigt wird.
5. Wenn die Gruppe und alle verschachtelten Gruppen für das Onboarding aktiviert werden sollen, wählen Sie **Verschachtelte Verzeichnisgruppen** aus.
6. Um der Gruppe eine Richtlinie zuzuweisen, klicken Sie auf ⊕ und wählen den Typ der Richtlinie aus, die Sie hinzufügen möchten.
7. Wählen Sie die Richtlinie aus und klicken Sie auf **Speichern**.

Lokale Gruppe hinzufügen

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Assets > Benutzergruppen**.
2. Klicken Sie auf **Gruppe hinzufügen > Lokale Gruppe**.
3. Geben Sie einen Namen und eine Beschreibung für die Gruppe ein.
4. Um der Gruppe eine Richtlinie zuzuweisen, klicken Sie auf ⊕ und wählen den Typ der Richtlinie aus, die Sie hinzufügen möchten.
5. Wählen Sie die Richtlinie aus und klicken Sie auf **Speichern**.
6. Wenn Sie die Zuweisung der Richtlinien abgeschlossen haben, klicken Sie auf **Speichern**.
7. Um Benutzer zur Gruppe hinzuzufügen, klicken Sie auf der Seite **Benutzergruppen** auf den Gruppennamen und dann auf **Benutzer**.
8. Klicken Sie auf **Benutzer hinzufügen**.
9. Geben Sie einen Namen ein, um nach dem Benutzer zu suchen, der hinzugefügt werden soll.
10. Wählen Sie mindestens einen Namen aus den Suchergebnissen aus.
11. Klicken Sie auf **Speichern**.

    Sie können auf der Seite „Benutzer“ auch einzelne Benutzer zu Gruppen hinzufügen und aus diesen entfernen.

Hinzufügen eines Authentifikators

Sie fügen Authentifikatoren hinzu, damit Sie sie zu Authentifizierungsrichtlinien hinzufügen können. In der Regel wird mit dem Authentifikator eine Authentifizierungsmethode wie ein Kennwort (z. B. ein Kennwort für die Cylance-Konsole) oder eine Authentifizierung für Verbindungen zu Drittanbietern wie Active Directory, Okta oder Ping Identity konfiguriert. Sie fügen sie den Authentifizierungsrichtlinien hinzu, um die Authentifizierungstypen anzugeben, die Administratoren durchlaufen müssen, um sich bei der Cylance-Konsole anzumelden, und die Benutzer durchlaufen müssen, um Cylance Endpoint Security-Apps oder -Agenten zu aktivieren (z. B. die CylancePROTECT Mobile-App oder CylanceGATEWAY). Sie können mehrere Authentifikatoren in einer Authentifizierungsrichtlinie kombinieren, um mehrere Authentifizierungsschritte bereitzustellen. Sie können beispielsweise einen Unternehmensauthentifikator mit einer Eingabeaufforderung für ein Einmalkennwort in einer Richtlinie kombinieren, damit sich Benutzer sowohl mit ihren geschäftlichen Anmeldedaten als auch mit ihrem Kennwort für die Cylance-Konsole und einem Einmalkennwort authentifizieren müssen.

Bevor Sie beginnen:

- **Wichtig:** Stellen Sie sicher, dass Sie die entsprechenden Schritte für Erweiterte Authentifizierungsanmeldung in der Cylance-Konsole geprüft und ausgeführt haben, bevor Sie Ihren IDP-SAML-Authentifikator konfigurieren.

Wenn die erforderlichen Schritte nicht abgeschlossen werden, kann der Drittanbieter-Authentifikator nicht mit Cylance Endpoint Security kommunizieren. Weitere Informationen finden Sie unter:

- Schritte zum Konfigurieren eines IDP für die erweiterte Authentifizierung und den IDP-initiierten Zugriff auf die Cylance-Konsole finden Sie unter Erweiterte Authentifizierungsanmeldung.
- Eine Übersicht zur Konfiguration einer neuen IDP-SAML finden Sie unter Konfigurieren von IDP-SAMLs für die erweiterte Authentifizierung und den IDP-initiierten Zugriff auf die Cylance-Konsole.
- Eine Anleitung zur Aktivierung des IDP-initiierten Zugriffs auf die Konsole für eine vorhandene IDP-SAML, die vor Dezember 2023 erstellt wurde, finden Sie unter Aktualisieren externer IDP-(SAML-)Authentifikatoren für SSO, um auf die Cylance-Konsole zuzugreifen.

- Wenn Sie einen SAML-Authentifikator hinzufügen, laden Sie eine Kopie des Signaturzertifikats für Ihren Identitätsanbieter (IDP) herunter.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Authentifizierung**.
2. Klicken Sie auf **Authentifikator hinzufügen**.
3. Wählen Sie in der Dropdown-Liste **Authentifikatortyp** einen der folgenden Authentifikatoren aus:

Element	Beschreibung
Entra (SAML)	Wählen Sie diese Option aus, wenn Benutzer ihre Entra-Anmeldedaten auf der primären Anmeldeseite eingeben und IDP-initiierten Zugriff auf die Cylance-Konsole aktivieren möchten. Eine Anleitung zu den Schritten zur Konfiguration Ihres Entra (SAML) finden Sie unter: • Konfigurieren Sie einen neuen Entra (SAML): Konfigurieren des Entra (SAML-Authentifikators für die erweiterte Authentifizierung • Aktivieren Sie Entra-initiierten Zugriff für einen vorhandenen Entra (SAML): Aktualisieren des Entra (SAML-)Authentifikators, um den IDP-initiierten Zugriff auf die Cylance-Konsole zu aktivieren **Hinweis:** Die SSO-Callback-URL wird generiert, wenn Sie den Authentifikator speichern, und hat das Format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. Gehen Sie wie folgt vor: **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Aktivieren Sie die Option **Validierung erforderlich**, wenn Benutzer ihre E-Mail-Adresse bei der ersten Anmeldung mit einem einmaligen Code validieren sollen. Der Code wird an die E-Mail-Adresse gesendet, die mit dem Benutzer in Ihrem Mandanten verknüpft ist. **c.** Geben Sie im Feld **Anmeldeanforderungs-URL** die Anmelde-URL ein, die in den Einstellungen für die einmalige Anmeldung bei der App-Registrierung für Ihren Identitätsanbieter angegeben ist. Gehen Sie beispielsweise im Entra-Portal zu „Unternehmensanwendung“ > <*Name of the newly created application*> > „Einrichten von *application name*“ > Anmelde-URL. **d.** Fügen Sie im Feld **IDP-Signaturzertifikat** den Text des heruntergeladenen Signaturzertifikats ein, einschließlich der Zeilen „Zertifikat beginnen“ und „Zertifikat beenden“. Wenn Sie den Text des Zertifikats kopieren und einfügen, stellen Sie sicher, dass Sie keine Zeilenumbrüche und auch nicht das Format der Zertifikatsinformationen ändern. **e.** Geben Sie im Feld **Entitätskennung des SP** die **ID (Entitätskennung)** ein, die Sie in der SAML-Konfiguration im Entra-Portal notiert haben. Dies ist ein Pflichtfeld. Der Wert im Feld „Entitätskennung des SP“ muss der „ID (Entitätskennung)“ entsprechen, die Sie in der IDP-Konsole notiert haben. **f.** Aktivieren Sie **Erweiterte Einstellungen anzeigen**, und fügen Sie im Feld **E-Mail-Anspruch** den Wert aus dem „Anspruchsnamen“ ein, den Sie im Entra-Portal notiert haben (z. B. http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress). **g.** Legen Sie weitere optionale Einstellungen fest. **h.** Klicken Sie auf **Speichern**. **i.** Öffnen Sie den hinzugefügten Authentifikator. Notieren Sie die **SSO-Callback-URL**. Diese URL ist im Entra-Portal > „SAML-Basiskonfiguration“ > „Antwort-URL“ (Assertion Consumer-URL)“ erforderlich.

Element	Beschreibung
Benutzerdefiniert (SAML)	Wählen Sie diese Option aus, wenn Benutzer kundenspezifische Anmeldedaten auf der primären Anmeldeseite eingeben und IDP-initiierten Zugriff auf die Cylance-Konsole aktivieren möchten. Eine Anleitung zu den Schritten zur Konfiguration Ihrer kundenspezifischen (SAML) finden Sie unter: • Konfigurieren Sie eine kundenspezifische (SAML): Konfigurieren des kundenspezifischen (SAML)-Authentifikators für die erweiterte Authentifizierung • Aktivieren Sie kundenspezifisch initiierten Zugriff für eine kundenspezifische (SAML): Aktualisieren des kundenspezifischen (SAML-)Authentifikators, um den IDP-initiierten Zugriff auf die Cylance-Konsole zu aktivieren **Hinweis:** Die SSO-Callback-URL wird generiert, wenn Sie den Authentifikator speichern, und hat das Format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Aktivieren Sie die Option **Validierung erforderlich**, wenn Benutzer ihre E-Mail-Adresse bei der ersten Anmeldung mit einem einmaligen Code validieren sollen. **c.** Geben Sie im Feld **Anmeldeanforderungs-URL** die Single Sign-On-URL für den Identitätsanbieter ein. **d.** Fügen Sie im Feld **IDP-Signaturzertifikat** den Text des heruntergeladenen Signaturzertifikats ein, einschließlich der Zeilen „Zertifikat beginnen“ und „Zertifikat beenden“. Wenn Sie den Text des Zertifikats kopieren und einfügen, stellen Sie sicher, dass Sie keine Zeilenumbrüche und auch nicht das Format der Zertifikatsinformationen ändern. **e.** Geben Sie im Feld **Entitätskennung des SP** die „Audience-URI (Entitätskennung des SP)“ ein, die Sie im kundenspezifischen IDP-Portal notiert haben. Dies ist ein Pflichtfeld. Der Wert im Feld „Entitätskennung des SP“ muss der „Audience-URI (Entitätskennung des SP)“ entsprechen, die Sie in der IDP-Konsole notiert haben. **f.** Geben Sie im Feld **Namenskennungsformat** das Format der Namenskennung an, das vom IDP angefordert werden soll (z. B. urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress). **g.** Geben Sie im Feld **E-Mail-Anspruch** den Wert `NameID` ein. Dieser Wert muss mit dem „NameID-Format“ übereinstimmen, das Sie in der IDP-Konsole angegeben haben. Die E-Mail-Adresse stellt sicher, dass sich der richtige Benutzer bei der Verwaltungskonsole anmeldet. **h.** Legen Sie weitere optionale Einstellungen fest. **i.** Klicken Sie auf **Speichern**. **j.** Öffnen Sie den hinzugefügten Authentifikator. Notieren Sie die **Single-Sign-On-URL**. Diese URL wird zum kundenspezifischen IDP hinzugefügt.

Element	Beschreibung
Cylance-Administratorkennwort	Wählen Sie diese Option, wenn Benutzer ihre Cylance-Konsolenanmeldedaten eingeben sollen. Gehen Sie wie folgt vor: **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Klicken Sie auf **Speichern**.
Direkte Authentifizierung	Wählen Sie diese Option aus, wenn Sie eine Authentifizierungsrichtlinie verwenden möchten, um zu verhindern, dass Benutzer oder Gruppen von Benutzern auf die Cylance-Konsole oder einen anderen Dienst zugreifen. Sie können eine weitere Richtlinie oder eine App-Ausnahme hinzufügen, um den Zugriff auf eine Untergruppe von Benutzern zu ermöglichen. **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Klicken Sie auf **Speichern**.
Duo MFA	Wählen Sie diese Option aus, wenn Benutzer sich mithilfe der Duo-Multi-Faktor-Authentifizierung authentifizieren sollen. Bevor Sie Duo als Authentifikator hinzufügen, sollten Sie eine API-Anwendung zur Authentifizierung erstellen. Weitere Informationen finden Sie in den Informationen von Duo. Gehen Sie wie folgt vor: **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Geben Sie im Abschnitt **Duo MFA-Konfiguration** den API-Hostnamen, den Integrationsschlüssel und den geheimen Schlüssel ein. Diese Informationen finden Sie auf der Registerkarte „Anwendungen“ im Duo-Konto Ihres Unternehmens. Weitere Informationen finden Sie in der Duo-Dokumentation.
Enterprise	Wählen Sie diese Option aus, wenn Benutzer sich mit ihren Anmeldeinformationen für Active Directory, LDAP oder *my*Account authentifizieren sollen. Die Anmeldedaten, die ein Benutzer verwendet, hängen von dem Kontotyp ab, der als Ausgangsbasis für sein Benutzerkonto in der Konsole dient. Gehen Sie wie folgt vor: **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Klicken Sie auf **Speichern**.

Element	Beschreibung
FIDO	Wählen Sie diese Option aus, wenn Benutzer ein FIDO2 -Gerät registrieren und verwenden sollen, um ihre Identität zu verifizieren. Zu den unterstützten Gerätetypen gehören Smartphones, USB-Sicherheitsschlüssel oder Windows Hello. **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Klicken Sie auf **Speichern**. Wenn FIDO der erste Authentifizierungsfaktor ist und ein Benutzer ein Gerät zum ersten Mal registriert, wird auch ein einmaliges Kennwort an die E-Mail-Adresse gesendet, mit der er sich anmeldet. Wenn FIDO als zweiter Faktor in einer Richtlinie verwendet wird und ein Benutzer ein Gerät zum ersten Mal registriert, ist kein einmaliges Kennwort erforderlich. Informationen zum Entfernen registrierter Geräte aus einem Benutzerkonto finden Sie unter Entfernen eines registrierten FIDO-Geräts für ein Benutzerkonto in der Dokumentation für Administratoren.
Integriertes Verzeichnis (Active Directory/Entra ID/LDAP)	Wählen Sie diese Option aus, wenn Benutzer ihr Active Directory-Kennwort eingeben sollen. Wenn Sie diese Option auswählen, muss der Cylance Endpoint Security-Mandant über eine Verbindung zur Unternehmensverzeichnis-Instanz verfügen. Weitere Informationen finden Sie unter Verknüpfung mit Ihrem Unternehmensverzeichnis. Gehen Sie wie folgt vor: **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Klicken Sie auf **Speichern**.
IP-Adresse	Wählen Sie diese Option aus, wenn Sie den Zugriff der Benutzer basierend auf ihrer IP-Adresse einschränken möchten. Sie können mehrere Authentifikatoren für IP-Adressen erstellen und diese verwenden, um den Zugriff für verschiedene Gruppen zu verwalten. Sie können jedoch nur einen IP-Adressen-Authentifikator in einer Richtlinie zuweisen. Eine Anleitung zum Hinzufügen oder Entfernen von IP-Adressbeschränkungen für die Konsole finden Sie unter Hinzufügen eines Authentifikators für die IP-Adressbeschränkung in der Cylance-Konsole. **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Geben Sie im Feld **IP-Adressbereiche** eine oder mehrere IP-Adressen, IP-Bereiche oder CIDRs an. Trennen Sie die Einträge durch ein Komma. Beispiel: IP-Bereich 192.168.0.100-192.168.1.255 oder CIDR: 192.168.0.10/24. **c.** Klicken Sie auf **Speichern**.

Element	Beschreibung
Lokales Konto	Wählen Sie diese Option, wenn Benutzer ihre Anmeldedaten für BlackBerry Online Account (*my*Account) eingeben sollen. Gehen Sie wie folgt vor: **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Klicken Sie auf **Speichern**.
Okta MFA	Wählen Sie diese Option aus, wenn Benutzer sich mithilfe von Okta authentifizieren sollen. Gehen Sie wie folgt vor: **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Geben Sie im Abschnitt **Okta MFA-Konfiguration** den API-Schlüssel und die Domäne des Authentifikators ein. **c.** Klicken Sie auf **Speichern**.
Okta (OIDC)	Wählen Sie diese Option aus, wenn Benutzer sich mithilfe von Okta authentifizieren sollen. Gehen Sie wie folgt vor: **a.** Wählen Sie in der Dropdown-Liste unter **Okta** die Option **OIDC** aus. **b.** Geben Sie einen Namen für den Authentifikator ein. **c.** Geben Sie im Abschnitt **Client des Identitätsanbieters** die URL des OIDC-Suchdokuments, die Client-ID und den privaten Schlüssel JWKS ein. **d.** Klicken Sie auf **Speichern**.

Element	Beschreibung
Okta (SAML)	Wählen Sie diese Option aus, wenn Benutzer ihre Okta-Anmeldedaten auf der primären Anmeldeseite eingeben und IDP-initiierten Zugriff auf die Cylance-Konsole aktivieren möchten. Eine Anleitung zu den Schritten zur Konfiguration Ihres Okta (SAML) finden Sie unter: • Konfigurieren Sie einen neuen Okta (SAML): Konfigurieren des Okta (SAML-Authentifikators für die erweiterte Authentifizierung • Aktivieren Sie Okta-initiierten Zugriff für einen vorhandenen Okta (SAML): Aktualisieren des Okta (SAML-)Authentifikators, um den IDP-initiierten Zugriff auf die Cylance-Konsole zu aktivieren **Hinweis:** Die SSO-Callback-URL wird generiert, wenn Sie den Authentifikator speichern, und hat das Format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. **a.** Wählen Sie in der Dropdown-Liste unter **Okta** die Option **SAML** aus. **b.** Geben Sie einen Namen für den Authentifikator ein. **c.** Aktivieren Sie die Option **Validierung erforderlich**, wenn Benutzer ihre E-Mail-Adresse bei der ersten Anmeldung mit einem einmaligen Code validieren sollen. **d.** Geben Sie im Feld **Anmeldeanforderungs-URL** die Single Sign-On-URL für den Identitätsanbieter ein. **e.** Fügen Sie im Feld **IDP-Signaturzertifikat** den Text des heruntergeladenen Signaturzertifikats ein, einschließlich der Zeilen „Zertifikat beginnen“ und „Zertifikat beenden“. Wenn Sie den Text des Zertifikats kopieren und einfügen, stellen Sie sicher, dass Sie keine Zeilenumbrüche und auch nicht das Format der Zertifikatsinformationen ändern. **f.** Geben Sie im Feld **Entitätskennung des SP** die „Audience-URI (Entitätskennung des SP)“ ein, die Sie im Okta-Portal notiert haben. Dies ist ein Pflichtfeld. Der Wert im Feld „Entitätskennung des SP“ muss der „Audience-URI (Entitätskennung des SP)“ entsprechen, die Sie in der IDP-Konsole notiert haben. **g.** Fügen Sie im Feld **Entitätskennung des IDP** den „IdentityProvider-Aussteller“ ein, den Sie in Okta notiert haben. **h.** Wählen Sie im Feld **Namenskennungsformat** das NameID-Format aus, das Sie im Okta angegeben haben (z. B. urn:oasis:names:tc:SAML:2.0:nameid-format:persistent). **i.** Geben Sie im Feld **E-Mail-Anspruch** den Wert `Email` ein. Er muss mit dem „Attribut“-Namen übereinstimmen, den Sie in der Okta-Konsole konfiguriert haben. Die E-Mail-Adresse stellt sicher, dass sich der richtige Benutzer bei der Verwaltungskonsole anmeldet. **j.** Legen Sie weitere optionale Einstellungen fest. **k.** Klicken Sie auf **Speichern**. **l.** Öffnen Sie den hinzugefügten Authentifikator. Notieren Sie die Single-Sign-On-URL. Diese URL wird zu den folgenden Feldern in der Okta-Konsole > Bildschirm „SAML-Einstellungen“ hinzugefügt. • Single-Sign-On-URL • Anforderbare SSO-URLs

Element	Beschreibung
OneLogin (OIDC)	Wählen Sie diese Option aus, wenn Benutzer sich mithilfe von OneLogin authentifizieren sollen. Gehen Sie wie folgt vor: **a.** Wählen Sie in der Dropdown-Liste unter **OneLogin** die Option **OIDC** aus. **b.** Geben Sie einen Namen für den Authentifikator ein. **c.** Aktivieren Sie die Option **Validierung erforderlich**, wenn Benutzer ihre E-Mail-Adresse bei der ersten Anmeldung mit einem einmaligen Code validieren sollen. **d.** Geben Sie im Abschnitt **OneLogin-Konfiguration** die URL des OIDC-Suchdokuments, die Client-ID, den Client-Schlüssel und die Authentifizierungsmethode ein. **e.** Klicken Sie auf **Speichern**.

Element	Beschreibung
OneLogin (SAML)	Wählen Sie diese Option aus, wenn Benutzer ihre OneLogin-Anmeldedaten auf der primären Anmeldeseite eingeben und IDP-initiierten Zugriff auf die Cylance-Konsole aktivieren möchten. Eine Anleitung zu den Schritten zur Konfiguration Ihres OneLogin (SAML) finden Sie unter: • Konfigurieren Sie einen neuen OneLogin (SAML): Konfigurieren des OneLogin (SAML-Authentifikators für die erweiterte Authentifizierung • Aktivieren Sie OneLogin-initiierten Zugriff für einen vorhandenen OneLogin (SAML): Aktualisieren des OneLogin (SAML-)Authentifikators, um den IDP-initiierten Zugriff auf die Cylance-Konsole zu aktivieren **Hinweis:** Die SSO-Callback-URL wird generiert, wenn Sie den Authentifikator speichern, und hat das Format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Aktivieren Sie die Option **Validierung erforderlich**, wenn Benutzer ihre E-Mail-Adresse bei der ersten Anmeldung mit einem einmaligen Code validieren sollen. **c.** Geben Sie im Feld **Anmeldeanforderungs-URL** die Single Sign-On-URL für den Identitätsanbieter ein. **d.** Fügen Sie im Feld **IDP-Signaturzertifikat** den Text des heruntergeladenen Signaturzertifikats ein, einschließlich der Zeilen „Zertifikat beginnen“ und „Zertifikat beenden“. Wenn Sie den Text des Zertifikats kopieren und einfügen, stellen Sie sicher, dass Sie keine Zeilenumbrüche und auch nicht das Format der Zertifikatsinformationen ändern. **e.** Geben Sie im Feld **Entitätskennung des SP** die „ID (Entitätskennung)“ ein, die Sie in der OneLogin-Konsole notiert haben. Dies ist ein Pflichtfeld. Der Wert im Feld „Entitätskennung des SP“ muss der „ID (Entitätskennung)“ entsprechen, die Sie in der IDP-Konsole notiert haben. **f.** Legen Sie weitere optionale Einstellungen fest. **g.** Klicken Sie auf **Speichern**. **h.** Öffnen Sie den hinzugefügten Authentifikator. Notieren Sie die Single-Sign-On-URL. Diese URL wird den folgenden Feldern in der OneLogin-Konsole hinzugefügt: • ACS (Verbraucher) URL-Validator* • ACS (Verbraucher) URL* • Single-Logout-URL

Element	Beschreibung
Einmalkennwort	Wählen Sie diese Option aus, wenn Benutzer zusätzlich zu einem anderen Authentifizierungstyp ein einmaliges Kennwort eingeben sollen. **Hinweis:** Wenn Sie diese Option auswählen, müssen Sie Ihrer Authentifizierungsrichtlinie auch einen anderen Authentifikator hinzufügen und diesen höher als das Einmalkennwort einstufen. Eine Anleitung zum Hinzufügen und Entfernen einer Authentifizierung per Einmalkennwort für Administratoren finden Sie unter: • Hinzufügen einer Authentifizierung per Einmalkennwort für Administratoren • Entfernen einer Authentifizierung per Einmalkennwort für Administratoren Gehen Sie wie folgt vor: **a.** Geben Sie einen Namen für den Authentifikator ein. **b.** Wählen Sie im Abschnitt **Einmalkennwort-Konfiguration** in der ersten Dropdown-Liste eine Anzahl von Intervallen in der Dropdown-Liste aus. Jeder Code innerhalb des Fensters ist gültig, wenn er dem erwarteten Code um die von Ihnen angegebene Anzahl von Aktualisierungsintervallen vorangeht oder folgt. Das Aktualisierungsintervall beträgt 30 Sekunden und die Standardeinstellung ist 1. **c.** Geben Sie im Abschnitt **Einmalkennwort-Konfiguration** in der zweiten Dropdown-Liste an, wie oft Benutzer die Einrichtung der OTP-App überspringen und sich authentifizieren können, ohne einen Code einzugeben.
Ping Identity (OIDC)	Wählen Sie diese Option aus, wenn Benutzer sich mithilfe von Ping Identity authentifizieren sollen. Führen Sie die folgenden Schritte aus: **a.** Wählen Sie in der Dropdown-Liste unter **Ping** die Option **OIDC** aus. **b.** Geben Sie einen Namen für den Authentifikator ein. **c.** Geben Sie im Abschnitt **Client des Identitätsanbieters** die URL des OIDC-Suchdokuments, die Client-ID und den privaten Schlüssel JWKS ein. **d.** Wählen Sie in der Dropdown-Liste **Signaturalgorithmus für ID-Token** einen Signaturalgorithmus aus. **e.** Klicken Sie auf **Speichern**.

Element	Beschreibung
Ping Identity (SAML)	Wählen Sie diese Option aus, wenn Benutzer ihre Ping Identity-Anmeldedaten auf der primären Anmeldeseite eingeben und IDP-initiierten Zugriff auf die Cylance-Konsole aktivieren möchten. Eine Anleitung zu den Schritten zur Konfiguration Ihres Ping Identity (SAML) finden Sie unter: • Konfigurieren Sie einen neuen Ping Identity (SAML): Konfigurieren des Ping Identity (SAML-Authentifikators für die erweiterte Authentifizierung • Aktivieren Sie Ping Identity-initiierten Zugriff für einen vorhandenen OneLogin (SAML): Aktualisieren des Ping Identity (SAML-)Authentifikators, um den IDP-initiierten Zugriff auf die Cylance-Konsole zu aktivieren **Hinweis:** Die SSO-Callback-URL wird generiert, wenn Sie den Authentifikator hinzufügen, und hat das Format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. **a.** Wählen Sie in der Dropdown-Liste unter **Ping-Identität** die Option **SAML** aus. **b.** Geben Sie einen Namen für den Authentifikator ein. **c.** Aktivieren Sie die Option **Validierung erforderlich**, wenn Benutzer ihre E-Mail-Adresse bei der ersten Anmeldung mit einem einmaligen Code validieren sollen. **d.** Geben Sie im Feld **Anmeldeanforderungs-URL** die Single Sign-On-URL für den Identitätsanbieter ein. **e.** Fügen Sie im Feld **IDP-Signaturzertifikat** den Text des heruntergeladenen Signaturzertifikats ein, einschließlich der Zeilen „Zertifikat beginnen“ und „Zertifikat beenden“. Wenn Sie den Text des Zertifikats kopieren und einfügen, stellen Sie sicher, dass Sie keine Zeilenumbrüche und auch nicht das Format der Zertifikatsinformationen ändern. **f.** Geben Sie im Feld **Entitätskennung des SP** die „ID (Entitätskennung)“ ein, die Sie in der PingOne-Konsole notiert haben. Dies ist ein Pflichtfeld. Der Wert im Feld „Entitätskennung des SP“ muss dem Wert „Entitätskennung“ entsprechen, den Sie in der IDP-Konsole notiert haben. **g.** Legen Sie weitere optionale Einstellungen fest. **h.** Klicken Sie auf **Speichern**. **i.** Öffnen Sie den hinzugefügten Authentifikator. Notieren Sie die **Single-Sign-On**-URL. Diese URL wird in den folgenden Feldern des Konfigurationsbildschirms für die PingOne-Konsole benötigt: • Assertion Consumer Service (ACS) • Anwendungs-URL

4. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Erstellen einer Authentifizierungsrichtlinie.

Überlegungen zum Hinzufügen von SAML-Authentifikatoren

Wenn Sie einen SAML-Authentifikator hinzufügen, sind die Werte für die Anmeldeanforderungs-URL und das IdP-Signaturzertifikat erforderlich. Beachten Sie bei optionalen Feldern die folgenden Hinweise.

Hinweis: Wenn Sie einen externen Identitätsanbieter konfigurieren, müssen Sie die URL für die Cylance Endpoint Security-Anmeldeanforderung hinzufügen. Die URL muss das Format https://login.eid.blackberry.com/_/resume/saml20/<*hash*> haben. Da externe SAML-Konfigurationen eine Liste von Single Sign-On- oder Assertion Consumer Service-Antwort-URLs unterstützen, können Sie in vorhandenen Konfigurationen die neue oder neu generierte URL als sekundäre Option zur Liste hinzufügen oder das Original ersetzen. Wenn Sie Ihren Authentifikator vor Dezember 2023 erstellt haben und Benutzer über Single Sign-On auf die Cylance-Konsole zugreifen können sollen, müssen Sie eine aktualisierte URL für die Anmeldeanforderung generieren. Weitere Informationen zur Aktualisierung Ihres Authentifikators finden Sie unter Erweiterte Authentifizierungsanmeldung.

Element	Beschreibung
NameID-Format	In diesem Feld können Sie ein optionales Format für die Namenskennung angeben, die vom Identitätsanbieter angefordert werden soll.
Anspruch auf Verbund-ID	In diesem Feld können Sie einen optionalen Anspruchswert angeben, der als Ihre Verbund-ID verwendet wird, um Konten systemübergreifend zu verknüpfen. Der Standardwert ist NameID. Wenn Ihr IdP so eingerichtet ist, dass bei einem anderen Anspruch als „NameID“ die E-Mail-Adresse zurückgegeben wird, müssen Sie den Anspruch in diesem Feld angeben. Sie sollten einen eindeutigen, unveränderbaren und beständigen Wert in diesem Anspruch verwenden (z. B. eine objectGUID oder UUID). Es wird nicht empfohlen, einen Wert zu verwenden, der nicht eindeutig ist oder sich ändern kann, wie z. B. eine E-Mail-Adresse. Wenn sich Benutzer anmelden, verwendet Cylance Endpoint Security den Wert in „Anspruch auf Verbund-ID“, um eine eindeutige ID zu erstellen, mit der der Benutzer seine Identitäten in beiden Systemen zuordnen kann. Nachdem Sie den Wert angegeben haben, der für „Anspruch auf Verbund-ID“ verwendet werden soll, kann er nicht geändert werden, da der Benutzer im externen Identitätsanbieter und Cylance Endpoint Security nach der erstmaligen Anmeldung darüber verknüpft wird.
Anspruch auf Active Directory	In diesem Feld können Sie einen optionalen Anspruchswert angeben, der verwendet wird, um objectGUIDs von Active Directory systemübergreifend abzugleichen und Benutzer zu validieren.

Element	Beschreibung
E-Mail-Anspruch	In diesem Feld können Sie einen optionalen Anspruchswert angeben, der für den systemübergreifenden Abgleich von E-Mail-Adressen verwendet wird. Der Standardwert ist „email“. Cylance Endpoint Security erfordert, dass alle SAML-Antworten die vollständige E-Mail-Adresse des Benutzers enthalten müssen. Diese muss mit der E-Mail-Adresse übereinstimmen, die bei Cylance Endpoint Security registriert ist. Wenn Ihr IdP so eingerichtet ist, dass bei einem anderen Anspruch als „email“ die E-Mail-Adresse zurückgegeben wird, müssen Sie den Anspruch in diesem Feld angeben. Wenn der bei Ihrem IdP konfigurierte Anspruch beispielsweise „emailAddress“ heißt, müssen Sie im Feld „E-Mail-Anspruch“ „emailAddress“ festlegen. Wenn diese Ansprüche nicht übereinstimmen, können sich die Benutzer nicht anmelden.
Entitätskennung des SP	In diesem Feld können Sie eine optionale Entitätskennung des Dienstanbieters (Service Provider, SP) angeben, die an den Identitätsanbieter gesendet werden soll (auch als Ausstellerzeichenfolge bezeichnet). Für Entra SAML-Authentifikatoren ist dieses Feld erforderlich, und der eingegebene Wert muss mit der ID (Entitätskennung) in der SAML-Konfiguration in Entra übereinstimmen.
Entitätskennung des IdP	In diesem Feld können Sie eine optionale Entitätskennung des Identitätsanbieters angeben (auch als IdP-Aussteller bezeichnet). Wenn Sie diese angeben, wird der IdP-Aussteller bei allen Antworten validiert.
Akzeptierte Taktabweichung	In diesem Feld können Sie die zulässige Taktabweichung zwischen Client und Server in Millisekunden angeben.
Signatur-Algorithmus	In diesem Feld können Sie den Signatur-Algorithmus für Signaturanforderungen angeben.
Privater Signaturschlüssel	In diesem Feld können Sie einen optionalen privaten Schlüssel im PEM-Format angeben, der zum Signieren aller ausgehenden Anforderungen verwendet wird.

Migrieren benutzerdefinierter Authentifizierungseinstellungen in die Liste der Authentifikatoren

In den Einstellungen können Sie Ihre vorhandenen SAML-Authentifikatoren in die Liste der Authentifikatoren migrieren, sodass Sie sie zu Authentifizierungsrichtlinien für Benutzer und Gruppen oder Ihren Mandanten hinzufügen können. Wenn Sie die Authentifikatoren migrieren, müssen Sie die Single Sign-On-URL auf die von Cylance Endpoint Security verwendete URL aktualisieren. Sie müssen auch den NameID-Anspruch in Ihrer externen IdP-Konfiguration aktualisieren, damit er anstelle der E-Mail-Adresse eines Benutzers einen beständigen, unveränderbaren Wert zurückgibt, oder Sie müssen beim Identitätsanbieter einen Anspruch erstellen, der für „Anspruch auf Verbund-ID“ verwendet werden kann.

Bevor Sie Ihre Einstellungen migrieren, sollten Sie als Sicherheitsmaßnahme eine Authentifizierungsrichtlinie erstellen, die nur das Cylance-Konsolenkennwort erfordert, und sie einem Administrator zuweisen.

Hinweis: Wenn Sie die kundenspezifischen Authentifizierungseinstellungen zum externen Identitätsanbieter migrieren, müssen Sie die folgende URL für die Cylance Endpoint Security-Anmeldeanforderung hinzufügen:

`https://idp.blackberry.com/_/resume`. Da externe SAML-Konfigurationen eine Liste von Single Sign-On- oder Assertion Consumer Service-Antwort-URLs unterstützen, können Sie in vorhandenen Konfigurationen die neue URL als sekundäre Option zur Liste hinzufügen oder das Original ersetzen.

Weitere Informationen zu SAML-Authentifikatoren finden Sie unter Überlegungen zum Hinzufügen von SAML-Authentifikatoren.

Bevor Sie beginnen: Laden Sie eine Kopie des Signaturzertifikats für Ihren IdP herunter.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen** > **Anwendung**.
2. Führen Sie im Abschnitt **Kundenspezifische Authentifizierung** die folgende Aktion aus:
   a) Kopieren Sie die folgenden Informationen in eine Textdatei:
      - Anbietername
      - Anmelde-URL

   b) Aktivieren Sie das Kontrollkästchen **Kennwortanmeldung zulassen**. Weitere Informationen zu der Einstellung finden Sie unter Benutzerdefinierte Authentifizierungsbeschreibungen.
3. Klicken Sie in der Menüleiste auf **Einstellungen** > **Authentifizierung**.
4. Klicken Sie auf der Registerkarte **Authentifikatoren** auf **Authentifikator hinzufügen**.
5. Klicken Sie in der Dropdown-Liste **Authentifikatortyp** auf den SAML-Authentifikator, der dem in Schritt 2 kopierten Anbieter entspricht (z. B. Entra oder Okta), oder klicken Sie auf „Benutzerdefinierte SAML“.
6. Geben Sie im Abschnitt **Allgemeine Informationen** einen Namen für den Authentifikator ein.
7. Aktivieren Sie im Abschnitt **SAML-Konfiguration** die Option **Validierung erforderlich**, wenn Benutzer ihre E-Mail-Adresse bei der ersten Anmeldung mit einem einmaligen Code validieren sollen.
8. Geben Sie im Feld **Anmeldeanforderungs-URL** die Single Sign-On-URL für den Identitätsanbieter ein.
9. Fügen Sie im Feld **IdP-Signaturzertifikat** den Text des heruntergeladenen Signaturzertifikats ein, einschließlich der Zeilen „Begin Certificate“ (Zertifikat beginnen) und „End Certificate“ (Zertifikat beenden).

   Wenn Sie den Text des Zertifikats kopieren und einfügen, stellen Sie sicher, dass Sie keine Zeilenumbrüche und auch nicht das Format der Zertifikatsinformationen ändern.
10. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktualisieren Sie die Werte des NameID- und des E-Mail-Anspruchs im externen Identitätsanbieter.	**a.** Melden Sie sich bei Ihrem externen Identitätsanbieter an. **b.** Aktualisieren Sie die Single Sign-On-URL für Cylance Endpoint Security auf `https://idp.blackberry.com/_/resume`. Sie können diese URL zur vorhandenen URL login.<*region*>.cylance.com hinzufügen. **c.** Bearbeiten Sie den NameID-Anspruch so, dass er einen beständigen, unveränderbaren Wert (z. B. objectGUID oder UUID) zurückgibt, der unter „Anspruch auf Verbund-ID“ anstelle der E-Mail-Adresse des Benutzers verwendet werden kann. Anweisungen hierzu finden Sie in der Dokumentation des Identitätsanbieters. **d.** Erstellen Sie einen neuen E-Mail-Anspruch, der die E-Mail-Adresse des Benutzers zurückgibt.

Aufgabe	Schritte
Erstellen Sie einen neuen Anspruch in Ihrem externen Identitätsanbieter und fügen Sie ihn in den Authentifikator-Einstellungen hinzu.	**a.** Melden Sie sich bei Ihrem externen Identitätsanbieter an. **b.** Aktualisieren Sie die Single Sign-On-URL für Cylance Endpoint Security auf `https://idp.blackberry.com/_/resume`. Sie können diese URL zur vorhandenen URL login.<*region*>.cylance.com hinzufügen. **c.** Erstellen Sie einen neuen Anspruch, der eine beständige, unveränderbare ID für einen Benutzer zurückgibt. Anweisungen hierzu finden Sie in der Dokumentation des Identitätsanbieters. **d.** Geben Sie in der Cylance-Verwaltungskonsole im Feld **E-Mail-Anspruch** `nameID` ein. Der Wert für nameID muss kleingeschrieben werden („n“). **e.** Geben Sie in das Feld **Anspruch auf Verbund-ID** den Namen des neuen Anspruchs ein, den Sie im externen Identitätsanbieter erstellt haben.

11. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Erstellen einer Authentifizierungsrichtlinie.
- Wenn bei der Anmeldung mit dem SAML-Authentifikator in einer Authentifizierungsrichtlinie Probleme auftreten, können Sie eine Beispiel-SAML-Antwort von Ihrem IdP herunterladen und die Anspruchsnamen validieren.

Verwalten von Authentifizierungsrichtlinien für Mandanten

Standardmäßig hat Cylance Endpoint Security drei Authentifizierungsrichtlinien für Mandanten, die für die Verwaltung der Authentifizierungstypen verwendet werden, die Administratoren für die Anmeldung bei der Cylance-Konsole und Benutzer für die Aktivierung der Cylance Endpoint Security-Apps oder -Agenten (z. B. die CylancePROTECT Mobile-App oder CylanceGATEWAY) durchlaufen müssen. Die Mandantenrichtlinien werden angewendet, wenn dem Benutzer für die Konsole oder die App, auf die er zugreifen möchte, keine App-Ausnahme oder Authentifizierungsrichtlinie zugewiesen ist. Die Standardrichtlinien und ihre Authentifikatoren sind:

- Administrationskonsole: Diese Richtlinie verwendet das Cylance-Konsolenkennwort als Standardauthentifikator. Für Mandanten, die nach März 2024 erstellt wurden, verwendet diese Policy das Kennwort der Cylance-Konsole und das Einmalkennwort als Standardauthentifikatoren. Es wird für die Authentifizierung an der Cylance Endpoint Security-Verwaltungskonsole verwendet.
- CylanceGATEWAY: Diese Richtlinie verwendet das Unternehmenskennwort des Benutzers als Standardauthentifikator. Sie wird verwendet, wenn Benutzer die CylanceGATEWAY-App oder den Desktop-Agenten aktivieren.
- CylancePROTECT Mobile-App: Diese Richtlinie verwendet das Unternehmenskennwort des Benutzers als Standardauthentifikator. Sie wird verwendet, wenn Benutzer die CylancePROTECT-App auf Mobilgeräten aktivieren. Sie wird nicht angewendet, wenn der Benutzer den Desktop-Agenten aktiviert.

Sie können die Richtlinien bearbeiten, um andere Authentifizierungstypen hinzuzufügen, die Benutzer in der von Ihnen in der Richtlinie angegebenen Reihenfolge durchlaufen müssen. Wenn Sie beispielsweise Einmalkennwort nach Unternehmensauthentifikator hinzufügen, geben Benutzer ihre geschäftlichen oder *my*Account-Anmeldedaten ein, bevor sie eine Eingabeaufforderung für das Einmalkennwort erhalten.

Bevor Sie beginnen: Hinzufügen eines Authentifikators.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Authentifizierung > Standardauthentifizierung**.

2. Klicken Sie auf die Richtlinie, die Sie bearbeiten möchten.
3. Klicken Sie im Abschnitt **App-Authentifizierung** auf **Authentifikator hinzufügen**.
4. Wählen Sie im Dialogfeld **Authentifikator hinzufügen** in der Dropdown-Liste einen Authentifikator aus. Klicken Sie auf **Hinzufügen**.

   Wiederholen Sie diesen Schritt, um weitere Authentifikatoren zur Richtlinie hinzuzufügen. Benutzer müssen die Authentifizierungstypen in der Reihenfolge bearbeiten, die Sie angeben. Um die Reihenfolge zu ändern, klicken Sie auf **Reihenfolge festlegen**, ziehen Sie die Authentifikatoren in die gewünschte Reihenfolge und klicken Sie erneut auf **Reihenfolge festlegen**.

   Hinweis: Wenn Sie ein Einmalkennwort als Authentifikator hinzufügen, muss es nach dem Unternehmenskennwort angegeben werden.

   erneut.
5. Klicken Sie auf **Speichern**.

Wenn Sie einer Standardrichtlinie Authentifikatoren hinzufügen, können Sie auf der Seite mit der Richtlinienliste auf „Auf Standardmethode zurücksetzen“ klicken, um die Standardeinstellung wiederherzustellen.

Erstellen einer Authentifizierungsrichtlinie

Sie können Authentifizierungsrichtlinien erstellen, um die Authentifizierungstypen anzugeben, die Administratoren durchlaufen müssen, um sich bei der Cylance Endpoint Security-Verwaltungskonsole anzumelden, und die Benutzer durchlaufen müssen, um Cylance Endpoint Security-Apps oder -Agenten zu aktivieren (z. B. CylancePROTECT Mobile oder CylanceGATEWAY). Benutzer müssen die Authentifizierungstypen in der Reihenfolge bearbeiten, die Sie in der Richtlinie angeben. Wenn Sie beispielsweise „Enterprise“ vor „Einmalkennwort“ hinzufügen, geben Benutzer ihre geschäftlichen oder *my*Account-Anmeldedaten ein, bevor sie eine Eingabeaufforderung für das Einmalkennwort erhalten.

In einer Richtlinie können Sie auch App-Ausnahmen konfigurieren und verschiedene Authentifikatoren für bestimmte Apps angeben. Anwendungsausnahmen haben Vorrang vor der Authentifizierungsrichtlinie. Alle Authentifizierungsrichtlinien, die in Ihrem Mandanten konfiguriert sind, werden in der folgenden Reihenfolge angewendet:

1. Anwendungsausnahmen in Authentifizierungsrichtlinien, die Benutzern oder Gruppen zugewiesen sind
2. Authentifizierungsrichtlinien, die Benutzern oder Gruppen zugewiesen sind
3. Authentifizierungsrichtlinie für Mandanten

Bevor Sie beginnen: Hinzufügen eines Authentifikators

1. Klicken Sie in der Menüleiste auf **Richtlinien > Benutzerrichtlinie**.
2. Klicken Sie auf die Registerkarte **Authentifizierung**.
3. Klicken Sie auf **Richtlinie hinzufügen**.
4. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.
5. Klicken Sie im Abschnitt **Authentifizierungsregeln** auf **Authentifikator hinzufügen**.

   Wenn Ihr Authentifikator vor Dezember 2023 erstellt wurde und Sie die URL für die Cylance Endpoint Security-Anmeldeanforderung aktualisiert haben, um den IDP-initiierten Proxy zu aktivieren, sodass die Benutzer beim Zugriff auf die Cylance-Konsole den Single Sign-On (SSO) verwenden können, nachdem sie sich beim IDP-Portal ihrer Benutzer angemeldet haben, fügen Sie den aktualisierten Authentifikator hinzu, und entfernen Sie die ursprünglich erstellte Authentifizierung. Weitere Informationen finden Sie unter Erweiterte Authentifizierungsanmeldung.
6. Wählen Sie im Dialogfeld **Authentifikator hinzufügen** in der Dropdown-Liste einen Authentifikator aus.

   Wiederholen Sie diesen Schritt, um weitere Authentifikatoren zur Richtlinie hinzuzufügen. Benutzer erhalten Eingabeaufforderungen von den einzelnen Authentifikatoren in der Reihenfolge, in der diese in der Richtlinie

aufgeführt sind. Wenn Sie Duo-MFA zur Richtlinie hinzufügen, sollten Sie auch einen weiteren Authentifikator hinzufügen, damit Duo als zweiter Faktor für die Authentifizierung verwendet wird. Um die Reihenfolge zu ändern, klicken Sie auf **Reihenfolge festlegen** und ziehen Sie die Authentifikatoren in die gewünschte Reihenfolge und klicken Sie erneut auf **Reihenfolge festlegen**.

7. Wenn Sie Anwendungsausnahmen hinzufügen möchten, klicken Sie auf **App-Ausnahmen verwalten**.
8. Wählen Sie im Dialogfeld **App-Ausnahmen verwalten** die Apps aus, die im Bereich **Verfügbare Apps** enthalten sein sollen.
9. Klicken Sie auf ›.
10. Klicken Sie auf **Speichern**.
11. Klicken Sie im Abschnitt **App-Ausnahmen verwalten** auf die Registerkarte für eine der Apps, die Sie als Ausnahme hinzugefügt haben.
12. Klicken Sie auf **Authentifikator hinzufügen**.
13. Wählen Sie im Dialogfeld **Authentifikator hinzufügen** aus der Dropdown-Liste einen Authentifikator aus. Klicken Sie auf **Speichern**.

    Wiederholen Sie diesen Schritt, um weitere Authentifikatoren zu App-Ausnahmen hinzuzufügen. Benutzer müssen die Authentifizierungstypen in der Reihenfolge bearbeiten, die Sie angeben. Um die Reihenfolge zu ändern, klicken Sie auf **Reihenfolge festlegen** und ziehen Sie die Authentifikatoren in die gewünschte Reihenfolge, und klicken Sie erneut auf **Reihenfolge festlegen**.
14. Um die Richtlinie zu speichern, klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Zuweisen von Richtlinien zu Administratoren, Benutzern und Gruppen.

Zuweisen von Richtlinien zu Administratoren, Benutzern und Gruppen

Sie können Benutzerrichtlinien einer beliebigen Anzahl von Gruppen, Administratoren und Benutzern zuweisen, jedem Benutzer kann jedoch nur eine Benutzerrichtlinie pro Typ zugewiesen werden. Eine einem Benutzer oder Administrator direkt zugewiesene Richtlinie hat Vorrang vor Richtlinien, die Gruppen zugewiesen sind, zu denen der Benutzer oder Administrator gehört. Wenn einem Benutzer oder Administrator keine Richtlinie direkt zugewiesen ist und der Administrator oder Benutzer zu zwei oder mehr Gruppen gehört, denen unterschiedliche Richtlinien desselben Typs zugewiesen sind, wird die Richtlinie mit der höchsten Rangordnung auf den Administrator oder Benutzer angewendet.

Jede Anmeldung bei der Verwaltungskonsole wird mit den Richtlinien verglichen, die Administratoren und Benutzern zugewiesen sind, bis eine zugewiesene Richtlinie übereinstimmt. Wenn dem Administrator oder Benutzer direkt oder über eine Gruppe, der er angehört, keine Richtlinie zugewiesen ist, wird die Standardrichtlinie angewendet und er kann sich bei der Cylance-Konsole nur mit seinem Cylance-Kennwort anmelden. Die erweiterten Authentifizierungsrichtlinien werden in der folgenden Reihenfolge auf Administratoren und Benutzer angewendet:

- App-Ausnahmen für Benutzerrichtlinie
- Benutzerrichtlinie
- App-Richtlinie für Mandanten
- Standardrichtlinie

Bevor Sie beginnen: Erstellen Sie mindestens einen der folgenden Richtlinientypen:

- Registrierungsrichtlinie
- CylancePROTECT Mobile-Richtlinie
- CylanceGATEWAY-Dienstrichtlinie
- Authentifizierungsrichtlinie

1. Klicken Sie in der Menüleiste auf **Richtlinien > Benutzerrichtlinie**.

2. Wählen Sie die Registerkarte für den Richtlinientyp aus, den Sie zuweisen möchten.
3. Klicken Sie auf den Namen der Richtlinie, die Sie zuweisen möchten.
4. Klicken Sie auf **Zugewiesene Benutzer und Gruppen**.
5. Klicken Sie auf **Benutzer oder Gruppe hinzufügen**.
6. Klicken Sie auf die Registerkarte **Benutzer**.
7. Geben Sie einen Namen ein, um nach dem Benutzer zu suchen. Standardmäßig werden maximal 50 Suchergebnisse ausgegeben. Verfeinern Sie Ihre Suche, wenn mehr als 50 Suchergebnisse ausgegeben werden.

   Administratorkonten werden mit dem Symbol in der Benutzerliste angezeigt. In einigen Szenarien sehen Sie möglicherweise zwei Benutzerkonten für einen Benutzer, ein Administratorkonto und ein Active Directory-Benutzerkonto.
8. Wählen Sie mindestens einen Namen aus den Suchergebnissen aus. Klicken Sie auf **Hinzufügen**.

   Sie können einem Benutzer auch auf der Seite Benutzerkonfiguration Richtlinien zuweisen.
9. Klicken Sie auf die Registerkarte **Benutzergruppe**.
10. Geben Sie einen Namen ein, um nach der Gruppe zu suchen, die hinzugefügt werden soll. Standardmäßig werden maximal 50 Suchergebnisse ausgegeben. Verfeinern Sie Ihre Suche, wenn mehr als 50 Suchergebnisse ausgegeben werden.
11. Wählen Sie mindestens einen Namen aus den Suchergebnissen aus. Klicken Sie auf **Hinzufügen**.

    Sie können einer Gruppe auch auf der Seite Gruppeneinstellungen Richtlinien zuweisen.
12. Um die zugewiesene Richtlinie für einen Benutzer oder eine Gruppe aufzuheben, wählen Sie die Benutzer und Gruppen aus, für die Sie die Zuweisung der Richtlinie aufheben möchten, und klicken auf **Entfernen**.

Richtlinien einen Rang zuweisen

Sie können einzelnen Benutzern und Benutzergruppen Richtlinien zuweisen. Wenn Sie einem einzelnen Benutzer eine Richtlinie zuweisen, hat diese Vorrang vor den Richtlinien, die den Gruppen zugewiesen sind, zu denen der Benutzer gehört. Wenn einem Benutzer keine Richtlinie direkt zugewiesen ist und der Benutzer zu zwei oder mehr Gruppen gehört, denen unterschiedliche Richtlinien zugewiesen sind, werden die Richtlinien mit der höchsten Rangordnung auf den Benutzer angewendet.

Bevor Sie Richtlinien eine Rangordnung zuweisen, sollten Sie sich auf der Grundlage Ihrer Ziele und der Gruppen, denen Sie Richtlinien zuweisen, für eine Strategie entscheiden. Sie können beispielsweise festlegen, dass Richtlinien für die Netzwerkzugriffssteuerung, die für bestimmte Abteilungsgruppen gelten, mit der höchsten Rangordnung und restriktivere Richtlinien unter ihnen eingestuft werden. Oder Sie können festlegen, dass Ihre restriktivste Richtlinie die höchste Rangordnung erhält.

1. Klicken Sie in der Menüleiste auf **Richtlinien > Benutzerrichtlinie**.
2. Wählen Sie die Registerkarte für den Richtlinientyp aus, den Sie zuweisen möchten.
3. Klicken Sie auf **Rang**.
4. Um die Reihenfolge einer Richtlinie in der Liste zu ändern, ziehen Sie für die Richtlinie an eine neue Position in der Liste.
5. Klicken Sie auf **Speichern**.

Registrieren von CylancePROTECT Mobile- und CylanceGATEWAY-Benutzern

Sie weisen den Benutzern eine Registrierungsrichtlinie zu, damit sie die CylancePROTECT Mobile-App auf mobilen Geräten und den CylanceGATEWAY-Agenten auf Windows- und macOS-Geräten aktivieren können.

Die Registrierungsrichtlinie enthält separate Einstellungen für Mobil- und Desktopgeräte. Sie können die unterstützten Gerätetypen und den Text für E-Mail-Nachrichten angeben, die an Benutzer gesendet werden sollen, um Aktivierungsanweisungen und ein Kennwort oder den erforderlichen QR Code zum Starten des Aktivierungsvorgangs bereitzustellen. Sie können die Anzahl der Tage, die das Aktivierungskennwort oder der QR Code gültig ist, unter **Einstellungen > Aktivierung** angeben. Die Einstellung gilt für alle Registrierungsrichtlinien.

Den Benutzern müssen die folgenden Richtlinien zugewiesen werden, damit sie die CylancePROTECT Mobile-App oder den CylanceGATEWAY-Agent aktivieren können.

Benutzertyp	Erforderliche Richtlinien
CylancePROTECT Mobile-App-Benutzer ohne CylanceGATEWAY-Unterstützung	• Registrierungsrichtlinie • CylancePROTECT Mobile Richtlinie
CylancePROTECT Mobile-App-Benutzer nur mit CylanceGATEWAY-Unterstützung	• Registrierungsrichtlinie • Gateway-Dienstrichtlinie
CylancePROTECT Mobile-App-Benutzer mit CylancePROTECT Mobile- und CylanceGATEWAY-Unterstützung	• Registrierungsrichtlinie • CylancePROTECT Mobile Richtlinie • Gateway-Dienstrichtlinie
Desktop-Benutzer mit CylanceGATEWAY-Agent	• Registrierungsrichtlinie • Gateway-Dienstrichtlinie

Hinweis: Der CylanceGATEWAY-Agent kommuniziert über sichere WebSockets (WSS) mit der Verwaltungskonsole und muss diese Verbindung direkt herstellen können. Sie müssen das Netzwerk Ihres Unternehmens so konfigurieren, dass Verbindungen zu entsprechenden Domänen zugelassen werden. Damit beispielsweise der CylanceGATEWAY-Agent aktiviert und regelmäßig authentifiziert werden kann, müssen Sie den Zugriff auf idp.blackberry.com und die Domäne für Ihre Region zulassen. Wenn in Ihrer Umgebung ein Authentifizierungs-Proxy verwendet wird, müssen Sie den Datenverkehr auf dem Proxy-Server zulassen. Wenn die entsprechenden Domänen nicht zulässig sind, kann der CylanceGATEWAY-Agent den Browser nicht öffnen, um den Authentifizierungsprozess abzuschließen. Weitere Informationen zu Domänen, die für CylanceGATEWAY zugelassen werden müssen, finden Sie unter support.blackberry.com/community im Artikel 79017. Informationen zu Netzwerkanforderungen für Cylance Endpoint Security finden Sie unter Cylance Endpoint Security-Netzwerkanforderungen.

Erstellen einer Registrierungsrichtlinie

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Benutzerrichtlinie**.
2. Klicken Sie auf die Registerkarte **Registrierung**.
3. Klicken Sie auf **Richtlinie hinzufügen**.
4. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.

5. Führen Sie die folgenden Schritte aus, um mit der CylancePROTECT Mobile-App Registrierungsoptionen für Benutzer von Mobilgeräten festzulegen:
   a) Klicken Sie auf **Mobil**.
   b) Um die Gerätetypen einzuschränken, die der Benutzer registrieren kann, deaktivieren Sie unter **Zulässige Plattformen iOS** oder **Android**.
   c) Überprüfen Sie unter **UES Mobile Willkommens-E-Mail** den Betreff für die an die Benutzer gesendete E-Mail-Nachricht und aktualisieren Sie sie bei Bedarf.
   d) Aktualisieren Sie den Text der Nachricht nach Bedarf, um Informationen speziell für Ihr Unternehmen bereitzustellen.

      Sie können Variablen in der E-Mail-Nachricht verwenden.
6. Führen Sie die folgenden Schritte aus, um Registrierungsoptionen für den CylanceGATEWAY-Agenten auf Windows- und macOS-Geräten festzulegen:
   a) Klicken Sie auf **Gateway-Desktop**.
   b) Um die Gerätetypen einzuschränken, die der Benutzer registrieren kann, deaktivieren Sie unter **Zulässige Plattformen** die Optionen **Windows** oder **macOS**.
   c) Überprüfen Sie unter **Willkommens-E-Mail** den Betreff für die an die Benutzer gesendete E-Mail-Nachricht und aktualisieren Sie ihn bei Bedarf.
   d) Aktualisieren Sie ggf. den Text der Nachricht, um Informationen speziell für Ihr Unternehmen bereitzustellen.

      Sie können Variablen in der E-Mail-Nachricht verwenden. Benutzer müssen den Wert {{CustomDomain}} in das Feld „Benutzerdefinierte Domäne“ auf der ersten Anmeldeseite eingeben. Sie können die Variable verwenden, um den Wert einzufügen, oder Sie finden ihn unter **Einstellungen > Anwendung** im Feld **Unternehmen**.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie die Richtlinie Benutzern und Gruppen zu.

Unterstützte Variablen für Registrierungs-E-Mails

Sie können die folgenden Variablen im Text der in der Registrierungsrichtlinie angegebenen E-Mail-Nachricht verwenden:

Variable	Beschreibung
{{UserDisplayName}}	Benutzeranzeigename, wie er auf der Seite „Benutzer“ oder in dem Verzeichnis angezeigt wird, aus dem das Onboarding des Benutzers erfolgte.
{{FullUserName}}	Vollständiger Benutzername, wie er auf der Seite „Benutzer“ oder in dem Verzeichnis angezeigt wird, aus dem das Onboarding des Benutzers erfolgte.
{{UserName}}	Benutzername, wie er auf der Seite „Benutzer“ oder in dem Verzeichnis angezeigt wird, aus dem das Onboarding des Benutzers erfolgte.
{{UserEmailAddress}}	Benutzer-E-Mail-Adresse, wie sie auf der Seite „Benutzer“ oder in dem Verzeichnis angezeigt wird, aus dem das Onboarding des Benutzers erfolgte.

Variable	Beschreibung
{{CustomDomain}}	Der Cylance Endpoint Security-Firmendomänenname Ihres Unternehmens. Dieser Wert wird unter **Einstellungen > Anwendung** im Feld **Unternehmen** angezeigt.
{{EnrollmentQRCode}}	QR-Code, der von Cylance Endpoint Security generiert wird, um die Aktivierung der CylancePROTECT Mobile-App auf Mobilgeräten zu vereinfachen. Diese Variable kann nur in der E-Mail-Nachricht verwendet werden, die an Benutzer von Mobilgeräten gesendet wird.
{{EnrollmentPasscode}}	Von Cylance Endpoint Security generiertes Aktivierungskennwort
{{EnrollmentPasscodeExpiry}}	Das Datum, an dem das Aktivierungskennwort und der QR-Code ablaufen. Sie können die Anzahl der Tage, die das Aktivierungskennwort oder der QR-Code gültig ist, unter **Einstellungen > Aktivierung** festlegen.

Einrichten von Zonen für die Verwaltung von CylancePROTECT Desktop und CylanceOPTICS

Sie können Zonen verwenden, um CylancePROTECT Desktop- und CylanceOPTICS-Geräte zu gruppieren und zu verwalten. Sie können Geräte nach geografischer Region (z. B. Asien und Europa), nach Funktion (z. B. Vertriebs- und IT-Mitarbeiter) oder nach beliebigen Kriterien, die Ihr Unternehmen benötigt, gruppieren.

Sie können einer Zone eine Geräterichtlinie zuweisen und diese Geräterichtlinie auf CylancePROTECT Desktop- und CylanceOPTICS-Geräte anwenden, die dieser Zone angehören. Sie können auch eine Zonenregel hinzufügen, mit der Geräte einer Zone auf der Grundlage von Kriterien, die in einer gespeicherten Abfrage vorgegeben sind (z. B. Domänenname, IP-Adressbereich oder Betriebssystem), hinzugefügt werden können. Neue Geräte werden automatisch zu einer Zone hinzugefügt, sofern sie den Zonenregelkriterien entsprechen.

Standardmäßig folgen alle automatisch der Zone hinzugefügten Geräte den Zonenregeln. Wenn in den Zonenregeln die Option zum automatischen Entfernen von Geräten ausgewählt ist, werden die den Zonenregeln folgenden Geräte automatisch aus der Zone entfernt, wenn sie die Kriterien der Zonenregeln nicht erfüllen. Sie können auch manuell Geräte hinzufügen, die die Zonenregeln ignorieren, sodass sie nicht automatisch aus der Zone entfernt werden. Beim Verwalten einer Zone können Sie ändern, ob ein Gerät den Zonenregeln folgen oder sie ignorieren soll.

Beachten Sie, dass Administratorbenutzer mit der Rolle Zonenmanager Agenten auf Geräten installieren können, aber keinen Zugriff auf die Standardzone namens „Ohne Zonen“ haben. Das heißt, sie können Zonen keine Geräte zuweisen.

Wenn Sie einen neuen Cylance Endpoint Security-Mandanten erstellen oder einen Mandanten auf den empfohlenen Standardstatus zurücksetzen, bietet BlackBerry vorkonfigurierte Zonen und vorkonfigurierte Geräterichtlinien, mit deren Hilfe Sie Ihre Umgebung an die gewünschte Sicherheitseinstellung anpassen können. Weitere Informationen finden Sie unter Konfigurieren eines neuen Cylance Endpoint Security-Mandanten.

Hinzufügen und Konfigurieren von Zonen

Bevor Sie beginnen: Wenn Sie der Zone eine Zonenregel hinzufügen möchten, müssen Sie eine Abfrage über den Bildschirm „Assets > Geräte“ erstellen und speichern. Die Liste der Geräte in den Ergebnissen der gespeicherten Abfrage enthält alle Geräte, die der Zone automatisch hinzugefügt werden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Zonen**.
2. Klicken Sie auf **Neue Zone hinzufügen**.
3. Geben Sie in das Feld **Zonenname** einen Namen für die Zone ein.
4. Klicken Sie in der Dropdown-Liste **Richtlinie** auf eine Geräterichtlinie, die mit der Zone verknüpft werden soll.
5. Klicken Sie im Feld **Wert** auf die entsprechende Prioritätsstufe für die Zone. Diese Einstellung hat keine Auswirkungen auf die Verwaltung von Zonen oder Geräten.
6. Klicken Sie auf **Speichern**.
7. Klicken Sie in der Zonenliste auf den Namen der von Ihnen erstellten Zone.
8. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Fügen Sie eine Zonenregel hinzu, um Geräte automatisch hinzuzufügen.	Sie benötigen eine gespeicherte Abfrage, um eine Zonenregel hinzufügen zu können. **a.** Klicken Sie auf **Regel erstellen**. **b.** Wählen Sie eine gespeicherte Abfrage aus. Die Suchparameter werden angezeigt. **c.** Wenn Sie die mit der Zone verknüpfte Geräterichtlinie automatisch anwenden möchten, wählen Sie **Zonenrichtlinie auf Geräte anzuwenden, die der Zone hinzugefügt werden**. **d.** Wenn Sie Geräte, die nicht den Kriterien der Zonenregel entsprechen, automatisch aus der Zone entfernen möchten, wählen Sie **Geräte automatisch aus dieser Zone entfernen**. Dies betrifft nur Geräte, die den Zonenregeln folgen. **e.** Klicken Sie auf **Speichern**.
Fügen Sie der Zone manuell Geräte hinzu.	Wenn Sie ein Gerät manuell zu einer Zone hinzufügen, ignoriert das Gerät standardmäßig die Zonenregeln. Ein Gerät, das die Zonenregeln ignoriert, verbleibt in der Zone, auch wenn es nicht den Zonenregelkriterien entspricht. **a.** Klicken Sie auf der Registerkarte **Geräte** auf **Gerät zu Zone hinzufügen**. **b.** Wählen Sie die Geräte aus, die Sie hinzufügen möchten. Sie können Filter anwenden, um Geräte zu finden. **c.** Wenn Sie die Zonengerätrichtlinie auf diese Geräte anwenden möchten, aktivieren Sie das Kontrollkästchen **Zonenrichtlinie auf ausgewählte Geräte anwenden**. **d.** Klicken Sie auf **Speichern**.
Wenden Sie die Geräterichtlinie für Zonen auf alle Benutzer in der Zone an.	Diese Aktion ersetzt alle Geräterichtlinien, die Geräten derzeit zugewiesen sind, durch die Geräterichtlinie, die derzeit der Zone zugewiesen ist. **a.** Aktivieren Sie das Kontrollkästchen **Auf alle Geräte in dieser Zone anwenden**. **b.** Klicken Sie auf **Speichern**.
Stellen Sie ein Gerät so ein, dass es eine Zonenregel befolgt oder ignoriert.	In der Geräteliste einer Zone können Geräte, die dieser Zonenregel folgen, in der Spalte „Zonenregel“ identifiziert werden. Geräte, die den Zonenregeln folgen, werden automatisch aus der Zone gelöscht. Geräte, die die Zonenregeln ignorieren, verbleiben in der Zone (sofern Sie sie nicht manuell entfernen). **a.** Wählen Sie auf der Registerkarte **Geräte** mindestens ein Gerät aus. **b.** Klicken Sie auf **Zonenregel folgen** oder auf **Zonenregel ignorieren**. **c.** Klicken Sie auf **Ja**.

Aufgabe	Schritte
Kopieren Sie Geräte in eine andere Zone.	**a.** Wählen Sie auf der Registerkarte **Geräte** mindestens ein Gerät aus. **b.** Klicken Sie auf **Gerät kopieren**. **c.** Wählen Sie mindestens eine Zone aus. **d.** Klicken Sie auf **Speichern**.
Geräte aus einer Zone entfernen	**a.** Wählen Sie auf der Registerkarte **Geräte** mindestens ein Gerät aus. **b.** Klicken Sie auf **Gerät aus Zone entfernen**. **c.** Klicken Sie auf **Ja**.

Einrichten von CylancePROTECT Desktop

Schritt	Aktion
1	Lesen Sie die CylancePROTECT Desktop-Anforderungen.
2	Erstellen und konfigurieren Sie eine Geräterichtlinie. • Neue Mandanten umfassen vorkonfigurierte Zonen und Geräterichtlinien, mit deren Hilfe Sie Ihre Umgebung auf die gewünschte Sicherheitseinstellung abstimmen können. • Lesen Sie die Empfehlungen zum Erstellen und Testen von Geräterichtlinien. • Überprüfen Sie die Empfehlungen für die Zonenverwaltung.
3	Installieren Sie den CylancePROTECT Desktop-Agenten auf Geräten. • Installieren des CylancePROTECT Desktop-Agenten für Windows • Installieren des CylancePROTECT Desktop-Agenten für macOS • Installieren des CylancePROTECT Desktop-Agenten für Linux
4	Verwalten von Updates für die CylancePROTECT Desktop- und CylanceOPTICS-Agenten.

Testen Ihrer CylancePROTECT Desktop-Bereitstellung

Bevor Sie den CylancePROTECT Desktop-Agent auf Ihren Geräten bereitstellen, sollten Sie testen, wie er sich mit anderen Anwendungen in einer Testumgebung verhält, damit Sie sicherstellen können, dass die in Ihrem Unternehmen verwendeten Anwendungen wie erwartet ausgeführt werden können und funktionieren. Wenn Sie z. B. feststellen, dass der Agent einige Anwendungen blockiert und diese nicht ordnungsgemäß ausgeführt werden, können Sie Ausnahmen konfigurieren.

Wenn Sie einen neuen Cylance Endpoint Security-Mandanten erstellen oder einen Mandanten auf den empfohlenen Standardstatus zurücksetzen, bietet BlackBerry vorkonfigurierte Zonen und vorkonfigurierte Geräterichtlinien, mit deren Hilfe Sie Ihre Umgebung an die gewünschte Sicherheitseinstellung anpassen können. Weitere Informationen finden Sie unter Konfigurieren eines neuen Cylance Endpoint Security-Mandanten.

Wenn Sie den Agenten testen möchten, installieren Sie ihn auf Testsystemen mit Anwendungen, die in Ihrem Unternehmen verwendet werden, um sicherzustellen, dass die Praxisumgebung genau abgebildet wird.

Zum Testen des Agenten führen Sie die folgenden Schritte aus:

1. Erstellen von Testrichtlinien.
2. Erstellen von Testzonen.

Geräterichtlinien enthalten die Einstellungen für den Agenten und legen fest, was zu tun ist, wenn er auf eine Bedrohung stößt. Mithilfe von Zonen können Sie Ihre Systeme nach geografischem Standort, Geschäftseinheit, Betriebssystem oder anderen Gruppeneigenschaften gruppieren. Mithilfe von Zonenregeln können Sie Systeme basierend auf den von Ihnen festgelegten Kriterien (z. B. Betriebssystem, IP-Adressbereich und andere Kriterien) automatisch einer Zone zuweisen. Sie sollten Richtlinien und Zonen testen, um sich mit diesen Funktionen vertraut zu machen und besser planen zu können, wie diese Funktionen in Ihrem Unternehmen verwendet werden sollen.

Erstellen einer CylancePROTECT Desktop-Testrichtlinie

Sie sollten CylancePROTECT Desktop-Richtlinienfunktionen phasenweise implementieren, um sicherzustellen, dass weder die Leistung noch die Vorgänge beeinträchtigt werden. Standardmäßig sind Richtlinienfunktionen beim Erstellen einer Geräterichtlinie nicht aktiviert und müssen daher manuell aktiviert werden. Wenn Sie die Arten von Bedrohungen kennen, die in Ihrer Umgebung protokolliert werden, und wissen, wie sich der CylancePROTECT Desktop-Agent verhält, können Sie nach und nach weitere Richtlinienfunktionen aktivieren.

Es wird empfohlen, Geräterichtlinien auf Geräten zu testen, die die in Ihrem Unternehmen verwendeten Anwendungen enthalten. Es ist wichtig, dass die Geräte, die Sie zum Testen von Geräterichtlinien verwenden, die Geräte in Ihrer Produktionsumgebung möglichst genau widerspiegeln (nicht nur auf einer „sauberen" Maschine testen), um sicherzustellen, dass Anwendungen ordnungsgemäß ausgeführt werden können, wenn Richtlinien durch den CylancePROTECT Desktop-Agenten durchgesetzt werden. Sie können beispielsweise einen Teil der Geräte in Ihrer Produktionsumgebung auswählen, die alle Anwendungen (proprietär und benutzerdefiniert) enthalten, die Benutzer für ihre täglichen Aktivitäten benötigen.

Der Agent verwendet nur die Ausführungssteuerung und Prozessüberwachung, um laufende Prozesse zu analysieren. Dies umfasst alle Dateien, die beim Start ausgeführt werden, auf automatische Ausführung eingestellt sind oder manuell vom Benutzer ausgeführt werden. Der Agent sendet nur Warnungen an die Verwaltungskonsole. Standardmäßig werden keine Dateien blockiert oder unter Quarantäne gestellt.

1. Klicken Sie in der Verwaltungskonsole auf **Richtlinien > Geräterichtlinie > Neue Richtlinie hinzufügen**.
2. Geben Sie im Feld **Richtlinienname** einen Namen für die Testrichtlinie ein.
3. Aktivieren Sie **Automatisches Hochladen**, um verdächtige Dateien zu analysieren und zur weiteren Analyse an die CylancePROTECT-Cloud-Dienste zu senden.
   a) Wählen Sie auf der Registerkarte **Dateiaktionen** im Abschnitt **Automatisches Hochladen** alle verfügbaren Dateitypen aus.
   b) Klicken Sie auf **Erstellen**, um die erste Testrichtlinie zu erstellen.
   c) Weisen Sie die anfängliche Testrichtlinie CylancePROTECT Desktop-Endpunkten zu, die Sie für Tests verwenden.
   d) Lassen Sie diese Testrichtlinie einen Tag lang auf den zugewiesenen Geräten laufen, um Anwendungen und Prozesse, die normalerweise auf dem Gerät verwendet werden, auszuführen und zu analysieren. Sie sollten zudem erforderliche Anwendungen berücksichtigen, die regelmäßig auf einem Gerät ausgeführt werden (z. B. einmal pro Woche), und die außerhalb dieses Testlaufs überwacht werden müssen.
   e) Navigieren Sie beim Testen der Richtlinie in der Verwaltungskonsole zum Bildschirm **Schutz > Bedrohungen**, um eine Liste der Anwendungen und Prozesse anzuzeigen, die CylancePROTECT als Bedrohung betrachtet (anormal oder unsicher), und identifizieren Sie die Anwendungen, die auf dem Endpunkt ausgeführt werden dürfen. Sie können auf eine Bedrohung klicken, um weitere Informationen dazu anzuzeigen, und die schädliche Datei herunterladen, um eine eigene Bedrohungsanalyse durchzuführen. Die schädliche Datei wird nicht verändert, aber mit dem SHA256-Hash ohne Dateierweiterung umbenannt, um eine versehentliche Ausbreitung zu verhindern. Wenn Sie den Dateinamen so ändern, dass er die ursprüngliche Dateierweiterung enthält, wird die schädliche Datei möglicherweise ausgeführt. Es werden keine personenbezogenen Daten an die Konsole oder an andere Mandanten bzw. Unternehmen weitergegeben.
   f) Navigieren Sie zu **Richtlinien > Geräterichtlinie** und bearbeiten Sie die Geräterichtlinie, damit bestimmte Anwendungen und Prozesse auf Endpunkten ausgeführt werden können, denen diese Richtlinie zugewiesen ist. Auf der Registerkarte **Dateiaktionen** können Sie Dateien zum Abschnitt **Richtlinie „Sichere Liste"** hinzufügen.

      Sie können auch Dateien auf bestimmten Geräten oder auf allen Geräten in Ihrem Unternehmen unter Quarantäne stellen oder ignorieren. Weitere Informationen finden Sie unter Verwalten von sicheren und unsicheren Listen für CylancePROTECT Desktop.

4. Bearbeiten Sie die Geräterichtlinie, damit die Scans zur Erkennung von Bedrohungen im Hintergrund ausführbare Dateien auf der Festplatte analysieren können, bei denen es sich möglicherweise um inaktive Bedrohungen handelt.
   a) Aktivieren Sie auf der Registerkarte **Schutzeinstellungen** die Einstellung **Bedrohungserkennung im Hintergrund**, und wählen Sie die Option **Einmal ausführen** aus. Auch wenn regelmäßige Scans aufgrund der Vorhersagefähigkeit der Lösung nicht erforderlich sind, können Sie die Option **Wiederholt ausführen** auswählen, um sie beispielsweise für Compliance-Zwecke zu aktivieren.
   b) Aktivieren Sie die Einstellung **Auf neue Dateien überwachen**. Diese Einstellung kann jedoch die Leistung des Geräts beeinträchtigen. Das Hinzufügen von Ordnerausschlüssen kann dazu beitragen, die Leistungsbeeinträchtigung zu verringern.
   c) Um bestimmte Ordner von der Bedrohungserkennung im Hintergrund auszuschließen, wählen Sie **Bestimmte Ordner ausschließen (einschließlich Unterordner)** aus, und geben Sie die auszuschließenden Ordner an. Um die Ausführung von Dateien in den angegebenen Ordnern zuzulassen, wählen Sie **Ausführung zulassen** aus. Weitere Informationen zu diesen Feldern finden Sie unter Schutzeinstellungen.
   d) Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.
   e) Testen Sie die Richtlinie erneut, und stellen Sie sicher, dass alle Anwendungen, die Benutzer verwenden müssen, ausgeführt werden dürfen. Der Bedrohungsscan im Hintergrund kann bis zu einer Woche dauern, je nachdem, wie stark das System ausgelastet ist und wie viele Dateien analysiert werden müssen. Stellen Sie bei Bedarf sicher, dass Sie Dateien zur Richtlinie „Sichere Liste“ oder zur globalen sicheren Liste hinzufügen oder für einzelne Geräte ignorieren. Sie können in den Schutzeinstellungen auch den Ordner ausschließen, der die Datei enthält.
5. Bearbeiten Sie die Geräterichtlinie, um unsichere Prozesse zu beenden, die auf dem System ausgeführt werden. Wenn beispielsweise eine Bedrohung in einer ausführbaren Datei (.exe oder .msi) erkannt wird und diese als unsicher gilt, werden mit dieser Einstellung die laufenden Prozesse und deren Unterprozesse beendet.
   a) Aktivieren Sie auf der Registerkarte **Schutzeinstellungen** die Einstellung **Unsichere laufende Prozesse beenden**.
6. Bearbeiten Sie die Richtlinie, um die Einstellungen für die automatische Quarantäne für unsichere und anormale Dateien zu aktivieren.
   a) Aktivieren Sie auf der Registerkarte **Dateiaktionen** unter der Tabellenspalte **Unsicher** die Einstellung **Automatische Quarantäne** neben **Ausführbare Datei**, um unsichere Dateien automatisch in den Quarantäneordner auf dem Gerät zu verschieben. Unsichere Dateien weisen Malware-Merkmale auf und sind wahrscheinlich Malware.
   b) Aktivieren Sie unter **Anormal**die Option **Automatische Quarantäne**, um anormale Dateien automatisch in den Quarantäneordner auf dem Gerät zu verschieben. Anormale Dateien weisen einige Malware-Merkmale auf, aber in geringerem Maße als unsichere Dateien, und sind mit geringerer Wahrscheinlichkeit Malware.
7. Bearbeiten Sie die Richtlinie, um die Speicherschutzeinstellungen zu aktivieren und Speicher-Exploits, Prozessinjektionen und Eskalationen zu verarbeiten.
   a) Aktivieren Sie auf der Registerkarte **Speicheraktionen** der Geräterichtlinie den **Speicherschutz** und stellen Sie den Verletzungstyp auf **Warnung** ein. Wenn der Verletzungstyp auf „Warnung“ eingestellt ist und eine Bedrohung dieses Typs erkannt wird, sendet der Agent Informationen an die Konsole, blockiert oder beendet jedoch keine Prozesse, die im Gerätespeicher ausgeführt werden.
   b) Navigieren Sie beim Testen der Richtlinie zum Bildschirm **Schutz > Speicherschutz** in der Konsole, um eine Liste der Speicherschutzwarnungen für Prozesse anzuzeigen, die eine Gefahr darstellen können.
   c) Wenn Sie festgestellt haben, dass ein Prozess für tägliche Geschäftsaktivitäten sicher ist, können Sie Ausschlüsse für die Prozesse hinzufügen, die ausgeführt werden sollen. Klicken Sie auf der Registerkarte **Speicheraktionen** der Geräterichtlinie auf **Ausschluss hinzufügen** und geben Sie den relativen Pfad zur Datei an.
   d) Nachdem Sie die Ausschlüsse für Prozesse angegeben haben, die ausgeführt werden sollen, legen Sie die Aktion für alle Verletzungstypen auf **Blockieren** fest. Wenn ein Verletzungstyp blockiert wird, sendet der

Agent Informationen an die Konsole und blockiert die Ausführung des schädlichen Prozesses im Speicher. Die Anwendung, die den bösartigen Prozess aufgerufen hat, kann weiterhin ausgeführt werden.

8. Bearbeiten Sie die Richtlinie, um die Einstellungen der Gerätesteuerung zu aktivieren. In diesem Beispiel wird gezeigt, wie der Zugriff auf alle Gerätetypen gesperrt und die Ausnahmen zugelassen werden. Sie können aber auch den vollen Zugriff auf alle Gerätetypen zulassen und stattdessen die Ausnahmen blockieren.
   a) Aktivieren Sie auf der Registerkarte **Gerätesteuerung** der Geräterichtlinie die Richtlinie **Gerätesteuerung**.
   b) Stellen Sie die Zugriffsebene für jeden USB-Gerätetyp auf **Vollzugriff** ein.
   c) Speichern Sie die Richtlinie.
   d) Schließen Sie ein USB-Gerät an das Testgerät an.
   e) Navigieren Sie in der Verwaltungskonsole zu **Schutz > Externe Geräte** und geben Sie die Anbieter-ID, die Produkt-ID und die Seriennummer aller Geräte an, die Sie zulassen möchten. Nicht alle Hersteller verwenden eine eindeutige Seriennummer für ihre Produkte; einige Hersteller verwenden die gleiche Seriennummer für mehrere Produkte.
   f) Klicken Sie auf der Registerkarte **Gerätesteuerung** der Geräterichtlinie im Abschnitt **Ausschlussliste für externen Speicher** auf **Gerät hinzufügen**, um Geräte hinzuzufügen, die Sie zulassen möchten.
   g) Stellen Sie nach Abschluss des Tests die Zugriffsebene für jeden Gerätetyp auf **Blockieren**. Sie können nach Bedarf Ausschlüsse hinzufügen.
9. Bearbeiten Sie die Richtlinie, um die Skriptsteuerungseinstellungen zu aktivieren. Die empfohlene Testdauer beträgt 1 bis 3 Wochen.
   a) Aktivieren Sie auf der Registerkarte **Skriptsteuerung** der Geräterichtlinie die Richtlinie **Skriptsteuerung**.
   b) Stellen Sie die Richtlinie für jeden der Skripttypen auf **Warnung** ein. Je länger die Skriptsteuerung auf Warnung eingestellt ist, desto wahrscheinlicher ist es, dass Sie selten ausgeführte in der Organisation verwendete Skripte finden.

      Hinweis: Die Aktivierung der Skriptsteuerungseinstellung kann zu einer hohen Anzahl von Ereignissen führen, wenn Skripte zur Verwaltung von Active Directory-Einstellungen verwendet werden.
   c) Navigieren Sie zu **Schutz > Skriptsteuerung** und identifizieren Sie die Skripte, die auf Geräten ausgeführt wurden, die Sie zulassen möchten.
   d) Klicken Sie auf der Registerkarte **Skriptsteuerung** der Geräterichtlinie im Abschnitt **Dateien, Skripte oder Prozesse ausschließen** auf **Ausschluss hinzufügen** und geben Sie einen relativen Prozesspfad der Skripte an, die Sie zulassen möchten (z. B. `\Cases\AllowedScripts`).
   e) Nachdem Sie die Ausschlüsse für Skripte hinzugefügt haben, die Sie ausführen lassen möchten, können Sie die Richtlinie für jeden der Skripttypen auf **Blockieren** setzen.

Ausschlüsse und wann sie verwendet werden sollten

Die folgende Tabelle enthält eine Beschreibung der einzelnen Ausschlusstypen und allgemeine Hinweise dazu, wann und wie sie angemessen verwendet werden.

Ausschlusstyp	Beschreibung und Beispiel
Richtlinie „Sichere Liste“ (Dateiaktionen)	Die Richtlinie „Sichere Liste“ wird auf der Registerkarte **Dateiaktionen** in einer Geräterichtlinie angegeben. Wenn eine Geräterichtlinie einem Gerät zugewiesen ist, kann das Gerät Dateien ausführen, die in der sicheren Liste angegeben sind. Die Richtlinie „Sichere Liste“ wird auf Richtlinienebene für bestimmte Geräte angewendet, während die globale Sicherheitsliste oder Quarantäneliste auf globaler Ebene für alle Geräte angewendet wird. Die Richtlinie „Sichere Liste“ hat Vorrang vor der globalen Quarantäneliste. Eine Datei, die der Richtlinie „Sichere Liste“ hinzugefügt wird, kann auf jedem Gerät ausgeführt werden, dem die Richtlinie zugewiesen ist, selbst wenn sich diese Datei in der globalen Quarantäneliste befindet, wodurch die Ausführung von Dateien auf allen Geräten verhindert wird. Beispiel: Sie verwenden häufig Berechtigungseskalationstools wie PSEXEC für Ihre täglichen Aufgaben. Sie möchten jedoch nicht, dass alle Benutzer diese Möglichkeit haben, und Sie möchten verhindern, dass sie solche Tools verwenden, ohne dass Sie dadurch in der Ausführung Ihrer täglichen Aufgaben beeinträchtigt werden. Zu diesem Zweck können Sie PSEXEC zur globalen Quarantäneliste hinzufügen und denselben Datei-Hash in die Richtlinie „Sichere Liste“ aufnehmen. Damit stellen Sie sicher, dass nur Sie und weitere autorisierte Benutzer dieser speziellen Geräterichtlinie zugewiesen sind, in der Sie PSEXEC zur sicheren Liste hinzugefügt haben. Ergebnis: Für alle Benutzer, die der Geräterichtlinie nicht zugewiesen sind, wird PSEXEC unter Quarantäne gestellt, aber Benutzer, die der Geräterichtlinie zugewiesen sind, können PSEXEC verwenden.

Ausschlusstyp	Beschreibung und Beispiel
Ausführbare Dateien oder Makro-Dateien ausschließen (Speicherschutz)	Ausschlüsse für die Richtlinie zum Speicherschutz werden auf der Registerkarte **Speicheraktionen** in einer Geräterichtlinie angegeben, wenn der **Speicherschutz** aktiviert ist. Wenn Sie Ausschlüsse für den Speicherschutz angeben, ignoriert der Agent Verletzungen bestimmter Typen aus jeder spezifischen Anwendung. Mit anderen Worten: Sie vermeiden das Blockieren oder Beenden einer Anwendung, wenn eine Aktion ausgeführt wird, die eine Verletzung eines bestimmten Typs verursacht. Wenn der Speicherschutz aktiviert ist, überwacht der Agent Anwendungsprozesse auf bestimmte Aktionen, die er ausführt. Wenn ein Prozess eine bestimmte Aktion ausführt, die der Agent überwacht, z. B. LSASS-Lesen, reagiert der Agent je nach Geräterichtlinie auf diese Aktion. Manchmal treten falsch positive Ergebnisse auf und der Speicherschutz blockiert eine Aktion, die von einer Anwendung ausgeführt werden soll, oder beendet die Anwendung vollständig. In dieser Situation können Sie Ausschlüsse für den Speicherschutz festlegen, sodass bestimmte Anwendungen von bestimmten Verletzungstypen ausgenommen sind und wie vorgesehen ausgeführt werden können, ohne blockiert oder beendet zu werden. Beispiel: Ihr Unternehmen blockiert standardmäßig alle Speicherschutzverletzungen von allen Anwendungen. Sie verwenden Test.exe häufig und wissen, dass es nur berechtigte Gründe für LSASS-Leseverletzungen gibt. Sie können einen Ausschluss hinzufügen, damit der Agent nur LSASS-Leseverletzungen aus Test.exe ignoriert. Der Agent blockiert weiterhin Test.exe, wenn eine andere Verletzung auftritt. Speicherschutzausschlüsse verwenden relative Pfade (Laufwerksbuchstaben sind nicht erforderlich) und können bis zur ausführbaren Ebene angegeben werden. Beispiel: • `\Application\Subfolder\Test.exe` • `\Subfolder\executable` **Hinweis:** Es wird nicht empfohlen, einen Ausschluss auf ausführbarer Ebene ohne relativen Pfad anzugeben. Wenn beispielsweise ein Ausschluss für `\Test.exe` festgelegt ist, kann eine schädliche Datei mit demselben Namen aus einem beliebigen Ordner auf dem Gerät ausgeführt werden.

Ausschlusstyp	Beschreibung und Beispiel
Bestimmte Ordner ausschließen (Schutzeinstellungen)	Ausschlüsse für die Bedrohungserkennung im Hintergrund werden auf der Registerkarte **Schutzeinstellungen** in einer Geräterichtlinie angegeben, wenn **Bedrohungserkennung im Hintergrund** aktiviert ist. Dies kann als Verzeichnis-Safelisting bezeichnet werden. Wenn ein Verzeichnis ausgeschlossen wird, ignoriert der Agent während eines Scans alle Dateien in diesem Verzeichnis, einschließlich aller Unterordner. Wenn Sie **Ausführung zulassen** auswählen, ignoriert der Agent alle ausführbaren Dateien, die aus den ausgeschlossenen Verzeichnissen gestartet werden. Beispiel: Ein Anwendungsentwickler in Ihrem Unternehmen verwendet ein Verzeichnis (z. B. `C:\DevFiles\Temp`), um temporäre Dateien zu speichern, die während der Kompilierung generiert werden. Der Agent scannt diese Dateien, stuft sie aufgrund verschiedener Eigenschaften als unsicher ein und stellt sie anschließend unter Quarantäne. Der Entwickler sendet eine Anforderung zur Zulassung des temporären Verzeichnisses. Sie können das Verzeichnis `C:\DevFiles\Temp` hinzufügen, damit die temporären Dateien ignoriert werden und der Entwickler seine Arbeit ausführen kann.
Ordnerausschlüsse (Skriptsteuerung)	Ausschlüsse für die Skriptsteuerungsrichtlinie werden auf der Registerkarte **Skriptsteuerung** in einer Geräterichtlinie angegeben, wenn die **Skriptsteuerung** aktiviert ist. Sie können Ausschlüsse hinzufügen, wenn Sie zulassen möchten, dass Skripte in einem angegebenen Verzeichnis ausgeführt werden. Geben Sie beim Hinzufügen von Ausschlüssen für die Skriptsteuerung die relativen Pfade an. Unterordner sind ebenfalls vom Ausschluss betroffen. Beispiel: Ein IT-Administrator versucht, ein Skript auszuführen, das sich im Verzeichnis `C:\Scripts\Subfolder\Test` befindet. Das Skript wird jedes Mal von der Skriptsteuerung blockiert, wenn der IT-Administrator versucht, das Skript auszuführen. Damit das Skript ausgeführt werden kann, können Sie einen der folgenden relativen Pfade als Ausschluss zur Richtlinie für die Skriptsteuerung hinzufügen: • `\Scripts\Subfolder\Test` • `\Subfolder\Test\` • `\Scripts\Subfolder\` • `\Scripts\` • `\Subfolder\` • `\Test\`

Verwenden von IT-Richtlinien für die Verwaltung von CylancePROTECT Desktop-Geräten

Geräterichtlinien definieren, wie der CylancePROTECT Desktop-Agent mit verdächtigen Dateien und erkannter Malware umgeht. Die Ausführungssteuerung ist standardmäßig in allen Geräterichtlinien aktiviert, sodass der

Agent die Verwaltungskonsole benachrichtigen kann, wenn versucht wird, unsichere oder anormale Dateien auszuführen. Nach der Installation des Agenten analysiert der Agent auch alle ausgeführten Prozesse und Module auf bereits aktive Bedrohungen. Jedes Gerät ist einer Geräterichtlinie zugewiesen. Die Standardrichtlinie wird zugewiesen, wenn einem Gerät keine andere Richtlinie zugewiesen ist.

Sie können die Geräterichtlinien wie folgt verwenden:

- Aktivieren Sie die automatische Quarantäne für unsichere oder anormale Dateien, damit sie nicht auf dem Gerät ausgeführt werden können. Sie können die Richtlinie „Sichere Liste“ für Dateien definieren, die Ihr Unternehmen als sicher erachtet, selbst wenn die Dateien eine Bedrohungsbewertung aufweisen, die darauf hinweist, dass sie unsicher oder anormal sind.
- Aktivieren Sie Speicherschutzeinstellungen, um Speicher-Exploits, einschließlich Prozessinjektionen und Eskalationen, zu verhindern. Sie können Ausschlüsse für ausführbare Dateien und Makrodateien hinzufügen, die Sie ausführen lassen möchten.
- Aktivieren Sie Schutzeinstellungen, um z. B. das Herunterfahren des CylancePROTECT-Dienstes zu verhindern, unsichere Prozesse und laufende Unterprozesse zu beenden, und mithilfe der Bedrohungserkennung im Hintergrund Dateien zu analysieren, bei denen es sich möglicherweise um inaktive Bedrohungen handelt.
- Aktivieren und konfigurieren Sie CylanceOPTICS-Einstellungen.
- Aktivieren Sie die Anwendungssteuerungsfunktion, um die Ausführung neuer Anwendungen einzuschränken, und blockieren Sie alle Updates oder Änderungen an bereits installierten Anwendungen.
- Aktivieren Sie Agent-Einstellungen, wie das automatische Hochladen von Protokolldateien oder Desktop-Benachrichtigungen.
- Aktivieren Sie die Einstellungen für die Skriptsteuerung, um die Ausführung schädlicher Skripte auf Geräten zu verhindern. Sie können Ausschlüsse hinzufügen, um die Ausführung bestimmter Skripte zuzulassen, wenn Ihre Organisation diese als sicher erachtet.
- Aktivieren Sie die Einstellungen der Gerätesteuerung, um zu verhindern, dass USB-Massenspeichergeräte (wie USB-Flash-Laufwerke, externe Festplatten und Smartphones) mit einem Gerät verbunden werden.

Erstellen und Verwalten einer Geräterichtlinie

Mithilfe von Geräterichtlinien können Sie die Funktionen der CylancePROTECT Desktop- und CylanceOPTICS-Agenten steuern. Sie können verschiedene Geräterichtlinien erstellen, um die Anforderungen verschiedener Gruppen innerhalb ihrer Organisation zu erfüllen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Geräterichtlinie**.
2. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Hinzufügen einer neuen Geräterichtlinie	**a.** Klicken Sie auf **Neue Richtlinie hinzufügen**. **b.** Geben Sie im Feld **Richtlinienname** einen Namen für die Geräterichtlinie ein. **c.** Geräterichtlinieneinstellungen auswählen **d.** Klicken Sie auf **Erstellen**.
Bearbeiten einer Geräterichtlinie	**a.** Klicken Sie auf den Namen der Geräterichtlinie, die Sie bearbeiten möchten. **b.** Aktualisieren Sie die Einstellungen für die Geräterichtlinie. **c.** Klicken Sie auf **Speichern**.

Aufgabe	Schritte
Kopieren einer Geräterichtlinie	**a.** Klicken Sie auf den Namen der Geräterichtlinie, die Sie kopieren möchten. **b.** Geben Sie im Feld **Richtlinienname** den Namen der Geräterichtlinie ein. **c.** Aktualisieren Sie, falls erforderlich, die Geräterichtlinien-Einstellungen. **d.** Klicken Sie auf **Speichern unter**.
Geräterichtlinien-Einstellungen	Weitere Informationen zu den Einstellungen für Geräterichtlinien finden Sie in den folgenden Abschnitten: • Dateiaktionen • Speicheraktionen • Schutzeinstellungen • Anwendungssteuerung • Agent-Einstellungen • Skriptsteuerung • Gerätesteuerung • CylanceOPTICS-Einstellungen
Geräten in einer Zone eine Geräterichtlinie automatisch zuweisen	Sie können eine Geräterichtlinie festlegen, wenn Sie eine Zone konfigurieren, sodass Geräte, die dieser Zone hinzugefügt werden, automatisch einer Richtlinie zugewiesen werden. Weitere Informationen finden Sie unter Hinzufügen und Konfigurieren von Zonen.
Einem Gerät manuell eine Geräterichtlinie zuweisen	**a.** Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Assets > Geräte**. **b.** Wählen Sie die Geräte aus, denen Sie eine Geräterichtlinie zuweisen möchten. **c.** Klicken Sie auf **Richtlinie zuweisen**. **d.** Wählen Sie die Geräterichtlinie, die Sie zuweisen möchten. **e.** Klicken Sie auf **Speichern**.

Dateiaktionen

Die folgenden Einstellungen finden Sie auf der Registerkarte **Dateiaktionen** in einer Geräterichtlinie. Sie können damit festlegen, wie der CylancePROTECT Desktop-Agent eine Datei behandelt, wenn er eine Bedrohung erkennt und die Datei dadurch als unsicher oder anormal gilt.

Option	Beschreibung

Automatische Quarantäne mit Ausführungssteuerung	Diese Einstellung legt fest, ob unsichere oder anormale Dateien automatisch unter Quarantäne gestellt werden, um deren Ausführung zu verhindern. Wenn Sie anormale Dateien unter Quarantäne stellen möchten, müssen Sie zunächst die Option zur Quarantäne unsicherer Dateien auswählen. Unsichere Dateien enthalten deutlich mehr Malware-Attribute und die Wahrscheinlichkeit, dass es sich um Malware handelt, ist größer als bei anormalen Dateien.
	
	Wenn eine Datei unter Quarantäne gestellt wird, passiert Folgendes:
	• Die Datei wird mit der Dateinamenerweiterung `.quarantine` umbenannt.
	• Die Datei wird von ihrem ursprünglichen Speicherort in eines der folgenden Quarantäneverzeichnisse verschoben:
	  • **Für Windows-Geräte:** `C:\ProgramData\Cylance\Desktop\q`
	  • **Für macOS-Geräte:** `/Library/Application Support/Cylance/Desktop/q`
	  • **Für Linux-Geräte:** `/opt/cylance/desktop/q`
	• Die Zugriffssteuerungsliste (ACL) für die Datei wird geändert, um die Interaktion des Benutzers mit der Datei zu verhindern.
	
	Einige Malware-Programme sind darauf ausgelegt, Dateien in anderen Verzeichnissen zu erstellen und dies so lange zu tun, bis sie erfolgreich sind. Anstatt die Dateien zu entfernen, modifiziert CylancePROTECT Desktop sie so, dass die Malware nicht erneut versucht, sie zu erstellen, und dass sie nicht ausgeführt werden können.

Automatische Löschung für Dateien in Quarantäne aktivieren	Diese Einstellung legt fest, ob Dateien in Quarantäne nach einer bestimmten Anzahl von Tagen automatisch gelöscht werden sollen. Sie können sie beispielsweise so einstellen, dass eine Datei gelöscht wird, nachdem sie 14 Tage lang unter Quarantäne gestellt wurde. Die Anzahl der Tage kann zwischen 14 und 365 liegen. Wenn die Datei gelöscht wird, geschieht Folgendes: • Die Aktion wird zu Prüfzwecken in die Protokolldatei des Agenten aufgenommen. • Die Datei wird aus der Quarantäneliste in der Agent-UI entfernt.
Automatisches Hochladen	Stellen Sie sicher, dass die Option **Automatisches Hochladen** für alle verfügbaren Dateitypen aktiviert ist. Wenn der Agent eine Datei findet, die von den CylancePROTECT Cloud-Diensten noch nie analysiert wurde, fordert er den Upload der Datei zur Analyse an. CylancePROTECT Desktop lädt nur unbekannte Dateien hoch und analysiert sie, wie z. B. Dateien im Format „Portable Executable“ (PE), „Executable and Linkable Format“ (ELF) und „Mach Object File Format“ (Mach-O). Wenn dieselbe unbekannte Datei auf mehreren Geräten im Unternehmen erkannt wird, lädt CylancePROTECT Desktop nur eine Datei von einem einzelnen Gerät zur Analyse hoch, nicht eine Datei pro Gerät.
Liste sicherer Richtlinien	Fügen Sie Dateien, die Sie als sicher einstufen, zur Richtlinie „Sichere Liste“ hinzu, damit sie ausgeführt werden können. Die Richtlinie „Sichere Liste“ hat Vorrang vor der globalen Quarantäneliste oder der globalen Sicherheitsliste. Eine Datei, die der Richtlinie „Sichere Liste“ hinzugefügt wird, kann z. B. auf einem Gerät ausgeführt werden, dem die Richtlinie zugewiesen ist, selbst wenn sich diese Datei in der globalen Quarantäneliste befindet, wodurch die Ausführung von Dateien auf allen Geräten verhindert wird.

Hinzufügen von Dateien zur Richtlinie „Sichere Liste“

Sie können Dateien zur Richtlinie „Sichere Liste“ hinzufügen, sodass alle Agenten in dieser Richtlinie sie als sicher erachten, selbst wenn die Bedrohungsbewertung darauf hinweist, dass sie unsicher oder anormal sind. Weitere Informationen zur Richtlinie „Sichere Liste“ finden Sie unter Ausschlüsse und wann sie verwendet werden sollten.

Bevor Sie beginnen: Ermitteln Sie den SHA256-Wert der Datei, die Sie ausschließen möchten, über den Bildschirm **Schutz > Bedrohungen**.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Geräterichtlinie**.
2. Klicken Sie auf den Namen einer Richtlinie, um sie zu bearbeiten, oder klicken Sie auf **Neue Richtlinie hinzufügen**.
3. Klicken Sie auf der Registerkarte **Dateiaktionen** im Abschnitt **Richtlinie „Sichere Liste“** auf **Datei hinzufügen**.
4. Geben Sie den SHA256-Wert für die Datei an, die Sie ausschließen möchten.
5. Geben Sie optional den MD5-Wert und den Dateinamen an.
6. Wählen Sie eine Kategorie aus und geben Sie den Grund für diesen Ausschluss ein.
7. Klicken Sie auf **Senden**.

Speicheraktionen

Die folgenden Einstellungen finden Sie auf der Registerkarte **Speicheraktionen** in einer Geräterichtlinie. Sie können den **Speicherschutz** aktivieren und festlegen, wie der CylancePROTECT Desktop-Agent Speicher-Exploits verarbeitet, einschließlich Prozessinjektionen und Eskalationen. Sie können auch ausführbare Dateien zu einer Ausschlussliste hinzufügen, sodass diese Dateien ausgeführt werden können, wenn diese Richtlinie angewendet wird.

Option	Beschreibung
Speicherschutz	Diese Einstellung gibt an, ob in der Richtlinie Einstellungen zum Speicherschutz aktiviert werden sollen. Wenn diese Option aktiviert ist, erkennt der Agent verschiedene Arten von Prozessaufrufen, die eine Bedrohung darstellen können, und verarbeitet jeden Typ entsprechend der von Ihnen gewählten Einstellung. • **Ignorieren**: Der Agent ergreift keine Maßnahmen. • **Warnung**: Der Agent protokolliert den Verstoß und meldet den Vorfall an die Verwaltungskonsole. • **Blockieren**: Der Agent protokolliert den Verstoß, meldet den Vorfall an die Verwaltungskonsole und blockiert den Prozessaufruf. Die Anwendung, die den Aufruf getätigt hat, kann weiterhin ausgeführt werden. • **Beenden**: Der Agent protokolliert den Verstoß, meldet den Vorfall an die Verwaltungskonsole, blockiert den Prozessaufruf und beendet die Anwendung, die den Aufruf getätigt hat.

Option	Beschreibung
Ausführbare Dateien ausschließen	Diese Einstellung gibt den relativen Pfad der Dateien an, die ignoriert werden sollen. Wenn Dateien zu dieser Ausschlussliste hinzugefügt werden, können sie auf Geräten ausgeführt oder installiert werden, denen diese Richtlinie zugewiesen ist. Sie geben den relativen Pfad der Datei und die Verletzungstypen an, die ignoriert werden sollen. Auf Windows-Geräten können Sie auch den absoluten Dateipfad angeben. Verwenden Sie gekürzte relative Pfade mit Vorsicht, da andere ausführbare Dateien mit demselben relativen Pfad ausgeschlossen werden könnten. Nach Anwendung des Ausschlusses müssen alle Instanzen dieses Prozesses beendet werden, damit der Treiber nicht mehr in den Prozess eingreift. **Beispiele für Windows** • Relativer Pfad: `\Application\Subfolder\application.exe` • Absoluter Pfad: `C:\Application\Subfolder\application.exe` **Beispiele für Linux** • Relativer Pfad: `/opt/application/executable` • Relativer Pfad für Dynamic Library-Dateien: `/executable.dylib` **Beispiele für macOS** • Relativer Pfad ohne Leerzeichen: `/Applications/SampleApplication.app/Contents/MacOS/executable` • Relativer Pfad mit Leerzeichen: `/Applications/Sample Application.app/Contents/MacOS/executable` • Relativer Pfad für Dynamic Library-Dateien: `/executable.dylib` Sie können auch Platzhalter für Speicherschutzausschlüsse verwenden. Weitere Informationen finden Sie unter Platzhalter in Ausschlüssen zum Speicherschutz. **Hinweis:** Wenn Sie einen Ausschluss speichern, ohne mindestens einen zu ignorierenden Verletzungstyp hinzuzufügen, wird der Ausschluss sowohl auf Speicherschutz- als auch auf Skriptsteuerungsereignisse angewendet. Wenn mindestens ein zu ignorierender Verletzungstyp hinzugefügt wird, wird der Ausschluss nur auf den Speicherschutz angewendet.

Option	Beschreibung
Bestimmte Verletzungstypen ignorieren	Wenn Sie einen Ausschluss hinzufügen, aktivieren Sie dieses Kontrollkästchen, um eine Dateiverletzung basierend auf einem oder allen der folgenden Elemente zu ignorieren: • Verletzungstypkategorien (z. B. Exploitation, Prozessinjektion, Eskalation) • Individuelle Verletzungstypen unter jeder Kategorie (z. B. Stack Pivot, Remote-Speicherzuweisung, Nullzuteilung usw.) Wenn Sie einer Speicherschutz-Geräterichtlinie Ausschlüsse hinzufügen und die Richtlinie nur für Verletzungen des Speicherschutzes und nicht für Verletzungen der Skriptsteuerung gelten soll, geben Sie mindestens einen Verletzungstyp an, den Sie ignorieren möchten. Wenn Sie keine zu ignorierenden Verletzungstypen auswählen, wird eine Warnmeldung angezeigt, und der Ausschluss gilt sowohl für die Speicherschutz- als auch für die Skriptsteuerungsrichtlinien. Für vorhandene Speicherschutzrichtlinien gilt: • Wenn die Ausschlusseinstellung **Bestimmte Verletzungstypen ignorieren** bereits aktiviert ist, die Skriptsteuerungs-Richtlinie jedoch nicht aktiviert ist, ist keine Aktion erforderlich. • Wenn die Ausschlusseinstellung **Bestimmte Verletzungstypen ignorieren** deaktiviert ist und Sie sicherstellen möchten, dass die Richtlinie nur auf Verletzungen des Speicherschutzes (und nicht auf die Skriptsteuerung) angewendet wird, müssen Sie sie aktivieren und mindestens einen zu ignorierenden Verletzungstyp angeben. Wenn Sie eine vorhandene Richtlinie bearbeiten und einen Ausschluss hinzufügen, wird das Kontrollkästchen „Bestimmte Verletzungstypen ignorieren“ erst angezeigt, wenn Sie den Verletzungstyp ändern (z. B. von „Sperren“ auf „Beenden“ oder „Warnung“). Für jede Datei mit bestimmten Verletzungsarten, die ignoriert werden, können Sie detaillierte Informationen anzeigen und die Einstellungen bearbeiten oder löschen.
Als DLL-Ausschluss behandeln	Wählen Sie diese Einstellung, wenn Sie Ausnahmen für DLLs von Drittanbietern hinzufügen möchten. Wenn Sie beispielsweise Sicherheitsprodukte von Drittanbietern zusätzlich zu CylancePROTECT Desktop für Windows ausführen, können Sie einen Ausschluss für die entsprechenden .dll-Dateien hinzufügen, damit CylancePROTECT bestimmte Verstöße für diese Produkte ignoriert. Diese Funktion unterstützt nur die Verletzungstypen „Schädliche Payload“ und „System-DLL-Überschreibung“. Die folgenden Regeln gelten, wenn Sie einen DLL-Ausschluss angeben: • Sie müssen die Option **Als DLL-Ausschluss behandeln** in der Geräterichtlinie auswählen. • Auf dem Gerät muss CylancePROTECT Desktop-Agent Version 3.1.1001 oder höher auf einem Windows-Gerät ausgeführt werden. • Der von Ihnen angegebene Dateipfad muss der vollständige, direkte Pfad zur .dll-Datei sein. Platzhalter sind nicht zulässig. • Die .dll-Datei muss mit einem Zertifikat signiert werden, das auf dem Gerät, auf dem CylancePROTECT Desktop installiert ist, als vertrauenswürdig gilt. Andernfalls wird sie nicht ausgeschlossen. Weitere Informationen zur Unterstützung von DLL-Ausschlüssen finden Sie unter support.blackberry.com in der KB 108909.

Speicherschutz-Verletzungstypen

Exploitation-Verletzungstypen

Verletzungstyp	Beschreibung	Unterstütztes Betriebssystem
Stack Pivot	Der Stack für einen Thread wurde durch einen anderen Stack ersetzt. Im Allgemeinen weist das System nur einen einzelnen Stack für einen Thread zu. Ein Angreifer könnte einen anderen Stack verwenden, um die Ausführung so zu steuern, dass sie nicht von der Datenausführungsverhinderung (DEP, Data Execution Prevention) blockiert wird.	Windows macOS* Linux
Stackschutz	Der Speicherschutz des Thread-Stacks wurde geändert, um die Ausführungsberechtigung zu aktivieren. Der Stapelspeicher sollte nicht ausführbar sein. Denn dies könnte bedeuten, dass ein Angreifer sich darauf vorbereitet, im Stapelspeicher gespeicherten bösartigen Code als Teil eines Exploits auszuführen, ein Versuch, der andernfalls durch die Datenausführungsverhinderung (DEP, Data Execution Prevention) blockiert werden würde.	Windows macOS* Linux
Codeüberschreibung	Code, der sich im Speicher eines Prozesses befindet, wurde mit einer Technik geändert, die auf Versuche hinweisen kann, die Datenausführungsverhinderung (DEP) zu umgehen.	Windows
RAM-Scraping	Ein Prozess versucht, gültige Magnetstreifenspurdaten von einem anderen Prozess zu lesen. In der Regel wird dieser Verstoß mit POS-Systemen (Point of Sale Systems) in Verbindung gebracht.	Windows
Schädliche Payload	Es wurde ein generischer Shellcode und eine Payload im Zusammenhang mit Exploitation erkannt. Diese Art der Speicherschutzverletzung unterstützt DLL-Ausschlüsse.	Windows
Verletzungstypen, die mit Agent 2.1.1580 oder höher verfügbar sind		
System-aufrufüberwachung	Es wurde ein Systemaufruf bei einer Anwendung oder einem Betriebssystem erkannt.	Windows
Direkte Systemaufrufe	Es wurde ein Versuch erkannt, unauffällig bösartigen Code in andere Prozesse zu injizieren. Dieser Verletzungstyp kann nicht blockiert werden.	Windows
System-DLL-Überschreibung	Es wurde ein Versuch erkannt, eine System-DLL zu überschreiben. Diese Art der Speicherschutzverletzung unterstützt DLL-Ausschlüsse.	Windows

Verletzungstyp	Beschreibung	Unterstütztes Betriebssystem
Gefährliches COM-Objekt	Es wurde schädlicher Code erkannt, der auf ein Component Object Model (COM)-Objekt verweist.	Windows
Injection über APC	Ein Prozess, der einen asynchronen Prozeduraufruf (APC) oder einen Start-Remote-Thread verwendet, um `LoadLibrary` oder eine ähnliche Funktion aufzurufen und dadurch beliebigen Code in den Zielprozess zu injizieren, wurde erkannt. Wenn diese Richtlinie auf „Warnung“ gesetzt ist, werden Warnungen sowohl für ungefährliche als auch für schädliche Injektionen für Anwendungen auf Windows-Geräten angezeigt. Die Warnung meldet die Anwendung, die die Injektion erhalten hat, aber Sie müssen die ausführbare Quelle bestimmen, die die Warnung verursacht hat. Informationen zum Sammeln der erforderlichen Daten, mit denen Sie feststellen können, ob eine Injektion gültig oder schädlich ist, finden Sie unter support.blackberry.com in KB 92422. Wenn diese Richtlinie so eingestellt ist, dass die Anwendung blockiert oder beendet wird, verhindert sie, dass gemeldete Anwendungen auf dem Gerät ausgeführt werden, selbst wenn sie unschädlich sind. Dadurch können die alltäglichen Aktivitäten eines Benutzers beeinträchtigt werden.	Windows
Verletzungstypen, die mit Agent 3.0.1000 oder höher verfügbar sind		
Gefährliche VBA-Makros	Ein Makro, das gefährliche Implementierungen enthält, wurde erkannt. Diese Einstellung schützt Geräte mit Agent-Version 2.1.1580 und höher vor schädlichen Makros. Die Ausschlüsse, die in der Speicherschutzrichtlinie angegeben sind, werden unter Agent-Version 3.0 und höher unterstützt. Um Geräte mit Agent-Version 2.1.1578 und früher vor schädlichen Makros zu schützen, aktivieren und konfigurieren Sie die Skriptsteuerungsrichtlinie und die entsprechenden Ausschlüsse.	Windows

* Nur unter macOS Catalina und früheren Versionen unterstützt.

Prozessinjektion-Verletzungstypen

Verletzungstyp	Beschreibung	Unterstütztes Betriebssystem
Remote-Speicherzuweisung	Ein Prozess hat in einem anderen Prozess Speicher zugewiesen. Die meisten Zuweisungen erfolgen nur innerhalb desselben Prozesses. Dies kann auf einen Versuch hindeuten, Code oder Daten in einen anderen Prozess einzuschleusen, um eine schädliche Präsenz auf einem System zu verstärken.	Windows macOS
Remote-Speicherzuordnung	Ein Prozess hat Code oder Daten in einen anderen Prozess eingebracht. Dies kann ein Hinweis darauf sein, dass versucht wird, Code in einem anderen Prozess auszuführen und dadurch eine schädliche Präsenz zu verstärken.	macOS
Remote-Schreiben in Speicher	Ein Prozess hat Speicher in einem anderen Prozess geändert. Dies kann auf einen Versuch hindeuten, Code oder Daten in zuvor zugewiesenem Speicher zu speichern (siehe `OutOfProcessAllocation`). Es ist jedoch möglich, dass ein Angreifer versucht, den vorhandenen Speicher zu überschreiben, um die Ausführung zu einem schädlichen Zweck umzuleiten.	Windows macOS
Remote-PE-Schreibvorgang in Speicher	Ein Prozess hat den Speicher in einem anderen Prozess so geändert, dass er ein ausführbares Image enthält. Im Allgemeinen weist dies darauf hin, dass ein Angreifer versucht, Code auszuführen, ohne diesen zuerst auf den Datenträger zu schreiben.	Windows
Remote-Überschreiben von Code	Ein Prozess hat den ausführbaren Speicher in einem anderen Prozess geändert. Unter normalen Bedingungen wird der ausführbare Speicher nicht geändert, insbesondere nicht durch einen anderen Prozess. Dies weist in der Regel auf einen Versuch hin, die Ausführung in einen anderen Prozess umzuleiten.	Windows
Remote-Aufhebung der Speicherzuordnung	Ein Prozess hat eine ausführbare Windows-Datei aus dem Speicher eines anderen Prozesses entfernt. Dies kann ein Hinweis darauf sein, dass das ausführbare Image durch eine geänderte Kopie ersetzt werden soll, um die Ausführung umzuleiten.	Windows macOS
Remote-Thread-Erstellung	Ein Prozess hat einen neuen Thread in einem anderen Prozess erstellt. Die Threads eines Prozesses werden in der Regel nur von demselben Prozess erstellt. Diese Methode wird in der Regel von einem Angreifer verwendet, um eine schädliche Präsenz zu aktivieren, die in einen anderen Prozess injiziert worden ist.	Windows macOS*
Remote-APC-Planung	Ein Prozess hat die Ausführung des Threads eines anderen Prozesses umgeleitet. Diese Methode wird in der Regel von einem Angreifer verwendet, um eine schädliche Präsenz zu aktivieren, die in einen anderen Prozess injiziert worden ist.	Windows

Verletzungstyp	Beschreibung	Unterstütztes Betriebssystem
DYLD-Injektion	Es wurde eine Umgebungsvariable festgelegt, die dazu führt, dass eine Shared Library in einen gestarteten Prozess eingeschleust wird. Angreifer können Anwendungslisten wie Safari ändern oder Anwendungen durch Bash-Skripte ersetzen, was dazu führt, dass ihre Module automatisch geladen werden, wenn eine Anwendung gestartet wird.	macOS* Linux
Verletzungstypen, die mit Agent 2.1.1580 oder höher verfügbar sind		
Doppelgänger	Ein neuer, bösartiger Prozess wurde von einer Datei gestartet, die noch nicht in das Dateisystem geschrieben wurde. Die Dateischreibtransaktion wird in der Regel nach dem Prozessstart zurückgesetzt (sodass die schädliche Datei nie auf der Festplatte gespeichert wird). Beim Versuch, die Datei auf der Festplatte zu scannen, wird nur die unveränderte ungefährliche Datei gefunden.	Windows
Gefährliche Umgebungsvariable	Es wurde eine Umgebungsvariable erkannt, mit der möglicherweise schädlicher Code verknüpft ist.	Windows

* Nur unter macOS Catalina und früheren Versionen unterstützt.

Escalation-Verletzungstypen

Verletzungstyp	Beschreibung	Unterstütztes Betriebssystem
LSASS-Lesen	Auf den Speicher des Prozesses Windows Local Security Authority wurde in einer Weise zugegriffen, die auf einen Versuch hindeutet, an die Kennwörter der Benutzer zu gelangen.	Windows
Nullzuteilung	Es wurde eine Nullseite zugewiesen. Der Speicherbereich ist in der Regel reserviert, kann aber unter bestimmten Umständen zugewiesen werden. Bei Angriffen kann dies verwendet werden, um eine Berechtigungseskalation einzurichten, indem ein bekannter Null-Dereferenz-Exploit genutzt wird, in der Regel im Kernel.	Windows macOS*
Verletzungstypen, die mit Agent 2.1.1580 oder höher verfügbar sind		
Änderungen der Speicherberechtigun in anderen Prozessen	Ein Verletzungsprozess hat Speicherzugriffsberechtigungen innerhalb eines anderen Prozesses geändert. Dies geschieht in der Regel, um Code in einen anderen Prozess zu injizieren und den Speicher durch Ändern der Speicherzugriffsberechtigungen ausführbar zu machen.	Windows

Verletzungstyp	Beschreibung	Unterstütztes Betriebssystem
Änderungen der Speicherberechtigung in untergeordneten Prozessen	Ein Verletzungsprozess hat einen untergeordneten Prozess erstellt und die Speicherzugriffsberechtigungen in diesem untergeordneten Prozess geändert.	Windows
Gestohlenes Systemtoken	Ein Zugriffstoken wurde geändert, damit ein Benutzer Sicherheitszugriffskontrollen umgehen kann.	Windows
Prozessstart mit geringer Integrität	Ein Prozess wurde so angepasst, dass er mit einem niedrigen Integritätsniveau ausgeführt wird.	Windows

* Nur unter macOS Catalina und früheren Versionen unterstützt.

Platzhalter in Ausschlüssen zum Speicherschutz

Ausschlüsse zum Speicherschutz können die folgenden Sonderzeichen enthalten (alle Betriebssysteme): ^ & ' @ { } [ ] , $ = ! - # ( ) % . + ~ _ *

Auf Windows-Geräten werden auch alle Buchstaben mit anschließendem Doppelpunkt (z. B. C:) unterstützt.

Das Escaping des Sternchens (*) wird derzeit nicht unterstützt. Sie können es beispielsweise nicht verwenden, um eine Datei auszuschließen, die im Dateinamen ein Sternchen enthält.

Beim Hinzufügen von DLL-Ausschlüssen sind Platzhalter nicht zulässig.

Platzhalter	Beschreibung
*	Entspricht null oder mehr Zeichen, mit Ausnahme des plattformspezifischen Pfadtrennzeichens. Die Dateipfadtrennzeichen sind auf Windows-Geräten „\“ und „/“ unter Linux und macOS.
**	Entspricht null oder mehr Verzeichnissen in einem absoluten Pfad, um Laufwerke, Verzeichnisse und untergeordnete Verzeichnisse auszuschließen. Beispiel: `C:\MyApp\''\**\''`. Befolgen Sie diese Regeln, wenn Sie den Platzhalter `**` verwenden: • Verwenden Sie `**` immer mit Dateipfadtrennzeichen, z. B. `\**\` oder `/**/` • Das Muster `**\` ist nur gültig, wenn es sich am Anfang des Musters für Windows-Geräte befindet. Dies entspricht allen Verzeichnissen auf allen Laufwerken. • Sie können `\**\` oder `/**/` mehrmals in einem Pfad ohne Einschränkung verwenden.

Hinweis: Bei normalen Platzhaltern sind drei Sternchen „***“ gültig und entsprechen einem einzelnen Sternchen „*“. Drei Sternchen sind jedoch nicht für Ausschlüsse gültig, da damit Tippfehler verborgen würden. Bei dem Muster „C:***.exe“ kann es z. B. sein, dass der Benutzer „C:***.exe“ schreiben wollte, aber versehentlich ein „\“ ausgelassen hat. Wenn „***“ als ein einzelnes „*“ behandelt werden würde, könnte dies zu einem anderen Verhalten führen als beabsichtigt.

Windows-Beispiele für die Verwendung von Platzhaltern in Speicherschutzausschlüssen

Die folgenden Beispiele basieren auf dem Ausschluss einer ausführbaren Datei, die im folgenden Pfad gespeichert ist: `C:\Application\TestApp\MyApp\program.exe`

	Beispiele

Beispiele für gültige Ausschlusspfade	**Relativer Pfadausschluss ohne Platzhalter**:
	`\Application\TestApp\MyApp\program.exe`
	Ausschluss von program.exe, solange program.exe sich im Verzeichnis „MyApp“ unter C:\Application befindet:
	`C:\Application\**\MyApp\program.exe`
	Ausschluss aller .exe-Dateien, die sich im Verzeichnis „MyApp“ unter C:\Application befinden:
	`C:\Application\**\MyApp\*.exe`
	Ausschluss aller ausführbaren Dateien (unabhängig von der Dateierweiterung), solange sie sich im Verzeichnis „MyApp“ unter C:\Application befinden:
	`C:\Application\**\MyApp\*`
	Ausschluss der Datei program.exe, solange sie sich in einem beliebigen untergeordneten Verzeichnis von C:\Application\TestApp befindet:
	`C:\Application\TestApp\**\program.exe`
	Ausschluss von program.exe, solange sich die Datei unter \Application\TestApp \MyApp\ auf dem Laufwerk C: befindet:
	`C:\**\Application\TestApp\MyApp\program.exe`
	Ausschluss aller ausführbarer Dateien, solange sie sich unter \Application \TestApp\MyApp\ auf dem Laufwerk C: befinden:
	`C:\**\Application\TestApp\MyApp\*.exe`
	Ausschluss aller ausführbarer Dateien (unabhängig von der Erweiterung), solange sie sich unter \Application\TestApp\MyApp\ auf dem Laufwerk C: befinden
	`C:\**\Application\TestApp\MyApp\*`

	Beispiele
Falsche Verwendung von Sternchen in Ausschlüssen	Verwenden Sie nur ein einzelnes Sternchen (*), das einem Zeichen in einem Ordner- oder Dateinamen entspricht. Doppelte Sternchen sind für Verzeichnispfade reserviert und dürfen nicht am Ende von Ausschlüssen verwendet werden. Im Folgenden finden Sie eine Liste von Beispielen im Kontext des Ausschlusses von `C:\Application\TestApp\MyApp\program.exe`. • **Falsch:** `C:\Application\TestApp\MyApp**.exe` • **Falsch:** `C:\Application**\MyApp\program.exe` • **Richtig:** `C:\Application\TestApp\MyApp\*.exe` • **Richtig:** `C:\Application\TestApp\*\*.exe` • **Richtig:**`C:\Application\**\program.exe`
Nicht empfohlene Ausschlüsse	Vermeiden Sie es, direkt nach einem Laufwerksbuchstaben ein doppeltes Sternchen (**) zu verwenden. Beispiel: `C:\**\program.exe` In diesem Beispiel kann `program.exe` von jedem Ordner auf Laufwerk `C:` aus ausgeführt werden. Obwohl dieser Ausschluss technisch korrekt ist, würde er alles in allen Verzeichnissen auf dem Laufwerk ausschließen (einschließlich untergeordneter Verzeichnisse).

macOS-Beispiele zu den in Speicherschutzausschlüssen verwendeten Platzhaltern

Die folgenden Beispiele basieren auf dem Ausschluss einer ausführbaren Datei, die im folgenden Pfad gespeichert ist: `/Application/TestApp/MyApp/program.dmg`

Typ	Beschreibung

Korrekte Verwendung von Ausschlüssen	**Schließt program.dmg aus, solange sich program.dmg unter dem untergeordneten Verzeichnis „MyApp“ befindet**:
	`/Application/**/MyApp/program.dmg`
	Schließt jede ausführbare Dateien mit der Erweiterung .dmg aus, solange sich die ausführbare Datei unter dem untergeordneten Verzeichnis „MyApp“ befindet:
	`/Application/**/MyApp/*.dmg`
	Schließt jede ausführbare Dateien aus, solange sich die ausführbare Datei unter dem untergeordneten Verzeichnis „MyApp“ befindet:
	`/Application/**/MyApp/*`
	Schließt program.dmg aus, solange sich die Datei unter einem Verzeichnis befindet, das ein untergeordnetes Verzeichnis des Verzeichnisses „TestApp“ ist:
	`/Application/TestApp/**/program.dmg`

Typ	Beschreibung
Falsche Verwendung von Sternchen in Ausschlüssen	Verwenden Sie nur ein einzelnes Sternchen (*), das einem Zeichen in einem Ordner- oder Dateinamen entspricht. Doppelte Sternchen sind für Verzeichnispfade reserviert und dürfen nicht am Ende von Ausschlüssen verwendet werden. Im Folgenden finden Sie eine Liste von Beispielen im Zusammenhang mit dem Ausschluss `/Application/TestApp/MyApp/Program.dmg`. • • **Falsch:** /Application/TestApp/MyApp/pro**am.dmg • **Richtig:** /Application/TestApp/MyApp/progra*.dmg • • • **Falsch:** /Application/** • **Richtig:** /Application/**/*
Nicht empfohlene Ausschlüsse	Vermeiden Sie die Verwendung eines doppelten Sternchens (**) am Anfang eines Ausschlusses. Beispiel: `/**/program.dmg` In diesem Beispiel kann `program.dmg` von jedem Ordner auf dem Laufwerk aus ausgeführt werden. Obwohl dieser Ausschluss technisch korrekt ist, würde er alles in allen Verzeichnissen auf dem Laufwerk ausschließen (einschließlich untergeordneter Verzeichnisse).

Schutzeinstellungen

CylancePROTECT Desktop überwacht ständig die Ausführung schädlicher Prozesse und warnt die Konsole, wenn unsichere oder anormale Ausführungsversuche unternommen werden. Sie können den CylancePROTECT Desktop Agenten mit den folgenden Einstellungen konfigurieren, die Sie auf der Registerkarte **Schutzeinstellungen** in einer Geräterichtlinie finden.

Option	Beschreibung
Dienstbeendung über Gerät verhindern	Wenn diese Option ausgewählt ist, können Gerätebenutzer den Dienst für den CylancePROTECT Desktop-Agenten oder für die folgenden Versionen des CylanceOPTICS-Agenten nicht beenden: • CylanceOPTICS-Agent für Windows 3.1 oder höher mit CylancePROTECT Desktop 3.0 oder höher • CylanceOPTICS-Agent für macOS 3.3 oder höher mit CylancePROTECT Desktop 3.1 oder höher Wenn diese Einstellung aktiviert ist, können macOS-Benutzer die Dienste nur beenden, wenn die Selbstschutzstufe in den Geräteeigenschaften auf „Lokaler Administrator“ (Assets > Geräte > Ein Gerät auswählen) eingestellt ist. Windows-Benutzer können die Agentendienste nicht beenden, solange diese Einstellung aktiviert ist. CylancePROTECT Desktop-Agent Version 3.1 und höher wird als vertrauenswürdiger Dienst mit der AM-PPL-Technologie (Antimalware Protected Process Light) von Microsoft ausgeführt, wodurch auch verhindert wird, dass der Agent heruntergefahren wird. Für diese Funktion muss auf dem Gerät Windows 10 1709 oder höher oder Windows Server 2019 oder höher ausgeführt werden.
Unsichere laufende Prozesse und deren Unterprozesse beenden	Wenn diese Einstellung ausgewählt ist, beendet der Agent Prozesse und untergeordnete Prozesse (.exe oder .dll), unabhängig von ihrem Status, sobald eine Bedrohung erkannt wird. Dies bietet ein hohes Maß an Kontrolle über schädliche Prozesse, die möglicherweise auf einem Gerät ausgeführt werden. Die Datei muss mithilfe der globalen Quarantäneliste automatisch oder manuell unter Quarantäne gestellt werden. Diese Funktion muss aktiviert werden, bevor die Datei unter Quarantäne gestellt wird. Wenn diese Funktion aktiviert ist, die Datei jedoch weder manuell noch automatisch unter Quarantäne gestellt wurde, werden die Prozesse weiterhin ausgeführt. **Beispiel:** Die Ausführung einer Datei wird zugelassen, dann entscheiden Sie sich, die Datei unter Quarantäne zu stellen. Wenn diese Einstellung aktiviert ist, wird die Datei in Quarantäne verschoben, und der Prozess wird zusammen mit allen untergeordneten Prozessen beendet. Wenn diese Einstellung deaktiviert ist, wird die Datei unter Quarantäne gestellt. Da die Ausführung der Datei jedoch zugelassen wurde, konnten alle Prozesse, die von der Datei gestartet worden sind, weiterhin ausgeführt werden.

Option	Beschreibung

Bedrohungserkennung im Hintergrund	Es wird ein vollständiger Datenträgerscan durchgeführt, um inaktive Bedrohungen auf der Festplatte zu erkennen und zu analysieren. Der vollständige Datenträgerscan ist so konzipiert, dass die Auswirkungen auf den Endbenutzer durch den Einsatz relativ weniger Systemressourcen minimiert werden. Der Scan der Bedrohungserkennung im Hintergrund kann bis zu einer Woche dauern, je nachdem, wie stark das System ausgelastet ist und wie viele Dateien im System analysiert werden müssen. Das Datum und die Uhrzeit des letzten abgeschlossenen Hintergrundscans werden in der Konsole protokolliert.
	
	Sie können den Scan nur einmal bei der Installation ausführen oder ihn so einstellen, dass er in einem von Ihnen festgelegten Intervall ausgeführt wird. Das Standard-Scanintervall beträgt 10 Tage. Wichtige Upgrades des Erkennungsmodells, z. B. das Hinzufügen neuer Betriebssysteme, lösen ebenfalls einen vollständigen Datenträgerscan aus. Beachten Sie, dass eine Erhöhung der Häufigkeit der Scans die Leistung Geräts beeinträchtigen kann.
	
	Es wird empfohlen, dass Sie die Einstellung **Bedrohungserkennung im Hintergrund** auf **Einmal ausführen** festlegen und die Option **Auf neue Dateien überwachen** aktivieren, damit neue und aktualisierte Dateien auf der Festplatte überwacht werden. Wenn Sie nach neuen und aktualisierten Dateien suchen, müssen Sie alle vorhandenen Dateien nur einmal überprüfen. Aufgrund der Vorhersagbarkeit der Technologie sind regelmäßige Scans der gesamten Festplatte nicht erforderlich, können aber zu Compliance-Zwecken implementiert werden (z. B. PCI-Compliance).
	
	Hinweis: Wenn Scans zur Bedrohungserkennung im Hintergrund auf mehreren VM-Geräten ausgeführt werden, die gleichzeitig vom selben VM-Host stammen, wird die Geräteleistung beeinträchtigt. Ziehen Sie in Betracht, diese Funktion für VM-Geräte schrittweise zu aktivieren, um die Anzahl der gleichzeitig stattfindenden Scans zu begrenzen.
	
	Verwenden Sie einen der folgenden Befehle, um den Scan manuell auszuführen:
	
	• Auf Windows-Geräten:
	
	`C:\Program Files\Cylance\Desktop\CylanceSvc.exe / backgroundscan`
	
	• Auf macOS-Geräten:
	
	`/Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -background-scan`
	
	• Auf Linux-Geräten:
	
	`/opt/cylance/desktop/Cylance -b`
	`/opt/cylance/desktop/Cylance --start-bg-scan`

Option	Beschreibung
Auf neue Dateien überwachen	Diese Einstellung ermöglicht es dem Agenten, neue oder geänderte Dateien auf inaktive Bedrohungen zu scannen und zu analysieren. Wenn eine Bedrohung erkannt wird, wird die Datei in Quarantäne verschoben, auch wenn nicht versucht wurde, sie auszuführen. Es wird empfohlen, diese Einstellung zusammen mit der Erkennung von Hintergrundbedrohungen zu aktivieren (einmalige Ausführung). Der automatische Quarantänemodus (Ausführungssteuerung) blockiert unsichere oder anormale Dateien bei der Ausführung. Daher ist es nicht erforderlich, „Auf neue Dateien überwachen“ zu aktivieren, wenn der automatische Quarantänemodus ebenfalls aktiviert ist, es sei denn, Sie ziehen es vor, eine schädliche Datei in Quarantäne zu stellen, sobald der Agent die Bedrohung während eines Scans erkennt. Diese Einstellung kann sich auf die Leistung auswirken. Sie sollten daher die Datenträger- oder Nachrichtenverarbeitungsleistung prüfen, um festzustellen, ob sie sich geändert hat. Das Ausschließen von Ordnern kann die Leistung verbessern und sicherstellen, dass bestimmte Ordner und Dateien nicht vom Agenten gescannt oder analysiert werden.
Festlegen der maximalen Größe zu scannender Archivdateien	Geben Sie die maximale Größe der Archivdatei an, die vom Agenten gescannt werden soll. Diese Einstellung gilt für die **Bedrohungserkennung im Hintergrund** und für **Auf neue Dateien überwachen**. Wenn Sie keine Archivdateien scannen möchten, stellen Sie die Dateigröße auf 0 MB ein.

Option	Beschreibung
Bestimmte Ordner ausschließen	Mit dieser Einstellung können Sie Ordner und Unterordner festlegen, die über die Funktionen **Bedrohungserkennung im Hintergrund** und **Auf neue Dateien überwachen** vom Scannen ausgeschlossen werden sollen. Verwenden Sie für Windows einen absoluten Pfad mit Laufwerksbuchstabe. Beispiel: `C:\Test`. Verwenden Sie für macOS einen absoluten Pfad aus dem Stammverzeichnis ohne Laufwerksbuchstabe. Beispiel: `/Applications/SampleApplication.app`. Verwenden Sie für Linux einen absoluten Pfad aus dem Stammverzeichnis ohne Laufwerksbuchstabe. Beispiel: `/opt/application`. **Beispiel für Windows**: `C:\Test` **Beispiel für macOS (ohne Leerzeichen)**: `/Applications/SampleApplication.app` **Beispiel für macOS (mit Leerzeichen)**: `/Applications/Sample\ Application.app` **Beispiel für Linux**: `/opt/application/` Der Platzhalter „*“ wird auch für Ordnerausschlüsse unterstützt. Weitere Informationen finden Sie im Abschnitt Platzhalter in den Ordnerausschlüssen der Schutzeinstellungen. Ausschlüsse werden nicht rückwirkend angewendet. Nach der Erstinstallation des Agenten ignorieren die Funktionen „Bedrohungserkennung im Hintergrund“ und „Auf neue Dateien überwachen“ Dateien gemäß der Ausschlussliste, die sie empfangen haben. Das Hinzufügen eines Ausschlusses nach der ersten Erkennung oder dem ersten Befund der Gefährlichkeit schließt die bereits erkannten oder als für gefährlich befundenen Dateien nicht rückwirkend aus. Alle Dateien, die zuvor erkannt oder als für gefährlich befunden wurden, bleiben in diesem Zustand, bis sie lokal ignoriert oder der globalen Sicherheitsliste hinzugefügt werden. Wenn beispielsweise die Option „Auf neue Dateien überwachen“ eine Datei mit dem Namen C:\Windows\ccmcache\test.exe als für gefährlich befindet und der Registerkarte „Schutzeinstellungen“ für C:\Windows\ccmcache\ später ein Ausschluss hinzugefügt wird, wird die als für gefährlich befundene Datei trotz des neuen Ordnerausschlusses weiterhin als für gefährlich befunden. Dies gilt, bis Sie die Datei lokal ignorieren oder sie der globalen Sicherheitsliste hinzufügen.
Ausführung zulassen	Dateien, die aus einem beliebigen Ordner ausgeführt werden, unterliegen der Ausführungssteuerung/automatischen Quarantäne, auch wenn sie unter „Bestimmte Ordner ausschließen“ angegeben sind. Sie können die Einstellung „Ausführung zulassen“ aktivieren, um zu erlauben, dass Dateien aus Ordnern ausgeführt werden, die in der Liste „Bestimmte Ordner ausschließen“ angegeben sind. Diese Einstellung gilt für alle unter „Bestimmte Ordner ausschließen“ aufgeführten Ordner, nicht nur für das erste oder letzte eingegebene Element. Dateien und Bedrohungen, die in diesen Ordnern abgelegt werden, können ausgeführt werden und Ihr Gerät und Ihr Unternehmen gefährden. Treffen Sie daher die geeigneten Vorkehrungen, um sicherzustellen, dass anormale Dateien nicht zu ausgeschlossenen Ordnern hinzugefügt werden können.

Option	Beschreibung
Dateiproben kopieren (Malware)	Geben Sie ein freigegebenes Netzlaufwerk an, um Kopien von Dateiproben zu speichern, die durch die Erkennung von Hintergrundbedrohungen, die Überwachung auf neue Dateien und die Ausführungssteuerung gefunden wurden. Auf diese Weise können Sie eigene Analysen von Dateien durchführen, die von CylancePROTECT Desktop als unsicher oder anormal eingestuft werden. • Es werden CIFS/SMB-Netzwerkfreigaben unterstützt. • Geben Sie einen Speicherort für die Netzwerkfreigabe an. Sie sollten einen vollständig qualifizierten Pfad verwenden. Beispiel: `\\server_name \shared_folder`. • Alle Dateien, die die Kriterien erfüllen, werden auf die Netzwerkfreigabe kopiert, auch wenn es sich um Duplikate handelt. Es wird keine Eindeutigkeitsprüfung durchgeführt. • Dateien werden komprimiert. • Dateien sind kennwortgeschützt. Das Kennwort lautet „infected“.

Platzhalter in den Ordnerausschlüssen der Schutzeinstellungen

Sie können das Sternchen (*) als Platzhalter für alle Betriebssysteme verwenden, wenn Sie auf der Registerkarte **Schutzeinstellungen** Ordnerausschlüsse angeben.

Zeichen	Bedeutung
*	Verwenden Sie das Sternchen zum Ausschließen von Ordnern und zur Darstellung eines Präfix oder Suffix für einen Ordnernamen. • Das Sternchen entspricht einem oder mehr Zeichen, mit Ausnahme des plattformspezifischen Pfadtrennzeichens (\). • In einem Ausschlusspfad sind mehrere Platzhalter zulässig. • Derzeit wird „*“-Escaping nicht unterstützt. Sie können beispielsweise keinen Ordner ausschließen, der im Ordnernamen ein Sternchen „*“ enthält. • Die vorherige Ordnerausschlussfunktion gilt weiterhin. Dies bedeutet, dass Ausschlüsse auch für alle untergeordneten Ordner gelten.

Zeichen	Bedeutung

Beispiele für Ordnerausschlüsse:	Im Folgenden finden Sie Beispiele für den Ausschluss von `C:\Application\TestFolder1\MyApp\program.exe`.
	Beispiele für die korrekte Verwendung von Platzhaltern in Ordnerausschlüssen
	• Ein Ausschluss ohne Platzhalter.
	`C:\Application\TestFolder1\MyApp\`
	• Es wird ein Platzhalter verwendet, um einen übergeordneten Ordner des „MyApp“-Ordners darzustellen.
	C:\Application*\MyApp\
	• Der Platzhalter gibt an, dass in diesem Ordnernamen ein Präfix (z. B. „Test“) vorhanden ist, mit dem der Agent vergleichen kann.
	C:\Application*Folder1\MyApp\
	• Der Platzhalter gibt an, dass in diesem Ordnernamen ein Suffix (d. h. „1“) vorhanden ist, mit dem der Agent vergleichen kann.
	C:\Application\TestFolder*\MyApp\
	• Der Platzhalter gibt an, dass in diesem Ordnernamen ein Präfix (d. h. „Test“) und ein Suffix (d. h. „1“) vorhanden ist, mit dem der Agent vergleichen kann.
	C:\Application*Folder*\MyApp\
	• Ein Platzhalter wird verwendet, um alle Ordner unter „Application“ im Laufwerk C: auszuschließen.
	C:\Application*\
	• Dieser Platzhalter schließt alle Ordner unter „Application“ für alle Laufwerke aus.
	\Application\
	Beispiele für die falsche Verwendung von Platzhaltern in Ordnerausschlüssen
	• `C:\Application\TestFolder1\MyApp\*.exe`
	Im Dateinamen einer ausführbaren Datei kann kein Platzhalter verwendet werden. Verwenden Sie Platzhalter nur für Ordner- oder Verzeichnisnamen.
	• C:\Application**
	Doppelte Sternchen (**) werden in Ordnerausschlüssen nicht unterstützt. Verwenden Sie stattdessen ein einzelnes Sternchen (*).
	Nicht empfohlene Ordnerausschlüsse
	`C:\*`
	Obwohl dieser Ausschluss als Eingabe gültig ist, würde er alles in allen Verzeichnissen auf dem Laufwerk C: ausschließen (einschließlich untergeordneter Verzeichnisse).

Anwendungssteuerung

Die Anwendungssteuerung ist eine optionale Einstellung für Windows- und Linux-Geräte, mit der Benutzer Änderungen an ausführbaren Dateien auf dem Gerät einschränken können. Nur Anwendungen, die sich bereits vor der Aktivierung der Anwendungssteuerung auf dem Gerät befinden, können ausgeführt werden. Die Anwendungssteuerung ist für Geräte mit festgelegter Funktion vorgesehen, die nach der Einrichtung nicht geändert werden (z. B. Point-of-Sale-Geräte).

Wenn die Anwendungssteuerung aktiviert ist, werden Versuche, Anwendungen hinzuzufügen und Änderungen an Anwendungen auf dem Gerät vorzunehmen, abgelehnt. Dies bedeutet, dass Anwendungen nicht von einem Webbrowser heruntergeladen oder von einem anderen Gerät oder Computer (z. B. einem externen oder gemeinsam genutzten Laufwerk) kopiert werden können.

Die Hauptziele der Anwendungssteuerung sind:

- Verweigern der Ausführung von ausführbaren Dateien von Remote- oder externen Laufwerken.
- Verweigern der Erstellung neuer ausführbarer Dateien auf dem lokalen Laufwerk.
- Verweigern von Änderungen an vorhandenen Dateien auf dem lokalen Laufwerk.

Beachten Sie bei der Verwendung der Anwendungssteuerung Folgendes:

- Der Aktualisierungsvorgang für den CylancePROTECT Desktop- und CylanceOPTICS-Agent ist deaktiviert, wenn die Anwendungssteuerung aktiviert ist.
- Sie können die CylancePROTECT Desktop- und CylanceOPTICS-Agenten nicht entfernen, wenn die Anwendungssteuerung aktiviert ist.
- Es wird nicht empfohlen, CylanceOPTICS auf Systemen mit Anwendungssteuerung auszuführen. Wenn die Anwendungssteuerung aktiviert ist, funktioniert CylanceOPTICS wegen der durch die Anwendungssteuerung auferlegten Restriktionen nicht ordnungsgemäß.
- Die Ausführung aller ausführbaren Dateien auf Remote- oder externen Laufwerken wird verweigert, wenn die Anwendungssteuerung aktiviert ist. Um Produktionsausfälle oder übermäßige Netzwerkaktivitäten zu vermeiden, überwacht die Anwendungssteuerung keine Dateiübertragungen auf Remote- oder externe Laufwerke.
- Siehe Überlegungen zur Verwendung der Anwendungssteuerung auf Linux-Geräten.

Einstellungen der Anwendungssteuerung

Option	Beschreibung
Anwendungssteuerung	Diese Einstellung gibt an, ob Benutzer die Anwendungssteuerung aktivieren können. Wenn Sie die Anwendungssteuerung aktivieren, werden die folgenden empfohlenen Einstellungen automatisch angewendet: • Auf der Registerkarte **Dateiaktionen** werden die Einstellungen für **Automatische Quarantäne mit Ausführungssteuerung** für unsichere und anormale Dateien ausgewählt. • Auf der Registerkarte **Speicheraktionen** wird das Kontrollkästchen **Speicherschutz** aktiviert. Alle Speicherschutz-Verletzungstypen werden auf **Beenden** gesetzt. • Auf der Registerkarte **Schutzeinstellungen** wird die Einstellung **Auf neue Dateien überwachen** ausgewählt. Wenn Sie eine dieser Einstellungen ändern möchten, heben Sie die Auswahl auf den angegebenen Registerkarten auf.

Option	Beschreibung
Fenster ändern	Wenn diese Einstellung aktiviert ist, wird die Anwendungssteuerung vorübergehend deaktiviert, um das Bearbeiten und Ausführen neuer Anwendungen oder das Durchführen von Aktualisierungen, einschließlich der Aktualisierung des Agenten, zu ermöglichen. Deaktivieren Sie nach Durchführung der erforderlichen Änderungen dieses Kontrollkästchen, um das Änderungsfenster zu schließen und die Anwendungssteuerung wieder zu aktivieren. Wenn Sie diese Einstellung verwenden, um die Anwendungssteuerung vorübergehend zu deaktivieren, werden Änderungen, wie z. B. Ordnerausschlüsse, beibehalten. Wenn Sie die Einstellungen der **Anwendungssteuerung** deaktivieren, werden die Einstellungen auf die Standardeinstellungen zurückgesetzt.
Ordnerausschlüsse (einschließlich Unterordnern)	Diese Einstellung gibt einen absoluten Pfad von Ordnern an, die bei aktivierter Anwendungssteuerung Änderungen und Ergänzungen vornehmen dürfen. Diese Einstellung gilt nur für Geräte mit Windows-Agent 1410 oder höher. Beispiel: `C:\Programme\Microsoft SQL Server` Ordnerausschlüsse sind nur für lokale interne Laufwerke verfügbar. Ausschlüsse für Wechseldatenträger oder Remote-Laufwerke werden nicht unterstützt.

Anzeigen der Anwendungssteuerungsaktivität

Die Aktivität der Anwendungssteuerung eines Geräts finden Sie auf der Seite **Gerätedetails** im Abschnitt **Bedrohungen und Aktivitäten**.

Überlegungen zur Verwendung der Anwendungssteuerung auf Linux-Geräten

Beachten Sie Folgendes, bevor Sie die Anwendungssteuerung in einer Geräterichtlinie für Linux-Geräte aktivieren:

- Ordnerausschlüsse in der Anwendungssteuerungsrichtlinie werden vom Linux-Agent nicht unterstützt.
- Wenn die Anwendungssteuerung aktiviert ist, wird ein Bestand aller ausführbaren Dateien auf dem lokalen Dateisystem erstellt. Die Dateiausführung ist auf die Dateien in diesem Bestand beschränkt.
- Ausführbare Dateien können dem Gerät hinzugefügt werden, nachdem die Anwendungssteuerung aktiviert wurde, diese können jedoch nicht ausgeführt werden. Wenn die Anwendungssteuerung aktiviert ist, dürfen nur die im Bestand enthaltenen Anwendungen ausgeführt werden.
- Das Zulassen eines Updates auf einem Linux-Gerät mit aktivierter Anwendungssteuerung kann zu Problemen führen.

Agent-Einstellungen

Verwenden Sie die Agent-Einstellungen, um Desktop-Benachrichtigungen anzuzeigen, z. B., wenn eine Datei auf Geräten unter Quarantäne gestellt wird. Sie können von dieser Seite aus auch Agent-Protokolldateien in die Konsole hochladen.

Option	Beschreibung
Automatisches Hochladen von Protokolldateien aktivieren	Ermöglicht das Hochladen von Agent-Protokollen und deren Anzeige in der Konsole. Hochgeladene Protokolldateien werden 30 Tage lang gespeichert. Nach der Aktivierung dieser Option wird die Registerkarte „Agent-Protokolle“ angezeigt, wenn Sie ein Gerät auswählen, das dieser Richtlinie auf der Registerkarte „Geräte“ zugewiesen ist. Der Name der Protokolldatei ist das Protokolldatum.
Desktop-Benachrichtigungen aktivieren	Popup-Fenster für Agenten-Benachrichtigungen können auf jedem Gerät konfiguriert oder auf Richtlinienebene in der Konsole festgelegt werden. Das Aktivieren bzw. Deaktivieren der Popup-Fenster für Agenten-Benachrichtigungen auf Geräteebene hat Vorrang vor den Konsoleneinstellungen. Stellen Sie sicher, dass das Gerät, für das Sie Dateien protokollieren möchten, dieser Richtlinie zugewiesen ist. In der Agenten-UI wird die Registerkarte „Ereignisse“ gelöscht, wenn die CylanceUI neu gestartet oder das Gerät neu hochgefahren wird.
Softwarebestand aktivieren	Diese Einstellung gibt an, ob der Agent eine Liste der auf Geräten installierten Anwendungen an die Verwaltungskonsole meldet. Mit dieser Funktion können Administratoren auf Geräten installierte Anwendungen identifizieren, die eine Quelle für Schwachstellen sein könnten, und Maßnahmen zur Behebung von Schwachstellen nach Priorität ordnen und diese entsprechend verwalten. Diese Funktion erfordert CylancePROTECT Desktop für Windows-Version 3.2. Über den Bildschirm **Assets > Installierte Anwendungen** können Sie eine Liste aller Anwendungen abrufen, die auf den beim Mandanten registrierten Geräten installiert sind, und für jede Anwendung die Liste der Geräte anzeigen, auf denen sie installiert ist. Über den Bildschirm **Assets > Geräte > Gerätedetails > Installierte Anwendungen** können Sie auch eine Liste der auf einzelnen Geräten installierten Anwendungen anzeigen.

Skriptsteuerung

Die Skriptsteuerung schützt Windows-Geräte, indem die Ausführung von Skripts blockiert wird. Wenn Sie die Ausführung von Skripts zulassen möchten, können Sie Ausschlüsse auf verschiedene Weise mithilfe von Platzhaltern hinzufügen. Sie können die Richtlinie beispielsweise so einstellen, dass die Ausführung von Skripten blockiert wird und nur Skripte ausgeführt werden können, die der Ausschlussliste hinzugefügt wurden.

Element	Beschreibung
Aktion	Für jeden Skripttyp können Sie eine der folgenden Aktionen auswählen: • **Deaktiviert**: Mit dieser Aktion können alle Skripte ausgeführt werden, ohne an die Konsole gemeldet zu werden. Diese Einstellung wird nicht empfohlen. • **Warnung**: Mit dieser Aktion können alle Skripte ausgeführt werden, dabei werden sie an die Konsole gemeldet. Verwenden Sie diese Einstellung, wenn Sie alle Skripte überwachen und beobachten möchten, die in Ihrer Umgebung ausgeführt werden. Diese Einstellung wird für die anfängliche Bereitstellung empfohlen, während der Sie festlegen, welche Skripte zugelassen oder blockiert werden sollen. • **Blockieren**: Diese Aktion blockiert die Ausführung aller Skripte, dabei werden sie an die Konsole gemeldet. Nur Dateien, die der Ausschlussliste hinzugefügt wurden, können ausgeführt werden. Verwenden Sie diese Einstellung nach dem Testen und Überwachen auf Bedrohungen im Warnungsmodus. Die folgenden Einstellungen sind für Einstellungen für aktive Skripte und PowerShell-Skripte verfügbar: • **UNSICHERE Skripte blockieren**: Wenn sich das Skript nicht bereits in der Ausschlussliste befindet, ruft CylancePROTECT eine Bedrohungsbewertung für das Skript von den Cylance-Cloud-Diensten ab. Wenn es eine unsichere Bedrohungsbewertung erhält, wird die Ausführung des Skripts blockiert. Unsichere Dateien haben große Ähnlichkeit mit Malware. Nicht ausgewertete und abnormale Skripte werden an die Konsole gemeldet, aber nicht blockiert. • **ABNORMALE und UNSICHERE Skripte blockieren**: Wenn sich das Skript nicht bereits in der Ausschlussliste befindet, ruft CylancePROTECT eine Bedrohungsauswertung für das Skript von den Cylance-Cloud-Diensten ab. Wenn es eine abnormale oder unsichere Bedrohungsbewertung erhält, wird die Ausführung des Skripts blockiert. Unsichere Dateien haben große Ähnlichkeit mit Malware. Abnormale Dateien weisen einige Attribute auf, die Malware ähneln, es ist aber weniger wahrscheinlich, dass sie Malware sind, als bei unsicheren Dateien. Nicht ausgewertete Skripte werden an die Konsole gemeldet, aber nicht blockiert. Sie finden Skriptsteuerungswarnungen und Blockierungsereignisse im Bildschirm **Schutz > Skriptsteuerung**.
Aktives Skript	Mit dieser Einstellung wird festgelegt, ob die Ausführung von aktiven Skripten zugelassen oder die Ausführung verhindert werden soll. Aktive Skripte umfassen VBScript und JScript. Verwenden Sie für eine verbesserte Skriptsteuerung die Einstellung **UNSICHERE Skripte blockieren** oder **ABNORMALE und UNSICHERE Skripte blockieren**. Diese Einstellungen erfordern einen CylancePROTECT Desktop-Agenten der Version 3.2 oder höher. Wenn auf einem Gerät ein älterer Agent ausgeführt wird, wird das Skript standardmäßig blockiert.

Element	Beschreibung
PowerShell-Skript	Diese Einstellung steuert, ob die Ausführung von PowerShell-Skripten zugelassen oder blockiert werden soll. Verwenden Sie für eine verbesserte Skriptsteuerung die Einstellung **UNSICHERE Skripte blockieren** oder **ABNORMALE und UNSICHERE Skripte blockieren**. Diese Einstellungen erfordern einen CylancePROTECT Desktop-Agenten der Version 3.2 oder höher. Wenn auf einem Gerät ein älterer Agent ausgeführt wird, wird das Skript standardmäßig blockiert.
PowerShell-Konsole	Mit dieser Einstellung wird festgelegt, ob die Ausführung der PowerShell-Konsole zugelassen oder ihr Start verhindert werden soll. Das Blockieren der PowerShell-Konsole bietet zusätzliche Sicherheit durch Schutz vor der Verwendung von PowerShell im interaktiven Modus. Der Warnungsmodus für die PowerShell-Konsole erfordert einen CylancePROTECT Desktop-Agenten der Version 3.2 oder höher. Er ermöglicht die Ausführung von Skripten und meldet das erkannte Ereignis an die Verwaltungskonsole. Bei Agenten, die den Warnungsmodus nicht unterstützen, ist die Verwendung der PowerShell-Konsole standardmäßig zulässig und es wird keine Warnung generiert. Wenn Sie ein Skript verwenden, das die PowerShell-Konsole startet, und die PowerShell-Konsole wird blockiert, kann das Skript nicht ausgeführt werden. Den Benutzern wird empfohlen, ihre Skripte so zu ändern, dass die PowerShell-Skripte aufgerufen werden und nicht die PowerShell-Konsole. Das kann mit dem Parameter `-file` erreicht werden. Ein grundlegender Befehl zur Ausführung eines PowerShell-Skripts ohne Aufruf der Konsole wäre: `Powershell.exe -file [script name]`

Element	Beschreibung
Makros (Version 2.1.1578 und früher)	Diese Einstellung steuert, ob für Microsoft Office-Makros Warnungen angezeigt oder diese blockiert werden sollen. Makros verwenden Visual Basic for Applications (VBA), das das Einbetten von Code in ein Microsoft Office-Dokument (in der Regel Microsoft Office, Excel und PowerPoint) ermöglicht. Der Hauptzweck von Makros ist die Vereinfachung von Routinevorgängen wie die Bearbeitung von Daten in einer Tabelle oder die Formatierung von Text in einem Dokument. Malware-Programmierer können jedoch Makros verwenden, um Befehle auszuführen und das System anzugreifen. Wenn ein Makro versucht, das System zu manipulieren, ist davon auszugehen, dass es eine bösartige Aktion durchführt. Der Agent sucht nach schädlichen Aktionen, die von einem Makro stammen, das sich auf Bereiche außerhalb der Microsoft Office-Produkte auswirkt. Beachten Sie bitte Folgendes: • Die Funktion „Skriptsteuerungsmakros“ kann mit Agent-Version 2.1.1578 und früher genutzt werden. Verwenden Sie für neuere Agenten den Verletzungstyp **Gefährliche VBA-Makros** in der Speicherschutz-Richtlinie. • Alle Makro-Ausschlüsse, die für die Skriptsteuerung erstellt worden sind, müssen zu den Speicherschutzausschlüssen für den Verletzungstyp **Gefährliche VBA-Makros** hinzugefügt werden. • Ab Microsoft Office 2013 sind Makros standardmäßig deaktiviert. Meistens brauchen Sie keine Makros zu aktivieren, um den Inhalt von Microsoft Office-Dokumenten anzuzeigen. Sie sollten nur Makros für Dokumente aktivieren, die Sie von vertrauenswürdigen Benutzern erhalten, und nur, wenn Sie einen guten Grund haben, sie zu aktivieren. Andernfalls sollten Makros immer deaktiviert werden.
Python	Diese Einstellung steuert, ob Python-Skripte (Version 2.7 und 3.0 bis 3.8) zugelassen oder deren Ausführung blockiert werden. Diese Einstellung gilt für Agent 2.1.1580 oder höher.
.NET DLR	Diese Einstellung steuert, ob die Ausführung von .NET DLR-Skripten zugelassen oder blockiert werden soll. Diese Einstellung gilt für Agent 2.1.1580 oder höher.

Element	Beschreibung
XLM-Makros (Vorschau)	**Hinweis:** Die XLM-Makros-Funktion ist derzeit im Vorschaumodus verfügbar, wo sie möglicherweise unerwartetes Verhalten zeigt. Diese Einstellung steuert, ob CylancePROTECT Desktop die Ausführung von Excel 4.0 (XLM)-Makros zulässt oder blockiert. Wenn Makros aktiviert und ausgeführt werden, kommuniziert die Microsoft AMSI-Schnittstelle mit dem Agenten, um zu bestimmen, ob das Makro ausgeführt oder gemäß der Geräterichtlinie gesperrt werden soll. Diese Funktion erfordert Folgendes: • Microsoft Windows Version 10 oder höher • CylancePROTECT Desktop-Agent Version 3.1 • VBA-Makros müssen im Excel-Menü **Datei > Trust Center > Excel Trust Center > Makroeinstellungen** deaktiviert werden.
Erweiterte Einstellungen	Die folgenden erweiterten Einstellungen unterstützen die Skriptauswertung und sind für die Skriptsteuerung von Vorteil: • **Alle Skripte auswerten**: Mit dieser Einstellung wird sichergestellt, dass alle Skripte unabhängig von der Skriptsteuerungseinstellung bewertet werden. Wenn die Einstellung für die Skriptsteuerung auf „Warnung“ oder „Blockieren“ gesetzt ist, werden Skripte nicht ausgewertet. • **Skript in die Cloud hochladen**: Diese Einstellung legt fest, ob eine Kopie des Skripts zur Bedrohungsanalyse und -auswertung in die CylancePROTECT-Cloud-Dienste hochgeladen wird. Wenn diese Option nicht ausgewählt ist, versucht CylancePROTECT eine Auswertung für das Skript anhand der Hash-Details zu erhalten. • **Warnung nur bei Ausführung verdächtiger Skripte**: Wenn ein Skript ausgewertet wird und keine Bedrohung erkannt wird, legt diese Einstellung fest, dass die Ausführung des Skripts nicht an die Verwaltungskonsole gemeldet wird. Wenn diese Option nicht ausgewählt ist, wird die Ausführung von Skripten an die Verwaltungskonsole gemeldet, selbst wenn keine Bedrohung zu erkennen ist.

Element	Beschreibung
Dateien, Skripte oder Prozesse ausschließen	Sie können Ordner angeben, um die Ausführung aller Skripte in diesem Ordner (und in entsprechenden Unterordnern) zuzulassen, ohne dass eine Warnmeldung generiert wird, selbst wenn die Skriptsteuerungen auf „Blockieren“ eingestellt sind. Sie können auch Ausschlüsse für Prozesse hinzufügen, damit Skripte von bestimmten Anwendungen ordnungsgemäß ausgeführt werden können, die andernfalls blockiert würden. Wenn die IT-Abteilung beispielsweise regelmäßig ein bestimmtes Tool zur Ausführung von Skripten verwendet, können Sie den Prozess für dieses Tool als Ausschluss hinzufügen, damit Skripte über dieses Tool ausgeführt werden können. Sie müssen den relativen Pfad des Ordners oder Unterordners angeben. Ordnerpfade können auf ein lokales Laufwerk, ein zugeordnetes Netzlaufwerk oder einen UNC-Pfad (Universal Naming Convention) verweisen. **Ordner und Skripte ausschließen** • Ordnerausschlüsse dürfen den Skript- oder Makrodateinamen nicht enthalten. Diese Einträge sind ungültig und werden vom Agenten ignoriert. • Wenn Sie ein bestimmtes Skript ausschließen möchten, müssen Sie einen Platzhalter verwenden. Weitere Informationen über die Verwendung von Platzhaltern zum Ausschließen bestimmter Skripte finden Sie unter Platzhalter in Skriptsteuerungsausschlüssen. • Wenn die Gruppe „Alle“ Schreibberechtigungen für einen Ordner erhält, kann jeder innerhalb oder außerhalb des Unternehmens ein Skript in dem Ordner ablegen und verfügt über Schreibrechte für diesen Ordner. CylancePROTECT Desktop sendet weiterhin Warnungen zu Skripten und blockiert sie. Die Schreibrechte gelten nicht nur für den direkten übergeordneten Ordner, sondern auch für alle übergeordneten Ordner bis hin zum Stammverzeichnis. **Prozesse ausschließen** • Für Prozessausschlüsse ist Agent-Version 2.1.1580 oder höher erforderlich. • Die ausführbare Datei im Prozessausschluss kann von der Ausführungssteuerung unter Quarantäne gestellt werden und daher nicht ausführbar sein. Wenn die ausführbare Datei in Quarantäne verschoben wurde, müssen Sie sie der **Richtlinie „Sichere Liste“** auf der Registerkarte **Dateiaktionen** hinzufügen. • Prozessausschlüsse lassen die Ausführung von Skripten weiterhin zu und verhindern nicht, dass sie im angegebenen Ordner ausgeführt werden.

Platzhalter in Skriptsteuerungsausschlüssen

Sie können das Sternchen (*) als Platzhalter verwenden, wenn Sie Ausschlüsse auf der Registerkarte **Skriptsteuerung** angeben.

Durch die Verwendung von Platzhaltern in Skriptsteuerungsausschlüssen wird die Anzahl der in Ihrer Konsole angezeigten Warnungen reduziert, während Benutzer bestimmte Skripte ausführen können, die dem

Ausschlusspfad und Dateinamen entsprechen. Sie können beispielsweise ein bestimmtes Skript ausschließen, indem Sie den vollständigen Namen verwenden, wenn Sie einen Platzhalter im Verzeichnispfad verwenden, oder Sie können den Platzhalter verwenden, um eine Gruppe von Skripten mit einem ähnlichen Namen zu finden, indem Sie ihn als Teil des Dateinamens selbst verwenden.

Die Verwendung von Platzhaltern bei Ausschlüssen bietet zwar Flexibilität, kann aber auch Ihre Sicherheitsstandards verschlechtern, wenn Ihre Ausschlüsse zu weit gefasst sind. Vermeiden Sie beispielsweise, ganze Ordner wie `/windows/temp` auszuschließen. Verwenden Sie stattdessen einen Platzhalter, wenn Sie den vollständigen oder teilweisen Dateinamen des Skripts angeben, das Sie ausschließen möchten (z. B. `/windows/temp/myscript*.vbs`).

In der folgenden Tabelle werden die Regeln für Ausschlüsse für die Skriptsteuerung beschrieben:

Element	Beschreibung
Unterstützte Platzhalterzeichen	Nur das Sternchen (*) wird als Platzhalter für Ausschlüsse für die Skriptsteuerung unterstützt. Der Platzhalter stellt ein oder mehrere Zeichen dar.
Schrägstriche im UNIX-Stil	Wenn Sie Platzhalter verwenden, müssen Ausschlüsse Unix-Schrägstriche verwenden (auch für Windows-Systeme). Beispiel: `/windows/system*/*`
Ordnerausschlüsse	Wenn Sie einen Ordner ausschließen möchten, muss der Ausschluss am Ende des Pfads einen Platzhalter enthalten, um den Ausschluss als Ordner (und nicht als Datei) erkennbar zu machen. Beispiel: • `/windows/system32/*` • `/windows/*/test/*` • `/windows/system32/test*/*`

Dateiausschlüsse	Wenn Sie eine Datei ausschließen möchten, muss der Ausschluss mit einer Dateierweiterung enden, um den Ausschluss als Datei (und nicht als Ordner) erkennbar zu machen. Beispiel:
	• `/windows/system32/*.vbs`
	• `/windows/system32/script*.vbs`
	• `/windows/system32/*/script.vbs`
	• Jeder Platzhalter stellt nur eine Ordnerebene dar. Die Anzahl der im Ausschluss dargestellten Ordnerebenen muss mit der Dateiebene übereinstimmen, die Sie ausschließen möchten.
	  • Zum Beispiel passt /folder/*/script.vbs zu \folder\test\script.vbs, aber nicht zu \folder\test\001\script.vbs. In diesem Fall ist entweder /folder/*/001/script.vbs oder /folder/*/*/script.vbs erforderlich.
	  • Der Platzhalter muss dann für jede Ebene bis zur Ebene, auf der sich das Skript befindet, verwendet werden.
	  • Zwei oder mehr Platzhalter pro Ebene sind nicht zulässig. /folder/*file*.ext ist zum Beispiel nicht erlaubt.

Element	Beschreibung
Prozessausschlüsse	Bei Prozessausschlüssen mit Platzhalter muss eine Dateierweiterung angegeben werden, um zwischen einem Ordner und einer Datei unterscheiden zu können. Um einen Prozess unabhängig vom Verzeichnis anzugeben, in dem er sich befindet, beachten Sie die folgenden Beispiele: • `/my*.exe` (lokales Laufwerk) • `//my*.exe` (Netzlaufwerk) Um einen Prozess anzugeben, der sich in einem bestimmten Verzeichnis befindet, beachten Sie die folgenden Beispiele: • `/directory/child/my*.exe` (lokales Laufwerk) • `//directory/child/my*.exe` (Netzlaufwerk)
Beispiele für vollständige und teilweise Übereinstimmungen bei Ausschlüssen	Platzhalter unterstützen vollständige und partielle Ausschlüsse. • `/folder/*/script.vbs` • `/folder/test*/script.vbs`
Absolute Pfade	Absolute Pfade werden bei Ausschlüssen für die Skriptsteuerung nicht unterstützt.
Relative Pfade	Wenn Sie einen gemeinsamen relativen Pfad identifizieren können, können Sie UNC (Universal Naming Convention)-Pfade mit einem Platzhalter ausschließen. Wenn Sie beispielsweise Gerätenamen in einem Pfad verwenden, z. B. „DC01“ bis „DC24“: `/dc*/path/to/script/*`
Netzwerkpfade	Netzwerkpfade können ausgeschlossen werden: Beispiel: • `//hostname/application/*` • `//host*/application/*` • `//*name/*/application/*` • `//hostname/*`

Beispiele zu Ausschlüssen für die Skriptsteuerung

Das Hinzufügen von Ausschlüssen für dynamische Skripte, die von einem bestimmten Verzeichnis ausgeführt werden, oder für ein Skript, das von mehreren verschiedenen Benutzerordnern ausgeführt wird, ist durch die Verwendung von Platzhaltern in Skriptsteuerungsausschlüssen möglich. Sie können beispielsweise das Token „*“ im Ausnahmepfad verwenden, um sicherzustellen, dass es Ihre Varianten abdeckt.

Die folgende Tabelle enthält einige Beispielausschlüsse mit Übereinstimmungen, die erfolgreich ausgeschlossen würden, und Nichtübereinstimmungen, die nicht ausgeschlossen werden.

Ausschlussbeispiel	Übereinstimmungen	Nichtübereinstimmungen
`/users/*/temp/*`	• `\users\john\temp` • `\users\jane\temp`	• `\users\folder\john\temp` • `\users\folder\jane\temp` Diese Ordner werden nicht ausgeschlossen, weil die Anzahl der Ordnerebenen nicht übereinstimmt.
`/program files*/app/script*.vbs`	• `\program files(x86)\app\script1.vbs` • `\program files(x64)\app\script2.vbs` • `\program files(x64)\app\script3.vbs`	• `\program files(x86)\app\script.vbs` • `\program files\app\script1.vbs` Diese Ordner werden nicht ausgeschlossen, da die Platzhalter für mindestens ein Zeichen stehen.
`//*example.local/sysvol/script*.vbs`	`\\ad.example.local\sysvol\script1.vbs`	`\\ad.example.local\sysvol\script.vbs` Dieses Skript wird nicht ausgeschlossen, da die Platzhalter für mindestens ein Zeichen stehen.
`/users/*/*/*.vbs`	• `/users/john/temp/script.vbs` • `/users/john/temp/anotherscript.vbs`	• `/users/john/temp1/temp2/script.vbs` Dieses Skript wird nicht ausgeschlossen, weil die Anzahl der Ordnerebenen nicht übereinstimmt.

Prozessausschluss

Sie können der Liste der Skriptsteuerungsausschlüsse Prozesse hinzufügen. Diese Funktion kann nützlich sein, wenn Sie bestimmte Prozesse ausschließen möchten, die Skripte aufrufen. Sie können z. B. SCCM ausschließen, damit es PowerShell-Skripte in einem temporären Verzeichnis starten kann. Ein Prozess ist jeder Prozess, der einen Skript-Interpreter aufruft, um ein Skript auszuführen.

- Das folgende Beispiel ermöglicht es dem myfile.exe-Prozess, einen Interpreter (z. B. PowerShell.exe) zum Ausführen eines Skripts aufzurufen.
  - /windows/*/myfile.exe
- Die folgenden Beispiele fügen der Ausschlussliste „myprocess.exe“ hinzu, sodass sie unabhängig vom Ordnerpfad ausgeführt werden kann:
  - `\myprocess.exe` (auf einem lokalen Windows-Laufwerk)
  - `\\myprocess.exe` (auf einem Windows-Netzlaufwerk)
- Im folgenden Beispiel wird der Ausschlussliste „myprocess.exe“ hinzugefügt, sodass die Ausführung nur über einen bestimmten Ordnerpfad möglich ist:
  - `\directory\child\myprocess.exe` (auf einem lokalen Windows-Laufwerk)
  - `\\directory\child\myprocess.exe` (auf einem Windows-Netzlaufwerk)

Hinweis:

- Absolute Pfade werden für Ausschlüsse nicht unterstützt.
- Vorgänger werden nicht unterstützt.
- Wenn eine ausführbare Datei (exe) zu einem Ausschluss hinzugefügt wird, wird automatisch /[CySc_process]/ zum Ausschluss hinzugefügt. Wenn Sie den obigen Beispielausschluss hinzugefügt haben, wäre das Ergebnis: /[CySc_process]/ /windows/*/myfile.exe.

Alternative Optionen für Ausschlüsse für die Skriptsteuerung

Als alternative Methode zum Ausschließen von Skripts können Sie die globale sichere Liste verwenden oder ein Zertifikat hinzufügen.

- Hinzufügen einer Datei zur globalen CylancePROTECT Desktop-Quarantäneliste oder zur globalen sicheren Liste
  - Diese Methode erfordert einen SHA256-Hash-Wert und geht davon aus, dass sich dieser Wert nicht ändert. Aktualisierungen des Skripts oder vom Skript vorgenommene Änderungen führen dazu, dass sich der Hash-Wert ändert. Daher ist für diese Methode mehr Verwaltungsaufwand erforderlich, wenn das Skript oder Makro häufig aktualisiert oder programmgesteuert geändert wird (z. B. Hinzufügen eines neuen Datums oder einer neuen Uhrzeit, Systemanfragen, Abrufen von Daten). Jedes Mal, wenn der CylancePROTECT Desktop-Agent ein Skript an die Verwaltungskonsole meldet, muss er einen SHA256-Hash-Wert melden. Bei jeder Änderung des Hash-Werts meldet der Agent den neuen Wert und Sie müssen den neuen Wert zur globalen sicheren Liste hinzufügen. Wenn ein Hash-Wert nicht generiert werden kann (z. B. weil das Skript nicht ordnungsgemäß ausgeführt wird, die Datei nicht vorhanden ist oder Berechtigungsprobleme vorliegen), wird ein generischer Hash verwendet, wenn das Skript an die Konsole gemeldet wird.
  - Der folgende SHA256-Hash-Wert ist ein generischer Hash, den der CylancePROTECT Desktop-Agent verwendet, wenn kein Hash für ein Skript generiert werden kann. Wenn Sie versuchen, diesen Wert zur globalen sicheren Liste hinzuzufügen, wird aufgrund der Agentenfunktionalität eine Fehlermeldung angezeigt.
    - `FE9B64DEFD8BF214C7490AA7F35B495A79A95E81F8943EE279DC99998D3D3440`
  - Der folgende SHA256-Hash-Wert ist ein generischer Hash, den der CylancePROTECT Desktop-Agent verwendet, wenn ein einzeiliger PowerShell-Befehl verwendet wird und kein Hash für ein Skript generiert werden kann. Wenn Sie versuchen, diesen Wert zur globalen sicheren Liste hinzuzufügen, wird aufgrund der Agentenfunktionalität eine Fehlermeldung angezeigt.
    - `FE9B64DEFD8BF214C7490BB7F35B495A79A95E81F8943EE279DC99998D3D3440`
- Hinzufügen eines Zertifikats zur globalen sicheren CylancePROTECT Desktop-Liste
  - Diese Methode erfordert, dass Sie ein gültiges Codesignaturzertifikat an die Konsole senden und ist nur für PowerShell- und Active-Skripte (keine Makros) verfügbar.

Gerätesteuerung

Die Gerätesteuerung schützt Geräte durch die Steuerung von USB-Massenspeichergeräten, die mit Geräten im Unternehmen verbunden sind. Wenn Sie die Gerätesteuerung aktivieren, können Sie vollständigen oder schreibgeschützten Zugriff zulassen oder USB-Massenspeichergeräte, wie USB-Flash-Laufwerke, externe Festplatten und Smartphones, blockieren. Als Teil der Richtlinie können Sie auch Ausschlüsse verwenden, um die Zugriffsebene für bestimmte Massenspeichergeräte mithilfe der Anbieter-ID, Produkt-ID und Seriennummer zu definieren. Sie können beispielsweise alle USB-Massenspeichergeräte blockieren, aber Ausnahmen erstellen, um nur den vollen Zugriff auf einige autorisierte Geräte zu ermöglichen.

- Die Gerätesteuerung steht für Windows-Geräte mit Agent-Version 2.1.1410 oder höher und macOS-Geräte mit Agent-Version 3.3.1000 oder höher zur Verfügung.
- Die Gerätesteuerung wirkt sich nicht auf USB-Peripheriegeräte wie Maus oder Tastatur aus. Wenn Sie beispielsweise eine Richtlinie zum Blockieren aller USB-Massenspeicher-Gerätetypen erstellen, kann ein Benutzer weiterhin eine USB-Tastatur verwenden.

- Die Gerätesteuerung wird derzeit für SD-Karten nicht unterstützt. Bei Verwendung mit einem USB-Kartenlesegerät kann die Gerätesteuerung das USB-Gerät jedoch erkennen.

Wenn die Gerätesteuerung aktiviert ist, protokolliert die Gerätesteuerung alle angeschlossenen USB-Massenspeichergeräte zusammen mit der angewendeten Richtlinienaktion (vollständiger Zugriff, schreibgeschützt oder blockieren). Wenn die Richtlinienaktion auf schreibgeschützt oder blockiert eingestellt ist und Desktop-Benachrichtigungen auf dem Gerät aktiviert sind, wird eine Popup-Benachrichtigung auf dem Gerät angezeigt, wenn ein USB-Massenspeichergerät angeschlossen wird. Sie finden das Protokoll der Gerätesteuerungsereignisse in der Konsole auf dem Bildschirm **Schutz > Externe Geräte**.

Einstellung der Gerätesteuerung	Beschreibung
Windows-Gerätesteuerung	Mit dieser Einstellung wird die Gerätesteuerung für Windows-Geräte eingeschaltet, und Sie können die Richtlinie auswählen, die für jeden USB-Gerätetyp angewendet werden soll. Die Ausschlussliste wird von Windows- und macOS-Geräten gemeinsam verwendet, sofern die Gerätesteuerung für beide Betriebssystemplattformen aktiviert ist.
macOS-Gerätesteuerung	Mit dieser Einstellung wird die Gerätesteuerung für macOS-Geräte eingeschaltet, und Sie können die Richtlinie auswählen, die für jeden USB-Gerätetyp angewendet werden soll. Die Ausschlussliste wird von Windows- und macOS-Geräten gemeinsam verwendet, sofern die Gerätesteuerung für beide Betriebssystemplattformen aktiviert ist.

Richtlinienaktion für Gerätesteuerung	Beschreibung
Sperren	Diese Einstellung verhindert, dass das Gerät auf externe USB-Speichergeräte zugreift.
Nur Lesezugriff	Mit dieser Einstellung können Sie den schreibgeschützten Zugriff auf externe USB-Speichergeräte zulassen. Der schreibgeschützte Zugriff ermöglicht es Geräten, den Inhalt eines externen USB-Geräts anzuzeigen, lässt jedoch keinen Schreib- oder Löschzugriff auf das USB-Gerät zu. Die folgenden USB-Gerätetypen können nur für den schreibgeschützten Zugriff für Windows-Geräte konfiguriert werden: • Digitalbild • USB CD/DVD RW • USB-Laufwerk • VMware USB-Passthrough • Tragbares Windows-Gerät Beim Hinzufügen von Ausschlüssen gilt diese Einstellung nur für Windows-Geräte und wird für macOS-Geräte ignoriert.
Vollzugriff	Diese Einstellung ermöglicht den Lese-, Schreib- und Löschzugriff auf externe USB-Speichergeräte.

Unterstützte USB-Gerätetypen	Beschreibung	Agentenplattform
Android	Ein tragbares Gerät mit Android-Betriebssystem, z. B. ein Smartphone oder Tablet. Verbundene Android-Geräte können als Android-, Digitalbild- oder tragbares Windows-Gerät identifiziert werden. Wenn Sie Android-Geräte blockieren möchten, können Sie auch Digitalbild- und tragbare Windows-Geräte blockieren.	Windows
iOS	Ein tragbares Apple-Gerät mit iOS-Betriebssystem, z. B. ein iPhone oder iPad. Einige iOS-Geräte werden nicht geladen, wenn die Gerätesteuerung aktiviert und auf „Sperren“ eingestellt ist, es sei denn, das Gerät ist ausgeschaltet. Die Ladefunktion von Apple ist in den Funktionen des Geräts integriert, die für unsere Geräteblockierfunktion für iOS erforderlich sind. Bei Geräten, die nicht von Apple stammen, wird die Ladefunktion nicht auf diese Weise integriert, sodass diese Geräte nicht beeinträchtigt werden.	Windows
Digitalbild	Dieser Gerätetyp umfasst Scanner, Digitalkameras, Multimode-Videokameras mit Bilderfassung und Framegrabber. **Hinweis:** Canon-Kameras erkennt der Agent nicht als Digitalbildgeräte, sondern als tragbare Windows-Geräte.	Windows
USB CD DVD RW	Hierbei handelt es sich um ein optisches USB-Laufwerk.	Windows, macOS
USB-Laufwerk	Hierbei handelt es sich um eine USB-Festplatte oder ein USB-Flash-Laufwerk.	Windows, macOS
VMware USB-Passthrough	Ein VMware-Client einer virtuellen Maschine, der über USB-Geräte mit dem Host verbunden ist.	Windows
Tragbares Windows-Gerät	Tragbare Geräte, die die Microsoft Windows-Treibertechnologie für tragbare Geräte (WPD) verwenden, z. B. Mobiltelefone, Digitalkameras und tragbare Media-Player.	Windows

Hinzufügen externer Speicherausschlüsse

Sie können Ausschlüsse für externe USB-Massenspeichergeräte hinzufügen, wenn Sie Zugriffsberechtigungen für bestimmte Speichergeräte festlegen möchten. Wenn Sie der Richtlinie für die Gerätesteuerung Ausschlüsse hinzufügen, benötigen Sie die Anbieter-ID des Geräts. Die Produkt-ID und die Seriennummer sind optional und können ebenfalls verwendet werden, wenn Sie den Ausschluss genauer definieren möchten. Um sicherzustellen,

dass Sie die richtigen Informationen für jeden Ausschluss verwenden, können Sie die Gerätesteuerung aktivieren, dann ein Gerät einfügen und den zugehörigen Protokolleintrag in der Konsole suchen (**Schutz > Externe Geräte**).

Beachten Sie Folgendes, wenn Sie externe Speicherausschlüsse hinzufügen:

- Nicht alle Hersteller verwenden eine Seriennummer für ihre Produkte. Einige Hersteller verwenden dieselbe Seriennummer auch für mehrere Produkte.
- Externe Speicherausschlüsse können nicht bearbeitet werden. Fügen Sie bei Bedarf neue Ausschlüsse hinzu und löschen Sie alle Ausschlüsse, die nicht mehr benötigt werden.
- Für jede Gerätesteuerungsrichtlinie gilt eine Grenze von 5.000 Ausschlüssen. Die Schaltfläche **Gerät hinzufügen** wird deaktiviert, wenn dieser Grenzwert erreicht ist.
- Die Ausschlussliste wird von Windows- und macOS-Geräten gemeinsam verwendet, sofern die Gerätesteuerung für beide Betriebssystemplattformen aktiviert ist.

1. Navigieren Sie in der Konsole zu **Einstellungen > Geräterichtlinie**.
2. Erstellen Sie eine neue Richtlinie oder bearbeiten Sie eine vorhandene Richtlinie.
3. Klicken Sie auf die Registerkarte **Gerätesteuerung**, und stellen Sie sicher, dass die Gerätesteuerung aktiviert und konfiguriert ist.
4. Klicken Sie unter **Ausschlussliste für externen Speicher** auf **Gerät hinzufügen**.
5. Geben Sie die **Anbieter-ID** ein.
6. Geben Sie optional die **Produkt-ID** und die **Seriennummer** an, um den Ausschluss weiter einzugrenzen. Sie können auch einen Kommentar zur Ausschlussbeschreibung hinzufügen.
7. Wählen Sie im Feld **Zugriff** die Zugriffsebene aus, die Sie zuweisen möchten:
   - **Vollzugriff**
   - **Nur Lesezugriff**

     Diese Einstellung gilt nur für Windows-Geräte und wird bei macOS-Geräten ignoriert.
   - **Sperren**
8. Klicken Sie auf **Senden**.
9. Speichern (oder erstellen) Sie die Richtlinie.

Massenimport von Gerätesteuerungsausschlüssen

Administratoren können mithilfe einer CSV-Datei den Massenimport von Gerätesteuerungsausschlüssen durchführen. Pro Datei sind bis zu 500 Ausschlüsse zulässig. Weitere Informationen zu den Formatierungsanforderungen und zum Herunterladen einer Beispielvorlage finden Sie unter support.blackberry.com in KB 65484.

CSV-Vorlage für den Gerätesteuerungsausschluss herunterladen

1. Aktivieren Sie auf der Registerkarte **Gerätesteuerung** einer Geräterichtlinie die Option „Gerätesteuerung“.
2. Klicken Sie auf **Ausschluss importieren**.
3. Klicken Sie auf **Unsere Vorlage herunterladen** und speichern Sie die Datei.
4. Ändern Sie die Vorlage entsprechend den Formatierungsanforderungen.

CSV-Datei mit den Gerätesteuerungsausschlüssen importieren

1. Aktivieren Sie auf der Registerkarte **Gerätesteuerung** einer Geräterichtlinie die Option „Gerätesteuerung“.
2. Klicken Sie auf **Ausschluss importieren**.
3. Klicken Sie auf **Nach CSV-Datei zum Importieren suchen** und wählen Sie die CSV-Datei aus, die Sie importieren möchten.

4. Klicken Sie auf **Hochladen**.

Formatierungsanforderungen der CSV-Datei

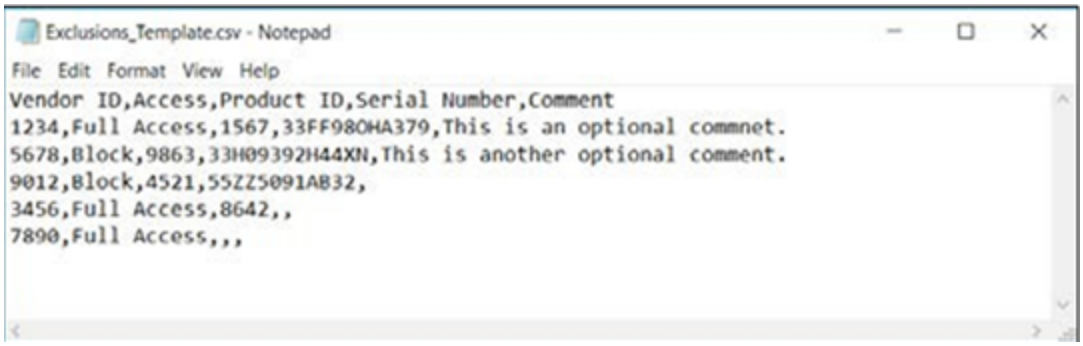
- Es werden nur CSV-Dateien akzeptiert.
- Die CSV-Datei muss entsprechende Kopfzeileninformationen für jede Spalte enthalten. Die Importfunktion ignoriert die erste Zeile der CSV-Datei. Wenn die erste Zeile der Importdatei ein Ausschluss ist, wird sie nicht importiert. Die Spaltenüberschriften müssen in der folgenden Reihenfolge angeordnet sein:
  - Anbieter-ID
  - Zugriff
  - Produkt-ID
  - Seriennummer
  - Kommentar
- Für jeden Ausschluss sind die Felder „Anbieter-ID“ und „Zugriff“ erforderlich.
- Die Felder „Produkt-ID“, „Seriennummer“ und „Kommentar“ sind für jeden Ausschluss optional.
- Die Spalte „Zugriff“ erfordert entweder `Full Access` (Vollzugriff), `Read Only` (Schreibgeschützt) oder `Block` (Sperren) als Wert und akzeptiert die Werte nur in englischer Sprache.
- Die Spalte „Kommentare“ unterstützt keine Kommas (,).

Beispiel: Massenimport mit einer Tabelle

	A	B	C	D	E	F
1	Vendor ID	Access	Product ID	Serial Number	Comment	
2	1234	Full Access	1567	33FF98OHA379	This is an optional commnet.	
3	5678	Block	9863	33H09392H44XN	This is another optional comment.	
4	9012	Block	4521	55ZZ5091AB32		
5	3456	Full Access	8642			
6	7890	Full Access				
7						
8						
9						
10						
11						

Exclusions_Template

Beispiel: Massenimport mit einem Texteditor



Einschränkungen

- Die maximale Anzahl von Ausschlüssen pro CSV-Datei beträgt 500. Wenn Sie versuchen, eine Datei zu importieren, die mehr als 500 Ausschlüsse enthält, wird eine Fehlermeldung angezeigt.

- Die maximale Anzahl der Gerätesteuerungsausschlüsse pro Richtlinie beträgt 5.000. Wenn diese Anzahl überschritten wird, sollte eine Warnmeldung angezeigt werden.
- Wenn Sie ein Gerät verwenden, dessen Sprache nicht auf Englisch eingestellt ist, müssen Sie die Optionen möglicherweise auf UTF-8 und durch Komma getrennt setzen, wenn Sie die Vorlage importieren und mit Microsoft Excel bearbeiten. Wenn Sie die Datei öffnen, ohne die Optionen zu ändern, werden möglicherweise nicht erkennbare Zeichen angezeigt.

Installieren des CylancePROTECT Desktop-Agenten für Windows

CylancePROTECT Desktop erkennt und blockiert Malware, bevor diese Geräte beeinträchtigen kann. BlackBerry verwendet einen mathematischen Ansatz zur Malware-Identifizierung, wobei maschinelles Lernen anstelle von reaktiven Signaturen, vertrauensbasierten Systemen oder Sandboxes verwendet wird. Dieser Ansatz macht neue Malware, Viren, Bots und zukünftige Varianten unschädlich. CylancePROTECT Desktop analysiert potenzielle Dateiausführungen auf Malware in den Betriebssystem- und Speicherschichten, um die Bereitstellung schädlicher Payloads zu verhindern.

Sie können den Agenten auf einzelnen Geräten installieren oder ihn unter Verwendung der Installationsparameter mithilfe eines Bereitstellungstools in Ihrer gesamten Umgebung bereitstellen.

Installieren des Windows-Agenten

Bevor Sie beginnen:

- Laden Sie die CylancePROTECT Desktop-Installationsdateien von der Verwaltungskonsole herunter. Klicken Sie auf **Einstellungen > Bereitstellungen**. Wählen Sie in der Dropdown-Liste **Produkt** die Option **CylancePROTECT** aus und legen Sie das Zielbetriebssystem, die Agentenversion und den Dateityp fest. Klicken Sie auf **Download**.
- Kopieren Sie in der Verwaltungskonsole über **Einstellungen > Anwendung** das Installationstoken.

1. Doppelklicken Sie auf das CylancePROTECT Desktop-Installationsprogramm.
2. Klicken Sie im CylancePROTECT Desktop-Einrichtungsfenster auf **Installieren**.
3. Geben Sie das Installationstoken ein und klicken Sie auf **Weiter**.
4. Optional können Sie den Zielordner ändern.
5. Klicken Sie auf **OK**, um mit der Installation zu beginnen.
6. Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen. Stellen Sie sicher, dass das Kontrollkästchen zum Starten von CylancePROTECT Desktop ausgewählt ist.

Wenn Sie fertig sind: Wenn der Speicherschutz, die Skriptsteuerung und/oder die Gerätesteuerung in der Geräterichtlinie aktiviert sind, wird ein Neustart des Geräts nach der Installation oder Aktualisierung des Agenten empfohlen, ist aber nicht unbedingt erforderlich. Ein Neustart stellt sicher, dass alle neuen Richtlinieneinstellungen vollständig wirksam wurden.

Windows-Installationsparameter

Der Agent kann interaktiv oder nicht interaktiv über GPO, Microsoft System Center Configuration Manager (SCCM), MSIEXEC und andere Tools von Drittanbietern installiert werden. Die MSI-Dateien können mit integrierten Parametern angepasst werden (siehe unten), die Parameter können aber auch über die Befehlszeile eingegeben werden.

Parameter	Wert	Beschreibung
PIDKEY	*<Installation Token>*	Dieser Parameter gibt das Installationstoken automatisch ein.
LAUNCHAPP	0 oder 1	0: Bei diesem Wert werden das Taskleistensymbol und der Startmenüordner zur Laufzeit ausgeblendet. 1: Bei diesem Wert werden das Taskleistensymbol und der Startmenüordner zur Laufzeit angezeigt. Wenn kein Wert eingegeben wird, ist der Standardwert 1.
SELFPROTECTIONLEVEL	1 oder 2	1: Bei diesem Wert können nur lokale Administratoren Änderungen an der Registrierung und den Diensten vornehmen. 2: Bei diesem Wert kann nur der Systemadministrator Änderungen an der Registrierung und den Diensten vornehmen. Wenn kein Wert eingegeben wird, ist der Standardwert 2.
APPFOLDER	*<Target Installation Folder>*	Dieser Parameter gibt das Agent-Installationsverzeichnis an. Der Standardspeicherort lautet „C:\Program Files\Cylance\Desktop“.

Parameter	Wert	Beschreibung

REGWSC	0 oder 1	0: Dieser Wert gibt an, dass CylancePROTECT Desktop bei Windows nicht als Antivirenprogramm registriert ist. Das ermöglicht die gleichzeitige Ausführung von CylancePROTECT Desktop und Windows Defender auf dem Gerät.
		
		1: Dieser Wert gibt an, dass CylancePROTECT Desktop bei Windows als Antivirenprogramm registriert ist.
		
		Wenn kein Wert eingegeben wird, ist der Standardwert 1.
		
		Die obigen Befehle haben keine Auswirkung auf Windows Server 2016 und 2019. Um Windows Defender nach der Installation von CylancePROTECT Desktop unter Windows Server 2016 und 2019 zu deaktivieren, legen Sie den folgenden Registrierungswert fest:
		
		`HKLM\SOFTWARE\Policies\Microsoft \Windows Defender\DisableAntiSpyware`
		
		`REG_DWORD`
		
		`Value = 1`
		
		Wenn der Windows Defender-Unterschlüssel nicht vorhanden ist, müssen Sie ihn manuell erstellen.
		
		Weitere Informationen zur Verwaltung von Windows Defender über Gruppenrichtlinien finden Sie unter Verwenden von Gruppenrichtlinieneinstellungen zum Konfigurieren und Verwalten von Windows Defender AV.

VENUEZONE	"*<Zone_Name>*"	Verwenden Sie diesen Parameter, um den Namen einer Zone anzugeben, der Sie Geräte hinzufügen möchten. Wenn keine Zone mit diesem Namen gefunden wird, wird eine Zone mit dem angegebenen Namen erstellt. Zonennamen dürfen keine Leerzeichen, Tabulatoren, Wagenrückläufe, Gleichheitszeichen, Zeilenumbrüche oder andere unsichtbare Zeichen enthalten.

Parameter	Wert	Beschreibung
VDI	<X>	Wenn Sie CylancePROTECT Desktop auf einem Master-Image installieren, verwenden Sie den Installationsparameter VDI=<*X*>, wobei <*X*> ein „Zähler“ für die Gesamtzahl der Maschinen oder Images ist, die nicht mit der Domäne verbunden sind (einschließlich des Master-Images), bevor Sie einen Pool von Arbeitsstationen erstellen. Der Wert für <*X*> legt fest, wann der Agent die virtuelle Maschine mithilfe von VDI-Fingerprinting anstelle des standardmäßigen Agent-Fingerprinting-Mechanismus identifizieren soll. Für den VDI-Parameter, der eine verzögerte Wirkung hat, wird ein Zähler „X“ verwendet, während der AD-Parameter sofort bei der Installation wirkt. Weitere Informationen finden Sie unter Anforderungen und Überlegungen für die Verwendung von CylancePROTECT Desktop auf virtuellen Maschinen.
AD	1	Dieser Parameter erfordert Agent-Version 1520 oder höher. Verwenden Sie während der Erstinstallation den Active Directory-Parameter (AD) auf einem mit der Domäne verbundenen Master-Image. Bei der Installation auf einem mit einer Domäne verbundenen Master-Image wird sofort VDI-Fingerprinting auf dem Master-Image verwendet und anschließend ein Pool von Arbeitsstationen erstellt. AD-Fingerprinting hat Vorrang vor dem Installationsparameter VDI=<*X*>. Weitere Informationen finden Sie unter Anforderungen und Überlegungen für die Verwendung von CylancePROTECT Desktop auf virtuellen Maschinen.
PROXY_SERVER	<*ip_address*>:<*port_ number*>	Dieser Parameter gibt die IP-Adresse des Proxyservers an, über den der Agent kommunizieren muss. Proxyserver-Einstellungen werden der Geräteregistrierung hinzugefügt. Sie finden die Proxyserver-Informationen in der Protokolldatei des Agenten.

Parameter	Wert	Beschreibung
AWS	1	Dieser Parameter erfordert Agent-Version 1500 oder höher. Erfassen Sie mit diesem Parameter die Amazon EC2-Instanz-ID im Feld „Gerätename“, um Amazon Cloud-Hosts besser identifizieren zu können. Der Gerätename wird geändert und enthält Hostname und Instanz-ID. Wenn der Gerätename beispielsweise ABC-DE-12345678 und die AWS EC2-ID i-0a1b2cd34efg56789 lautet, lautet der vollständige Gerätename ABC-DE-123456789_i-0a1b2cd34efg56789. Diese Funktion ist nur für die Amazon EC2-Instanz-ID verfügbar.
PROTECTTEMPPATH	1	Dieser Parameter erfordert Agent-Version 1480 oder höher. Verwenden Sie diesen Parameter, um den Speicherort der Ordner „CylanceDesktopArchive“ und „CylanceDesktopRemoteFile“ in den Ordner „Cylance ProgramData“ zu ändern. Weitere Informationen finden Sie in KB 66457 Ändern des Speicherorts der Ordner „CylanceDesktopArchive“ und „CylanceDesktopRemoteFile“.

Beispiel: Parameter PIDKEY, APPFOLDER und LAUNCHAPP

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

In diesem Beispiel wird die Installation im Hintergrund ausgeführt und das Installationsprotokoll wird im Ordner `C:\temp` gespeichert. Möglicherweise müssen Sie diesen Ordner erstellen. Wenn der Agent ausgeführt wird, werden sowohl das Taskleistensymbol als auch der Cylance-Ordner im Startmenü ausgeblendet. Weitere Informationen zu zulässigen Befehlszeilenoptionen finden Sie unter https://docs.microsoft.com/en-us/windows/win32/msi/command-line-options.

Beispiel: Parameter PIDKEY, VDI und LAUNCHAPP

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

In diesem Beispiel entspricht die „2“ für VDI der Gesamtzahl der Geräte oder Images, die nicht mit der Domäne verbunden sind (Master-Image plus zusätzliches oder übergeordnetes Image), bevor der Pool von Arbeitsstationen erstellt wird.

Beispiel: Parameter PIDKEY, AD und LAUNCHAPP

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

In diesem Beispiel verwendet der AD-Parameter sofort VDI-Fingerprinting auf dem Master-Image und dem Pool von Arbeitsstationen, der erstellt wird. Weitere Informationen zum Bearbeiten der MSI-Installationsdatei für die Bereitstellung über Gruppenrichtlinien finden Sie in KB 66391 Bearbeiten des MSI-Installationsprogramms mit Orca.

Installieren des CylancePROTECT Desktop-Agenten für macOS

CylancePROTECT Desktop erkennt und blockiert Malware, bevor diese Geräte beeinträchtigen kann. BlackBerry verwendet einen mathematischen Ansatz zur Malware-Identifizierung, wobei maschinelles Lernen anstelle von reaktiven Signaturen, vertrauensbasierten Systemen oder Sandboxes verwendet wird. Dieser Ansatz macht neue Malware, Viren, Bots und zukünftige Varianten unschädlich. CylancePROTECT Desktop analysiert potenzielle Dateiausführungen auf Malware in den Betriebssystem- und Speicherschichten, um die Bereitstellung schädlicher Payloads zu verhindern.

Sie können den Agenten auf einzelnen Geräten installieren oder ihn unter Verwendung der Installationsparameter mithilfe eines Bereitstellungstools in Ihrer gesamten Umgebung bereitstellen.

Installieren des CylancePROTECT Desktop-Agenten für macOS

Bevor Sie beginnen:

- Laden Sie die CylancePROTECT Desktop-Installationsdateien von der Verwaltungskonsole herunter. Klicken Sie auf **Einstellungen > Bereitstellungen**. Wählen Sie in der Dropdown-Liste **Produkt** die Option **CylancePROTECT** aus und legen Sie das Zielbetriebssystem, die Agentenversion und den Dateityp fest. Klicken Sie auf **Download**.
- Kopieren Sie in der Verwaltungskonsole über **Einstellungen > Anwendung** das Installationstoken.

1. Doppelklicken Sie auf die CylancePROTECT Desktop-Installationsdatei (Endung .dmg oder .pkg), um das Installationsprogramm bereitzustellen.
2. Doppelklicken Sie auf  in der Benutzeroberfläche von CylancePROTECT Desktop, um mit der Installation zu beginnen.
3. Klicken Sie auf **Fortfahren**, um zu überprüfen, ob Betriebssystem und Hardware die Anforderungen erfüllen.
4. Klicken Sie auf **Fortfahren**.
5. Geben Sie das Installationstoken ein.
6. Klicken Sie auf **Fortfahren**.
7. Ändern Sie optional das Installationsverzeichnis.
8. Klicken Sie auf **Installieren**.
9. Geben Sie Ihre Anmeldeinformationen ein.
10. Klicken Sie auf **Software installieren**.
11. Klicken Sie auf dem Zusammenfassungsbildschirm auf **Schließen**.
12. Klicken Sie auf **OK > Fertigstellen**.
13. Wenn Sie CylancePROTECT Desktop unter macOS Catalina installieren, werden Sie in einer Benachrichtigung aufgefordert, CylanceUI die Anzeige von Benachrichtigungen zu erlauben. Klicken Sie auf **Zulassen**.

CylancePROTECT Desktop-Konfigurationsanforderungen für macOS und höher

Um die CylancePROTECT Desktop-Agent-Version 2.1 oder höher auf Geräten mit macOS zu installieren, beachten Sie bitte die folgenden Konfigurationsanforderungen. Die Anforderungen hängen davon ab, ob Geräte von einer MDM-Lösung verwaltet werden (z. B. Jamf Pro).

Mit MDM verwaltete Geräte

Die folgenden Informationen beziehen sich auf Jamf Pro als MDM-Lösung, sind aber auch auf andere MDM-Lösungen anwendbar.

Anforderungen	Schritte
Allgemeine Einstellungen	Erstellen Sie ein Konfigurationsprofil und geben Sie auf der Registerkarte „Allgemein“ die folgenden Einstellungen an: • Geben Sie einen Namen und eine Beschreibung für das Profil an. • Ebene: Computerebene • Verteilungsmethode: Automatisch installieren
Aktivieren der CylancePROTECT-Kernelerweiterung. (nur macOS 10)	Konfigurieren Sie die folgenden Einstellungen über die Option „Genehmigte Kernel-Erweiterungen“: • Anzeigename: Cylance • Team-ID: 6ENJ69K633 • Überprüfen Sie auf der Registerkarte **Geltungsbereich**, ob das Konfigurationsprofil für macOS 10-Geräte Gültigkeit hat, auf denen CylancePROTECT Desktop und CylanceOPTICS ausgeführt werden.
Aktivieren der CylancePROTECT-Systemerweiterung (macOS 11+)	Konfigurieren Sie die folgenden Einstellungen über die Option „Systemerweiterungen“: • Anzeigename: CylanceSystemExtension • Systemerweiterungstypen: Zulässige Systemerweiterungen • Teamkennung: 6ENJ69K633 • Zulässige Systemerweiterungen: com.cylance.CylanceEndpointSecurity.extension

Anforderungen	Schritte
Aktivieren Sie den vollständigen Datenträgerzugriff für den CylancePROTECT-Agenten und die Systemerweiterungen.	Sie können die folgenden Einstellungen über die Option „Datenschutzeinstellungen Richtliniensteuerung“ aktivieren. Fügen Sie eine App-Zugriffskonfiguration hinzu und legen Sie die folgenden Einstellungen fest: • Kennung: com.cylance.Agent • Kennungstyp: Bundle-ID • Code-Anforderung: Kopieren Sie die Code-Anforderung aus der HTML-Version dieses Themas. Die Code-Anforderung sollte sich in einer Zeile befinden und keine zusätzlichen Leerzeichen oder Zeilenumbrüche enthalten. • Fügen Sie den Dienst **SystemPolicyAllFiles** hinzu und setzen Sie ihn auf **Zulassen**. Fügen Sie eine weitere Konfiguration für den App-Zugriff hinzu und legen Sie die folgenden Einstellungen fest: • Kennung: com.cylance.CylanceEndpointSecurity.extension • Kennungstyp: Bundle-ID • Code-Anforderung: Kopieren Sie die Code-Anforderung aus der HTML-Version dieses Themas. Die Code-Anforderung sollte sich in einer Zeile befinden und keine zusätzlichen Leerzeichen oder Zeilenumbrüche enthalten. • Fügen Sie den Dienst **SystemPolicyAllFiles** hinzu und setzen Sie ihn auf **Zulassen**.
Benachrichtigungen	Auf der Registerkarte „Benachrichtigungen“ des Konfigurationsprofils werden die folgenden Einstellungen empfohlen: • Kritische Warnungen: Aktiviert • Benachrichtigungen: Aktiviert • Banner-Warnungstyp: Dauerhaft • Benachrichtigungen auf Sperrbildschirm: Werden angezeigt • Benachrichtigungen in Mitteilungszentrale: Werden angezeigt • Symbol für Badge-App: Wird angezeigt • Ton für Benachrichtigungen wiedergeben: Aktiviert
Umfang	Konfigurieren Sie die folgenden Einstellungen auf der Registerkarte „Geltungsbereich“: • Stellen Sie sicher, dass das Konfigurationsprofil für macOS-Geräte, auf denen CylancePROTECT Desktop ausgeführt wird, Gültigkeit hat.
Neustart nach Installation	Starten Sie das Gerät neu, nachdem Sie die oben beschriebenen Konfigurationsschritte ausgeführt und den CylancePROTECT Desktop-Agenten installiert haben.

Nicht mit MDM verwaltete Geräte

Auf Geräten, die nicht mit MDM verwaltet werden, erhält der Benutzer nach der Installation des macOS-Agenten auf dem Gerät die Aufforderung, die „CylanceES-Systemerweiterung“ zu genehmigen. Befolgen Sie die Anweisungen in der Eingabeaufforderung, um die Systemerweiterung zu aktivieren und vollen Datenträgerzugriff zu ermöglichen. Benutzer können auch auf die Benachrichtigung von „CylanceUI“ tippen, um die Benachrichtigungseinstellungen zu konfigurieren.

1. Klicken Sie auf **Sicherheitseinstellungen öffnen**. Daraufhin wird die Registerkarte **Systemeinstellungen** > **Sicherheit und Datenschutz** > **Allgemein** geöffnet.
2. Klicken Sie bei Bedarf auf das Schloss, um die Änderungen zu authentifizieren, und klicken Sie auf **Zulassen**.
3. Klicken Sie neben der Meldung **Laden der Systemsoftware für Anwendung 'CylanceES' wurde gesperrt** auf **Zulassen**, um die Erweiterung zu genehmigen.
4. Um den vollständigen Datenträgerzugriff zu aktivieren, navigieren Sie auf dem Gerät zu **Systemeinstellungen** > **Sicherheit und Datenschutz** > Registerkarte **Datenschutz**.
5. Klicken Sie bei Bedarf auf das Schloss, um die Änderungen zu authentifizieren, und klicken Sie auf **Zulassen**.
6. Scrollen Sie nach unten und klicken Sie auf **Voller Datenträgerzugriff**.
7. Wählen Sie **CylanceEsExtension** aus.
8. Lassen Sie Benachrichtigungen für den Agenten über **Systemeinstellungen** > **Benachrichtigungen** > Registerkarte **CylanceUI** zu.

Befehle zum Installieren des macOS-Agenten über die Befehlszeile

Wenn Sie die Befehlszeile zum Installieren des macOS-Agenten verwenden, müssen Sie eine `cyagent_ install_token`-Datei erstellen, die die Installationsparameter enthält. Die Datei enthält das Installationstoken sowie weitere optionale Parameter, die Sie festlegen können.

In den folgenden Abschnitten finden Sie Beispiele, wie Sie die Datei über die Befehlszeile erstellen. Sie können die Datei jedoch auch über einen Texteditor erstellen, der jeden Parameter in eine eigene Zeile aufnimmt. Diese Datei muss sich im gleichen Ordner wie das Installationspaket befinden.

Installieren des macOS-Agenten nur mit Installationstoken

Über die folgenden Beispielbefehle im Terminal können Sie die Datei `cyagent_ install_token`mit dem Installationstoken erstellen und den Agenten installieren. Wenn Sie das .dmg-Installationsprogramm verwenden, ändern Sie die Dateierweiterung im Befehl entsprechend.

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

Im Folgenden finden Sie den Installationsbefehl ohne das Installationstoken:

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

Installieren des macOS-Agenten mit den angegebenen Parametern

Verwenden Sie die folgenden Beispielbefehle im Terminal, um die Datei `cyagent_ install_token`mit den angegebenen Parametern zu erstellen und den Agent zu installieren. Wenn Sie das .dmg-Installationsprogramm verwenden, ändern Sie die Dateierweiterung im Befehl entsprechend.

```
echo
```

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

Installationsparameter

Der CylancePROTECT Desktop-Agent kann über die Befehlszeilenoptionen in einem Terminal installiert werden.

Parameter	Wert	Beschreibung
`InstallToken`	*<Installationstoken>*	Das Installationstoken ist erforderlich, wenn Sie den Agenten installieren. Sie finden es in der Verwaltungskonsole, indem Sie auf **Einstellungen > Anwendung**klicken.
`NoCylanceUI`		Dieser Parameter blendet die Taskleiste beim Start aus.
`SelfProtectionLevel`	1 oder 2	1: Bei diesem Wert können nur lokale Administratoren Änderungen an der Registrierung und den Diensten vornehmen. 2: Bei diesem Wert kann nur der Systemadministrator Änderungen an der Registrierung und den Diensten vornehmen. Wenn kein Wert festgelegt wird, ist der Standardwert 2.
`LogLevel`	0, 1, 2 oder 3	0: Dieser Wert gibt an, dass nur Fehlermeldungen protokolliert werden. 1: Dieser Wert gibt an, dass Fehler- und Warnmeldungen protokolliert werden. 2: Dieser Wert gibt an, dass Fehler-, Warn- und Informationsmeldungen protokolliert wurden. 3: Dieser Wert aktiviert die ausführliche Protokollierung, bei der alle Meldungen protokolliert werden. Beachten Sie jedoch, dass ausführliche Protokolldateien sehr groß werden können. BlackBerryempfiehlt daher, die ausführliche Protokollierung während der Fehlerbehebung zu aktivieren und nach dem Abschluss der Fehlerbehebung den Wert wieder auf „2“ zu ändern. Wenn kein Wert festgelegt wird, ist der Standardwert 2.
`VenueZone`	*<Zonenname>*	Verwenden Sie diesen Parameter, um Geräte zu einer vorhandenen Zone oder zu einer Zone hinzuzufügen, die Sie erstellen möchten. Wenn die Zone nicht vorhanden ist, wird sie mit dem eingegebenen Namen erstellt. Tabulatoren, Zeilenumbrüche, Zeilenvorschübe, Gleichheitszeichen, Leerzeichen oder andere unsichtbare Zeichen sind im Zonennamen nicht zulässig. Dieser Parameter erfordert Agent-Version 1380 oder höher.

Parameter	Wert	Beschreibung
`ProxyServer`	*<IP-Adresse>*:*<Port-Nummer>*	Dadurch werden Proxyserver-Einstellungen zur Geräteregistrierung hinzugefügt. Die Proxyserver-Informationen finden Sie in der Agent-Protokolldatei. Dieser Parameter erfordert Agent-Version 1470 oder höher.

Fehlerbehebung bei macOS-Installationen

In der folgenden Tabelle sind die Maßnahmen aufgeführt, die Sie zur Fehlerbehebung bei macOS-Installationen ergreifen können.

Problem	Aktion

Fehlerbehebung mit Installationstoken und ausführlicher Installationsprogrammprotokollierung	Geben Sie die folgenden Befehle ein und ersetzen Sie „IHRINSTALLTOKEN“ durch das Installationstoken auf der Registerkarte **Einstellungen > Anwendung** der Verwaltungskonsole:
	`echo IHRINSTALLATIONSTOKEN >cyagent_install_token`
	`sudo installer -verboseR -dumplog -pkg CylancePROTECT.pkg -target /`
	Der Echo-Befehl gibt eine `cyagent_install_token`-Datei aus, bei der es sich um eine Textdatei mit einer Installationsoption pro Zeile handelt. Diese Datei muss sich im gleichen Ordner wie das `CylancePROTECT.pkg`-Installationspaket befinden.
	Wenn Sie den CylancePROTECT Desktop-Agenten über Terminal auf macOS Catalina installieren, wird manchmal eine DYLD-Warnung angezeigt. Diese Warnung wirkt sich nicht auf die Installation aus, da sie vom Betriebssystem und nicht von CylancePROTECT Desktop generiert wird.

Starten oder Stoppen des macOS-Agent-Dienstes	Um den Agent-Dienst zu starten, führen Sie den folgenden Befehl aus: `sudo launchctl load /Library/launchdaemons/com.cylance.agent_service.plist` Um den Agent-Dienst zu stoppen, führen Sie den folgenden Befehl aus: `sudo launchctl load /Library/launchdaemons/com.cylance.agent_service.plist`

Problem	Aktion
Unterstützung der Endpoint Security-Systemerweiterung auf macOS Big Sur	BlackBerry empfiehlt, MDM für die Bereitstellung eines Konfigurationsprofils zu verwenden, das die Genehmigung und den vollständigen Festplattenzugriff für die CylancePROTECT Desktop-Systemerweiterung enthält. macOS Big Sur unterstützt standardmäßig keine Remote-Installationen im Hintergrund von MDM-Profilen auf einem System mit einer Neuinstallation des Big Sur-Betriebssystems. Um Konfigurationsprofile auf macOS-Remote-Systemen ohne Benutzerinteraktion (Installation im Hintergrund) zu installieren, ist Apple Mobile Device Management (MDM) erforderlich. Vor dem Upgrade auf macOS Big Sur sollten die Geräte bei einem MDM-Anbieter registriert werden. Geräte, die vor dem Upgrade nicht registriert worden sind, erfordern eine Benutzerinteraktion mit Administratorrechten. Zur Unterstützung von Remote-Installationen im Hintergrund gehen Sie wie folgt vor: **1.** Installieren Sie macOS Catalina. **2.** Wenden Sie das MDM-Profil an. **3.** Laden Sie die Konfigurationsprofile auf das Gerät herunter. **4.** Führen Sie ein Upgrade des Geräts auf macOS Big Sur durch. Die CylancePROTECT Desktop-Agentenversionen und die Erweiterungstypen, die sie unterstützen, lauten wie folgt: • Die CylancePROTECT Desktop-Agentenversion 1570 oder niedriger enthält die Kernel-Erweiterung, die unter macOS Catalina oder niedriger unterstützt wird. • Die CylancePROTECT Desktop-Agentenversion 1580 und höher umfasst die Kernel-Erweiterung, die unter macOS Catalina oder niedriger unterstützt wird, und die Endpoint Security-Systemerweiterung, die unter macOS Big Sur und höher unterstützt wird.

Installieren des CylancePROTECT Desktop-Agenten für Linux

Der Agent kann direkt auf jedem System oder über eine Systemverwaltungssoftware wie Ansible, SCCM oder cloud-init installiert werden. Bei der Installation des Agenten werden Installationsparameter für die Konfiguration einiger Installationseinstellungen bereitgestellt.

Stellen Sie sicher, dass die Zielgeräte die Systemanforderungen erfüllen und dass Sie über die richtigen Berechtigungen für die Installation der Software verfügen.

- Lesen Sie die CylancePROTECT Desktop-Anforderungen.
- Für die Installation des Linux-Agenten ist die Root-Berechtigung erforderlich.
- Erstellen einer Konfigurationsdatei für die Installation des Linux-Agenten

Stellen Sie nach der Installation des CylancePROTECT Desktop-Agenten auf Linux-Geräten sicher, dass die Linux Treiber aktualisiert sind, um die neuesten Kernel auf den Systemen zu unterstützen. Aktualisierte Treiberpakete werden regelmäßig und unabhängig von den Agent-Releases veröffentlicht. Weitere Informationen finden Sie unter Update des Linux-Treibers.

Installationspaket für den Linux-Agenten

Ab Agent-Version 2.1.1590 sind der CylancePROTECT Desktop-Agent, die Agent-UI und die Treiberpakete in einer komprimierten .tgz-Datei enthalten.

Debian-Paket	Komponente
cylance-protect-driver	Proprietärer Treiber
cylance-protect-open-driver	Offener Treiber
cylance-protect	CylancePROTECT Desktop-Agent/Dienst
cylance-protect-ui	CylancePROTECT Desktop-UI

RPM-Paket	Komponente
CylancePROTECTDriver	Proprietärer Treiber
CylancePROTECTOpenDriver	Offener Treiber
CylancePROTECT	CylancePROTECT Desktop-Agent/Dienst
CylancePROTECTUI	CylancePROTECT Desktop-UI

Linux-Installationsvoraussetzungen

Der Agent kann direkt auf jedem System oder über eine Systemverwaltungssoftware wie Ansible, SCCM oder cloud-init installiert werden. Bei der Installation des Agenten werden Installationsparameter für die Konfiguration einiger Installationseinstellungen bereitgestellt.

Stellen Sie sicher, dass die Zielgeräte die Systemanforderungen erfüllen und dass Sie über die richtigen Anmeldeinformationen für die Installation der Software verfügen.

- Anforderungen: CylancePROTECT Desktop
- Für die Installation des Linux-Agenten ist die Root-Berechtigung erforderlich.

Erstellen einer Konfigurationsdatei für die Installation des Linux-Agenten

Bevor Sie den CylancePROTECT Desktop-Agenten auf Linux-Geräten installieren, müssen Sie eine Konfigurationsdatei erstellen, mit der Sie das Gerät bei Ihrem Cylance Endpoint Security-Mandanten registrieren und lokale Agenteneinstellungen festlegen. Nach der Installation des Agenten wird die Konfigurationsdatei vom Gerät entfernt.

CylancePROTECT Desktop verlangt, dass `config_defaults.txt` nur Zeilenvorschub als Zeilenende enthält. Wenn Sie die Datei auf einem DOS/Windows-Computer erstellen, enthält das Zeilenende Zeilenumbruch und Zeilenvorschub. Anweisungen zum Konvertieren der Datei config_defaults.txt in ein geeignetes Format finden Sie unter support.blackberry.com/community im Artikel 65749.

1. Erstellen Sie im Verzeichnis `/opt/cylance/` die Datei `config_defaults.txt`.
2. Bearbeiten Sie die Datei mit den folgenden Informationen.

```
InstallToken=YOUR_INSTALL_TOKEN
SelfProtectionLevel=2
```

```
LogLevel=2
VenueZone=ZONE_NAME
UiMode=2
AWS=1
```

- Ersetzen Sie *YOUR_INSTALL_TOKEN* durch das Installationstoken der Verwaltungskonsole.
- Ersetzen Sie *ZONE_NAME* durch den Namen der Zone, der Sie das Gerät hinzufügen möchten. Wenn die angegebene Zone nicht in der Konsole vorhanden ist, wird sie automatisch erstellt.

Parameter	Beschreibung
InstallToken	Dieses Feld ist erforderlich und gibt den Cylance Endpoint Security-Mandanten an, bei dem das Gerät registriert werden soll. Verwenden Sie das Installationstoken aus dem Menü **Einstellungen > Anwendung** in der Verwaltungskonsole.
SelfProtectionLevel	Diese Einstellung schränkt den Zugriff auf den Cylance-Dienst und die Ordner ein. • `1`: Nur lokale Administratoren können Änderungen an der Registrierung und den Diensten vornehmen. • `2`: Nur der Systemadministrator kann Änderungen an der Registrierung und den Diensten vornehmen. Die Standardeinstellung ist „2“.
LogLevel	Diese Einstellung legt die Ebene der Informationen fest, die in den Debug-Protokollen erfasst werden. • `0`: Fehler • `1`: Warnung • `2`: Informationen • `3`: Ausführlich Die Standardeinstellung ist „2“. Wenn die ausführliche Protokollierung ausgewählt ist, gewinnt das Protokoll schnell an Größe.
VenueZone	Diese Einstellung gibt die Zone an, zu der Sie das Gerät hinzufügen möchten. • Wenn der angegebene Zonenname nicht in der Konsole vorhanden ist, wird die Zone mit dem angegebenen Namen erstellt. • Wenn der Zonen- oder Gerätename mit einem Leerzeichen beginnt oder endet (z. B. „ Hallo“ oder „Hallo “), wird es bei der Geräteregistrierung entfernt. Tabulatoren, Wagenrückläufe, Zeilenvorschübe oder andere unsichtbare Zeichen sind nicht zulässig. • Zonennamen dürfen kein Gleichheitszeichen (=) enthalten. „Hallo=Welt“ ist zum Beispiel nicht zulässig.
UiMode	Diese Einstellung legt den Modus der Benutzeroberfläche des Agenten beim Systemstart fest. • `1`: Minimale Benutzeroberfläche • `2`: Vollständige Benutzeroberfläche Die Standardeinstellung ist „2“.

Parameter	Beschreibung
AWS	Diese Einstellung legt fest, dass der Agent auf einem Amazon Web Services-Host ausgeführt wird. Standardmäßig wird der Hostname des Geräts als Gerätename in der Verwaltungskonsole verwendet. Aktivieren Sie diese Einstellung, damit der Agent die Instanz-ID vom Host erfassen und mit dem Hostnamen im Feld „Gerätename“ in der Konsole speichern kann. Diese Einstellung stellt sicher, dass jeder Agent auf einem Amazon Web Services-Host einen eindeutigen Gerätenamen an die Verwaltungskonsole meldet. `1`: Aktivieren Sie den Agenten, um die Instanz-ID zu erfassen. Der Gerätename wird geändert und enthält Hostname + Instanz-ID. Die Instanz-ID ist mit dem Präfix „i-“ gekennzeichnet. ABC-DE-123456789_i-0a1b2cd34efg56789, wobei der Gerätename ABCDE-12345678 und die AWS EC2 ID i-0a1b2cd34efg56789 lautet.

Automatische Installation des Linux-Agenten

Bevor Sie beginnen:

- Lesen Sie die CylancePROTECT Desktop-Anforderungen.
- Laden Sie die CylancePROTECT Desktop-Installationsdateien von der Verwaltungskonsole herunter. Klicken Sie auf **Einstellungen > Bereitstellungen**. Wählen Sie in der Dropdown-Liste **Produkt** die Option **CylancePROTECT** aus und legen Sie das Zielbetriebssystem, die Agentenversion und den Dateityp fest. Klicken Sie auf **Download**.
- Kopieren Sie in der Verwaltungskonsole über **Einstellungen > Anwendung** das Installationstoken.
- Vergewissern Sie sich, dass Sie über Root-Berechtigungen verfügen.

1. Erstellen einer Konfigurationsdatei für die Installation des Linux-Agenten.
2. Führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus, um den Treiber und den Agenten zu installieren. Verwenden Sie die aus der .tgz-Datei extrahierten Dateien, um den Wert von *<version>* zu ermitteln.

Linux-Distribution	Befehle
• Red Hat Enterprise Linux • CentOS • Amazon Linux • Oracle	Führen Sie die folgenden Befehle aus, um den Treiber und den Agenten zu installieren: **a.** `yum install CylancePROTECTOpenDriver-<version>.rpm CylancePROTECTDriver-<version>.rpm` **b.** `yum install CylancePROTECT.<version>.rpm CylancePROTECTUI.<version>.rpm`
SUSE Linux Enterprise Server	Führen Sie die folgenden Befehle aus, um den Treiber und den Agenten zu installieren: **a.** `zypper install CylancePROTECTOpenDriver-<version>.rpm CylancePROTECTDriver-<version>.rpm` **b.** `zypper install CylancePROTECT.<version>.rpm CylancePROTECTUI.<version>.rpm`

Wenn Sie fertig sind:

- Wenn die Benutzeroberfläche des Agenten nach der Installation nicht automatisch startet (z. B. auf CentOS- , SUSE- oder Ubuntu-Geräten), müssen Sie die GNOME-Shell neu starten, um die Benutzeroberfläche von CylancePROTECT anzuzeigen. Siehe Manuelles Starten der Benutzeroberfläche.

Manuelle Installation des Linux-Agenten

Bevor Sie beginnen:

- Lesen Sie die CylancePROTECT Desktop-Anforderungen.
- Laden Sie die CylancePROTECT Desktop-Installationsdateien von der Verwaltungskonsole herunter. Klicken Sie auf **Einstellungen > Bereitstellungen**. Wählen Sie in der Dropdown-Liste **Produkt** die Option **CylancePROTECT** aus und legen Sie das Zielbetriebssystem, die Agentenversion und den Dateityp fest. Klicken Sie auf **Download**.
- Kopieren Sie in der Verwaltungskonsole über **Einstellungen > Anwendung** das Installationstoken.
- Vergewissern Sie sich, dass Sie über Root-Berechtigungen verfügen.

1. Erstellen einer Konfigurationsdatei für die Installation des Linux-Agenten.
2. Führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus, um den Treiber und den Agenten zu installieren. Verwenden Sie die aus der .tgz-Datei extrahierten Dateien, um den Wert von *<version>* zu ermitteln.

Linux-Distribution	Befehle

• Red Hat Enterprise Linux oder CentOS
• Amazon Linux
• Oracle
• SUSE Linux Enterprise Server
	a. Installieren Sie den offenen Treiber:
	`rpm -ivh CylancePROTECTOpenDriver-<version>.rpm`
	b. Installieren Sie den Agent-Treiber:
	`rpm -ivh CylancePROTECTDriver-<version>.rpm`
	c. Installieren Sie den Agenten:
	`rpm -ivh CylancePROTECT.<version>.rpm`
	d. Installieren Sie die Benutzeroberfläche des Agenten*:
	`rpm -ivh CylancePROTECTUI.<version>.rpm`
	* Bei Geräten, auf denen SUSE Linux Enterprise Server ausgeführt wird, müssen Sie möglicherweise die Gnome 3-Bibliothek (libgtk-3-0) vor der Installation der Benutzeroberfläche des Agenten installieren. Verwenden Sie ggf. die folgenden Befehle: `zypper install libgtk-3-0`

Linux-Distribution	Befehle

• Ubuntu
• Debian
	a. Installieren Sie den offenen Treiber:
	`dpkg -i cylance-protect-open-driver_<version>.deb`
	b. Installieren Sie den Agent-Treiber:
	`dpkg -i cylance-protect-driver_<version>.deb`
	c. Installieren Sie den Agenten:
	`dpkg -i cylance-protect.version.deb`
	d. Installieren Sie die Benutzeroberfläche des Agenten:
	`dpkg -i cylance-protect-ui.version.deb`

Wenn Sie fertig sind:

Wenn die Benutzeroberfläche des Agenten nach der Installation nicht automatisch startet (z. B. auf CentOS- , SUSE- oder Ubuntu-Geräten), müssen Sie die GNOME-Shell neu starten, um die Benutzeroberfläche von CylancePROTECT anzuzeigen. Siehe Manuelles Starten der Benutzeroberfläche.

Update des Linux-Treibers

Jeder unterstützte Linux-Kernel erfordert einen unterstützten Treiber, damit der CylancePROTECT Desktop-Agent auf dem Gerät ausgeführt werden kann. Wenn Sie den Linux-Kernel auf einem Gerät aktualisieren, müssen Sie sicherstellen, dass auf dem Gerät ein Treiber ausgeführt wird, der dies unterstützt. Ein Upgrade auf den neuesten Kernel stellt sicher, dass Ihr Gerät die neuesten Sicherheitsupdates des Betriebssystems erhält, während die Verwendung des neuesten Agenten und Treibers dafür sorgt, dass CylancePROTECT den Schutz aufrecht erhalten kann.

Sie haben folgende Wahlmöglichkeiten, um den Linux-Treiber auf dem neuesten Stand zu halten:

Szenario	Maßnahmen
Automatische Aktualisierung des Treibers, sobald ein Update verfügbar ist, wenn ein Upgrade des Linux-Kernels erfolgt	• Stellen Sie sicher, dass auf den Geräten Version 3.1 oder höher des Agenten und Version 3.1 oder höher des Treibers ausgeführt werden. • Aktivieren Sie die Funktion „Linux-Treiber automatisch aktualisieren“ in der Aktualisierungsregel.

Szenario	Maßnahmen
Manuelle Aktualisierung des Treibers, wenn ein Upgrade des Linux-Kernels erfolgt	• Wenn Sie den Linux-Kernel aktualisieren, müssen Sie das Treiberpaket jedes Mal manuell herunterladen, sobald es in der Verwaltungskonsole verfügbar wird. Informationen zur Bestimmung der Mindesttreiberversion, die Sie für den verwendeten Linux-Kernel benötigen, finden Sie in der Tabelle „Unterstützte Linux-Treiber und -Kernels“. • Sie können einen Paket-Manager oder ähnliche Tools und Methoden verwenden, um den Agent und den Treiber zu aktualisieren. • Wenn Sie den Agenten manuell aktualisieren möchten, empfiehlt BlackBerry, die zonenbasierten Aktualisierungseinstellungen des Agenten für diese Geräte in „Nicht aktualisieren“ zu ändern. **Hinweis:** Der 3.1.1100-Treiber ist mit Agent 2.1.1590 und höher kompatibel. Sie können den Treiber auf Geräten installieren, auf denen Agent-Version 2.1.1590 oder höher ausgeführt wird, sodass Sie die Funktion „Linux-Treiber automatisch aktualisieren“ nutzen können, wenn Sie auf Agent 3.1 aktualisieren.

Linux-Treiber automatisch aktualisieren

Wenn Sie den Linux-Kernel auf einem Gerät aktualisieren, müssen Sie sicherstellen, dass auf dem Gerät ein Treiber ausgeführt wird, der dies unterstützt. Für Geräte mit CylancePROTECT Desktop Agent 3.1 und höher können Sie die Funktion „Linux-Treiber automatisch aktualisieren“ aktivieren, mit der der Agent den Treiber automatisch aktualisiert, sobald ein aktualisierter Kernel auf dem System erkannt wird und verfügbar ist. Ein Upgrade auf den neuesten Kernel stellt sicher, dass Ihr Gerät die neuesten Sicherheitsupdates des Betriebssystems erhält, während die Verwendung des neuesten Agenten und Treibers dafür sorgt, dass CylancePROTECT den Schutz aufrecht erhalten kann.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Aktualisieren**.
2. Klicken Sie auf eine Aktualisierungsregel, die Sie zum Verwalten von Aktualisierungen für Linux-Geräte verwenden. Informationen zum Erstellen einer Regel finden Sie unter Verwalten von Updates für die CylancePROTECT Desktop- und CylanceOPTICS-Agenten.
3. Erweitern Sie den Abschnitt **Agent**.
4. Wählen Sie die Option **Linux-Treiber automatisch aktualisieren** aus.
5. Klicken Sie auf **Speichern**.

Linux-Treiber manuell aktualisieren

Wenn Sie den Kernel auf Ihrem Linux-Gerät aktualisieren, müssen Sie sicherstellen, dass auf dem Gerät ein Treiber ausgeführt wird, der dies unterstützt. Wenn für eine Linux-Distribution ein Kernel-Update veröffentlicht wird, erstellt BlackBerry ein aktualisiertes Linux-Treiberpaket und stellt es über die Verwaltungskonsole zur Verfügung. Ein Treiberupdate-Paket ist nur verfügbar, wenn es eine neuere Version als die in der Agentenversion enthaltene Version gibt.

BlackBerry empfiehlt, ein Upgrade auf Agent-Version 3.1 oder höher durchzuführen. Hierdurch wird eine Funktion aktiviert, mit der der Agent den Linux-Treiber automatisch aktualisiert, nachdem ein aktualisierter Kernel

erkannt wurde, sobald dieser verfügbar ist. Wenn Sie Agent-Versionen 3.0 oder 2.1.1590 ausführen oder die Funktion für die automatische Aktualisierung des Linux-Treibers nicht verwenden möchten, müssen Sie einen unterstützten Treiber für den Linux-Kernel manuell installieren. Sie können kompatible Treiber mithilfe der in Ihrem Unternehmen üblichen Tools und Methoden auf Ihren Geräten bereitstellen.

Bevor Sie beginnen:

- Vergewissern Sie sich, dass Sie über Root- oder Sudo-Berechtigungen verfügen.
- Ermitteln Sie die Treiberversion, die zur Unterstützung des Linux-Kernels auf Ihrem Gerät mindestens erforderlich ist.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Bereitstellungen**.
2. Wählen Sie in der **Produktliste** die Option **CylancePROTECT-Treiber** aus.
3. Wählen Sie in der **Betriebssystemliste** das Betriebssystem aus, für das Sie den Treiber herunterladen möchten.
4. Wählen Sie in der **Versionsliste** die Treiberversion aus.
5. Wählen Sie in der Liste **Format** das Format des Treibers aus.
6. Klicken Sie auf **Download**.
7. Um das RPM-Paket zu aktualisieren, verwenden Sie einen der folgenden Befehle:

   Fügen Sie beide Treiber in dieselbe Befehlszeile ein und ersetzen Sie „xx“ durch die Versionsnummer des Pakets:

Distribution	Befehle
Oracle 6, Oracle UEK 6	`rpm -Uvh CylancePROTECTOpenDriver-xx.el6.noarch.rpm CylancePROTECTDriver-xx.el6.noarch.rpm`
CentOS 7, RHEL 7, Oracle 7, Oracle UEK 7	`rpm -Uvh CylancePROTECTOpenDriver-xx.el7.x86_64.rpm CylancePROTECTDriver-xx.el7.x86_64.rpm`
Amazon Linux 2	`rpm -Uvh CylancePROTECTOpenDriver-xx.amzn2.x86_64.rpm CylancePROTECTDriver-xx.amzn2.x86_64.rpm`
SUSE Linux Enterprise Server	`rpm -Uvh CylancePROTECTOpenDriver-xx.x86_64.rpm CylancePROTECTDriver-xx.x86_64.rpm`

Unterstützte 32-Bit-Ubuntu- und Xubuntu-Distributionen	• Installieren Sie die Abhängigkeiten mit dem folgenden Befehl:
	`apt-get update -y && apt-get install`
	• Installieren Sie die DEB-Pakete des CylancePROTECT Desktop-Treibers mit den folgenden Befehlen:
	`dpkg -i cylance-protect-open-driver_xx_i386_32.deb`
	`dpkg -i cylance-protect-driver_xx_i386_32.deb`

Distribution	Befehle

Unterstützte 64-Bit-Ubuntu-, Xubuntu- und Debian-Distributionen	• Installieren Sie die Abhängigkeiten mit dem folgenden Befehl:
	`apt-get update -y && apt-get install`
	• Installieren Sie die DEB-Pakete des CylancePROTECT Desktop-Treibers mit den folgenden Befehlen:
	`dpkg -i cylance-protect-open-driver_xx_amd64.deb`
	`dpkg -i cylance-protect-driver_xx_amd64.deb`

8. Starten Sie den Dienst mit dem folgenden Befehl neu: `systemctl start cylancesvc`

Linux-Befehle für den Agenten

Um eine Liste der Linux-Befehle für den CylancePROTECT Desktop-Agenten anzuzeigen, verwenden Sie Folgendes:

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

Beispiel für die Verwendung von Befehlen: `cylance <option>`

Option	Beschreibung
-r, --register=<*token*>	Agenten bei der Konsole mit dem angegebenen Token registrieren
-s, --status	Nach Agenten-Updates suchen
-b, --start-bg-scan	Scan zur Erkennung von Hintergrundbedrohungen starten
-B, --stop-bg-scan	Scan zur Erkennung von Hintergrundbedrohungen beenden
-d, --scan-dir=<*dir*>	Ein Verzeichnis durchsuchen
-l, --getloglevel	Aktuelle Protokollierungsebene abrufen
-L, --setloglevel=<*level*>	Protokollierungsebene festlegen, um die Ebene der in den Debug-Protokollen erfassten Informationen zu bestimmen
-P, --getpolicytime	Richtlinienaktualisierungszeit abrufen
-p, --checkpolicy	Nach Richtlinienaktualisierungen suchen
-t, --threats	Liste der Bedrohungen anzeigen
-q, --quarantine=<*id*>	Eine Datei unter Angabe der Hash-ID unter Quarantäne stellen
-w, --waive=<*id*>	Eine Datei unter Angabe der Hash-ID ignorieren
-v, --version	Die Version dieses Tools anzeigen
-h, --help	Eine Liste der Befehle anzeigen

Fehlerbehebung bei der Installation von Linux-Agenten

In der folgenden Tabelle sind die Maßnahmen aufgeführt, die Sie zur Fehlerbehebung bei der Installation von Linux-Agenten ergreifen können.

Aufgabe oder Fehler	Aktion

Starten oder Stoppen des Agenten-Dienstes	Verwenden Sie die folgenden Befehle zum Starten und Stoppen des Cylance-Dienstes auf einem Linux-Gerät.
	• Zum Starten des Cylance-Dienstes:
	`systemctl start cylancesvc`
	• Zum Beenden des Cylance-Dienstes:
	`systemctl stop cylancesvc`

Prüfen, ob die Kernel-Treiber geladen sind	Um zu überprüfen, ob die Kernel-Treiber geladen sind, geben Sie den folgenden Befehl ein:
	`lsmod | grep CyProtectDrv`
	Wenn die Kernel-Module geladen sind, sollte der Befehl Folgendes ausgeben:
	`CyProtectDrv 210706  0CyProtectDrvOpen 16384 1 CyProtectDrv`
	Wenn die Kernel-Module nicht geladen sind, wird keine Ausgabe zurückgegeben.

Laden und Entladen der Kernel-Treiber	Auf CylancePROTECT Desktop Linux-Agent 2.1.1590 und höher werden zwei Treiber zusammen geladen und entladen: `CyProtectDrv` und `CyProtectDrvOpen`. In früheren Versionen des Agenten wurde nur der `CyProtectDrv`-Treiber geladen.
	Um die Kernel-Treiber zu laden, geben Sie einen der folgenden Befehle ein:
	• Bei SUSE Linux-Distributionen:
	`modprobe --allow-unsupported cyprotect`
	Wenn Sie das Flag `--allow-unsupported` nicht ständig verwenden möchten, bearbeiten Sie `/etc/modprobe.d/10-unsupported-modules.conf` und ändern Sie „allow_unsupported_modules“ auf „1“.
	• Für alle anderen Linux-Distributionen:
	`modprobe cyprotect`

Linux-Benutzeroberfläche manuell starten	Wenn die Benutzeroberfläche des Agenten nach der Installation nicht automatisch gestartet wurde, finden Sie weitere Informationen unter Manuelles Starten der Benutzeroberfläche.
Fehler: Multilib-Versionsprobleme gefunden	Wenn der „Fehler: Multilib-Versionsprobleme gefunden“ bei der Installation eines Pakets auf einem Gerät auftritt, finden Sie weitere Informationen unter Fehler: Multilib-Versionsprobleme gefunden.

Manuelles Starten der Benutzeroberfläche

Die Benutzeroberfläche des Agenten wird nach der Installation möglicherweise nicht automatisch gestartet (z. B. auf CentOS- Ubuntu- und SUSE-Geräten). Um sie manuell zu starten, können Sie die GNOME Shell-Erweiterung neu starten oder sich ab- und wieder anmelden.

Das GNOME Tweak Tool muss installiert sein, bevor Sie die GNOME Shell-Erweiterung neu starten. Ubuntu enthält das GNOME Tweak Tool möglicherweise nicht standardmäßig.

1. Wenn Sie das GNOME Tweak Tool installieren müssen, führen Sie die folgenden Befehle aus:

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

2. Um die GNOME Shell-Erweiterung neu zu starten, drücken Sie `Alt+F2`, geben Sie „`r`“ in das Dialogfeld ein und drücken Sie `ENTER`.
   Wenn das CylanceUI-Symbol nicht angezeigt wird, aktivieren Sie die GNOME Shell-Erweiterung manuell im Tweak Tool. Um das GNOME Tweak Tool zu starten, geben Sie „`gnome-tweaks`“ in ein Terminal ein. Navigieren Sie im GNOME Tweak Tool zur Registerkarte **Erweiterungen** und aktivieren Sie die CylanceUI.

Fehler: Multilib-Versionsprobleme gefunden

Wenn die Meldung „Fehler: Multilib-Versionsprobleme gefunden“ bei der Installation eines Pakets auf einem Gerät mit Red Hat Enterprise Linux oder CentOS auftritt, bedeutet dies in der Regel, dass die entsprechende 64-Bit-Bibliothek zusammen mit der 32-Bit-Bibliothek installiert oder aktualisiert werden muss. Die `multilib`-Versionsprüfung weist lediglich darauf hin, dass es ein Problem gibt.

Wenn der Fehler beispielsweise mit der `sqlite`-Bibliothek in Zusammenhang steht:

- Sie verwenden ein Upgrade für `sqlite`, bei dem eine Abhängigkeit fehlt, die für ein anderes Paket erforderlich ist. `Yum` versucht, dieses Problem zu lösen, indem eine ältere Version von `sqlite` der anderen Architektur installiert wird. Wenn Sie die andere Architektur ausschließen, zeigt `yum` die Grundursache des Problems an, z. B. fehlende Paketabhängigkeiten. Um eine Fehlermeldung mit der Grundursache des Problems anzuzeigen, können Sie versuchen, das Upgrade mit `--exclude sqlite.otherarch` erneut durchzuführen.
- Sie haben mehrere Architekturen von `sqlite` installiert, aber `yum` kann nur ein Upgrade für eine dieser Architekturen sehen. Wenn Sie nicht beide Architekturen benötigen, können Sie `sqlite`, bei der das Architektur-Update fehlt, entfernen und prüfen, ob der Fehler behoben wurde.
- Es sind bereits doppelte Versionen von `sqlite` installiert. Sie können diese Fehler mit „yum check“ anzeigen.
- Um die passende `sqlite`-Bibliothek zu installieren oder zu aktualisieren, verwenden Sie den folgenden Befehl:

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

  Wenn der Fehler mit den `dbus-libs`-, `openssl`- oder `libgcc`-Bibliotheken zusammenhängt, ersetzen Sie `sqlite` durch die entsprechende Bibliothek im Befehl.

Benutzer müssen ein Kennwort angeben, um die CylancePROTECT Desktop- und CylanceOPTICS-Agenten zu entfernen

Sie können von den Benutzern verlangen, für die Deinstallation des CylancePROTECT Desktop-Agenten für Windows und macOS, des CylanceOPTICS-Agenten für Windows Version 3.1 und höher sowie des CylanceOPTICS-Agenten für macOS Version 3.3 und höher ein Kennwort anzugeben. Die Verwendung dieser Funktion für den CylanceOPTICS-Agenten für macOS erfordert auch CylancePROTECT Desktop Version 3.1 oder höher.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Anwendung**.
2. Aktivieren Sie das Kontrollkästchen **Kennwort für Deinstallation von Agent erforderlich**.
3. Geben Sie ein Kennwort an.
4. Klicken Sie auf **Speichern**.

Einrichten von CylancePROTECT Mobile

Schritt	Aktion
1	Lesen Sie die Softwareanforderungen und Netzwerkanforderungen für die CylancePROTECT Mobile-App.
2	Wenn Sie CylancePROTECT Mobile-Benutzer aus Ihrem Unternehmensverzeichnis zu Cylance Endpoint Security hinzufügen möchten, stellen Sie eine Verknüpfung zu Ihrem Unternehmensverzeichnis her.
3	Fügen Sie Benutzer der CylancePROTECT Mobile-App hinzu. Fügen Sie zur Verwaltung von Benutzern optional Gruppen hinzu.
4	Erstellen einer CylancePROTECT Mobile-Richtlinie.
5	Erstellen einer Registrierungsrichtlinie.
6	Gerätebenutzer installieren und aktivieren die CylancePROTECT Mobile-App. Anweisungen hierzu finden Sie im Cylance Endpoint Security-Benutzerhandbuch.
7	Optional können Sie eine Risikobewertungsrichtlinie erstellen, um Warnungen den Geräterisikostufen zuzuordnen. Wenn Sie keine kundenspezifische Risikobewertungsrichtlinie zuweisen, wird eine Standard-Risikobewertungsrichtlinie auf Benutzer Ihres Mandanten angewendet.
8	Optional können Sie Cylance Endpoint Security mit Microsoft Intune integrieren, um die Risikostufen des Geräts an Intune zu melden, sodass Intune die gewünschten Maßnahmen zur Risikominderung auf Geräten ausführen kann.

Cylance Endpoint Security unterstützt auch die Verwendung von Schutzrichtlinien für Microsoft Intune-Apps, um den Zugriff auf bestimmte Microsoft-Apps basierend auf der von CylancePROTECT Mobile gemeldeten Bedrohungsstufe des Geräts zuzulassen oder einzuschränken. Die Aktivierung dieser Funktion erfordert weitere Bereitstellungsschritte. Informationen zum Konfigurieren dieser Funktion finden Sie unter Verwenden von Schutzrichtlinien für Intune-Apps mit CylancePROTECT Mobile.

Erstellen einer CylancePROTECT Mobile-Richtlinie

Sie erstellen eine CylancePROTECT Mobile-Richtlinie und weisen diese Benutzern und Gruppen zu, um den Dienst zu aktivieren und zu steuern, welche Funktionen Sie verwenden möchten.

Bevor Sie beginnen: Hinzufügen der CylancePROTECT Mobile-App und von CylanceGATEWAY-Benutzern.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Benutzerrichtlinie**.
2. Klicken Sie auf der Registerkarte **Protect Mobile** auf **Richtlinie hinzufügen**.
3. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.

4. Im Abschnitt **Benachrichtigungen** können Sie die Anzahl und das Intervall der Benachrichtigungen festlegen, die die CylancePROTECT Mobile-App dem Benutzer bereitstellt, wenn eine Bedrohung erkannt wird. Sie geben den Benachrichtigungstyp (Gerät, E-Mail oder keine Benachrichtigung) im Abschnitt **Geräteeinstellungen** an (Schritt 6).
5. Wenn Sie bestimmte Informationen verschleiern möchten, wenn die CylancePROTECT Mobile-App eine Bedrohung meldet, sodass die Informationen nicht gespeichert und in der Verwaltungskonsole als Klartext angezeigt werden können, aktivieren Sie im Abschnitt **Datenschutz** die Option **Datenschutz** und wählen dann die Felder aus, die Sie verschleiern möchten.
6. Klicken Sie im Abschnitt **Geräteeinstellungen** auf **Android** oder **iOS** und aktivieren Sie die Funktionen, die Sie verwenden möchten. Weitere Informationen zu den Funktionen von CylancePROTECT Mobile finden Sie unter Wichtige Funktionen von CylancePROTECT Mobile.
   a) Aktivieren Sie für jede Funktion, die Sie auswählen, das entsprechende Kontrollkästchen, um Gerätebenachrichtigungen und E-Mail-Benachrichtigungen zu aktivieren oder zu deaktivieren. Wenn Sie Geräte- und E-Mail-Benachrichtigungen deaktivieren, muss der Benutzer die CylancePROTECT Mobile-App öffnen, um Warnmeldungen anzuzeigen.
   b) Wenn Sie eine der folgenden Funktionen aktivieren, führen Sie die folgenden zusätzlichen Schritte aus:

Funktion	Plattform	Zusätzliche Schritte
Schädliche Apps	Android	**a.** Um Apps auf der sicheren Liste vom Malware-Scan auszunehmen, aktivieren Sie die Option **Apps in der Liste sicherer Apps immer zulassen**. **b.** Um Apps, die auf der unsicheren Liste stehen, automatisch zu blockieren, aktivieren Sie **Apps in der Liste gesperrter Apps immer blockieren**. **c.** Wenn Sie System-Apps scannen möchten, die in der Systempartition auf dem Gerät vorinstalliert sind, aktivieren Sie **System-Apps scannen**. **d.** Wenn Sie das Hochladen von Apps auf die CylancePROTECT Mobile-Dienste über eine Wi-Fi-Verbindung aktivieren möchten, aktivieren Sie **App-Pakete für die Sicherheitsprüfung über eine WLAN-Verbindung hochladen**. Geben Sie die maximale Größe einer App in MB an, die über Wi-Fi hochgeladen werden kann, sowie die maximale Größe aller Apps, die in einem Monat (30 Tage) hochgeladen werden können. Wenn einer der beiden Höchstwerte überschritten wird, erfolgt kein Hochladen und dem Geräteprotokoll wird eine Fehlermeldung hinzugefügt. **e.** Wenn Sie das Hochladen von Apps auf die CylancePROTECT Mobile-Dienste über ein mobiles Netzwerk aktivieren möchten, aktivieren Sie **App-Pakete für die Sicherheitsprüfung über eine mobile Netzwerkverbindung hochladen**. Geben Sie die maximale Größe einer App in MB an, die über ein mobiles Netzwerk hochgeladen werden kann, sowie die maximale Größe aller Apps, die in einem Monat (30 Tage) hochgeladen werden können. Wenn einer der beiden Höchstwerte überschritten wird, erfolgt kein Hochladen und dem Geräteprotokoll wird eine Fehlermeldung hinzugefügt.

Funktion	Plattform	Zusätzliche Schritte
Nicht unterstütztes Gerätemodell	Android iOS	Klicken Sie auf **Bearbeiten** und wählen Sie die Gerätemodelle aus, die Sie einschränken möchten.
Nicht unterstützte OS	Android iOS	Fügen Sie die verfügbaren Betriebssystemversionen basierend auf den Sicherheitsstandards Ihres Unternehmens zu den unterstützten und nicht unterstützten Listen hinzu.
Fehlgeschlagener SafetyNet- oder Play Integrity-Nachweis	Android	Wenn Sie die Compatibility Test Suite-Anpassung für die CylancePROTECT Mobile-App aktivieren möchten, aktivieren Sie die Option **CTS-Profilanpassung aktivieren**.
Fehlgeschlagener Hardware-Nachweis	Android	**a.** Klicken Sie in der Dropdown-Liste **Mindestsicherheitsstufe erforderlich** auf die entsprechende Stufe. Weitere Informationen finden Sie unter Sicherheitsstufe auf der Android Developers Website. **b.** Wenn Sie eine minimale Sicherheitspatch-Stufe auf Geräten erzwingen möchten, aktivieren Sie **Sicherheitspatch-Stufe**. Fügen Sie die entsprechenden Gerätemodelle hinzu und geben Sie das Datum des Sicherheitspatches an.
Unsicheres Wi-Fi	Android	Fügen Sie die verfügbaren Wi-Fi-Zugriffsalgorithmen zu den Listen „sicher“ und „unsicher“ hinzu, die auf den Sicherheitsstandards Ihres Unternehmens basieren.
Unsichere Nachricht	Android iOS	**a.** Wählen Sie in der Dropdown-Liste **Scanoption** eine der folgenden Optionen aus: • Wenn Sie Nachrichten an die CylancePROTECT Mobile-Dienste senden möchten, um festzustellen, ob sie sicher sind, klicken Sie auf **Cloud-Scan**. • Wenn Sie nur die lokalen Modelle des maschinellen Lernens der CylancePROTECT Mobile-App verwenden möchten, um unsichere URLs zu identifizieren, klicken Sie auf **Gerätescan**. • Wenn Sie die URL-Suche deaktivieren möchten, klicken Sie auf **Kein Scan**. **b.** Geben Sie für Android-Geräte im Feld **Scanstart-Offset** das Alter von Textnachrichten in Stunden an, die gescannt werden sollen. Wenn Sie 0 angeben, werden nur neue Nachrichten gescannt.

7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie die Richtlinie Benutzern und Gruppen zu.
- Gegebenenfalls müssen Sie den Richtlinien einen Rang zuweisen.
- Erstellen Sie eine Registrierungsrichtlinie und weisen Sie sie Benutzern zu. Nachdem Benutzern eine Registrierungsrichtlinie zugewiesen worden ist, erhalten sie eine E-Mail mit Anweisungen zum Herunterladen

und Aktivieren der CylancePROTECT Mobile-App. Weitere Informationen finden Sie im Cylance Endpoint Security-Benutzerhandbuch.
  - Bitten Sie die Benutzer, in ihrem standardmäßigen mobilen Browser JavaScript zu aktivieren (die CylancePROTECT Mobile-App unterstützt Google Chrome, Samsung und Safari). Dies ist erforderlich, um die CylancePROTECT Mobile-App zu aktivieren.
  - Bitten Sie Android-Benutzer, nach der Installation der CylancePROTECT Mobile-App Hintergrundaktivitäten für diese zuzulassen.
- Optional: Erstellen Sie eine Risikobewertungsrichtlinie. Wenn Sie keine kundenspezifische Risikobewertungsrichtlinie erstellen und zuweisen, wird eine Standard-Risikobewertungsrichtlinie auf Benutzer Ihres Mandanten angewendet.

Erstellen einer Risikobewertungsrichtlinie

Eine Risikobewertungsrichtlinie ordnet Warnungen, die von der CylancePROTECT Mobile-App erkannt werden, Risikostufen zu. (Sie können beispielsweise angeben, dass kompromittierte Geräte als hohes Risiko behandelt werden sollen.) Die Risikostufen der Warnungen werden zur Bestimmung der Gesamtrisikostufe eines Geräts verwendet. Sie können die Risikostufe des Geräts in der Verwaltungskonsole (Assets > Mobilgeräte und dann in den Gerätedetails) anzeigen.

Wenn Sie keine Risikobewertungsrichtlinie erstellen, wird eine Standardrichtlinie auf Benutzer Ihres Mandanten angewendet. Sie können die Standardrichtlinie bearbeiten, sie aber nicht löschen.

Risikobewertungsrichtlinien können für die folgenden Cylance Endpoint Security-Funktionen verwendet werden:

- Wenn Sie Cylance Endpoint Security mit Microsoft Intune integrieren, sendet Cylance Endpoint Security in regelmäßigen Abständen die Gesamtrisikostufe eines Mobilgeräts an Intune. Sie können Intune verwenden, um Risikominderungsmaßnahmen für Geräterisikostufen zu konfigurieren.
- Sie können die Risikostufe des Mobilgeräts in die CylanceGATEWAY-Netzwerkzugriffsregeln aufnehmen.

Bevor Sie beginnen: Richten Sie CylancePROTECT Mobile ein.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Benutzerrichtlinie**.
2. Klicken Sie auf die Registerkarte **Risikobewertung**.
3. Klicken Sie auf **Richtlinie hinzufügen**.
4. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.
5. Klicken Sie im Abschnitt **Risikobewertung** auf **Erkennungen hinzufügen > Erkennungen**.
6. Ziehen Sie die Erkennungen per Drag-and-drop zu der Risikostufe, die Sie darauf anwenden möchten.

   Weitere Informationen zu den Erkennungen finden Sie unter Wichtige Funktionen von CylancePROTECT Mobile.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie die Richtlinie Benutzern und Gruppen zu.
- Gegebenenfalls müssen Sie den Richtlinien einen Rang zuweisen.
- Optional können Sie Cylance Endpoint Security mit Intune integrieren, um auf mobile Bedrohungen zu reagieren.

Integration von Cylance Endpoint Security mit Microsoft Intune, um auf mobile Bedrohungen zu reagieren

Sie können eine Verbindung zwischen Cylance Endpoint Security und Microsoft Intune herstellen, damit Cylance Endpoint Security die Risikostufe von Geräten an Intune weiterleiten kann. Die Geräterisikostufe wird auf der Grundlage der Erkennung mobiler Bedrohungen durch die CylancePROTECT Mobile-App auf von Intune-verwalteten Geräten berechnet. Intune kann Risikominderungsmaßnahmen auf Basis der Geräterisikostufe ausführen.

Wenn Sie eine Verbindung zwischen Cylance Endpoint Security und Intune herstellen, erstellen Sie App-Konfigurationsrichtlinien, die die Gerätetypen und Intune-Gruppen definieren, für die die Integration gilt. Sie erstellen Risikobewertungsrichtlinien, die von der CylancePROTECT Mobile-App erkannte Ereignisse der von Ihnen gewählten Risikostufe zuordnen (hoch, mittel oder niedrig). Wenn die CylancePROTECT Mobile-App auf einem von Intune verwalteten Gerät eine Bedrohung erkennt (z. B. eine schädliche App oder eine Sideloading-App), wird die Risikostufe, die dieser Bedrohung zugeordnet ist, in eine allgemeine Risikostufe einbezogen, die von Cylance Endpoint Security für das Gerät berechnet wird. Cylance Endpoint Security meldet die Risikostufe des Geräts an Intune und Intune führt die Risikominderungsmaßnahmen aus, die für diese Risikostufe konfiguriert worden sind.

Beachten Sie, dass alle von Intune verwalteten Geräte, die diese Funktion verwenden sollen, in einer App-Konfigurationsrichtlinie auf der Cylance-Konsole enthalten sein müssen. Diese Funktion erfordert die CylancePROTECT Mobile-App-Version 2.0.1.1099 oder höher.

Cylance Endpoint Security unterstützt auch die Verwendung von Schutzrichtlinien für Microsoft Intune-Apps, um den Zugriff auf bestimmte Microsoft-Apps basierend auf der von CylancePROTECT Mobile gemeldeten Bedrohungsstufe des Geräts zuzulassen oder einzuschränken. Informationen zum Aktivieren dieser Funktion finden Sie unter Verwenden von Schutzrichtlinien für Intune-Apps mit CylancePROTECT Mobile.

Cylance Endpoint Security mit Intune verbinden

Bevor Sie beginnen: Das Cylance Endpoint Security-Administratorkonto, mit dem Sie die Verbindung zu Intune herstellen, muss über eine Intune-Lizenz verfügen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Connectors**.
2. Klicken Sie auf **Verbindung hinzufügen > Microsoft Intune**.
3. Geben Sie Ihre Entra-Mandanten-ID ein. Klicken Sie auf **Weiter**.
4. Geben Sie Ihre Administratorzugangsdaten für Entra an.

   Befolgen Sie die Anweisungen zur Administratorzustimmung. Falls erforderlich, stimmen Sie sich mit dem Intune-Administrator Ihres Unternehmens ab, um die Zustimmung für den CylancePROTECT Mobile-MTD-Connector im Microsoft Intune Admin Center zu erhalten.
5. Aktivieren Sie auf dem Bildschirm **App-Konfigurationsrichtlinien** die Betriebssystemplattformen, für die die Intune-Integration gelten soll, und führen Sie die folgenden Schritte für die jeweilige Plattform aus. Beachten Sie, dass alle Intune-verwalteten Geräte, die diese Funktion verwenden sollen, in einer App-Konfigurationsrichtlinie enthalten sein müssen. Wenn Sie die App-Konfigurationsrichtlinien später erstellen möchten, klicken Sie auf **Abbrechen**.
   a) Optional können Sie den Namen der Richtlinie ändern. Ändern Sie die Ziel-App nicht.
   b) Wenn Sie möchten, dass die Richtlinie für alle Gruppen der Intune-Instanz gilt, aktivieren Sie **Alle Gruppen**.
   c) Wenn Sie möchten, dass die Richtlinie für bestimmte Gruppen der Intune-Instanz gilt, klicken Sie auf ⊕. Suchen Sie nach Gruppen, wählen Sie sie aus und klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern**. Wenn Sie eine App-Konfigurationsrichtlinie für Android hinzugefügt haben, befolgen Sie die angezeigten Aufforderungen zur Administratorzustimmung.

Die von Ihnen erstellten App-Konfigurationsrichtlinien sind im Intune Admin Center sichtbar.

Wenn Sie fertig sind:

- Wenn Sie dies noch nicht getan haben, erstellen Sie eine Risikobewertungsrichtlinie, um die von der CylancePROTECT Mobile-App erkannten Bedrohungen den gewünschten Risikostufen zuzuordnen.
- Bearbeiten Sie im Intune-Admin-Center den CylancePROTECT Mobile-MTD-Connector, und aktivieren Sie die Optionen für die Kompatibilitätsrichtlinie, um Android- und iOS-Geräte mit CylancePROTECT zu verbinden.

Verwenden von Schutzrichtlinien für Intune-Apps mit CylancePROTECT Mobile

Sie können die Schutzrichtlinien für Microsoft Intune-Apps mit CylancePROTECT Mobile verwenden, um den Zugriff auf bestimmte Microsoft-Apps basierend auf der von CylancePROTECT Mobile gemeldeten Bedrohungsstufe des Geräts zuzulassen oder einzuschränken.

1. Lesen Sie die Softwareanforderungen und Netzwerkanforderungen für die CylancePROTECT Mobile-App.
2. Verknüpfen Sie Cylance Endpoint Security mit Ihrem Unternehmensverzeichnis.
3. Fügen Sie Intune-Benutzer zu Cylance Endpoint Security als CylancePROTECT Mobile-Benutzer hinzu.
4. Erstellen Sie eine CylancePROTECT Mobile-Richtlinie, und weisen Sie sie den Benutzern zu.
5. Erstellen Sie eine Registrierungsrichtlinie, und weisen Sie sie den Benutzern zu.

   Die Benutzer erhalten eine E-Mail mit Anweisungen zum Herunterladen und Aktivieren der CylancePROTECT Mobile-App. Weisen Sie die Benutzer an, die E-Mail vorerst zu ignorieren. Sie werden die App in Schritt 10 herunterladen und aktivieren. Weisen Sie die Benutzer an, die E-Mail aufzubewahren, da sie den QR-Code benötigen, um die CylancePROTECT Mobile-App zu aktivieren.
6. Erstellen Sie eine Risikobewertungsrichtlinie, um Benachrichtigungen den Geräterisikostufen zuzuordnen. Wenn Sie keine kundenspezifische Risikobewertungsrichtlinie zuweisen, wird eine Standard-Risikobewertungsrichtlinie auf Benutzer Ihres Mandanten angewendet.
7. Cylance Endpoint Security mit Intune verbinden.
8. Im Intune-Admin-Center:
   a) Bearbeiten Sie den CylancePROTECT Mobile-MTD-Connector, und aktivieren Sie die Optionen für die App-Schutzrichtlinie, um Android- und iOS-Geräte mit CylancePROTECT zu verbinden.
   b) Erstellen und konfigurieren Sie App-Schutzrichtlinien für Android- und iOS-Geräte, um anzugeben, wie CylancePROTECT Mobile den Zugriff auf bestimmte Apps je nach gemeldeter Risikostufe zulassen oder einschränken soll.
   c) Weisen Sie Benutzergruppen die App-Schutzrichtlinien zu.
9. Stellen Sie die Microsoft-Apps bereit, die Sie mithilfe der Intune-App-Schutzrichtlinie schützen möchten. Nachdem eine geschützte Microsoft-App installiert wurde, werden die Benutzer aufgefordert, die Microsoft Authenticator-App (iOS) oder die App für das Intune-Unternehmensportal (Android) zu installieren und das Gerät zu registrieren.
10. Weisen Sie die Benutzer an, eine geschützte Microsoft-App zu starten und der Aufforderung „Zugriff erhalten“ zu folgen, um die CylancePROTECT Mobile-App zu installieren und zu aktivieren. Weisen Sie die Benutzer an, den QR-Code zu verwenden, den sie in Schritt 5 erhalten haben.

    Wenn die Android-Benutzer nicht aufgefordert werden, die CylancePROTECT Mobile-App zu installieren, weisen Sie sie an, die geschützte Microsoft-App zu schließen und erneut zu öffnen.

Wenn ein Benutzer eine geschützte Microsoft-App öffnet, erhält er eine Benachrichtigung, sofern der Zugriff auf die App aufgrund der aktuellen Risikostufe des Geräts eingeschränkt ist.

Einrichten von CylanceOPTICS

Schritt	Aktion
1	Überprüfen Sie die Softwareanforderungen.
2	Installieren des CylanceOPTICS-Agenten auf Geräten.
3	Aktivieren und Konfigurieren von CylanceOPTICS.
4	Verwalten von Updates für die CylancePROTECT Desktop- und CylanceOPTICS-Agenten.

Installieren des CylanceOPTICS-Agenten auf Geräten

Um ein Gerät für CylanceOPTICSzu aktivieren, müssen Sie den CylanceOPTICS-Agenten auf dem Gerät installieren. Sie laden das Installationsprogramm für den CylanceOPTICS-Agenten von der Verwaltungskonsole herunter und führen es dann mit der bevorzugten Methode Ihres Unternehmens auf Geräten aus. Sie können beispielsweise IT-Administratoren den Agenten auf Geräten vorinstallieren lassen, bevor die Geräte den Benutzern zur Verfügung gestellt werden, oder Sie können die Installation per Push mithilfe eines vertrauenswürdigen Softwareverteilungsprozesses übertragen.

Bevor Sie beginnen:

- Überprüfen Sie die CylanceOPTICS-Softwareanforderungen.
- Sie müssen den CylancePROTECT Desktop-Agenten auf Geräten installieren, bevor Sie den CylanceOPTICS-Agenten installieren.
- Wenn Sie den CylanceOPTICS-Agenten auf macOSBig Sur (11.x)-Geräten oder höher installieren möchten, finden Sie unter Konfigurationsanforderungen für macOS 11.x und höherweitere Informationen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Bereitstellungen**.
2. Klicken Sie in der Dropdown-Liste **Produkt**auf **CylanceOPTICS**.
3. Wählen Sie das Betriebssystem, die Version und das Format aus.

   Hinweis:

   - Für macOS-Geräte empfiehlt es sich, die PKG-Datei zu verwenden. Die DMG-Datei ist ein Datenträger-Image der PKG-Datei, das verwendet werden kann, wenn ein Datenträger-Image für die Installation gemountet werden muss.
   - Bevor Sie den Agenten auf macOS-Geräten bereitstellen, lesen Sie den KB-Artikel 66578: Zulassen, dass Cylance Kernel-Erweiterungen Fehler der Art „Treiber konnte keine Verbindung herstellen“ behandeln.
   - Verwenden Sie für Geräte mit Oracle LinuxServer UEK 8 und Oracle LinuxServer 8 die Oracle 8-Installationsdatei (erfordert CylanceOPTICSAgent 3.2 oder höher).
4. Klicken Sie auf **Download**.
5. Stellen Sie die Installationsdatei mithilfe der bevorzugten Softwareverteilungsmethode Ihres Unternehmens auf Geräten bereit und führen Sie sie aus.

Wenn Sie den CylanceOPTICS-Agenten auf Windows- oder macOS-Geräten mit Betriebssystembefehlen installieren möchten oder wenn Sie auf Linuxinstallieren, finden Sie unter Betriebssystembefehle für den CylanceOPTICS-Agentenweitere Informationen.

Wenn Sie fertig sind:

- Aktivieren und konfigurieren Sie CylanceOPTICSin einer Geräterichtlinie und weisen Sie die Richtlinie mindestens einer Zone zu.
- Weitere Informationen zum Verwalten von CylanceOPTICS-Agent-Upgrades finden Sie unter Verwalten von Updates für die CylancePROTECT Desktop- und CylanceOPTICS-Agenten.

Konfigurationsanforderungen für macOS 11.x und höher

Um die CylanceOPTICS-Agent-Version 3.0 oder höher auf Geräten mit macOS Big Sur (11.x) oder höher zu installieren, beachten Sie bitte die folgenden Konfigurationsanforderungen. Die Anforderungen hängen davon ab, ob Geräte von einer MDM-Lösung verwaltet werden (z. B. Jamf Pro).

Mit MDM verwaltete Geräte

Die folgenden Informationen beziehen sich auf Jamf Pro als MDM-Lösung, sind aber auch auf andere MDM-Lösungen anwendbar.

Anforderungen	Schritte
Aktivieren des vollen Datenträgerzugriffs für CylanceOPTICS	Erstellen Sie ein Konfigurationsprofil und konfigurieren Sie die folgenden Datenschutzeinstellungen: • Kennung: com.cylance.Optics • Kennungstyp: Bundle-ID • Code-Anforderung: `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"` • SystemPolicyAllFiles-Dienst: Zulassen
Aktivieren der CylanceOPTICS-Systemerweiterung	Erstellen Sie ein Konfigurationsprofil und konfigurieren Sie die folgenden Datenschutzeinstellungen: • Anzeigename: Optics-Systemerweiterung für Cylance Endpoint Security • Systemerweiterungstypen: Zulässige Systemerweiterungen • Teamkennung: 6ENJ69K633 • Zulässige Systemerweiterungen: com.cylance.CyOpticsESF.extension

Anforderungen	Schritte
Aktivieren des vollen Datenträgerzugriffs der CylanceOPTICS-Systemerweiterung	Erstellen Sie ein Konfigurationsprofil und konfigurieren Sie die folgenden Datenschutzeinstellungen: • Kennung: com.cylance.CyOpticsESF.extension • Kennungstyp: Bundle-ID • Code-Anforderung: `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")` • SystemPolicyAllFiles-Dienst: Zulassen
Aktivieren der CylanceOPTICS-Netzwerkerweiterung	Erstellen Sie ein Konfigurationsprofil und konfigurieren Sie die folgenden Inhaltsfiltereinstellungen: • Filtername: com.cylance.CyOpticsESF.extension • Kennung: com.cylance.CyOpticsESF.extension • Socket-Filter-Bundle-Kennung: com.cylance.CyOpticsESF.extension • Vorgesehene Socket-Filter-Anforderung: `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")` • Netzwerkfilter-Bundle-Kennung: com.cylance.CyOpticsESF.extension • Vorgesehene Netzwerkfilter-Anforderung: `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")`
Neustart nach Installation	Starten Sie das Gerät neu, nachdem Sie die oben beschriebenen Konfigurationsschritte ausgeführt und den CylanceOPTICS-Agenten installiert haben.

Nicht mit MDM verwaltete Geräte

Gehen Sie nach der Installation des CylanceOPTICS-Agenten wie folgt vor:

1. Starten Sie das Gerät neu.

2. Navigieren Sie zu den Einstellungen für „Sicherheit und Datenschutz“ und genehmigen Sie CyOpticsESFLoader.
3. Lassen Sie den CylanceOPTICS-Netzwerkfilter zu, wenn Sie dazu aufgefordert werden.
4. Wenn der Systemintegritätsschutz (SIP) auf dem Gerät aktiviert ist, klicken Sie auf der Registerkarte „Datenschutz“ auf „Voller Datenträgerzugriff“ und überprüfen, ob CyOpticsESFLoader ausgewählt ist. Wenn CyOpticsESFLoader nicht in der Liste enthalten ist, klicken Sie auf „+“, navigieren zu /Library/Application Support/Cylance/Optics und wählen „CyOptics“ aus.
5. Starten Sie das Gerät neu.

So überprüfen Sie, ob die Systemerweiterung geladen ist:

1. Führen Sie `$ systemextensionsctl list` aus und stellen Sie sicher, dass die Ausgabe `com.cylance.CyOpticsESF.extension` enthält.
2. Führen Sie `$ ps aux | grep -i extension | grep -i Cylance` aus und stellen Sie sicher, dass die Ausgabe `com.cylance.CyOpticsESF.extension.systemextension` enthält.

Betriebssystembefehle für den CylanceOPTICS-Agenten

Das CylanceOPTICS-Agent-Installationsprogramm unterstützt die folgenden Betriebssystembefehle.

Windows

Maßnahmen	Befehle
Geben Sie das Installationsverzeichnis an.	`INSTALLFOLDER=<path>`
Geben Sie das Verzeichnis für den lokalen CylanceOPTICS-Datenspeicher an.	`OPTICSROOTDATAFOLDER=<path>`
Führen Sie eine Installation im Hintergrund durch, die keine Benutzeraktionen erfordert.	Verwenden Sie für das EXE-Paket eine der folgenden Optionen: • `-q` • `-quiet` • `-s` • `-silent` Verwenden Sie für das MSI-Paket eine der folgenden Optionen: • `/q` • `/quiet`
Erstellen Sie eine Installationsprotokolldatei.	Verwenden Sie für das EXE-Paket eine der folgenden Optionen: • `-l <path_for_log>` • `-log <path_for_log>` Verwenden Sie für das MSI-Paket eine der folgenden Optionen: • `/l <path_for_log>` • `/log <path_for_log>`

Maßnahmen	Befehle
Proxy-Umgehung für den CylanceOPTICS-Agent deaktivieren (nur MSI-Paket).	Verwenden Sie diese Option, wenn der CylanceOPTICS-Agent immer eine bestimmte Proxyverbindung zu den CylanceOPTICS-Cloud-Diensten verwenden soll. Dies ist in den meisten Umgebungen optional, aber bei Verwendung von CylanceHYBRID erforderlich. Bevor Sie das Installationsprogramm mit dem folgenden Befehl ausführen, erstellen Sie den ProxyServer-Registrierungsschlüssel auf dem Gerät. Weitere Informationen finden Sie unter Konfigurieren eines Proxys für die CylancePROTECT Desktop- und Cylance OPTICS-Agenten. Wenn Sie CylanceHYBRID verwenden, lesen Sie die Windows-Installationsanweisungen im CylanceHYBRID-Administratorhandbuch und erstellen Sie den ProxyServer-Registrierungsschlüssel mit dem erforderlichen Wert für CylanceHYBRID. Nachdem Sie den ProxyServer-Registrierungsschlüssel auf dem Gerät erstellt haben, verwenden Sie bei der Installation des Agenten den folgenden Befehl: `HYBRID=True` Das Installationsprogramm erstellt den DisableProxyBypass-Registrierungsschlüssel auf dem Gerät mit dem Wert „True“. Weitere Informationen finden Sie unter Proxyoptionen für den CylanceOPTICS-Agent. Wenn der Befehl auf `False` gesetzt ist, erstellt das Installationsprogramm den Registrierungsschlüssel nicht.
Deinstallieren Sie den CylanceOPTICS-Agent.	`"<CylanceOPTICS_program_directory>\CyOpticsUninstaller.exe"` Beispiel: `"C:\Program Files\Cylance\Optics \CyOpticsUninstaller.exe"` Um eine Deinstallation im Hintergrund durchzuführen, die keine Benutzerinteraktion erfordert, fügen Sie die folgenden Befehle hinzu: `--use_cli -t v20` Wenn Sie den CylanceOPTICS-Agenten so konfiguriert haben, dass ein Deinstallationskennwort erforderlich ist, fügen Sie den folgenden Befehl hinzu: `--password <password>` Beispiel: `"C:\Program Files\Cylance\Optics \CyOpticsUninstaller.exe" --use_cli -t v20 --password samplepass`

macOS

Aktion	Befehle
Installieren Sie den CylanceOPTICS-Agent.	`sudo installer -pkg CylanceOPTICS.pkg -target /`
Installieren Sie den CylanceOPTICS-Agent und erstellen Sie eine Installationsprotokolldatei.	`sudo installer -verboseR -dumplog -pkg CylanceOPTICS.pkg -target /`

Aktion	Befehle
Proxyumgehung für den CylanceOPTICS-Agent deaktivieren	Verwenden Sie diese Option, wenn der CylanceOPTICS-Agent immer eine bestimmte Proxyverbindung zu den CylanceOPTICS-Cloud-Diensten verwenden soll. Dies ist in den meisten Umgebungen optional, aber bei Verwendung von CylanceHYBRID erforderlich. Bevor Sie den CylanceOPTICS-Agent installieren, befolgen Sie die Anweisungen unter Cylance Endpoint Security-Proxy-Anforderungen, um die Proxy-Umgehung für macOS-Geräte zu konfigurieren.
Starten Sie den CylanceOPTICS-Dienst.	`sudo launchctl load /Library/LaunchDaemons/com.cylance.cyoptics_service.plist`
Beenden Sie den CylanceOPTICS-Dienst.	`sudo launchctl unload /Library/LaunchDaemons/com.cylance.cyoptics_service.plist`
Deinstallieren Sie den CylanceOPTICS-Agent.	`sudo /Applications/Cylance/Optics/Uninstall\ CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS`
Deinstallieren Sie den CylanceOPTICS-Agent ohne UI.	`sudo /Applications/Cylance/Optics/Uninstall\ CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS --noui` Wenn Sie diesen Befehl verwenden möchten, sind auf macOS 11.x-Geräten zusätzliche Aktionen erforderlich. Weitere Informationen finden Sie in der Dokumentation zu Cylance Endpoint Security für Administratoren.

Linux

Aktion	Befehle
Installieren Sie den CylanceOPTICS-Agent auf RHEL/CentOS, SUSE oder Amazon Linux 2.	`yum install CylanceOPTICS-<version>.rpm`, wobei <version> die Version der .rpm-Datei ist.
Installieren Sie den CylanceOPTICS-Agent auf Ubuntu.	`dpkg -i cylance-optics_<version>_amd64.deb`, wobei <version> die Version der .deb-Datei ist.
Starten Sie den CylanceOPTICS-Dienst.	`systemctl start cyoptics.service`
Beenden Sie den CylanceOPTICS-Dienst.	`systemctl stop cyoptics.service`
Deinstallieren Sie den CylanceOPTICS-Agent auf RHEL/CentOS, SUSE oder Amazon Linux 2.	`rpm -e CylanceOPTICS`

Aktion	Befehle
Deinstallieren Sie den CylanceOPTICS-Agent unter Ubuntu.	`dpkg -P cylance-optics`

Aktivieren und Konfigurieren von CylanceOPTICS

Wenn Sie CylanceOPTICS in einer Geräterichtlinie aktivieren und diese Richtlinie Geräten und Zonen zuweisen, erfasst der CylanceOPTICS-Agent auf jedem Gerät Ereignisse und speichert Daten in der CylanceOPTICS-Datenbank. Der Agent erfasst erst nach der Aktivierung von CylanceOPTICS Daten.

Bevor Sie beginnen: Stellen Sie sicher, dass die CylancePROTECT Desktop-Anwendungssteuerungsfunktion nicht aktiviert ist. Die Anwendungssteuerung ist für Geräte mit festgelegter Funktion vorgesehen, die nach der Einrichtung nicht geändert werden (z. B. Point-of-Sale-Maschinen). Wenn die Anwendungssteuerung aktiviert ist, funktioniert der CylanceOPTICS-Agent nicht wie erwartet.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Geräterichtlinie**.
2. Erstellen Sie eine neue Richtlinie oder klicken Sie auf eine vorhandene Richtlinie.
3. Aktivieren Sie auf der Registerkarte **CylanceOPTICS-Einstellungen** das Kontrollkästchen **CylanceOPTICS**.
4. Wenn Sie das automatische Hochladen von Fokusdaten mit Bedrohungsbezug aus der CylanceOPTICS-Datenbank auf die Konsole aktivieren möchten, aktivieren Sie im Abschnitt **Bedrohungen** das Kontrollkästchen **Automatisches Hochladen**.

   Wenn Sie diese Option nicht aktivieren, müssen Sie die Konsole verwenden, um Fokusdaten für Geräte anzufordern.
5. Wenn Sie das automatische Hochladen von speicherbezogenen Fokusdaten aus der CylanceOPTICS-Datenbank auf die Konsole aktivieren möchten, aktivieren Sie im Abschnitt **Speicherschutz** das Kontrollkästchen **Automatisches Hochladen**.

   Wenn Sie diese Option nicht aktivieren, müssen Sie die Konsole verwenden, um Fokusdaten für Geräte anzufordern.
6. Wählen Sie im Abschnitt **Konfigurierbare Sensoren** die optionalen CylanceOPTICS-Sensoren aus, die Sie aktivieren möchten. Beachten Sie, dass die optionalen Sensoren nur für 64-Bit-Betriebssysteme unterstützt werden.
7. Geben Sie in das Feld **Maximalen Gerätespeicher festlegen** die maximale Speichermenge in MB an, auf die der CylanceOPTICS-Agent auf jedem Gerät zugreifen kann. Der Standardwert beträgt 1000 MB.
8. Wenn Sie zulassen möchten, dass der CylanceOPTICS-Agent auf Windows- oder macOS-Geräten Betriebssystembenachrichtigungen an den Benutzer sendet, aktivieren Sie das Kontrollkästchen **CylanceOPTICS-Desktop-Benachrichtigungen aktivieren**.
9. Wenn Sie einen Erkennungsregelsatz mit der Geräterichtlinie verknüpfen möchten, klicken Sie in der Dropdown-Liste **Erkennungssatz auswählen** auf einen Regelsatz.
10. Klicken Sie auf **Erstellen** oder auf **Speichern**.

    Wenn Sie eine vorhandene Richtlinie ändern und die aktuellen Einstellungen als neue Geräterichtlinie speichern möchten, klicken Sie stattdessen auf **Speichern unter**.

Wenn Sie fertig sind:

- Weisen Sie die Richtlinie Geräten oder Zonen zu.
- Wenn Sie verhindern möchten, dass Benutzer die Dienste für den CylanceOPTICS-Agent für Windows (CylanceOPTICS 3.1 oder höher mit CylancePROTECT Desktop 3.0 oder höher) und macOS (CylanceOPTICS 3.3 oder höher mit CylancePROTECT Desktop 3.1 oder höher), stoppen können, aktivieren

Sie in der Geräterichtlinie unter **Schutzeinstellungen** die Option **Dienstbeendung über Gerät verhindern**. Wenn diese Einstellung aktiviert ist, können macOS-Benutzer die Dienste nur beenden, wenn die Selbstschutzstufe in den Geräteeigenschaften auf „Lokaler Administrator“ (Assets > Geräte > Ein Gerät auswählen) eingestellt ist. Windows-Benutzer können den Agentendienst nicht beenden, solange diese Einstellung aktiviert ist.

- Wenn Sie möchten, dass Benutzer ein Kennwort eingeben müssen, um den CylancePROTECT Desktop-Agent, den CylanceOPTICS-Agent für Windows Version 3.1 oder höher und den CylanceOPTICS-Agent für macOS Version 3.3 oder höher zu deinstallieren, aktivieren Sie unter **Einstellungen > Anwendung** die Option **Kennwort für Deinstallation von Agent erforderlich**. Die Verwendung dieser Funktion für den CylanceOPTICS-Agenten für macOS erfordert auch CylancePROTECT Desktop Version 3.1 oder höher.

CylanceOPTICS-Sensoren

Die folgenden Sensoren sind standardmäßig im CylanceOPTICS-Agenten aktiviert, wenn Sie CylanceOPTICS in einer Geräterichtlinie aktivieren. Sie können diese Sensoren nicht deaktivieren. Weitere Informationen zu den optionalen Sensoren, die Sie aktivieren können, finden Sie unter CylanceOPTICS optionale Sensoren.

Weitere Informationen zu den Ereignissen, Artefakten und Ereignistypen, die sowohl dem Standardsensor als auch dem optionalen Sensor zugeordnet sind, finden Sie unter Datenstrukturen, die von CylanceOPTICS zur Identifizierung von Bedrohungen verwendet werden.

Sensor	Plattform	Beschreibung	Ereignistypen
Gerät	macOS Linux	Sammelt relevante Geräteinformationen	Mounten
Datei	Windows macOS Linux	Sammelt Informationen über Dateivorgänge	• Erstellen • Löschen • Überschreiben • Umbenennen • Schreiben
Speicher	macOS Linux	Sammelt Informationen über Speichervorgänge	• Mmap • MProtect
Netzwerk	Windows macOS Linux	Sammelt Informationen über Netzwerkverbindungen	Verbinden

Sensor	Plattform	Beschreibung	Ereignistypen
Prozess	Windows macOS Linux	Sammelt Informationen über Prozessvorgänge	Die unterstützten Ereignistypen unterscheiden sich je nach Plattform. Siehe Prozessabschnitt unter Datenstrukturen, die von CylanceOPTICS zur Identifizierung von Bedrohungen verwendet werden. • Anormales Beenden • Schließen • Erzwungenes Beenden • PTrace • Start • Aussetzen • Unbekanntes Linux-Prozessereignis
Registrierung	Windows	Sammelt Informationen über Registrierungsvorgänge	• KeyCreated • KeyDeleting • ValueChanging • ValueDeleting

CylanceOPTICS optionale Sensoren

Sie können die folgenden CylanceOPTICS-Sensoren aktivieren, um zusätzliche Daten zu erfassen, die über die standardmäßigen Prozess-, Datei-, Netzwerk-, Registrierungsereignisse hinausgehen. Die Aktivierung optionaler Sensoren kann sich auf die Leistung und die Ressourcennutzung auf Geräten sowie auf die in der CylanceOPTICS-Datenbank gespeicherte Datenmenge auswirken. BlackBerry empfiehlt die Aktivierung optionaler Sensoren bei einer kleinen Anzahl von Geräten, um die Auswirkungen zu beurteilen.

Die optionalen Sensoren werden nur für 64-Bit-Betriebssysteme unterstützt, wenn nicht anders dargestellt.

Sensor	Beschreibung	Bewährte Verfahren	Notizen
Erweiterte Scripting-Sichtbarkeit	Der CylanceOPTICS-Agent zeichnet Befehle, Argumente, Skripte und Inhalte von JScript-, PowerShell- (Konsole und integrierte Scripting-Umgebung), VBScript- und VBA-Makroskriptausführungen auf. Signal-Rausch-Verhältnis: hoch Potenzielle Auswirkungen auf Datenspeicherung und Leistung: gering bis moderat	Empfohlen für: • Desktops • Laptops • Server Nicht empfohlen für Microsoft Exchange- und E-Mail-Server.	• Von Microsoft bereitgestellte Tools und andere Drittanbieterlösungen können bei der Ausführung von Vorgängen stark auf PowerShell angewiesen sein. • Um eine optimale Datenspeicherung sicherzustellen, empfiehlt BlackBerry Erkennungsausnahmen für vertrauenswürdige Tools zu konfigurieren, die PowerShell intensiv nutzen.
Erweiterte WMI-Sichtbarkeit	Der CylanceOPTICS-Agent zeichnet zusätzliche WMI-Attribute und -Parameter auf. Signal-Rausch-Verhältnis: hoch Potenzielle Auswirkungen auf Datenspeicherung und Leistung: gering	Empfohlen für: • Desktops • Laptops • Server	• Einige Hintergrund- und Wartungsprozesse von Windows nutzen WMI zur Planung von Aufgaben oder Ausführung von Befehlen, was zu plötzlicher hoher WMI-Aktivität führen kann. • BlackBerry empfiehlt, die WMI-Nutzung in Ihrer Umgebung zu analysieren, bevor Sie diesen Sensor aktivieren.
API-Sensor	Der CylanceOPTICS-Agent überwacht eine identifizierte Gruppe von Windows API-Aufrufen. Signal-Rausch-Verhältnis: moderat Potenzielle Auswirkungen auf Datenspeicherung und Leistung: Die Aktivierung dieses Sensors kann sich auf die CPU-Leistung eines Geräts auswirken.	Empfohlen für: • Desktops • Laptops • Server	• Unterstützt auf x86- oder x64-Windows-Betriebssystemen. • Erfordert CylancePROTECT Desktop-Agent Version 3.0.1003 oder höher. • Erfordert CylanceOPTICS-Agent Version von 3.2 oder höher.

Sensor	Beschreibung	Bewährte Verfahren	Notizen
COM-Objekt-Sichtbarkeit	Der CylanceOPTICS-Agent überwacht COM-Schnittstellen- und API-Aufrufe, um schädliche Verhaltensweisen wie eine geplante Aufgabenerstellung zu erkennen. Signal-Rausch-Verhältnis: hoch Potenzielle Auswirkungen auf Datenspeicherung und Leistung: Die Aktivierung dieses Sensors kann sich auf die CPU-Leistung auswirken.	Empfohlen für: • Desktops • Laptops Nicht für Server empfohlen.	• Nur Windows. • Erfordert CylancePROTECT Desktop-Agenten Version 3.2 oder höher. • Erfordert CylanceOPTICS-Agent Version von 3.3 oder höher.
Cryptojacking-Erkennung	Der CylanceOPTICS-Agent überwacht die Intel-CPU-Aktivität mithilfe von Hardwareregistern auf potenzielle Cryptomining- und Cryptohacking-Aktivitäten. Signal-Rausch-Verhältnis: moderat Potenzielle Auswirkungen auf Datenspeicherung und Leistung: gering	Unterstützt für: • Windows 10 x64 • Intel Gen 6 bis 10	**Hinweis:** BlackBerry empfiehlt, diesen Sensor zu deaktivieren, da momentan Stabilitätsprobleme untersucht werden, die dieser Sensor mit dem Betriebssystem des Geräts verursachen kann. • Nicht unterstützt für virtuelle Maschinen. • Nicht unterstützt für Intel-Prozessoren der Generation 11 oder höher. BlackBerry rät davon ab, diesen Sensor für Gen 11 oder höher zu aktivieren.
DNS-Sichtbarkeit	Der CylanceOPTICS-Agent zeichnet DNS-Anforderungen, Antworten und zugehörige Datenfelder wie Domänenname, aufgelöste Adressen und Datensatztyp auf. Signal-Rausch-Verhältnis: moderat Potenzielle Auswirkungen auf Datenspeicherung und Leistung: moderat	Empfohlen für: • Desktops • Laptops Nicht empfohlen für DNS-Server.	• Beachten Sie, dass dieser Sensor erhebliche Datenmengen erfassen kann. Er kann aber auch Einblicke in Daten liefern, die mit anderen Tools nur schwer erfasst werden können. • Um eine optimale Datenspeicherung sicherzustellen, empfiehlt BlackBerry, Erkennungsausnahmen für vertrauenswürdige Tools zu konfigurieren, die Cloud-basierte Dienste intensiv nutzen.

Sensor	Beschreibung	Bewährte Verfahren	Notizen
Erweiterte Dateilesesichtbarkeit	Der CylanceOPTICS-Agent überwacht Dateilesevorgänge innerhalb einer angegebenen Verzeichnisgruppe. Signal-Rausch-Verhältnis: moderat Potenzielle Auswirkungen auf Datenspeicherung und Leistung: gering	Empfohlen für: • Desktops • Laptops • Server	• Einige Sicherheitstools von Drittanbietern verwenden möglicherweise die Windows-APIs, von denen dieser Sensor Daten erfasst. In einigen Fällen kann es sein, dass CylanceOPTICS irrelevante oder vertrauenswürdige Daten aufzeichnet. • Um eine optimale Datenspeicherung sicherzustellen und ein besseres Signal-Rausch-Verhältnis zu ermöglichen, empfiehlt BlackBerry, Erkennungsausnahmen für vertrauenswürdige Sicherheitstools zu konfigurieren.
Erweitertes Parsing übertragbarer ausführbarer Dateien	Der CylanceOPTICS-Agent zeichnet Datenfelder auf, die mit übertragbaren ausführbaren Dateien verknüpft sind, z. B. Dateiversion, Importfunktionen und Packertypen. Signal-Rausch-Verhältnis: moderat Potenzielle Auswirkungen auf Datenspeicherung und Leistung: gering	Empfohlen für: • Desktops • Laptops • Server	• Die von diesem Sensor erfassten Daten werden zur Unterstützung der erweiterten Analyse übertragbarer ausführbarer Dateien an die Kontextanalyse-Engine weitergeleitet und nicht in der CylanceOPTICS-Datenbank gespeichert. • Die Aktivierung dieses Sensors wirkt sich kaum oder gar nicht auf die Datenspeicherung von CylanceOPTICS aus. • Wenn Sie eine Erkennungsregel hinzufügen und aktivieren, die Zeichenfolgenressourcen analysiert, verbraucht der CylanceOPTICS-Agent möglicherweise erhebliche CPU- und Speicherressourcen.

Sensor	Beschreibung	Bewährte Verfahren	Notizen
Erweiterte Prozess- und Hooking-Sichtbarkeit	Der CylanceOPTICS-Agent zeichnet Prozessinformationen der Win32-API und von Kernel-Audit-Meldungen auf, um Formen von Prozess-Hooking und -Injektion zu erkennen. Signal-Rausch-Verhältnis: moderat Potenzielle Auswirkungen auf Datenspeicherung und Leistung: gering	Empfohlen für: • Desktops • Laptops • Server	• Einige Sicherheitstools von Drittanbietern verwenden möglicherweise die Windows-APIs, von denen dieser Sensor Daten erfasst. In einigen Fällen kann es sein, dass CylanceOPTICS irrelevante oder vertrauenswürdige Daten aufzeichnet. • Um eine optimale Datenspeicherung sicherzustellen und ein besseres Signal-Rausch-Verhältnis zu ermöglichen, empfiehlt BlackBerry, Erkennungsausnahmen für vertrauenswürdige Sicherheitstools zu konfigurieren.
HTTP-Sichtbarkeit	Der CylanceOPTICS-Agent verfolgt Windows HTTP-Transaktionen, einschließlich Event Tracing für Windows, WinINet-APIs und WinHTTP-APIs. Signal-Rausch-Verhältnis: hoch Potenzielle Auswirkungen auf Datenspeicherung und Leistung: Die Aktivierung dieses Sensors kann sich auf die CPU-Leistung auswirken.	Empfohlen für: • Desktops • Laptops Nicht für Server empfohlen.	• Nur Windows. • Erfordert CylancePROTECT Desktop-Agenten Version 3.2 oder höher. • Erfordert CylanceOPTICS-Agent Version von 3.3 oder höher.
Module-Load-Sichtbarkeit	Der CylanceOPTICS-Agent überwacht die Module-Loads. Signal-Rausch-Verhältnis: hoch Potenzielle Auswirkungen auf Datenspeicherung und Leistung: Die Aktivierung dieses Sensors kann sich auf die CPU-Leistung auswirken.	Empfohlen für: • Desktops • Laptops • Server	• Nur Windows. • Erfordert CylancePROTECT Desktop-Agenten Version 3.2 oder höher. • Erfordert CylanceOPTICS-Agent Version von 3.3 oder höher.

Sensor	Beschreibung	Bewährte Verfahren	Notizen
Sichtbarkeit private Netzwerkadresse	Der CylanceOPTICS-Agent erfasst Netzwerkverbindungen innerhalb der RFC 1918- und RFC 4193-Adressräume. Signal-Rausch-Verhältnis: gering Potenzielle Auswirkungen auf Datenspeicherung und Leistung: gering	Empfohlen für Desktops. Nicht empfohlen für: • DNS-Server • Mit wenigen oder sehr wenigen Ressourcen ausgestattete Systeme • Systeme, die RDP oder andere Remote-Zugriff-Software verwenden	• Dieser Sensor erfasst erhebliche Datenmengen und kann sich auf die Dauer der Datenspeicherung in der CylanceOPTICS-Datenbank auswirken. • BlackBerry empfiehlt, diesen Sensor nur in Umgebungen zu aktivieren, in denen vollständige Sichtbarkeit bei der Adresskommunikation im privaten Netzwerk erforderlich ist.
Windows Advanced Audit-Sichtbarkeit	Der CylanceOPTICS-Agent überwacht zusätzliche Windows-Ereignistypen und -Kategorien. Signal-Rausch-Verhältnis: moderat Potenzielle Auswirkungen auf Datenspeicherung und Leistung: gering	—	Dieser Sensor ermöglicht die Überwachung der folgenden Ereignis-IDs: • 4769 Kerberos-Ticket-Anforderung • 4662 Vorgang an Active Directory-Objekt • 4624 Erfolgreiche Anmeldung • 4702 Erstellung geplanter Aufgaben
Windows Event Log-Sichtbarkeit	Der CylanceOPTICS-Agent zeichnet Windows-Sicherheitsereignisse und die zugehörigen Attribute auf. Signal-Rausch-Verhältnis: moderat Potenzielle Auswirkungen auf Datenspeicherung und Leistung: moderat	Empfohlen für: • Desktops • Laptops • Server Nicht empfohlen für: • Domänencontrolle • Microsoft Exchange und E-Mail-Server	• Die Windows-Ereignisprotokolle, aus denen dieser Sensor Daten erfasst, werden während der normalen Systemnutzung regelmäßig generiert. • Um doppelte Daten zu reduzieren und eine optimale Datenspeicherung zu ermöglichen, sollten Sie ermitteln, ob Ihr Unternehmen bereits über Tools verfügt, mit denen Daten aus Windows-Ereignisprotokollen erfasst werden.

Datenstrukturen, die von CylanceOPTICS zur Identifizierung von Bedrohungen verwendet werden

Ereignisse, Artefakte und Facetten sind die drei primären Datenstrukturen, die von CylanceOPTICS zur Analyse, Aufzeichnung und Untersuchung von Aktivitäten auf Geräten verwendet werden. Die Funktionen von CylanceOPTICS basieren auf diesen Datenstrukturen. Dies schließt InstaQuery, Fokusdaten und die Kontextanalyse-Engine (Context Analysis Engine, CAE) ein.

Dieser Abschnitt enthält weitere Informationen darüber, wie CylanceOPTICS Aktivitäten auf Geräten interpretiert und mit diesen interagiert, damit Sie Erkennungen, Abfragen und Fokusdaten besser verstehen und nutzen können.

Datenquellen nach Betriebssystem

Der CylanceOPTICS-Agent verwendet die folgenden Datenquellen:

OS	Datenquellen
Windows	• Kernel-Treiber CyOpticsDrv • Ereignisverfolgung • Sicherheitsüberwachungsprotokoll
macOS	Kernel-Treiber CyOpticsDrvOSX
Linux	ZeroMQ

Informationen zu den Arten des Netzwerkverkehrs, die in CylanceOPTICS standardmäßig ausgeschlossen sind, finden Sie unter KB 65604.

Ereignisse

Ereignisse sind die Komponenten, die zu einer beobachtbaren Änderung oder Aktion auf einem Gerät führen. Ereignisse bestehen aus zwei primären Artefakten: dem auslösenden Artefakt, das eine Aktion auslöst, und dem Zielartefakt, auf das eingewirkt wird.

Die folgenden Tabellen enthalten Details zu den Ereignistypen, die CylanceOPTICS erkennen kann und mit denen es interagieren kann.

Ereignis: Beliebige

- Geräterichtlinienoption zur Aktivierung: Kontrollkästchen CylanceOPTICS
- Artefakttyp: Prozess, Benutzer
- Plattform: Windows, macOS, Linux

Ereignistyp	Beschreibung
Beliebige	Alle Ereignisse zeichnen den Prozess auf, über den sie generiert wurden, sowie den Benutzer, der mit der Aktion verknüpft ist.

Ereignis: Anwendung

- Geräterichtlinienoption zur Aktivierung: Erweiterte WMI-Sichtbarkeit
- Artefakttyp: WMI-Trace
- Plattform: Windows

Ereignistyp	Beschreibung
Filter-Consumer-Bindung erstellen	Ein Prozess hat WMI-Persistenz verwendet.
Temporären Consumer erstellen	Ein Prozess hat WMI-Ereignisse abonniert.
Vorgang ausführen	Ein Prozess hat einen WMI-Vorgang ausgeführt.

- Geräterichtlinienoption zur Aktivierung: Erweiterte Prozess- und Hooking-Sichtbarkeit
- Artefakttyp: Datei
- Plattform: Windows

Ereignistyp	Beschreibung
CBT	Die SetWindowsHookEx-API hat einen Hook installiert, um Benachrichtigungen zu erhalten, die für eine CBT-Anwendung nützlich sind.
DebugProc	Die SetWindowsHookEx-API hat einen Hook installiert, um andere Hook-Prozeduren zu debuggen.
Status asynchroner Schlüssel abrufen	Ein Prozess hat die Win32-GetAsyncKeyState-API aufgerufen.
JournalPlayback	Die SetWindowsHookEx-API hat einen Hook installiert, um Nachrichten zu überwachen, die zuvor über die Hook-Prozedur WH_JOURNALRECORD aufgezeichnet wurden.
JournalRecord	Die SetWindowsHookEx-API hat einen Hook zur Überwachung von Eingabemeldungen installiert, die in die Systemnachrichten-Warteschlange gestellt wurden.
Tastatur	Die SetWindowsHookEx-API hat einen Hook zur Überwachung von Tastaturanschlagmeldungen installiert.
LowLevel-Tastatur	Die SetWindowsHookEx-API hat einen Hook zur Überwachung von Low-Level-Tastatureingabe-Ereignissen installiert.
LowLevel-Maus	Die SetWindowsHookEx-API hat einen Hook zur Überwachung von Low-Level-Mauseingabe-Ereignissen installiert.
Nachricht	Die SetWindowsHookEx-API hat einen Hook zur Überwachung von Meldungen installiert, die in eine Nachrichtenwarteschlange gestellt wurden.
Maus	Die SetWindowsHookEx-API hat einen Hook zur Überwachung von Mausmeldungen installiert.
Raw-Eingabegeräte registrieren	Ein Prozess hat die Win32-RegisterRawInputDevices-API aufgerufen.
Windows-Ereignis-Hook festlegen	Ein Prozess hat die Win32-SetWinEventHook-API aufgerufen.

Ereignistyp	Beschreibung
Windows-Hook festlegen	Die SetWindowsHookEx-API hat einen nicht aufgeführten Hooktyp-Wert installiert.
ShellProc	Die SetWindowsHookEx-API hat einen Hook installiert, um Benachrichtigungen zu erhalten, die für Shell-Anwendungen nützlich sind.
SysMsg	Die SetWindowsHookEx-API hat einen Hook zur Überwachung von Meldungen installiert, die als Ergebnis eines Eingabeereignisses in einem Dialogfeld, einem Meldungsfeld oder einer Bildlaufleiste generiert werden.
WindowProc	Die SetWindowsHookEx-API hat einen Hook zur Überwachung von Windows-Prozedurmeldungen installiert.

- Geräterichtlinienoption zur Aktivierung: API-Sensor
- Artefakttyp: API-Aufruf
- Plattform: Windows

Ereignistyp	Beschreibung
Funktion	Es wurde ein auffälliger Funktionsaufruf erkannt.

- Geräterichtlinienoption zur Aktivierung: Module-Load-Sichtbarkeit
- Artefakttyp: Datei
- Plattform: Windows

Ereignistyp	Beschreibung
Laden	Eine Anwendung hat ein Modul geladen.

- Geräterichtlinienoption zur Aktivierung: COM-Objekt-Sichtbarkeit
- Plattform: Windows

Ereignistyp	Beschreibung
Erstellt	Ein COM-Objekt wurde erstellt.

Ereignis: Gerät

- Geräterichtlinienoption zur Aktivierung: Kontrollkästchen CylanceOPTICS
- Artefakttyp: Datei
- Plattform: macOS, Linux

Ereignistyp	Beschreibung
Mounten	Das Gerät ist mit einer Maschine verbunden oder Ordner werden auf bestimmte Netzwerkspeicherorte gemountet.

Ereignis: Datei

- Geräterichtlinienoption zur Aktivierung: Kontrollkästchen CylanceOPTICS
- Artefakttyp: Datei
- Plattform: Windows, macOS, Linux

Ereignistyp	Beschreibung
Erstellen	Es wurde eine Datei erstellt.
Löschen	Eine Datei wurde gelöscht.
Überschreiben	Eine Datei wurde überschrieben.
Umbenennen	Eine Datei wurde umbenannt.
Schreiben	Eine Datei wurde geändert.

- Geräterichtlinienoption zur Aktivierung: Erweiterte Dateilesesichtbarkeit
- Artefakttyp: Datei
- Plattform: Windows

Ereignistyp	Beschreibung
Offen	Eine Datei wurde geöffnet.

Ereignis: Arbeitsspeicher

- Geräterichtlinienoption zur Aktivierung: Kontrollkästchen CylanceOPTICS
- Artefakttyp: Prozess
- Plattform: macOS, Linux

Ereignistyp	Beschreibung
Mmap	Ein Arbeitsspeicherbereich wurde einem bestimmten Zweck zugeordnet, der in der Regel einem Prozess zugeordnet ist.
MProtect	Die Metadaten wurden für einen Arbeitsspeicherbereich geändert, in der Regel um den Status zu ändern (z. B. um sie ausführbar zu machen).

Ereignis: Netzwerk

- Geräterichtlinienoption zur Aktivierung: Kontrollkästchen CylanceOPTICS
- Artefakttyp: Netzwerk
- Plattform: Windows, macOS, Linux

Ereignistyp	Beschreibung
Verbinden	Es wurde eine Netzwerkverbindung geöffnet. Standardmäßig wird lokaler Datenverkehr nicht erfasst.

- Geräterichtlinienoption zur Aktivierung: Sichtbarkeit privater Netzwerkadressen
- Artefakttyp: Netzwerk

- Plattform: Windows

Ereignistyp	Beschreibung
Verbinden	Verbindungsereignisse schließen lokalen Datenverkehr ein.

- Geräterichtlinienoption zur Aktivierung: DNS-Sichtbarkeit
- Artefakttyp: DNS-Anforderung
- Plattform: Windows, Linux

Ereignistyp	Beschreibung
Anforderung	Ein Prozess hat eine Netzwerk-DNS-Anforderung erstellt, die nicht zwischengespeichert wurde.
Antwort	Ein Prozess hat eine DNS-Antwort empfangen.

- Geräterichtlinienoption zur Aktivierung: HTTP-Sichtbarkeit
- Artefakttyp: HTTP
- Plattform: Windows

Ereignistyp	Beschreibung
Get	Windows hat WinINet oder WinHTTP verwendet, um eine HTTP-Anforderung zu stellen.
Post	Windows hat WinINet oder WinHTTP zum Senden von Daten verwendet.

Ereignis: Prozess

- Geräterichtlinienoption zur Aktivierung: Kontrollkästchen CylanceOPTICS
- Artefakttyp: Prozess

Ereignistyp	Plattform	Beschreibung
Anormales Beenden	macOS Linux	Ein vom Vorauswahlsensor überwachter Prozess wurde ohne Abschluss beendet (eine Ausnahme hat z. B. dazu geführt, dass ein Prozess beendet wurde).
Schließen	Windows macOS Linux	Ein Prozess wurde beendet.
Erzwungenes Beenden	macOS Linux	Ein vom Vorauswahlsensor überwachter Prozess wurde durch einen anderen Prozess zur Beendigung gezwungen.
PTrace	macOS Linux	Dies ist ein Unix-Systemtool, mit dem ein Prozess einen anderen Prozess überwachen und steuern kann.

Ereignistyp	Plattform	Beschreibung
Start	Windows macOS Linux	Ein Prozess wurde gestartet.
Aussetzen	Linux	Ein vom Vorauswahlsensor überwachter Prozess wurde ausgesetzt.
Unbekanntes Linux-Prozessereignis	macOS Linux	Ein vom Vorauswahlsensor überwachtes unbekanntes Ereignis ist aufgetreten, das auf den Prozess abzielt. Dies kann ein Zeichen dafür sein, dass schädliche Software ihre Aktivität verdeckt.

- Geräterichtlinienoption zur Aktivierung: Erweiterte Prozess- und Hooking-Sichtbarkeit
- Artefakttyp: Prozess
- Plattform: Windows

Ereignistyp	Beschreibung
SetThreadContext	Ein Prozess hat die SetThreadContext-API aufgerufen.
Beenden	Ein auslösender Prozess hat einen anderen Zielprozess beendet.

Ereignis: Registrierung

- Geräterichtlinienoption zur Aktivierung: Kontrollkästchen CylanceOPTICS
- Artefakttyp: Registrierung, Datei (wenn der Registrierungsschlüssel auf eine bestimmte Datei verweist)
- Plattform: Windows

Ereignistyp	Beschreibung
KeyCreated	Ein Registrierungsschlüssel wurde erstellt.
KeyDeleting	Ein Registrierungsschlüssel wurde gelöscht.
ValueChanging	Der Wert eines Registrierungsschlüssels wurde geändert.
ValueDeleting	Ein Registrierungsschlüsselwert wurde gelöscht.

Ereignis: Scripting

- Geräterichtlinienoption zur Aktivierung: Erweiterte Scripting-Sichtbarkeit
- Artefakttyp: PowerShell-Trace
- Plattform: Windows

Ereignistyp	Beschreibung
Befehl ausführen	Windows PowerShell hat einen Befehl ausgeführt. Die Parameter sind unbekannt.

Ereignistyp	Beschreibung
Skript ausführen	Windows PowerShell hat ein Skript ausgeführt.
SkriptBlock ausführen	Windows PowerShell hat einen Skriptblock ausgeführt.
Befehl aufrufen	Windows PowerShell hat einen Befehl mit gebundenen Parametern aufgerufen.
Skript verhindern	Ein AMSI-ScanBuffer-Ergebnis zeigt an, dass ein Skript von einem Administrator erkannt oder blockiert wurde.

Ereignis: Benutzer

- Geräterichtlinienoption zur Aktivierung: Erweiterte Scripting-Sichtbarkeit
- Artefakttyp: Windows-Ereignis
- Plattform: Windows

Ereignistyp	Beschreibung
Batch-Abmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 4).
Batch-Anmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 4).
CachedInteractive-Abmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 11).
CachedInteractive-Anmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 11).
Interaktive Abmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 2).
Interaktive Anmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 2).
Netzwerkabmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 3).
Netzwerkanmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 3).
NetworkClearText-Abmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 8).
NetworkClearText-Anmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 8).
NewCredentials-Abmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 9).
NewCredentials-Anmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 9).

Ereignistyp	Beschreibung
RemoteInteractive-Abmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 10).
RemoteInteractive-Anmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 10).
Dienstabmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 5).
Dienstanmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 5).
Entsperr-Abmelden	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (Typ 7).
Entsperr-Anmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (Typ 7).
Benutzerabmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4634 (nicht aufgeführter Typwert).
Benutzeranmeldung	Die folgende Windows-Ereignis-ID ist aufgetreten: 4624 (nicht aufgeführter Typwert).

Artefakte und Facetten

Artefakte sind komplexe Informationen, die von CylanceOPTICS verwendet werden können. Die Kontextanalyse-Engine (Context Analysis Engine, CAE) kann Artefakte auf Geräten identifizieren und diese verwenden, um automatische Vorfallreaktionen und Behebungsaktionen auszulösen. InstaQueries verwenden Artefakte als Grundlage einer Abfrage.

Facetten sind die Attribute eines Artefakts, mit denen die Merkmale eines Artefakts identifiziert werden können, das mit einem Ereignis verknüpft ist. Facetten werden während der Analyse korreliert und kombiniert, um potenziell schädliche Aktivitäten zu identifizieren. Eine Datei mit dem Namen „Explorer.exe“ ist beispielsweise nicht von Natur aus verdächtig. Wenn die Datei jedoch nicht von Microsoft signiert ist und sich in einem temporären Verzeichnis befindet, kann sie in einigen Umgebungen als verdächtig identifiziert werden.

CylanceOPTICS verwendet die folgenden Artefakte und Facetten:

Artefakt	Facetten
API-Aufruf	• Funktion • DLL • Parameter
DNS	• Verbindung • IsRecursionDesired • IsUnsolicitedResponse • Opcode • RequestId • Auflösung • ResponseOriginatedFromThisDevice • Fragen

Artefakt	Facetten
Ereignis	• Zeitpunkt des Auftretens • Zeitpunkt der Registrierung
Datei	• Ausführbarer Datensatz (nur Binärdateien) • Dateierstellungszeitpunkt (vom Betriebssystem gemeldet) • Dateipfad • Dateisignatur (nur Binärdateien) • Dateigröße • Letzter Änderungszeitpunkt (vom Betriebssystem gemeldet) • MD5-Hash (nur Binärdateien) • Letzter Schreibort • SHA256-Hash (nur Binärdateien) • Vermuteter Dateityp • Benutzer
Netzwerk	• Lokale Adresse • Lokaler Port • Protokoll • Remote-Adresse • Remote-Port
PowerShell-Trace	• EventId • Payload • PayloadAnalysis • ScriptBlockText • ScriptBlockTextAnalysis
Prozess	• Befehlszeile • Datei, aus der die ausführbare Datei ausgeführt wurde • Übergeordneter Prozess • Prozess-ID • Anfangszeit • Benutzer
Registrierung	• Wenn der Wert auf eine Datei im System verweist • Registrierungspfad • Wert

Artefakt	Facetten
Benutzer	• Domäne • Betriebssystemspezifische Kennung (z. B. SID) • Benutzername Benutzerartefakte können einen der folgenden Werte enthalten. Die Daten sind jedoch auf den meisten Geräten nicht verfügbar: • AccountType • BadPasswordCount • Kommentar • CountryCode • FullName • HasPasswordExpired • HomeDirectory • IsAccountDisabled • IsLocalAccount • IsLockedOut • IsPasswordRequired • LanguageCodePage • LogonServer • PasswordAge • PasswordDoesNotExpire • ProfilePath • ScriptPath • UserPrivilege • Workstations
Windows-Ereignis	• Klasse • Ereignis-ID • ObjectServer • PrivilegeList • Prozess-ID • Prozessname • Anbietername • Dienst • SubjectDomainName • SubjectLogonId • SubjectUserName • SubjectUserSid
WMI-Trace	• ConsumerText • ConsumerTextAnalysis • EventId • Namespace • Vorgang • OperationAnalysis • OriginatingMachineName

Registrierungsschlüssel und -werte

CylanceOPTICS überwacht die allgemeinen Schlüssel und Werte für Persistenz, Prozessstart und Berechtigungseskalation sowie die in KB 66266 angegebenen Werte.

Weitere Informationen darüber, wie CylanceOPTICS Persistenzpunkte in der Registrierung überwacht, finden Sie unter KB 66357.

Einrichten von CylanceGATEWAY

Hinweis: Wenn CylanceGATEWAY für Ihren Mandanten nicht aktiviert ist, werden die Menüoptionen zur Konfiguration des Mandanten nicht in der Verwaltungskonsole angezeigt. Wenn sich ein Benutzer mit unzureichenden Berechtigungen bei der Verwaltungskonsole anmeldet, wird beim Auswählen einer Menüoption die Fehlermeldung „Keine Berechtigungen“ angezeigt. Weitere Informationen zu der Fehlermeldung finden Sie unter support.blackberry.com/community in Artikel 98223.

Die DNS-Auflösung von IPv6-Adressen wird nicht unterstützt. IPv6-Adressen werden nicht an den CylanceGATEWAY-Agent zurückgegeben.

Schritt	Aktion
1	Installieren Sie BlackBerry Connectivity Node und mindestens einen CylanceGATEWAY Connector und richten Sie sie ein.
2	Geben Sie die Adressen an, die Teil des privaten Netzwerks sind.
3	Geben Sie die privaten DNS-Einstellungen und -Suffixe an.
4	Prüfen Sie die vorhandenen CylanceGATEWAY-Netzwerkdienste oder definieren Sie Ihre eigenen, um das Erstellen von ACL-Regeln (Access Control List) auf Mandanten zu vereinfachen (optional).
5	Konfigurieren Sie ACL-Regeln für Mandanten, um zu verwalten, auf welche Internet- und privaten Netzwerkziele CylanceGATEWAY den Zugriff zulässt oder blockiert.
6	Konfigurieren des Netzwerkschutzes um die Bedrohungen anzugeben, die von CylanceGATEWAY erkannt werden, und wie sie behandelt werden
7	Fügen Sie Benutzer für CylanceGATEWAY hinzu.
8	Konfigurieren der Gateway-Dienstoptionen um betriebssystemspezifische Optionen anzugeben.
9	Konfigurieren Sie Registrierungsrichtlinien, damit die Benutzer die CylancePROTECT Mobile-App oder den CylanceGATEWAY-Agenten auf ihren Geräten aktivieren können.
10	Zuweisen von Richtlinien zu Administratoren, Benutzern und Gruppen. Benutzern müssen eine Registrierungsrichtlinie und eine Gateway-Service-Richtlinie zugewiesen sein, bevor sie den CylanceGATEWAY-Agent aktivieren können.

Schritt	Aktion
11	Gerätebenutzer installieren und aktivieren die CylancePROTECT Mobile-App auf iOS-, Android- und Chromebook-Geräten, und den CylanceGATEWAY-Agent auf Windows- und macOS-Geräten. Optional können Sie eine Installation im Hintergrund oder ein Upgrade des CylanceGATEWAY-Agenten durchführen. Sie können die Agenten von der BlackBerry-Website herunterladen. Weitere Informationen zur CylancePROTECT Mobile-App und zum CylanceGATEWAY-Agenten finden Sie im Cylance Endpoint Security-Benutzerhandbuch. Optional können Sie Cylance Endpoint Security mit BlackBerry UEM oder Microsoft Intune integrieren, um zu überprüfen, ob iOS- und Android-Geräte von UEM oder Intune verwaltet werden, bevor sie CylanceGATEWAY verwenden können. Weitere Informationen finden Sie unter Verbinden von Cylance Endpoint Security mit MDM-Lösungen, um zu überprüfen, ob Geräte verwaltet werden.
12	Verwenden eigener IP-Adressen (BYOIP) zur Bereitstellung größerer dedizierter IP-Adressen zur Steuerung des Datenverkehrs, wie z. B. die Verwendung der eigenen IP-Adresse Ihres Unternehmens für Quell-IP-Pinning und das Zulassen eines einzelnen IP-Adressbereichs oder einer CIDR-Adresse anstelle mehrerer nicht kontinuierlicher IP-Adressen. (Optional)

Definieren Ihres privaten Netzwerks

Um mit CylanceGATEWAY den Zugriff auf Ihre privaten Netzwerke zu steuern, müssen Sie Ihr privates Netzwerk definieren. Wenn Sie Ihre privaten Netzwerke definieren, können Sie CylanceGATEWAY so konfigurieren, dass die strengsten Berechtigungen und Mikrosegmentierungen angewendet werden, wenn Benutzer auf Ihre Netzwerkressourcen zugreifen. CylanceGATEWAY unterstützt den Zugriff auf mehr als ein privates Netzwerk (z. B. Segmente, Rechenzentren und VPCs) sowohl in lokalen als auch in Cloud-Umgebungen. CylanceGATEWAY verhindert, dass Benutzer eine Verbindung zu einem Standort in Ihrem privaten Netzwerk herstellen, es sei denn, dem Benutzer wird eine Zugriffssteuerungsregel (ACL-Regel) zugewiesen, die die Verbindung zulässt.

Sie definieren Ihre privaten Netzwerke, indem Sie eine Connector-Gruppe für jedes private Netzwerk hinzufügen, in dem Benutzer auf Ressourcen zugreifen können sollen. Wenn Ihr CylanceGATEWAY-Dienst vor Juli 2023 aktiviert wurde und mindestens einen CylanceGATEWAY Connectors umfasst, wurden alle vorhandenen Connectors in die „Standard-Connector-Gruppe“ verschoben. Sie können die Standard-Connector-Gruppe umbenennen oder zusätzliche Gruppen hinzufügen und die Connectors nach Bedarf zuweisen.

Jeder Mandant unterstützt maximal acht Connector-Gruppen.

Connector-Gruppen bestehen aus:

- IP-Adressen, IP-Adressbereichen und CIDR-Notation, die Sie für jede Gruppe angeben. CylanceGATEWAY Connectors erkennt diese Adressen als Teil eines Ihrer privaten Netzwerke.
- Die Systemdiagnose-URL. Diese ist für die Gruppe eindeutig und wird von jedem CylanceGATEWAY Connector in der Gruppe verwendet, um die Verbindung zu Ihrem privaten Netzwerk zu bestätigen.
- Die IP-Einschränkungen, die Sie festlegen können, damit das Gateway nur Verbindungen von Connectors mit den angegebenen IP-Adressen akzeptiert.

Um einen sicheren Tunnel zwischen Benutzergeräten und Ihrem privaten Netzwerk einzurichten, müssen Sie mindestens einen CylanceGATEWAY Connectors installieren und einer Gruppe zuweisen.

Jede Connector-Gruppe unterstützt maximal acht CylanceGATEWAY Connectors.

Sie können auch die Adressen Ihrer privaten DNS-Server und die privaten DNS-Suffixe angeben, die für Suchvorgänge verwendet werden. Die DNS-Einstellungen gelten für alle Gruppen-Connector in Ihrer Umgebung und müssen einer Gruppe hinzugefügt werden.

In Umgebungen, die mehrere Gruppen mit ähnlichen Ziel-IP-Adressen oder Adressbereichen enthalten, wird der Datenfluss der Reihe nach an die aufgeführten Connector-Gruppen geleitet, bis die IP-Adresse einer Connector-Gruppe zugeordnet ist. Die Connector-Gruppe, die die übereinstimmende IP-Adresse enthält, wird dann verwendet, um die Verbindung zum Ziel weiterzuleiten, um auf Ressourcen zuzugreifen.

Einrichten von CylanceGATEWAY Connector

CylanceGATEWAY Connector ist ein virtuelles Gerät, das Sie installieren müssen, wenn Sie mit CylanceGATEWAY einen sicheren Tunnel zwischen den Geräten der Benutzer und Ihrem privaten Netzwerk einrichten möchten. Der CylanceGATEWAY Connector muss in einem Teil des Netzwerks bereitgestellt und registriert werden, der vollen Zugriff auf die Adressen hat, die Sie beim Angeben Ihres privaten Netzwerks angeben. Wenn Sie CylanceGATEWAY Connector nicht installieren, können Sie CylanceGATEWAY nur dazu verwenden, den Zugriff zu öffentlichen Internetzielen zu blockieren und den sicheren Zugriff auf Cloud-Anwendungen mithilfe von Quell-IP-Pinning zu sichern.

Es empfiehlt sich, mehr als einen CylanceGATEWAY Connector zu installieren. Die Installation mehrerer Instanzen ermöglicht die Lastverteilung für den Zugriff auf separate Segmente oder private Clouds innerhalb Ihres Definieren Ihres privaten Netzwerks. Wenn in Ihrem Netzwerk mehrere Instanzen des CylanceGATEWAY Connector installiert und konfiguriert sind, werden Client-Verbindungen gleichmäßig auf alle fehlerfreien CylanceGATEWAY Connector s verteilt, die der gleichen Connector-Gruppe zugewiesen sind, sodass Redundanz für den Fall besteht, dass eine Instanz nicht verfügbar ist oder Probleme behoben werden müssen.

Jeder Mandant unterstützt maximal acht Connector-Gruppen.

Jede Connector-Gruppe unterstützt maximal acht CylanceGATEWAY Connectors.

BlackBerry empfiehlt, eine Systemdiagnose-URL in jeder Connector-Gruppe anzugeben, um den Status jedes CylanceGATEWAY Connector s regelmäßig zu überwachen. Wenn Sie keine Systemdiagnose-URL angeben, kann CylanceGATEWAY nicht bestätigen, ob eine Verbindung zu Ihrem privaten Netzwerk besteht, und in der Spalte „Status der Systemdiagnose“ (Privates Netzwerk > Gateway-Connector) für einen Connector werden die DNS- und HTTP-Informationen nicht angezeigt. Weitere Informationen finden Sie unter Verwalten von CylanceGATEWAY Connectors.

Wenden Sie sich an Ihren BlackBerry-Vertriebsmitarbeiter, wenn Sie CylanceGATEWAY in einer Umgebung installieren möchten, die eine andere Konfiguration erfordert.

Führen Sie zum Einrichten von CylanceGATEWAY Connector die folgenden Schritte durch.

Schritt	Aktion
1	Lesen Sie Anforderungen: CylanceGATEWAY Connector.

Schritt	Aktion
2	Installieren von CylanceGATEWAY Connector in Ihrer Umgebung Der CylanceGATEWAY Connector wird in den folgenden Umgebungen unterstützt. Eine Anleitung zur Installation des CylanceGATEWAY Connector in Ihrer Umgebung finden Sie im Abschnitt Installieren des CylanceGATEWAY Connector-Workflows für Ihre Umgebung. • vSphere-Umgebung • ESXi-Umgebung • Microsoft Entra ID-Umgebung • Hyper-V-Umgebung • AWS-Umgebung
3	Konfigurieren von CylanceGATEWAY Connector in der VM-Umgebung (optional).
4	Zugreifen auf den CylanceGATEWAY Connector mit OpenSSH (optional).
5	Konfigurieren Ihrer Firewall für CylanceGATEWAY Connector.
6	Registrieren des CylanceGATEWAY Connector bei BlackBerry Infrastructure.
7	Konfigurieren des CylanceGATEWAY Connector (optional).
8	Verwalten von CylanceGATEWAY Connectors , um Optionen festzulegen und den Connector-Status zu überprüfen.

Installieren des CylanceGATEWAY Connectors in einer vSphere-Umgebung

Sie können CylanceGATEWAY Connector mit einer statischen IP-Adresse konfigurieren. Wenn Sie nach der Installation Änderungen an der Netzwerkkonfiguration von CylanceGATEWAY Connector vornehmen möchten, können Sie die vApp-Optionen der VM bearbeiten und den CylanceGATEWAY Connector neu starten, damit die Änderungen wirksam werden. Anweisungen zum Bearbeiten der OVF-Details finden Sie in der VMWare-Dokumentation unter „OVF-Details für eine virtuelle Maschine bearbeiten“.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie über die Berechtigungen zur Bereitstellung einer OVF-Vorlage in einer vSphere-Umgebung verfügen.

1. Laden Sie die CylanceGATEWAY Connector OVA-Datei (cylance-gateway-connector-<*version*>.ova) von *my*Account herunter.
2. Melden Sie sich bei der vSphere-Umgebung an.
3. Klicken Sie mit der rechten Maustaste auf das Cluster, in dem Sie den CylanceGATEWAY Connector installieren möchten, und wählen Sie **OVF-Vorlage bereitstellen** aus.
4. Klicken Sie auf dem Bildschirm **Eine OVF-Vorlage auswählen** auf **Lokale Datei**.
5. Klicken Sie auf **Dateien hochladen** und navigieren Sie zur Datei „cylance-gateway-connector.ova“.
6. Klicken Sie auf **Weiter**.

7. Geben Sie auf dem Bildschirm **Einen Namen und Ordner auswählen** einen Namen für die virtuelle Maschine ein und klicken Sie auf **Weiter**.

   Der Standardname lautet „cylance-gateway-connector“.
8. Wählen Sie auf dem Bildschirm **Eine Computerressource auswählen** einen Speicherort für die virtuelle Maschine aus und klicken Sie auf **Weiter**.
9. Klicken Sie nach Abschluss der Kompatibilitätsprüfung auf **Weiter**.
10. Überprüfen Sie auf dem Bildschirm **Details prüfen** die Einrichtungsinformationen und klicken Sie auf **Weiter**.
11. Wählen Sie auf dem Bildschirm **Speicher auswählen** für **Virtuelles Datenträgerformat** die Option **Thin Provision** aus und klicken Sie auf **Weiter**.
12. Konfigurieren Sie auf dem Bildschirm **Netzwerke auswählen** das **Zielnetzwerk** für diesen CylanceGATEWAY Connector.

    Stellen Sie das **Quellnetzwerk** auf NAT ein.
13. Klicken Sie auf **Weiter**.
14. Geben Sie im Bildschirm **Vorlage anpassen** zusätzliche Eigenschaften für virtuelle Maschinen an (optional).

    Hinweis: IP-Adressen müssen als IPv4-Adressen in Dezimalschreibweise mit Punkten eingegeben werden.

    - Standardmäßig ist die Option **DHCP verwenden** aktiviert, und der Connector verwendet automatisch zugewiesene IP-Adressen. Wenn Sie den Connector mit einer statischen IP-Adresse konfigurieren möchten, müssen Sie das Kontrollkästchen „DHCP verwenden“ deaktivieren und die IP-Adressen für die folgenden Einstellungen angeben:
    - Geben Sie in das Feld **IP-Adresse / Präfixlänge** die IP-Adresse und das Präfix ein, die Geräten zugewiesen werden können (z. B. 192.0.2.100/24). Wenn Sie mehrere IP-Adressen hinzufügen, trennen Sie jede IP-Adresse und jedes Präfix durch ein Komma (,).
    - Geben Sie in das Feld **Gateway** die IP-Adresse für das Netzwerk-Gateway ein (z. B. 192.0.2.1).
    - Geben Sie im Feld **DNS** die IP-Adresse für die DNS-Server an, die Sie verwenden möchten (z. B. 192.0.2.120). Wenn Sie mehrere DNS-Server hinzufügen, trennen Sie die Adressen durch ein Komma (,).
15. Überprüfen Sie auf dem Bildschirm **Zum Fertigstellen bereit** die Konfigurationseinstellungen und klicken Sie auf **Fertigstellen**.

Wenn Sie fertig sind: Nachdem Sie den Connector installiert haben, können Sie überprüfen, ob die OVA-Datei in der virtuellen Umgebung korrekt installiert ist. Anweisungen finden Sie unter Konfigurieren von CylanceGATEWAY Connector in der VM-Umgebung.

Installieren des CylanceGATEWAY Connector in einer ESXi-Umgebung

Sie können die Netzwerkschnittstelle des CylanceGATEWAY Connector für die Verwendung von DHCP konfigurieren, oder eine statische IP nur dann konfigurieren, wenn Sie den CylanceGATEWAY Connector installieren. Wenn Sie Änderungen an der Konfiguration vornehmen möchten, müssen Sie den CylanceGATEWAY Connector deinstallieren und dann mit der neuen Netzwerkschnittstellenkonfiguration installieren.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie über die Berechtigungen zur Bereitstellung einer OVF-Vorlage in einer ESXi-Umgebung verfügen.

1. Laden Sie die CylanceGATEWAY Connector OVA-Datei (cylance-gateway-connector-<*version*>.ova) von *my*Account herunter.
2. Melden Sie sich bei der ESXi-Umgebung an.
3. Wählen Sie im Bereich **Navigator** die Option **Virtuelle Maschinen** aus.
4. Klicken Sie auf die Schaltfläche **VM erstellen/registrieren**.
5. Wählen Sie auf dem Bildschirm **Neue virtuelle Maschine** die Option **Virtuelle Maschine aus einer OVF- oder OVA-Datei bereitstellen** aus und klicken Sie auf **Weiter**.
6. Geben Sie einen Namen für die virtuelle Maschine ein.

7. Navigieren Sie zur Datei cylance-gateway-connector-<*version*>.ova. Ziehen Sie die Datei per Drag-and-Drop in das Dialogfeld.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie auf dem Bildschirm **Speicher auswählen** die Option **Standard** und einen Datenspeicher aus und klicken Sie dann auf **Weiter**.
10. Wählen Sie auf dem Bildschirm **Bereitstellungsoptionen** für **Datenträgerbereitstellung** die Option **Thin** aus.
11. Erweitern Sie auf dem Bildschirm **Zusätzliche Einstellungen** die Optionen für die Eingabe zusätzlicher VMware-Eigenschaften (optional).

    Hinweis: IP-Adressen müssen als IPv4-Adressen in Dezimalschreibweise mit Punkten eingegeben werden.

    - Standardmäßig ist **DHCP verwenden** aktiviert, und der Connector verwendet automatisch zugewiesene IP-Adressen. Wenn Sie den Connector mit einer statischen IP-Adresse konfigurieren möchten, müssen Sie das Kontrollkästchen „DHCP verwenden“ deaktivieren und die IP-Adressen für die folgenden Einstellungen angeben:
    - Geben Sie im Feld **IP-Adresse / Präfixlänge** die IP-Adresse und das Präfix an, die Geräten zugewiesen werden können (z. B. 192.0.2.100/24). Wenn Sie mehrere IP-Adressen verwenden möchten, trennen Sie die IP-Adressen durch ein Komma (,).
    - Geben Sie in das Feld **Gateway** die Adresse für das Netzwerk-Gateway ein (zum Beispiel 192.0.2.1).
    - Geben Sie im Feld **DNS** die IP-Adresse für die DNS-Server an, die Sie verwenden möchten (z. B. 192.0.2.120). Wenn Sie mehrere DNS-Server verwenden möchten, trennen Sie die Adressen durch ein Komma (,).
12. Klicken Sie auf **Weiter**.
13. Überprüfen Sie auf dem Bildschirm **Zum Fertigstellen bereit** die Konfigurationseinstellungen und klicken Sie auf **Fertigstellen**.

Wenn Sie fertig sind: Nachdem Sie den Connector installiert haben, können Sie überprüfen, ob die OVA-Datei in der virtuellen Umgebung korrekt installiert ist. Anweisungen finden Sie unter Konfigurieren von CylanceGATEWAY Connector in der VM-Umgebung.

Voraussetzungen für die Installation von CylanceGATEWAY Connector in einer Microsoft Entra ID-Umgebung

- Stellen Sie sicher, dass das DNS in Ihrem privaten Entra-Netzwerk aktiviert ist und Ihre Connector-VM darauf zugreifen kann.
- Stellen Sie optional sicher, dass Ihre private Netzwerkumgebung über einen Proxyserver für ausgehenden HTTP- und HTTPS-Datenverkehr verfügt.
- Stellen Sie sicher, dass CylanceGATEWAY Connector in Ihrem privaten Netzwerk auf die Dienste zugreifen kann, die Sie über CylanceGATEWAY zur Verfügung stellen möchten.
- Stellen Sie sicher, dass Sie eine VHD-Vorlage in einer Entra-Umgebung bereitstellen können.

Installieren von CylanceGATEWAY Connector in einer Microsoft Entra ID-Umgebung

Wenn Sie den Connector installieren, laden Sie die VHD-Datei als BLOB in das Microsoft Entra ID-Portal hoch. Sie verwenden das BLOB, um ein Image zu erstellen, das von der Connector-VM verwendet wird. Weitere Informationen zur Konfiguration Ihrer Entra-Umgebung finden Sie in der Dokumentation zum Azure-Portal – Azure-Portal | Microsoft Docs.

Bevor Sie beginnen: Überprüfen Sie Voraussetzungen für die Installation von CylanceGATEWAY Connector in einer Microsoft Entra ID-Umgebung.

1. Laden Sie die CylanceGATEWAY Connector VHD-Datei (cylance-gateway-connector-fixed-<*version*>.vhd) von *my*Account herunter.
2. Melden Sie sich beim Microsoft Entra ID-Verwaltungsportal unter https://portal.azure.com an.

3. Laden Sie die VHD-Datei als BLOB hoch.
   a) Klicken Sie im Abschnitt **Azure-Dienste** auf **Speicherkonten**. Wenn Sie kein Speicherkonto haben, erstellen Sie eines.
   b) Klicken Sie auf Ihr Speicherkonto.
   c) Klicken Sie in der linken Spalte im Abschnitt **Datenspeicherung** auf **Container**. Wenn Sie keinen Container haben, erstellen Sie einen.
   d) Klicken Sie auf Ihren Container.
   e) Klicken Sie auf **Hochladen**.
   f) Navigieren Sie auf dem Bildschirm **BLOB hochladen** zur heruntergeladenen Datei cylance-gateway-connector-fixed-<*version*>.vhd.
   g) Erweitern Sie **Erweitert** und stellen Sie die Dropdown-Liste **BLOB-Typ** auf **Seiten-BLOB** ein.
   h) Klicken Sie auf **Hochladen**.
4. Erstellen Sie ein Image aus dem hochgeladenen BLOB.
   a) Klicken Sie im Verwaltungsportal in der linken Spalte auf das Portalmenü **> Alle Dienste**.
   b) Geben Sie im Feld **Filterdienste** `images` ein.
   c) Klicken Sie auf **Images** und stellen Sie sicher, dass das Image den Ressourcentyp **Microsoft.Compute/images** verwendet.
   d) Klicken Sie auf **Erstellen**.
   e) Füllen Sie die Pflichtfelder für Ihre Umgebung aus. Nehmen Sie im Abschnitt **Betriebssystemdatenträger** die folgenden Einstellungen vor:
      - Betriebssystemtyp: Linux
      - VM-Generation: Generation 1
      - Speicher-BLOB: Navigieren Sie zu dem BLOB, das Sie in Schritt 3 erstellt haben.
   f) Klicken Sie auf die Registerkarte **Tags** und fügen Sie benötigte Tags hinzu (optional).
   g) Klicken Sie auf **Überprüfen + erstellen**.
   h) Klicken Sie auf **Erstellen**.
   i) Klicken Sie auf **Zur Ressource**. Der Bildschirm „Virtuelle Maschine erstellen“ wird angezeigt.
5. Erstellen Sie eine Connector-VM.
   a) Füllen Sie auf der Registerkarte **Grundlagen** die erforderlichen Felder für Ihre Umgebung aus. Nehmen Sie die folgenden Einstellungen vor:
      - Image: Wählen Sie das Image aus, das Sie in Schritt 4 erstellt haben.
      - Größe: Wählen Sie eine Größe aus, die 2 vCPUs und mindestens 4,5 GB Speicher umfasst.
      - Authentifizierungstyp: Wählen Sie **Kennwort** aus.
      - Benutzername: Geben Sie einen beliebigen Wert ein. Das Connector-VM-Image ignoriert dieses Feld.
      - Kennwort und Kennwort bestätigen: Geben Sie einen beliebigen Wert ein. Das Connector-VM-Image ignoriert diese Felder.
   b) Klicken Sie auf die Registerkarte **Festplatten**.
   c) Wählen Sie auf der Seite **Festplatten** in der Dropdown-Liste **Betriebssystemdatenträger** die Option **Standard-Festplatte** aus. Die Connector-VM erfordert keinen Festplattenzugriff mit geringer Latenz.
   d) Klicken Sie auf die Registerkarte **Netzwerk**. Füllen Sie die Pflichtfelder für Ihre Umgebung aus. Stellen Sie sicher, dass das Connector-Image Ihr privates Netzwerk verwendet. Der Connector unterstützt keine beschleunigte Netzwerkfunktion von Entra. Wenn Sie diese Einstellung aktivieren, funktioniert die Connector-VM möglicherweise nicht wie erwartet.
   e) Klicken Sie auf die Registerkarte **Verwaltung**. Das Image unterstützt „Login mit Azure AD“ nicht. Wenn Sie diese Einstellung aktivieren, funktioniert die Connector-VM möglicherweise nicht wie erwartet.
   f) Klicken Sie auf die Registerkarte **Erweitert**. Konfigurieren Sie sie nach Bedarf für Ihre Umgebung. Der Connector unterstützt die Einstellung „Benutzerdefinierte Daten“ oder „Benutzerdaten“ nicht. Die Einstellungen für „Benutzerdefinierte Daten“ oder „Benutzerdaten“ können entsprechend den

Anforderungen Ihrer Umgebung konfiguriert werden, werden jedoch von der Connector-VM ignoriert. BlackBerry empfiehlt nicht, zusätzliche VM-Anwendungen auf der VM zu installieren, auf der die Connector-VM ausgeführt wird.

g) Klicken Sie auf die Registerkarte **Tags**. Konfigurieren Sie Tags nach Bedarf für Ihre Umgebung.
h) Klicken Sie auf die Registerkarte **Überprüfen + erstellen**. Überprüfen Sie Ihre Konfiguration.
i) Klicken Sie auf **Erstellen**.

Hinweis: Beim Erstellen der VM-Ressource wird möglicherweise eine Fehlermeldung wegen einer Zeitüberschreitung angezeigt. Aktualisieren Sie ggf. den Bildschirm.

Installieren von CylanceGATEWAY Connector in einer Hyper-V-Umgebung

Bevor Sie beginnen: Stellen Sie sicher, dass Sie über die Berechtigungen zum Bereitstellen der VHD-Datei und zum Erstellen eines Connector-Images verfügen.

1. Laden Sie die CylanceGATEWAY Connector-VHD-Datei (cylance-gateway-connector-dynamic<*Version*>.vhd) von *my*Account herunter.
2. Führen Sie den Hyper-V-Manager als Administrator aus.
3. Klicken Sie im Menü des Hyper-V-Managers auf **Aktion > Neu > Virtuelle Maschine**. Klicken Sie auf **Weiter**.
4. Geben Sie auf dem Bildschirm **Name und Speicherort angeben** einen Namen für die VM an. Klicken Sie auf **Weiter**.
5. Wählen Sie auf dem Bildschirm **Generation angeben** die Option **Generation 1** aus. Klicken Sie auf **Weiter**.
6. Klicken Sie auf dem Bildschirm **Speicher zuweisen** auf **Weiter**.
7. Wählen Sie auf dem Bildschirm **Netzwerk konfigurieren** die entsprechende Verbindung aus. Klicken Sie auf **Weiter**.
8. Wählen Sie auf dem Bildschirm **Virtuelle Festplatte verbinden** die Option **Vorhandene virtuelle Festplatte verwenden** aus.
9. Navigieren Sie zur Datei cylance-gateway-connector-dynamics-<*version*>.vhd, die Sie in Schritt 1 heruntergeladen haben.
10. Stellen Sie auf dem Bildschirm **Speicher zuweisen** sicher, dass der Connector über mindestens 5 GB Speicher verfügt. Klicken Sie auf **Weiter**.
11. Überprüfen Sie auf dem Bildschirm **Fertigstellen des Assistenten für neue virtuelle Maschinen** die Konfigurationseinstellungen und klicken Sie auf **Fertigstellen**.
12. Starten Sie den Connector.

Wenn Sie fertig sind: Nachdem Sie den Connector installiert haben, können Sie überprüfen, ob die VHD-Datei in der virtuellen Umgebung korrekt installiert ist. Anweisungen finden Sie unter Konfigurieren von CylanceGATEWAY Connector in der VM-Umgebung.

Installieren von CylanceGATEWAY Connector in einer AWS-Umgebung

Sie installieren CylanceGATEWAY Connector über das AMI im AWS Marketplace.

1. Melden Sie sich bei der AWS-Verwaltungskonsole unter https://aws.amazon.com/console an.
2. Erstellen Sie die Instanz CylanceGATEWAY Connector. Führen Sie folgende Aktionen aus:
   a. Öffnen Sie den **EC2**-Dienst.
   b. Klicken Sie in der linken Spalte unter **Instanzen** auf **Instanzen**.
   c. Klicken Sie auf **Instanzen starten**.
   d. Geben Sie im Bildschirm **Instanz starten** einen Namen für die CylanceGATEWAY Connector-Instanz ein.
   e. Klicken Sie im Abschnitt **Amazon Machine Image** (AMI) auf **Weitere AMIs durchsuchen**.

f. Klicken Sie auf dem Bildschirm **Amazon Machine Image (AMI) auswählen** auf die Registerkarte **AWS Marketplace AMIs**.
g. Geben Sie `CylanceGATEWAY` im Feld **Ausgewählte AMI** ein. Drücken Sie die **Eingabetaste**.
h. Wählen Sie einen Instanztyp entsprechend den Anforderungen Ihres Unternehmens aus.

   Hinweis: BlackBerry empfiehlt, für Produktionsumgebungen eine Instanz des Typs c6in oder c5n auszuwählen.
i. Wählen Sie ein Schlüsselpaar aus, um eine sichere Verbindung zu Ihrer Connector-Instanz über OpenSSH herzustellen.
j. Klicken Sie im Abschnitt **Netzwerkeinstellungen** auf **Bearbeiten** und legen Sie die folgenden Einstellungen fest:

   1. Klicken Sie auf das Dropdown-Menü **VPC** und wählen Sie Ihr privates Netzwerk aus.
   2. Klicken Sie optional auf **Öffentliche IP automatisch zuweisen** und wählen Sie **Aktivieren**. Sie müssen dem CylanceGATEWAY Connector nur dann eine öffentliche IP-Adresse zuweisen, wenn Sie keine Möglichkeit haben, über das private Netzwerk, auf dem er installiert ist, auf die Webschnittstelle des Connectors zuzugreifen.
   3. Wählen oder erstellen Sie eine Sicherheitsgruppe entsprechend den Anforderungen Ihres Unternehmens. Die Sicherheitsgruppe muss über Port 22 (SSH), Port 80 (HTTP), und Port 443 (HTTPS) auf den CylanceGATEWAY Connector aus dem Netzwerk verfügen, von dem aus die Registrierung abgeschlossen wird.
k. Klicken Sie auf **Instanz starten**.

Wenn Sie fertig sind: Registrieren des CylanceGATEWAY Connector bei BlackBerry Infrastructure

Konfigurieren von CylanceGATEWAY Connector in der VM-Umgebung

Hinweis: Der AWS CylanceGATEWAY Connector AMI unterstützt keinen Zugriff auf die serielle EC2-Konsole. Führen Sie diese Aufgabe nicht aus, wenn Sie den Connector in Ihrer AWS-Umgebung installieren. Informationen zum Fortfahren mit der CylanceGATEWAY Connector-Einrichtung siehe Konfigurieren Ihrer Firewall für CylanceGATEWAY Connector.

Der CylanceGATEWAY Connector ist eine Minimalinstallation des Ubuntu-Betriebssystems, das ohne Anmeldung eines Benutzers betrieben werden kann. Sie müssen sich nur anmelden, wenn Sie die Standardeinstellungen aktualisieren oder überprüfen möchten, ob die OVA oder VHD korrekt bereitgestellt wurde.

1. Führen Sie einen der folgenden Schritte aus, um die Konsole in Ihrer Umgebung zu öffnen.

Umgebung	Schritte
vSphere	**a.** Melden Sie sich bei Ihrer Umgebung an. **b.** Klicken Sie auf den Hostnamen des CylanceGATEWAY Connector. **c.** Klicken Sie auf **Remote starten** oder **Web-Konsole starten**.
ESXi	**a.** Melden Sie sich bei Ihrer Umgebung an. **b.** Klicken Sie auf den Hostnamen des CylanceGATEWAY Connector. **c.** Klicken Sie auf **Konsole**.
Microsoft Entra ID	**a.** Melden Sie sich beim Microsoft Entra ID-Verwaltungsportal unter https://portal.azure.com an. **b.** Klicken Sie auf **Virtuelle Maschinen**. **c.** Klicken Sie in der linken Spalte im Abschnitt **Support + Fehlerbehebung** auf **Serielle Konsole**.

Umgebung	Schritte
Hyper-V	**a.** Öffnen Sie den Hyper-V-Manager. **b.** Klicken Sie mit der rechten Maustaste auf den gewünschten Connector, und wählen Sie **> Verbinden**.

2. Geben Sie an der UNIX-Eingabeaufforderung den Benutzernamen des Administrators ein und drücken Sie die **Eingabetaste**.

   Der Standardbenutzername ist **admin**.
3. Geben Sie das Administratorkennwort ein.

   Das Standardkennwort lautet **admin**.
4. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Umgebung	Schritte
Überprüfen Sie die Konfiguration der Netzwerkschnittstelle.	vSphere ESXi	Geben Sie `sudo /var/lib/cylance-gateway/scripts/configure-network --ovfenv --check` ein. Drücken Sie die **Eingabetaste**. Wenn Sie dazu aufgefordert werden, geben Sie das Administratorkennwort ein.
Ändern Sie das Tastaturlayout im Connector.	Alle	Standardmäßig werden nur US-Tastaturlayouts von Ubuntu unterstützt. **a.** Um ein neues Tastaturlayout auszuwählen, geben Sie `sudo dpkg-reconfigure keyboard-configuration` ein. Drücken Sie die **Eingabetaste**. **b.** Wenn Sie dazu aufgefordert werden, geben Sie das Administratorkennwort ein. **c.** Folgen Sie den Anweisungen auf dem Bildschirm.

Zugreifen auf den CylanceGATEWAY Connector mit OpenSSH

Hinweis: OpenSSH ist standardmäßig im AWS CylanceGATEWAY Connector AMI aktiviert. Führen Sie diese Aufgabe nicht aus, wenn Sie den Connector in Ihrer AWS-Umgebung installieren. Informationen zum Fortfahren mit der CylanceGATEWAY Connector-Einrichtung siehe Konfigurieren Ihrer Firewall für CylanceGATEWAY Connector.

OpenSSH ist auf dem Connector-Image vorinstalliert und ermöglicht Ihnen den Zugriff auf den CylanceGATEWAY Connector sowie die Durchführung von Systemvorgängen und Wartung unter Verwendung des SSH-Protokolls. Der OpenSSH-Dienst ist standardmäßig deaktiviert. Sie müssen den OpenSSH-Dienst aktivieren und jedes Mal die Hostschlüssel generieren, wenn Sie mit OpenSSH auf eine CylanceGATEWAY Connector-Instanz zugreifen. In Microsoft Entra ID-Umgebungen muss eingehender TCP-Datenverkehr zugelassen werden.

Bevor Sie beginnen: Port 22 (SSH), Port 80 (HTTP), und Port 443 (HTTPS) müssen offen sein, und die Sicherheitsgruppe muss Zugriff auf den CylanceGATEWAY Connector aus dem Netzwerk haben, von dem aus die Registrierung abgeschlossen wird.

1. Führen Sie einen der folgenden Schritte aus, um die Konsole in Ihrer Umgebung zu öffnen.

Umgebung	Beschreibung
vSphere	**a.** Melden Sie sich bei Ihrer Umgebung an. **b.** Klicken Sie auf den Hostnamen des CylanceGATEWAY Connector. **c.** Klicken Sie auf **Remote-Konsole starten** oder **Web-Konsole starten**.
ESXi	**a.** Melden Sie sich bei Ihrer Umgebung an. **b.** Klicken Sie auf den Hostnamen des CylanceGATEWAY Connector. **c.** Klicken Sie auf **Konsole**.
Microsoft Entra ID	**a.** Melden Sie sich beim Microsoft Entra ID-Verwaltungsportal unter https://portal.azure.com an. **b.** Klicken Sie auf **Virtuelle Maschinen**. **c.** Klicken Sie auf den Connector, den Sie unter Installieren von CylanceGATEWAY Connector in einer Microsoft Entra ID-Umgebung, Schritt 5 erstellt haben. **d.** Klicken Sie im linken Menü im Abschnitt **Support + Fehlerbehebung** auf **Serielle Konsole**. **e.** Klicken Sie in der linken Spalte auf **Diagnose starten**. **f.** Klicken Sie auf die Registerkarte **Einstellungen**. **g.** Wählen Sie **Mit benutzerdefiniertem Speicherkonto aktivieren**. **h.** Wählen Sie in der Dropdown-Liste **Diagnosespeicherkonto** das Speicherkonto aus, das Sie unter Installieren von CylanceGATEWAY Connector in einer Microsoft Entra ID-Umgebung, Schritt 3 erstellt haben. **i.** Klicken Sie auf **Speichern**. **j.** Klicken Sie auf dem Bildschirm „Connector“ im linken Menü im Abschnitt **Support + Fehlerbehebung** auf **Serielle Konsole**.
Hyper-V	**a.** Öffnen Sie den Hyper-V-Manager. **b.** Klicken Sie mit der rechten Maustaste auf den gewünschten Connector, und wählen Sie **> Verbinden**.

2. Geben Sie an der UNIX-Eingabeaufforderung den Benutzernamen des Administrators ein und drücken Sie die **Eingabetaste**. Der Standardbenutzername ist admin.
3. Geben Sie das Administratorkennwort ein. Das Standardkennwort lautet admin.
4. Generieren Sie die Hostschlüssel für den OpenSSH-Dienst. Geben Sie `sudo dpkg-reconfigure openssh-server` ein. Drücken Sie die **Eingabetaste**.
5. Wenn Sie dazu aufgefordert werden, geben Sie das Administratorkennwort ein.
6. Aktivieren Sie den OpenSSH-Dienst. Geben Sie `sudo systemctl --system enable ssh` ein. Drücken Sie die **Eingabetaste**.

   Hinweis: Dieser Befehl startet den Dienst nicht.
7. Starten Sie den OpenSSH-Dienst. Geben Sie `sudo systemctl --system start ssh` ein. Drücken Sie die **Eingabetaste**.
8. Sie können eine der folgenden Aktionen durchführen (optional):

Aufgabe	Schritte
Deaktivieren Sie den Start des OpenSSH-Dienstes während des Systemstarts.	Geben Sie `sudo systemctl --system disable ssh` ein. Dieser Befehl beendet den Dienst nicht.
Beenden Sie den OpenSSH-Dienst.	Geben Sie `sudo systemctl --system stop ssh` ein. Drücken Sie die **Eingabetaste**.
Überprüfen Sie, ob der OpenSSH-Dienst aktiviert ist.	Geben Sie `sudo systemctl --system is-enabled ssh` ein.
Überprüfen Sie, ob der OpenSSH-Dienst ausgeführt wird.	Geben Sie `sudo systemctl --system is-active ssh` ein.
Status des OpenSSH-Dienstes abrufen	Geben Sie `sudo systemctl --system status ssh` ein.

9. Beenden Sie die Konsole.
10. Optional können Sie in einer Microsoft Entra ID-Umgebung die Startdiagnoseeinstellungen für die Connector-VM deaktivieren, die Sie in Schritt 1 konfiguriert haben.

Konfigurieren Ihrer Firewall für CylanceGATEWAY Connector

Der CylanceGATEWAY Connector wird innerhalb Ihres privaten Netzwerks hinter Ihrer Firewall ausgeführt und verfügt über eine private IP-Adresse. Er stellt mit HTTPS und UDP eine Verbindung zum CylanceGATEWAY-Cloud-Dienst her. Der CylanceGATEWAY Connector muss über Ihre Firewall (über NAT) eine Verbindung mit dem CylanceGATEWAY herstellen können.

Der CylanceGATEWAY Connector muss DNS verwenden können, um öffentliche CylanceGATEWAY-FQDNs in Internet-IP-Adressen aufzulösen. Dazu verwendet der CylanceGATEWAY Connector Ihre privaten DNS-Server.

Der CylanceGATEWAY-Agent kommuniziert über sichere WebSockets (WSS) mit der Verwaltungskonsole und muss diese Verbindung direkt herstellen können. Damit der CylanceGATEWAY-Agent aktiviert und regelmäßig authentifiziert werden kann, müssen Sie den Zugriff auf die entsprechenden Domänen zulassen (z. B. idp.blackberry.com und die Domäne für Ihre Region). Wenn in Ihrer Umgebung ein Authentifizierungs-Proxy verwendet wird, müssen Sie den Datenverkehr auf dem Proxy-Server zulassen.

Weitere Informationen zu FQDNs, Ports, IP-Adressbereichen und anderen Firewall-Anforderungen finden Sie unter support.blackberry.com/community in Artikel 79017. Weitere Informationen zu Netzwerkanforderungen für Cylance Endpoint Security finden Sie unter Cylance Endpoint Security-Netzwerkanforderungen.

Registrieren des CylanceGATEWAY Connector bei BlackBerry Infrastructure

Nachdem Sie den CylanceGATEWAY Connector installiert und seine Firewall konfiguriert haben, müssen Sie ihn mit der BlackBerry Infrastructure verbinden.

1. Navigieren Sie in einem Browser zur IP-Adresse von CylanceGATEWAY Connector.
2. Um das selbstsignierte Zertifikat zu akzeptieren und mit dem HTTPS-Dienst fortzufahren, klicken Sie auf **Weiter zum HTTPs-Dienst**.

3. Geben Sie an der Eingabeaufforderung den standardmäßigen Administrator-Benutzernamen und das Kennwort ein, und klicken Sie auf **Anmelden**.

   Der Standardbenutzername ist admin. Das Standardkennwort lautet blackberry.
4. Wenn Sie sich das erste Mal bei der CylanceGATEWAY Connector-Webschnittstelle anmelden, müssen Sie das Standard-Administratorkennwort für den CylanceGATEWAY Connector ändern. Das Kennwort für den CylanceGATEWAY Connector in der ESXi, für vSphere, das Microsoft Entra ID-Portal, die AWS-Konsole oder die Hyper-V Manager-Konsole wird dadurch nicht geändert.
5. Melden Sie sich mit dem neuen Kennwort erneut an der CylanceGATEWAY Connector-Webschnittstelle an.
6. Überprüfen Sie auf dem Bildschirm **Lizenzvertrag für BlackBerry-Lösungen** die Lizenzvereinbarung und klicken Sie auf **Ich stimme zu**.
7. Um den CylanceGATEWAY Connector für BlackBerry Infrastructure und für Ihre Organisation zu autorisieren, müssen Sie den Connector registrieren.
   a) Lesen Sie die Datenschutzerklärung und stimmen Sie ihr zu. Aktivieren Sie das Kontrollkästchen **Ich stimme der Datenschutzerklärung von BlackBerry zu**.
   b) Geben Sie in das Feld die **URL** für den Connector ein, um auf die Verwaltungskonsole zuzugreifen.

      Um die URL abzurufen, klicken Sie in der Verwaltungskonsole auf **Einstellungen > Netzwerk > Privates Netzwerk** und auf der Registerkarte **Gateway Connectors** auf **Connectors hinzufügen**.
   c) Geben Sie im Feld **Proxy-URL** die URL für den Proxyserver ein. Wenn Sie die Proxy-URL auf diesem Bildschirm eingeben, wird das Feld **Proxy-URL** auf der Seite „Einstellungen“ mit derselben URL ausgefüllt und umgekehrt.
8. Klicken Sie auf **Connector registrieren**. Die Verwaltungskonsole wird geöffnet.
9. Melden Sie sich bei der Verwaltungskonsole als Administrator an.
10. Geben Sie in das Feld **Connector-Name** einen Namen für den Connector ein.
11. Wählen Sie in der Dropdown-Liste **Connector-Gruppe** die Connector-Gruppe aus, die Sie zuweisen möchten.
12. Klicken Sie auf **Autorisieren**.

Der Connector, seine Version und die Connector-Gruppe, der er zugeordnet ist, werden in der Liste der CylanceGATEWAY-Connectoren angezeigt. Die Spalte **Status** zeigt an, ob das private Netzwerk, sein DNS und die Systemdiagnoseprüfungen ordnungsgemäß funktionieren. Informationen zu den Status, die angezeigt werden können, finden Sie unter Verwalten von CylanceGATEWAY Connectors

Wenn Sie fertig sind: Wenn der CylanceGATEWAY Connector registriert ist, aber sein Tunnel nicht mit der BlackBerry Infrastructure verbunden ist, können Sie einen Konnektivitätstest initiieren, um zu überprüfen, ob die von Ihrem privaten Netzwerk gesendeten UDP-Pakete von der BlackBerry Infrastructure empfangen wurden, und ob die von der BlackBerry Infrastructure gesendeten UDP-Pakete von Ihrem privaten Netzwerk empfangen werden. In der Anmeldeaufforderung Ihrer Umgebung (z. B. vSphere). Geben Sie `/var/lib/cylance-gateway/bin/udp-connectivity-test` ein. Drücken Sie die **Eingabetaste**. Sie können diesen Befehl in jeder Shell ausführen (z. B. csh und bash). Weitere Informationen zu den Konnektivitätsergebnissen finden Sie unter Antworten auf UDP-Konnektivitätstests.

Details für einen registrierten CylanceGATEWAY Connector anzeigen

Sie können die Details zu CylanceGATEWAY Connector anzeigen, nachdem dieser in der CylanceGATEWAY Connector-Webschnittstelle registriert wurde. Wenn Ihr Netzwerk über mehrere Instanzen des CylanceGATEWAY Connector verfügt, benötigen Sie für jede Instanz Zugriff auf die Webschnittstelle. Sie können den Status aller Connectors in Ihrer Umgebung in der Verwaltungskonsole anzeigen.

- Wenn der Connector bei der BlackBerry Infrastructure registriert wurde, können Sie die folgenden Informationen anzeigen. Klicken Sie auf **Diesen Connector verwalten**, um die Cylance Endpoint Security-Verwaltungskonsole zu öffnen und die CylanceGATEWAY Connector s zu verwalten:

    - CylanceGATEWAY Connector-Kennungen, die von der BlackBerry Infrastructure zur Identifizierung der Instanz verwendet werden
    - Aktueller Status und Registrierungsinformationen der Instanz
    - Anzahl der Tunnel, die über den CylanceGATEWAY Connector mit der BlackBerry Infrastructure verbunden sind
- Sie können die Protokolldateien herunterladen. Die Protokolldateien werden in Ihren Download-Ordner als ZIP-Datei heruntergeladen und können mehrere CylanceGATEWAY Connector-Protokolldateien enthalten. Klicken Sie auf **Protokolle herunterladen**. Extrahieren Sie die Protokolle, um sie zu überprüfen, oder senden Sie die ZIP-Datei an den BlackBerry Support, um potenzielle Probleme zu beheben. Die Protokolldateien für die einzelnen Instanzen können auch über die Verwaltungskonsole aus dem Bereich „Connector-Informationen“ auf der Seite CylanceGATEWAY Connectors heruntergeladen werden.
- Sie können den CylanceGATEWAY Connector konfigurieren.

Konfigurieren des CylanceGATEWAY Connector

Sie können verschiedene Aufgaben in der webbasierten Schnittstelle von CylanceGATEWAY Connector ausführen. Wenn in Ihrem Netzwerk mehrere Instanzen des CylanceGATEWAY Connector installiert und konfiguriert sind, müssen die Aufgaben für jede CylanceGATEWAY Connector-Instanz in Ihrer Umgebung nach Bedarf ausgeführt werden. Sie können den Status aller Connector in Ihrer Umgebung auf der Seite mit den Gateway-Connectoren in der Verwaltungskonsole anzeigen. Sie können den Status der einzelnen CylanceGATEWAY Connector-Instanzen in der Verwaltungskonsole anzeigen. Weitere Informationen finden Sie Details für einen registrierten CylanceGATEWAY Connector anzeigen

Bevor Sie beginnen: Vergewissern Sie sich, dass Sie mindestens über eine CylanceGATEWAY Connector-Instanz verfügen.

1. Navigieren Sie in einem Browser zur IP-Adresse von CylanceGATEWAY Connector.
2. Geben Sie Ihre Anmeldeinformationen ein und klicken Sie auf **Anmelden**.
3. Führen Sie eine der folgenden Aufgaben aus:

Aufgaben	Schritte
Einstellungen bearbeiten	Sie können eine oder mehrere der folgenden Einstellungen angeben (optional). **a.** Klicken Sie auf **Einstellungen**. **b.** Nehmen Sie eine oder mehrere der folgenden Einstellungen vor: • Erstellen Sie ein neues selbstsigniertes TLS-Zertifikat: Sie können das TLS-Zertifikat jederzeit neu generieren. Das Zertifikat ist standardmäßig ein Jahr lang gültig. Die Webschnittstelle zeigt den Tag und die Uhrzeit des Zertifikatsablaufs, die Seriennummer und den Host an, der an das Zertifikat gebunden ist. Jedes Mal, wenn Sie ein neues TLS-Zertifikat erstellen, werden Sie aufgefordert, das neue Zertifikat zu akzeptieren. • HTTP(S)-Proxykonfiguration: Wenn Ihre Umgebung mit einem nicht authentifizierten Proxyserver konfiguriert ist, der für HTTP- und HTTPS-Anfragen an Internetziele verwendet wird, können Sie die URL des Proxys eingeben. Wenn die Proxy-URL hinzugefügt wird, verwenden HTTPS-Anfragen an die BlackBerry Infrastructure, die vom CylanceGATEWAY Connector ausgehen, diesen Proxy. Der Tunnelverkehr verwendet den Proxy nicht. • MTU-Konfiguration (Maximum Transfer Unit, maximale Übertragungseinheit): Standardmäßig erkennt der CylanceGATEWAY Connector die MTU Ihres Netzwerks automatisch. In einigen Fällen müssen Sie möglicherweise den MTU-Wert angeben, den CylanceGATEWAY Connector verwenden kann. BlackBerry empfiehlt die Verwendung der automatischen Erkennung. **Hinweis:** Wenn Sie die MTU angeben und die automatische Erkennung verwenden möchten, müssen Sie CylanceGATEWAY Connector innerhalb der vSphere-, Hyper-V-, Microsoft Entra ID-, AWS- oder ESXi-Umgebung neu starten. • NTP-Konfiguration (Network Time Protocol): Standardmäßig verwendet CylanceGATEWAY Connector den Ubuntu-Server ntp.ubuntu.com für die Zeitsynchronisierung. Sie können einen benutzerdefinierten NTP-Server angeben. • APT-Konfiguration (Advanced Package Tool): Standardmäßig verwendet CylanceGATEWAY Connector die Ubuntu-Repository-Hosts archive.unbunto.com und security.unbuntu.com. Weitere Informationen finden Sie unter support.blackberry.com/community in Artikel 79017. Sie können ein benutzerdefiniertes Paket-Repository angeben, das von CylanceGATEWAY Connector verwendet wird. Beachten Sie, dass Sicherheitsupdates automatisch angewendet werden und Sie CylanceGATEWAY Connector in der Verwaltungskonsole neu starten müssen, damit die Updates wirksam werden. **c.** Führen Sie einen der folgenden Schritte aus: • Klicken Sie auf **Einstellungen aktualisieren**, um die Änderungen im Bildschirm „Einstellungen“ zu speichern. • Klicken Sie auf **Standardeinstellungen wiederherstellen**, um alle Standardeinstellungen wiederherzustellen. Sie müssen Ihre Zugangsdaten eingeben, damit die Änderungen wirksam werden. Die Netzwerkverbindung kann unterbrochen werden (wenn Sie beispielsweise eine MTU angeben, muss CylanceGATEWAY Connector neu gestartet werden). • Klicken Sie auf **Werkseinstellungen**, um alle CylanceGATEWAY Connector-Konfigurationen, einschließlich des selbstsignierten TLS-Zertifikats, zu löschen. CylanceGATEWAY Connector muss neu gestartet werden, was zu einer Unterbrechung der Netzwerkverbindung führt.

Aufgaben	Schritte
Administratorkennwor ändern	Sie können das für CylanceGATEWAY Connector verwendete Administratorkennwort jederzeit ändern. Dadurch wird das Administratorkennwort, das für den Zugriff auf CylanceGATEWAY Connector in der vSphere-, Hyper-V-, Microsoft Entra ID-, AWS- oder ESXi-Umgebung verwendet wird, nicht geändert. Jedes Mal, wenn Sie das Kennwort ändern, werden Sie aufgefordert, sich mit dem neuen Kennwort erneut anzumelden. **a.** Klicken Sie auf **Administratorkennwort ändern**. **b.** Geben Sie das aktuelle Administratorkennwort ein. **c.** Geben Sie das neue Kennwort ein, und bestätigen Sie es. **d.** Klicken Sie auf **Kennwort ändern**. **e.** Wenn Sie dazu aufgefordert werden, klicken Sie auf **Jetzt anmelden**. Nach einer kurzen Wartezeit werden Sie automatisch zur Anmeldeaufforderung weitergeleitet. **f.** Geben Sie Ihren Administrator-Benutzernamen und Ihr neues Kennwort ein, und klicken Sie auf **Anmelden**.

Verwalten von CylanceGATEWAY Connectors

Nachdem Sie CylanceGATEWAY Connectors registriert haben, können Sie eine Systemdiagnose-URL angeben und die IP-Adressen für Ihre Connector einschränken. Wenn keine Systemdiagnose-URL angegeben wird, werden die DNS- und HTTP-Informationen nicht im Status der Systemdiagnose für einen Connector angezeigt. Für CylanceGATEWAY Connectors können Sie eine der folgenden Aktionen ausführen:

Bildschirm	Maßnahmen
Auf dem Listenbildschirm Gateway-Connector	• Die Anzahl der aktiven Verbindungen anzeigen. • Zeigen Sie die Connector-Gruppe an, zu der der CylanceGATEWAY Connector gehört. • Zeigen Sie zusätzliche Metadaten für die Systemdiagnose für jede Connector-Instanz an. • Die Version der einzelnen Connector-Instanzen anzeigen. • Den Status Ihrer Connectors anzeigen. • Die CylanceGATEWAY Connectors-Informationen erneut laden. • Die Protokolldateien der einzelnen Connector-Instanzen herunterladen. • Einen Connector deaktivieren, um zu verhindern, dass neue Verbindungen durch den Connector geleitet werden. Aktive Netzwerkverbindungen werden nicht unterbrochen.

Bildschirm	Maßnahmen
Auf der Connector-Info-Seite	• Zeigen Sie die Connector-Gruppe an, zu der der CylanceGATEWAY Connector gehört. • Das Feld Private URL für einen Connector bearbeiten und die URL auf einer separaten Seite öffnen. • Weisen Sie den Connector einer anderen Connector-Gruppe zu. • Einen Connector deaktivieren, um zu verhindern, dass neue Verbindungen durch den Connector geleitet werden. Aktive Netzwerkverbindungen werden nicht unterbrochen. • Die Version des Connectors anzeigen. • Den Verbindungsstatus des Connectors anzeigen. • Die Protokolldateien für den Connector herunterladen. • Den öffentlichen Schlüssel anzeigen. • Den Verbindungsverlauf des Connectors anzeigen. Für die Uhrzeit des Verbindungsverlaufs wird UTC verwendet.

Die Beschränkung von Quell-IP-Adressen bietet zusätzliche Sicherheit, um sicherzustellen, dass nur CylanceGATEWAY Connectors mit den von Ihnen angegebenen IP-Adressen eine Verbindung zu Ihrem privaten Netzwerk herstellen können. Wenn Sie die Quell-IP-Adressen einschränken, sollten Ihre CylanceGATEWAY Connectors über eine feste IP-Adresse verfügen, entweder indem Sie eine statische IP-Adresse für den CylanceGATEWAY Connector festlegen, wenn er in einer vSphere-Umgebung oder einer ESXi-Umgebung bereitgestellt wird, oder eine DHCP-IP-Reservierung in Ihrem Netzwerk erstellen.

Abhängig von der Anzahl der aktiven CylanceGATEWAY-Benutzer in Ihrer Umgebung kann eine Komponente der BlackBerry Infrastructure, die für die Verwaltung eingehender Tunnel über den Connector verantwortlich ist, die Ressourcen skalieren, die Ihrer Organisation zugewiesen sind. Jeder CylanceGATEWAY Connector erstellt einen Tunnel zu dieser Komponente und führt eine Integritätsprüfung für diese Komponente durch. Die Spalten „Status der Systemdiagnose“ und „Status“ stellen dann den Status dieser Tunnel vom Connector zur Komponente bereit, die für deren Verwaltung verantwortlich ist. Wenn beispielsweise in der Spalte „Status der Systemdiagnose“ $X/2$ angezeigt wird, bedeutet dies, dass zu diesem Zeitpunkt zwei der Komponenten Ihrer Organisation zugeordnet sind. Wenn in der Spalte 2/2 angezeigt wird, hat der Connector erfolgreich zwei Tunnel zur Komponente eingerichtet. Wenn Sie 0/2 oder 1/2 sehen, bedeutet dies, dass der Connector entweder keinen Tunnel erstellt hat oder einen der 2 erforderlichen Tunnel eingerichtet hat. Wenn der Status ⚠ lautet, können einige, aber nicht alle Benutzer auf Ressourcen in Ihrem privaten Netzwerk zugreifen.

Die Systemdiagnose-URL kann eine beliebige URL innerhalb Ihrer privaten Netzwerke sein, zu der CylanceGATEWAY-Benutzer eine Verbindung herstellen können sollen. CylanceGATEWAY sendet regelmäßig eine HTTP- oder HTTPS-GET-Anforderung einschließlich einer DNS-Anfrage über alle CylanceGATEWAY Connector-Tunnel zu dieser URL. Der Status der Systemdiagnose wird erweitert und zeigt den Tunnel-, DNS- und HTTP-Verbindungsstatus für jeden Connector an. Der Status 2/2 zeigt an, dass alles korrekt funktioniert. Der Status 0/0 zeigt an, dass die Statusprüfung einer neuen Verbindung noch aussteht.

Die Spalte „Status“ zeigt den Registrierungsstatus des CylanceGATEWAY Connector s bei der BlackBerry Infrastructure an. Das Symbol ✔ weist darauf hin, dass der CylanceGATEWAY Connector den Registrierungsprozess erfolgreich abgeschlossen und eine Verbindung zur BlackBerry Infrastructure hergestellt hat. Die Statusspalte zeigt den Verbindungsstatus an und kann eine Sicherheitsmeldung enthalten (z. B. wenn der Connector einen Neustart benötigt, um ein Update anzuwenden).

Spalte	Beschreibung
Status der Systemdiagnose	Dies ist der Gesamtstatus des CylanceGATEWAY Connector und enthält die folgenden Informationen: • **Tunnel**: Hierbei handelt es sich um den Status der CylanceGATEWAY Connector-Verbindung zur BlackBerry Infrastructure. Wenn der Status auf ein Verbindungsproblem hinweist, wenden Sie sich an Ihren BlackBerry-Kundendienstmitarbeiter. • **DNS**: Dies ist der Status der DNS-Abfrage, die vom CylanceGATEWAY Connector an Ihren angegebenen DNS-Server getätigt wurde. Wenn der Status auf ein Problem hinweist, überprüfen Sie, ob Sie Ihren privaten DNS-Server korrekt angegeben haben. • **HTTP**: Hierbei handelt es sich um den Status der HTTP-Anfrage, die an den CylanceGATEWAY Connector zum Abrufen der Systemdiagnose-URL gesendet wurde. Wenn der Status ein Problem anzeigt, überprüfen Sie, ob die Systemdiagnose-URL vom CylanceGATEWAY Connector erreichbar ist und ob Sie eine DNS-Forward-Lookup-Zone angegeben haben.

Status	Hierbei handelt es sich um den Status der CylanceGATEWAY Connector-Verbindung zur BlackBerry Infrastructure, einschließlich Status der Systemdiagnose.
	• : Der Connector hat die Registrierung nicht abgeschlossen. Dieser Status wird nur bei der Erstregistrierung des Connectors angezeigt.
	• : Der Connector hat den Registrierungsprozess abgeschlossen und stellt eine Verbindung zur BlackBerry Infrastructure her.
	• : Der Connector hat den Registrierungsprozess abgeschlossen, es wurden aber nicht alle Verbindungen zur BlackBerry Infrastructure hergestellt. Wenn dieser Status angezeigt wird, lesen Sie die zugehörige Sicherheitsmeldung und stellen Sie sicher, dass eine Systemdiagnose-URL in der Connector-Gruppe angegeben wurde.
	• : Der Connector-Registrierungsprozess wurde nicht abgeschlossen oder es liegt ein Fehler beim Herstellen der Verbindungen zur BlackBerry Infrastructure vor. Die folgenden Fehlermeldungen können angezeigt werden:
	  • Die Registrierung ist aufgrund eines Speicherfehlers fehlgeschlagen: Stellen Sie sicher, dass genügend Speicherplatz vorhanden ist, um den CylanceGATEWAY Connector zu registrieren.
	  • Fehler: Zeigen Sie den vollständigen Status der Systemdiagnose für den Connector an, einschließlich Tunnel-, DNS- und HTTP-Informationen. Wenn DNS beispielsweise „Fehlgeschlagen“ anzeigt, überprüfen Sie, ob Ihre DNS-Einstellungen korrekt sind.

Verwalten von CylanceGATEWAY Connectors

Führen Sie diese Aufgabe für jede Connector-Gruppe aus.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Privates Netzwerk**.
3. Klicken Sie auf **Connector-Gruppen**. Klicken Sie auf eine Connector-Gruppe.

4. Klicken Sie auf **Systemdiagnose**.
5. Geben Sie eine URL in Ihrem privaten Netzwerk an, auf die der CylanceGATEWAY Connector zugreifen kann, um zu überprüfen, ob CylanceGATEWAY eine Verbindung zur URL herstellen kann.

   Die Systemdiagnose-URL muss einen FQDN enthalten, den Ihr privater DNS-Server auflösen kann. Der FQDN muss in eine IP-Adresse aufgelöst werden, die sich innerhalb des für Ihr privates Netzwerk definierten IP-Bereichs befindet.
6. Um die zulässigen IP-Adressen der CylanceGATEWAY Connectors anzugeben, klicken Sie auf **Quell-IP-Beschränkung**.
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **Speichern**.
9. Um zusätzliche Informationen zu einem CylanceGATEWAY Connector anzuzeigen und die Connector-Protokolldateien herunterzuladen oder einen benutzerdefinierten FQDN oder eine IP-Adresse in der privaten URL einzugeben, klicken Sie auf den Namen des CylanceGATEWAY Connector.

   Hinweis: Wenn Sie einen benutzerdefinierten FQDN oder eine benutzerdefinierte IP-Adresse eingeben, wird der FQDN oder die IP-Adresse nicht validiert.
10. Um die CylanceGATEWAY Connectors-Informationen neu zu laden, klicken Sie auf ⟳.

Aktualisieren eines CylanceGATEWAY Connector s

Sie können prüfen, ob ein Update für den CylanceGATEWAY Connector oder das Betriebssystem der virtuellen Maschine verfügbar ist.

Bevor Sie beginnen: Überprüfen Sie die Version von CylanceGATEWAY Connector, die auf der Cylance Endpoint Security-Verwaltungskonsole installiert ist, unter „Einstellungen > Netzwerk > Privates Netzwerk > Gateway-Connectoren“.

1. Prüfen Sie *my*Account oder die Versionshinweise zu Cylance Endpoint Security, um festzustellen, ob eine neue Version der CylanceGATEWAY Connector-Software verfügbar ist, und führen Sie eine der folgenden Aktionen aus:
   - Wenn neue CylanceGATEWAY Connector-Software verfügbar ist, führen Sie Schritt 2 für Ihre Umgebung aus.
   - Wenn kein neues CylanceGATEWAY Connector-Software-Update verfügbar ist, suchen Sie nach einem Linux-Betriebssystem-Update.
2. Führen Sie eine der folgenden Aufgaben aus:

Umgebung	Schritte
Aktualisieren Sie die CylanceGATEWAY Connector-Version 2.9 oder höher.	Verwenden Sie die DEB-Datei, um die Connector-Instanz zu aktualisieren und Ihre Konfigurationen beizubehalten. **a.** Laden Sie die DEB-Version des Connectors in *my*Account herunter. **b.** Kopieren Sie das DEB-Paket auf den Connector, den Sie aktualisieren möchten. Wenn SSH aktiviert ist, können Sie SCP verwenden, um das DEB-Paket von jedem Host mit SSH-Zugriff auf den Connector zu kopieren. Anweisungen finden Sie unter Zugreifen auf den CylanceGATEWAY Connector mit OpenSSH. Andernfalls können Sie SCP auf dem Connector verwenden, um das DEB-Paket von einem beliebigen SSH-fähigen Host zu kopieren, den der Connector erreichen kann. **c.** Geben Sie in der Unix-Konsole `sudo apt install <path>/cylance-gateway-connector-<version>.deb` ein. Beispiel: `sudo apt install /home/admin/cylance-gateway-connector-2.10.0.938.deb` **d.** Drücken Sie die **Eingabetaste**.
Aktualisieren Sie die CylanceGATEWAY Connector-Version 2.8 oder früher, oder führen Sie eine vollständige Neuinstallation durch.	Erstellen Sie eine neue Connector-Instanz für Ihre Umgebung. Anweisungen finden Sie unter Einrichten von CylanceGATEWAY Connector.

3. Starten Sie die virtuelle Maschine für alle CylanceGATEWAY Connector neu, bei denen **Neustart erforderlich, um Betriebssystem-Updates und Sicherheitskorrekturen anzuwenden** in der Spalte **Status** angezeigt wird, um die Installation des Betriebssystem-Updates abzuschließen.

Wenn Sie fertig sind: Wenn der CylanceGATEWAY Connector registriert ist, aber sein Tunnel nicht mit der BlackBerry Infrastructure verbunden ist, können Sie einen Konnektivitätstest initiieren, um zu überprüfen, ob die von Ihrem privaten Netzwerk gesendeten UDP-Pakete von der BlackBerry Infrastructure empfangen wurden, und ob die von der BlackBerry Infrastructure gesendeten UDP-Pakete von Ihrem privaten Netzwerk empfangen werden. Geben Sie in der Anmeldeaufforderung Ihrer Umgebung (z. B. vSphere) `/var/lib/cylance-gateway/bin/udp-connectivity-test` ein. Drücken Sie die **Eingabetaste**. Sie können diesen Befehl in jeder Shell ausführen (z. B. csh und bash). Weitere Informationen zu den Konnektivitätsergebnissen finden Sie unter Antworten auf UDP-Konnektivitätstests.

Antworten auf UDP-Konnektivitätstests

Die folgenden Beispiele zeigen die Ausgaben, die angezeigt werden können, wenn Sie den UDP-Pfad zwischen dem CylanceGATEWAY Connector und der BlackBerry Infrastructure überprüfen.

In den folgenden Beispielen

- steht „Endpoint“ für die IP-Adresse und den Port des ausgeführten UDP-Konnektivitätstests.
- steht „Client Address:Port“ für die externe IP-Adresse und den Port des CylanceGATEWAY Connector, wie von der BlackBerry Infrastructure erkannt.
- steht „Server“ für die BlackBerry Infrastructure.

Beispiel: UDP-Datenverkehr wird erfolgreich gesendet und empfangen

In diesem Beispiel wird der UDP-Datenverkehr erfolgreich zwischen dem Connector in Ihrem privaten Netzwerk und dem BlackBerry Infrastructure gesendet und empfangen.

```
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
```

Beispiel: Der ausgehende UDP-Datenverkehr wird blockiert.

In diesem Beispiel konnte der UDP-Konnektivitätstest-Client die Client-Hello-Nachricht senden, aber die BlackBerry Infrastructure hat die Antwort nicht innerhalb des Zeitlimits erhalten.

```
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
```

Beispiel: Der eingehende UDP-Datenverkehr wird blockiert.

In diesem Beispiel hat der UDP-Konnektivitätstest-Client die Client-Hello-Nachricht gesendet und die BlackBerry Infrastructure hat sie empfangen und geantwortet, aber der Test-Client hat die Antwort nicht innerhalb des Zeitlimits erhalten.

```
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
```

Angeben Ihres privaten Netzwerks

Bevor Sie beginnen:

- Stellen Sie sicher, dass Sie eine Liste der IP-Adressen oder IP-Adressbereiche für alle Ziele pflegen, die Sie als Teil Ihres privaten Netzwerks definieren möchten. Die relevanten Informationen hierzu erhalten Sie von Ihrem Netzwerkadministrator.
- Sie können keinen privaten Netzwerkzugriff einrichten, wenn Sie keinen CylanceGATEWAY Connector installieren. Stellen Sie sicher, dass Sie einen oder mehrere CylanceGATEWAY Connector in einem Teil jedes Netzwerks installiert haben, der vollen Zugriff auf die hier angegebenen Adressen hat. Anweisungen zum Installieren eines CylanceGATEWAY Connector finden Sie unter Einrichten von CylanceGATEWAY Connector.
- Sie können maximal acht Connector-Gruppen erstellen. Sie können maximal acht CylanceGATEWAY Connectors pro Connector-Gruppe hinzufügen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Privates Netzwerk**.
3. Klicken Sie auf **Connector-Gruppen**.
4. Klicken Sie auf **Connector-Gruppe hinzufügen**.
5. Geben Sie einen Namen und eine Beschreibung ein. Der Connector-Name kann zwischen 3 und 250 Zeichen lang sein. Die Bezeichnung kann zwischen 3 und 500 Zeichen lang sein.
6. Klicken Sie auf der Registerkarte **Netzwerk-Routing** auf **Adresse hinzufügen**.
7. Geben Sie eine oder mehrere IP-Adressen, IP-Bereiche oder CIDRs ein und klicken Sie auf **Hinzufügen**.

   Wenn in Ihrer Umgebung der gesamte Netzwerkdatenverkehr zu Ihrer lokalen Infrastruktur umgeleitet werden muss, geben Sie `0.0.0.0/0` ein. BlackBerry empfiehlt, dass Sie nur Datenverkehr umleiten, der für Ressourcen in Ihrem privaten Netzwerk bestimmt ist, und Ihre Umgebung so konfigurieren, dass sie CylanceGATEWAY-Clouddienste für den Datenverkehr zu Internetzielen verwendet.

   Hinweis: Wenn Sie 0.0.0.0/0 für Ihr Netzwerk-Routing angeben, wird der gesamte Nicht-DNS-Datenverkehr (z. B. HTTP-Datenverkehr) über den CylanceGATEWAY Connector geleitet. Datenverkehr zu Ressourcen, die nicht Teil Ihres privaten Netzwerks sind, erfordert, dass die DNS-Abfrage an öffentliche DNS-Server und nicht an Ihren privaten DNS-Server gesendet wird, bevor die Verbindung hergestellt und der Datenverkehr über den CylanceGATEWAY Connector geleitet wird.
8. Um eine Adresse zu bearbeiten, klicken Sie neben der Adresse auf ✎.
9. Um eine Adresse zu entfernen, klicken Sie neben der Adresse auf ✕.
10. Um die Reihenfolge der Liste zu ändern, ziehen Sie ⠿ für die Connector-Gruppe an die entsprechende Stelle in der Liste.
11. Um eine Connector-Gruppe zu löschen, entfernen Sie alle zugewiesenen CylanceGATEWAY Connector aus der Connector-Gruppe oder weisen Sie sie neu zu. Klicken Sie auf 🗑.

Angeben eines privaten DNS

Sie können die Einstellungen für das private DNS festlegen, um den CylanceGATEWAY-Datenverkehr innerhalb des privaten Netzwerks weiterzuleiten. Sie können die IP-Adressen der DNS-Server, die an DNS-Server delegierten Domänennamen für Forward-Lookups und die an DNS-Server delegierten CIDRs für Reverse-Lookups

angeben. Die IP-Adressen der DNS-Server werden von allen Connector-Gruppen gemeinsam verwendet und müssen in einer Connector-Gruppe enthalten sein. Die relevanten Informationen hierzu erhalten Sie von Ihrem Netzwerkadministrator.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Privates Netzwerk**.
3. Klicken Sie auf **DNS**.
4. Führen Sie die folgenden Aktionen aus, um einen DNS-Server anzugeben:
   a) Klicken Sie auf **DNS-Server**.
   b) Klicken Sie auf **DNS-Server hinzufügen**.
   c) Geben Sie die IP-Adresse für Ihren DNS-Server ein und klicken Sie auf **Hinzufügen**.
5. Führen Sie die folgenden Aktionen aus, um eine Domäne für Forward-Lookups anzugeben. Sie können maximal 100 Forward-Lookup-Zonen angeben.
   a) Klicken Sie auf **Forward-Lookup-Zone**.
   b) Klicken Sie auf **Forward-Zone hinzufügen**.
   c) Geben Sie einen Dateinamen ein und klicken Sie auf **Hinzufügen**.

   Wenn Sie keine Forward-Lookup-Zone angeben, schlägt die CylanceGATEWAY Connector-Systemdiagnose fehl. Wenn Sie Split-Tunneling aktivieren und keine Forward-Lookup-Zone angeben, werden alle DNS-Abfragen durch den Tunnel geleitet.
6. Führen Sie die folgenden Aktionen aus, um ein CIDR für Reverse-Lookups anzugeben:
   a) Klicken Sie auf **Reverse-Lookup-Zone**.
   b) Klicken Sie auf **Reverse-Zone hinzufügen**.
   c) Geben Sie ein CIDR ein und klicken Sie auf **Hinzufügen**.
7. Um eine Adresse oder einen Domänennamen zu bearbeiten, klicken Sie auf .
8. Um eine Adresse oder einen Domänennamen zu entfernen, klicken Sie auf .

Angeben der DNS-Suffixe

Sie können bis zu 32 Suffixe angeben, die das private DNS an Suchen nach unqualifizierten Namen anhängt. Die relevanten Informationen hierzu erhalten Sie von Ihrem Netzwerkadministrator. Wenn Sie mehr als ein Suffix angeben, können Sie jedem Suffix einen Rang zuweisen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Client-DNS**.
3. Aktivieren Sie **DNS-Suchdomäne (oder Suffix)**
4. Klicken Sie auf **DNS-Suffix hinzufügen**.
5. Geben Sie den DNS-Suffixnamen ein und klicken Sie auf **Hinzufügen**.
6. Wiederholen Sie die Schritte 4 und 5 für jedes Suffix, das Sie hinzufügen möchten.
7. Um ein Suffix zu bearbeiten, klicken Sie auf .
8. Um ein Suffix zu entfernen, klicken Sie auf .
9. Um die Reihenfolge der Liste zu ändern, ziehen Sie für das Suffix an die entsprechende Stelle in der Liste.
10. Klicken Sie auf **Speichern**.

Angeben der IP-Bereiche des privaten CylanceGATEWAY-Agenten

CylanceGATEWAY weist dem CylanceGATEWAY-Agenten private IP-Adressen über Tunnel aus einem privaten IP-Bereich zu, der systemweit konfiguriert wird und für jeden Mandanten gleich ist. Sie sollten einen privaten IP-Adressbereich für den Endpunkttunnel angeben, der sich nicht mit dem privaten Netzwerkbereich des Mandanten für CylanceGATEWAY-Agenten überschneidet. Durch die Bereitstellung eines privaten IP-Adressbereichs können

potenzielle Konflikte verhindert werden, z. B. wenn ein Agent versucht, auf einen privaten Netzwerkdienst zuzugreifen, der dieselbe IP-Adresse wie die hat, die dem Agenten zugewiesen ist. Der IP-Bereich des Agenten muss im IPv4-CIDR-Format vorliegen und innerhalb Ihres privaten Netzwerks eindeutig sein, um Probleme beim Routing zu anderen Endpunkten in Ihrem Netzwerk zu vermeiden. Der Standardbereich ist 10.10.0.0/16. Suffixe müssen kleiner als 17 sein.

Warnung: Wenn Sie den Agent-IP-Bereich aktualisieren, werden die zugehörigen Agenten und CylanceGATEWAY Connector s möglicherweise getrennt und erneut verbunden. Wenn Sie während der Trennung und Wiederherstellung auf den Bildschirm „Gateway Connectors“ zugreifen (Einstellungen > Netzwerk > Privates Netzwerk), wird möglicherweise eine der folgenden Meldungen angezeigt. Klicken Sie auf .

- Registrierung konnte nicht abgeschlossen werden: 500
- Fehler. Neustart erforderlich, um Betriebssystem-Updates und Sicherheitskorrekturen anzuwenden

1. Klicken Sie in der Menüleiste auf **Einstellungen > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Privates Netzwerk**.
3. Klicken Sie auf **Agent-IP-Bereich**.
4. Geben Sie die CIDR ein.
5. Klicken Sie auf **Speichern**.

Verwenden eigener IP-Adressen (BYOIP)

Sie können dedizierte IP-Adressen in einem IPv4-CIDR-/24-Bereich zu CylanceGATEWAY hinzufügen, die zur Verwaltung des Netzwerkausgangverkehrs verwendet werden.

Sie können die dedizierten IP-Adressen für die folgenden Aufgaben verwenden:

- Nutzen der eigenen IP-Adressen Ihres Unternehmens als Quell-IP-Pinning.
- Vermeiden von Problemen, bei denen einige Websites die IP-Bereiche von AWS blockieren.
- Angeben von GeoIP-Informationen für die Adressen.
- Einzelne CIDR anstelle mehrerer nicht-kontinuierlicher IPs zulassen.

Um dedizierte IP-Adressen zu CylanceGATEWAY hinzufügen, senden Sie eine Anforderung an BlackBerry Technical Support Services. Weitere Anweisungen finden Sie unter https://support.blackberry.com/community in Artikel 100189.

Übersetzung der Netzwerkadresse mit CylanceGATEWAY

Standardmäßig wendet CylanceGATEWAY NAT (Network Address Translation) auf den Datenverkehr in Ihr privates Netzwerk an. NAT wird auch auf Ihre Endpunkte (z. B. Geräte) angewendet, wenn Benutzer auf das Internet und SaaS-Apps zugreifen. Nach der Anwendung von NAT wird die echte IP-Adresse verborgen, und alle eingehenden Verbindungen zu einem bestimmten Endpunkt werden verhindert. NAT wird nicht für Datenflüsse angewendet, die den CylanceGATEWAY-Tunnel nicht verwenden (z. B. Sicherheitsmodus).

Hinweis: Eingehende Verbindungen zu Endpunkten werden von CylanceGATEWAY verhindert (Sie können beispielsweise keine Verbindung zu Endpunkten mithilfe von Remote-IT-Tools wie Remote Desktop Connection herstellen).

NAT wird auf den Datenverkehr angewendet, der durch den CylanceGATEWAY Connector in Ihr privates Netzwerk fließt. Der Connector bietet zusätzliche Informationen zu UDP- und TCP-Strömen, die auf dem Bildschirm „Netzwerkereignisse“ (CylanceGATEWAY > Ereignisse) angezeigt werden. Sie können die private Quell-IP und den privaten Quellport eines blockierten oder als potenziell schädlich eingestuften Ereignisses identifizieren. Weitere Informationen finden Sie unter:

- Anzeigen der Seite „Ereignisdetails“
- Datenfluss: Zugreifen auf einen Anwendungs- oder Inhaltsserver in Ihrem privaten Netzwerk

NAT wird von CylanceGATEWAY auf den Datenverkehr angewendet, der durch den Tunnel fließt, um auf Internetziele und Cloud-basierte SaaS-Anwendungen zuzugreifen. Sie können die Ereignisse basierend auf der Gateway-Tunnel-IP-Adresse filtern, die von den Benutzern für den Zugriff auf die externen Ziele verwendet wurde. Weitere Informationen finden Sie unter:

- Anzeigen der Seite „Ereignisdetails“
- Datenfluss: Zugriff auf Cloud-basierte Anwendungen oder Internetziele

Definieren von Netzwerkdiensten

Ein Netzwerkdienst ist eine Gruppe von Adressen (FQDNs oder IP-Adressen), die Sie verwenden können, um die Einrichtung von Regeln der Zugriffssteuerungsliste (ACL) zu vereinfachen. Wenn Sie ACL-Regeln erstellen, können Sie einen Netzwerkdienst angeben, anstatt jede einzelne Adresse anzugeben. BlackBerry verwaltet und aktualisiert regelmäßig Netzwerkdienste für viele gängige SaaS-Anwendungen, um den Prozess für Sie zu vereinfachen. Sie können zusätzliche Netzwerkdienste für öffentliche und private Anwendungen definieren. Sie können vorhandene Netzwerkdienste verschachteln. Wenn Sie Netzwerkdienste verschachteln, werden die Ziele jedes hinzugefügten Netzwerkdienstes referenziert, und Sie haben Zugriff auf alle enthaltenen Ziele. Wenn eine Änderung an einem der kombinierten Netzwerkdienste vorgenommen wird, wird diese automatisch übernommen. Sie können eine Suche nach den von Ihnen hinzugefügten Netzwerkdiensten durchführen. Weitere Informationen zu Suchvorgängen finden Sie unter Durchsuchen von ACL-Regeln und Netzwerkdiensten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Netzwerkdienste**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie einen Namen und eine Beschreibung für den Netzwerkdienst ein.
5. Klicken Sie optional auf **Netzwerkdienste** und wählen Sie einen oder mehrere Netzwerkdienste aus.
6. Klicken Sie optional auf **Adresse**. optional eine IP-Adresse, einen FQDN oder eine Platzhalterdomäne für das Ziel ein. Klicken Sie auf +, um zusätzliche Adressen hinzuzufügen. Die folgenden Adressformate werden unterstützt:
   - IP-Adressbereich: 172.16.10.0–172.16.10.255
   - Einzelne Adresse: 172.16.10.2
   - IP-Adressbereich: 172.16.10.0–172.16.10.255
   - CIDR: 172.16.10.0/24
   - FQDN: domain.example.com
   - Domäne mit Platzhalterzeichen: *.example.com
7. Klicken Sie auf **Protokoll**, wählen Sie ein Protokoll für den Verbindungsversuch aus und geben Sie den zu verwendenden Port oder Portbereich an. Klicken Sie auf +, um ein zusätzliches Protokoll und zusätzliche Ports hinzuzufügen.
8. Wiederholen Sie die Schritte 6 und 7, um weitere Adressen und Ports hinzuzufügen.
9. Klicken Sie auf **Hinzufügen**.
10. Um einen Netzwerkdienst zu bearbeiten, klicken Sie auf das Feld, das Sie bearbeiten möchten, und nehmen Sie die Änderungen vor. Sie können keine von BlackBerry definierten Dienste bearbeiten.
11. Um einen Netzwerkdienst zu entfernen, klicken Sie neben dem Dienst, der Adresse oder dem Port auf ×. Um eine Adress- und Portzeile zu entfernen, klicken Sie neben der entsprechenden Zieladresse und Portzeile auf ×. Sie können keine von BlackBerry definierten Dienste löschen.

Wenn Sie fertig sind: Sie können die Liste der Netzwerkdienste durchsuchen, um die entsprechenden Informationen anzuzeigen. Klicken Sie auf , wählen Sie einen oder mehrere vordefinierte Geltungsbereiche und eine Bedingung aus und geben Sie die Kriterien an. Klicken Sie auf den Namen des Dienstes, dessen Einstellungen Sie anzeigen möchten. Klicken Sie auf , um die Suche zurückzusetzen.

Netzwerkzugriffssteuerung

Sie definieren die Netzwerkressourcen, mit denen Geräte, die mit CylanceGATEWAY registriert sind, über die Zugriffssteuerungsliste (ACL) eine Verbindung herstellen können. Die ACL definiert zulässige und blockierte Ziele in privaten und öffentlichen Netzwerken. Die Zugriffssteuerungsliste gilt nur für Benutzer, denen eine Gateway-Dienstrichtlinie zugewiesen worden ist.

Die Zugriffssteuerungsliste gilt für alle CylanceGATEWAY-Benutzer des Mandanten. Jeder Netzwerkzugriffsversuch eines Geräts wird für jede Verbindungsphase (DNS-Anfrage, Verbindungsaufbau und TLS-Handshake) mit den Regeln verglichen, bis eine Regel gefunden wird, die dem Versuch entspricht. Die Regel muss mit allen angegebenen Eigenschaften übereinstimmen, einschließlich Zielen oder Zielkategorien, angegebenen Benutzern oder Gruppen und der für das Ziel festgelegten Risikostufe. Die erste passende Regel legt fest, ob der Zugriffsversuch blockiert wird oder ob er zugelassen wird und in die nächste Phase übergehen kann. Ein Zugriffsversuch, der in allen Phasen zugelassen wird, kann vollständig aufgebaut werden. Wenn ein Netzwerkzugriffsversuch mit keiner Regel in der Zugriffssteuerungsliste übereinstimmt, wird der Zugriff blockiert. Die ACL unterstützt bis zu 1000 Regeln.

ACL-Regeln anwenden

Die ACL-Regeln gelten für alle CylanceGATEWAY-Benutzer des Mandanten. ACL-Regeln bewerten jeden Netzwerkzugriffsversuch in der Reihenfolge, in der sie in der Verwaltungskonsole von oben nach unten angezeigt werden. Die Standardregel wird immer zuletzt ausgewertet und wenn keine der vorherigen Regeln übereinstimmt, wird der Zugriff auf alle Ressourcen gesperrt. Die Standardregel kann nicht deaktiviert oder geändert werden

Beim Erstellen der ACL-Regeln empfiehlt BlackBerry daher darauf zu achten, dass diese in der folgenden Reihenfolge angezeigt werden:

1. Zugriff auf Internetinhalte sperren, die bestimmte CylanceGATEWAY-Kategorien enthalten
2. Zugriff auf nicht kategorisierte Dienste basierend auf den Anforderungen Ihres Unternehmens sperren
3. Zugriff auf unternehmensweite Dienste im privaten Netzwerk gewähren
4. Zugriff auf alle öffentlichen Internetziele zulassen
5. Standard

Die folgende Tabelle enthält Beispiele für Regeln und deren erforderliche Einstellungen:

Regel	Beschreibung

Benutzerzugriff auf öffentliche Internetziele zulassen	Mit dieser Regel können Benutzer auf jedes Ziel zugreifen, das in Ihrem Unternehmen als öffentliches Internet gilt. Benutzer können nicht auf die angegebenen RFC1918-Adressen zugreifen.
	Um diese Regel zu erstellen, legen Sie die folgenden Einstellungen fest:
	• Im Abschnitt **Aktion**
	  • In der Dropdown-Liste **Aktion** wird **Zulassen** angezeigt.
	  • Das Kontrollkästchen **Zugriffsversuche anhand des Netzwerkschutzes prüfen** ist aktiviert. Diese Einstellung ermöglicht die Übergabe der ACL durch die Regel, ermöglicht aber auch eine weitere Prüfung durch das Gateway.
	• Im Abschnitt **Ziel**
	  • In der Dropdown-Liste **Ziel** wird **Stimmt nicht überein** angezeigt.
	  • Geben Sie in das Feld **Adressen und Ports**, **Adresse** die RFC1918-Netzwerkbereiche ein.

Benutzerzugriff auf das private Netzwerk zulassen	Diese Regel ermöglicht Benutzern den Zugriff auf Netzwerkdienste innerhalb Ihres privaten Netzwerks.
	Damit Benutzer auf das private Netzwerk zugreifen können, müssen die folgenden Voraussetzungen erfüllt sein:
	• Stellen Sie sicher, dass der CylanceGATEWAY Connector im Netzwerk installiert ist, damit Datenverkehr Ihr privates Netzwerk erreichen kann. Anleitungen zur Installation von CylanceGATEWAY Connector in Ihrer Umgebung finden Sie unter Einrichten von CylanceGATEWAY Connector.
	• Stellen Sie sicher, dass Sie einen Netzwerkdienst definiert haben, der die privaten Netzwerkressourcen enthält, auf die Benutzer zugreifen sollen. Weitere Informationen zum Definieren von Netzwerkdiensten finden Sie unter Definieren von Netzwerkdiensten.
	Sie können die folgenden Einstellungen vornehmen:
	• Im Abschnitt **Aktion**:
	  • In der Dropdown-Liste **Aktion** wird **Zulassen** angezeigt.
	  • Deaktivieren Sie optional das Kontrollkästchen **Zugriffsversuche anhand des Netzwerkschutzes prüfen**. Es wird keine weitere Überprüfung durch das Gateway durchgeführt.
	• Im Abschnitt **Ziel**:
	  • In der Dropdown-Liste **Ziel** wird **Stimmt überein mit jeder/m** angezeigt.
	  • Wählen Sie im Feld **Netzwerkdienste** den Netzwerkdienst aus, auf den Benutzer zugreifen sollen.

ACL-Parameter

Die ACL ist eine geordnete Liste von Regeln, in der festgelegt wird, was geschieht, wenn ein CylanceGATEWAY-Benutzer versucht, auf ein Ziel im Internet oder in Ihrem privaten Netzwerk zuzugreifen. Jede Regel enthält

mehrere Parameter, die Ziele, Benutzer und andere Faktoren angeben können, mit denen eine Regel übereinstimmen kann, sowie die Aktion, die ausgeführt werden muss, wenn eine Regel übereinstimmt. Wenn ein Netzwerkzugriffsversuch mit keiner ACL-Regel übereinstimmt, wird der Zugriff blockiert.

Wenn Sie ACL-Regeln hinzufügen oder bearbeiten, werden die Aktualisierungen zu einer Liste von Entwurfsregeln hinzugefügt, bis Sie sie festlegen. Jeder Administrator hat eine eigene Entwurfsregelliste. Wenn ein Administrator eine Regelaktualisierung festlegt, werden alle anderen Administratoren mit einer Entwurfsregelliste aufgefordert, ihre Entwurfsliste zu löschen oder zu aktualisieren, bevor sie fortfahren.

Jede Regel kann die folgenden Parameter enthalten:

Element	Beschreibung
Allgemeine Informationen	
Name	Dies ist der Regelname.
Beschreibung	Dies ist eine kurze Beschreibung des Zwecks der Regel.
Aktiviert	Diese Einstellung gibt an, dass die Regel Teil der ACL ist. Sie können diese Option deaktivieren, um die Regel zu deaktivieren, ohne sie zu löschen.
Aktion	
Aktion	Diese Einstellung gibt an, ob der Zugriff zugelassen oder blockiert wird, wenn der Versuch mit der Regel übereinstimmt. Wenn die Fortsetzung des Zugriffsversuchs zugelassen wird, kann er in den nächsten Versuchsphasen erneut ausgewertet werden.
Adressen anhand Netzwerkschutz prüfen	Wenn die Regel „Aktion“ den Zugriff zulässt, wird mit dieser Einstellung angegeben, ob CylanceGATEWAY die Verbindung weiterhin blockiert, wenn eine potenzielle Netzwerkbedrohung erkannt wird. Sie sollten diese Option aktiviert lassen, es sei denn, genau festgelegte Benutzer müssen eine Verbindung zu potenziell schädlichen Zielen herstellen.
„Blockiert“-Benachrichtigungsmeldung auf Geräten anzeigen	Wenn die Regel „Aktion“ den Zugriff blockiert, wird mit dieser Einstellung eine Benachrichtigungsmeldung angegeben, die auf dem Gerät angezeigt wird, wenn ein Zugriffsversuch blockiert wird.
Datenverkehrsschutz	Diese Einstellung legt fest, ob Netzwerkzugriffsversuche auf dem Bildschirm „Netzwerkereignisse“ (CylanceGATEWAY > Ereignisse) angezeigt werden. Sie können den Datenverkehrsschutz aus Gründen der Haftung oder des Datenschutzes aktivieren. Wenn diese Einstellung aktiviert ist, werden keine Netzwerkzugriffsversuche auf dem Bildschirm „Netzwerkereignisse“ angezeigt. Wenn Ihre Umgebung Ereignisse an eine SIEM-Lösung oder einen Syslog-Server sendet und der Verbindungsversuch mit einer Regel mit Datenverkehrsschutz übereinstimmt, werden die Ereignisse nicht an die SIEM-Lösung oder den Syslog-Server gesendet.

Element	Beschreibung
Inhaltsprotokollierung	Diese Einstellung legt fest, ob die Seite Netzwerkereignisse > Ereignisdetails ursprüngliche unverschlüsselte HTTP-Verbindungsdaten im Nur-Text-Format enthalten soll. HTTP-Datenflüsse werden nicht entschlüsselt. Wenn diese Einstellung aktiviert ist, wird eine Zusammenfassung der Anforderungs- und Antwortdetails eines Ereignisses auf der Seite Ereignisdetails angezeigt. Sie können alle HTTP-Transaktionen innerhalb eines Ereignisses anzeigen. Die Seite „Ereignisdetails“ enthält die ersten drei HTTP-Ereignisse der Gesamtzahl der Ereignisse. Sie können alle Ereignisse und die zugehörigen Details anzeigen. Wenn Sie eine Regel erstellen, die sowohl Datenverkehrsschutz als auch Inhaltsprotokollierung enthält, hat der Datenverkehrsschutz Vorrang.
Port ignorieren	Mit dieser Einstellung wird angegeben, ob der Zielport des Zugriffssteuerungsversuchs als Teil dieser Regel ausgewertet oder ignoriert werden soll.
Ziele	
Ziel	Ziele können durch einen Netzwerkdienst, einen Adresssatz, einen Adresssatz mit definierten Protokollen und Ports oder nur durch definierte Protokolle und Ports festgelegt werden. Sie können eine der folgenden Optionen auswählen: • Nicht zutreffend: Die Regel enthält keine Ziele. Beispielsweise sind in der Regel nur Kategorien festgelegt, oder Sie möchten eine Regel erstellen, die alle Zugriffsversuche für bestimmte Benutzer zulässt, es sei denn, die Verbindung wird durch den Netzwerkschutz blockiert. • Stimmt überein mit jeder/m: Die Regel wird angewendet, wenn das Ziel mit einem in der Regel angegeben Ziel übereinstimmt. • Stimmt nicht überein: Die Regel wird angewendet, wenn das Ziel mit keinem der in der Regel angegebenen Ziele übereinstimmt.
Netzwerkdienste	Sie können einen oder mehrere Netzwerkdienste auswählen.
Adresse	Diese Einstellung gibt die IP-Adressen, FQDNs oder Platzhalterdomänen für die Zieladresse an. IP-Adressen können im IPv4- oder IPv6-Format vorliegen und durch eine einzelne IP-Adresse, einen IP-Adressbereich oder die CIDR-Schreibweise dargestellt werden. Die folgenden Adressformate werden beispielsweise unterstützt: • Einzelne IP-Adresse: 172.16.10.2 • IP-Adressbereich: 172.16.10.0–172.16.10.255 • CIDR: 172.16.10.0/24 • FQDN: domain.example.com • Domäne mit Platzhalterzeichen: *.example.com
Protokoll	Diese Einstellung legt fest, ob die Regel mit Verbindungsversuchen über TCP, UDP oder beiden übereinstimmt. Wenn Sie keine Option auswählen, sind TCP und UDP auf allen Ports die Standardeinstellung.
Port	Diese Einstellung gibt die für das Ziel verwendeten Ports an. Sie können entweder einen einzelnen Port oder einen Portbereich angeben.

Element	Beschreibung
Kategorie	Eine Kategorie definiert den auf einer Website verfügbaren Inhaltstyp. CylanceGATEWAY versucht, auf der Grundlage der verfügbaren Informationen, die Kategorie der Ziel-Websites bestmöglich zu bestimmen. Sie können eine der folgenden Optionen auswählen: • Nicht zutreffend: Die Regel enthält keine Kategorien. • Stimmt überein mit jeder/m: Die Regel wird angewendet, wenn das Ziel mit einer der in der Regel angegebenen Kategorien übereinstimmt. Wenn Sie diese Option aktivieren, wird eine Kategorieliste angezeigt, aus der Sie auswählen können. • Stimmt nicht überein: Die Regel wird angewendet, wenn das Ziel mit keiner der in der Regel angegebenen Kategorien übereinstimmt. Wenn Sie diese Option aktivieren, wird eine Kategorienliste angezeigt, aus der Sie auswählen können. Weitere Informationen zu den verfügbaren Kategorien, die angegeben werden können, finden Sie unter Inhaltskategorien von Zielen
Bedingungen	
Benutzereigenschaften	Diese Einstellung legt Benutzer, Benutzergruppen oder Betriebssysteme fest, die in die Regel aufgenommen werden sollen. Sie können eine beliebige Anzahl von Benutzern, Benutzergruppen und Betriebssystemen oder eine Kombination davon angeben. Wenn Sie auf die Dropdown-Liste „Benutzereigenschaften“ klicken, wählen Sie die Benutzereigenschaft aus, für die Sie die Bedingung festlegen möchten. Sie können eine der folgenden Optionen auswählen: • Nicht zutreffend: Die Regel gilt für alle Benutzer, Gruppen und Betriebssysteme. • Stimmt überein mit jeder/m: Die Regel gilt nur für die Benutzer, Gruppen und Betriebssysteme, die Sie der Regel hinzufügen. Wenn Sie diese Option auswählen, wird ein Feld zum Hinzufügen von Benutzereigenschaften angezeigt. • Stimmt nicht überein: Die Regel gilt nur für Benutzer, Gruppen und Betriebssysteme, die nicht in der Regel aufgeführt sind. Wenn Sie diese Option auswählen, wird ein Feld zum Hinzufügen von Benutzereigenschaften angezeigt. Wenn Sie mit der Eingabe eines Namens oder einer Benutzergruppe beginnen, wird eine Liste mit übereinstimmenden Benutzernamen angezeigt. Wenn Sie das Betriebssystem angeben, müssen Sie es aus der Liste auswählen. Sie können eine der folgenden Betriebssystemoptionen auswählen: • Android • iOS • macOS • Windows Sie können Zeilen hinzufügen, um eine beliebige Anzahl von Benutzern, Gruppen und Betriebssystemen anzugeben.

Element	Beschreibung
Risiko	Diese Einstellung gibt die akzeptable Risikostufe des Geräts entsprechend der Konfiguration in der Richtlinie zur Risikobewertung an. Informationen zum Erstellen einer Risikobewertungsrichtlinie finden Sie unter Erstellen einer Risikobewertungsrichtlinie. • Nicht zutreffend: Die Risikostufe gilt nicht als Bedingung für den Zugriff. • Stimmt überein mit jeder/m: Die Verbindung wird nur zugelassen, wenn das Gerät innerhalb des Bereichs akzeptabler Risikostufen liegt. Wenn Sie diese Option auswählen, können Sie die akzeptablen Risikostufen auswählen. Die Standardrisikostufe ist „Sicher“ (kein Risiko).

Inhaltskategorien von Zielen

Diese Kategorien steuern die Inhaltarten, auf die Benutzer auf einer verfügbaren Website zugreifen können. Sie können eine gesamte Kategorie oder eine Unterkategorie auswählen.

Erwachsene

Inhalte für Erwachsene. Mögliche Optionen:

- Erwachsene
- Alkohol und Tabak
- Partnersuche
- Glücksspiel
- Nacktdarstellungen
- Obszöne Sprache
- Nacktdarstellungen
- Obszöne Sprache
- Persönlich und Dating
- Pornografie
- Sexspielzeug
- Badesachen und Unterwäsche
- Waffen

Bandbreite

Sites, die die Geschwindigkeit der Datenübertragung in Ihrem Netzwerk beeinflussen können. Mögliche Optionen:

- Download von Anwendungssoftware
- Downloadsites
- Internetkommunikation und Telefonie
- Medienfreigabe
- Online-Speicherung und -Sicherung
- Geparkte Domänen
- Geparkte Domänen
- Peer-to-Peer
- Persönliche Netzwerkspeicherung und -sicherung
- Fotogalerien
- Shareware und Freeware
- Spam
- Streaming-Medien
- Überwachung
- Video-Hosting
- VVOIP

Computer- und Informationstechnologie

Computer- und IT-Inhalte. Mögliche Optionen:

- Computer- und Internetinformationen
- Content Delivery Networks (CDNs)
- Dialer-Sites
- DoH
- E-Mail
- Informationstechnologie
- Internet
- Internet-Portale
- Onlinedienste
- Remote-Zugriff
- Remote-Steuerung
- Suchmaschinen
- Technologie und Computertechnik
- Update-Sites
- URL-Weiterleitung
- URL-Verkürzung
- VPN-Sites
- Webanwendungen
- Webzusammenarbeit
- Webhosting
- Webinfrastruktur
- Webbasierte E-Mail

Allgemeines Interesse – Wirtschaft

Inhalte zum Thema Wirtschaft. Mögliche Optionen:

- Banking
- Bitcoin
- Unternehmen
- Unternehmen und Wirtschaft
- Geschäftsanwendungen
- Finanzdienste
- Gemeinnützige Organisationen
- Online-Zahlung
- Berufsverbände
- Aktienberatung und Tools

Allgemeines Interesse – Persönlich

Inhalte zu persönlichen Themen. Mögliche Optionen:

- Unterkunft
- Beratung
- Interessenvertretung
- Kunst und Kultur
- Astrologie
- Auktionsblogs und -foren
- Blogs und Wikis
- Cartoons
- Prominente
- Kochen
- Kult
- Ausbildung und Referenzen
- Bildungseinrichtungen
- Unterhaltung
- Unterhaltung und Kunst
- Mode und Schönheit
- Speisen und Getränke
- Spiele
- Allgemeine Organisationen
- Gesundheit und Medizin
- Haus und Garten
- Humor und Satire
- Jagen und Fischfang
- Institutionen
- Internetauktionen
- Einkaufen im Internet
- Jobsuche
- Kinder
- Lifestyle
- Mobile Kommunikation
- Mobiltelefon
- Kraftfahrzeuge
- Musik
- News
- Okkultismus
- Meinung
- Pay to Surf
- Persönlich
- Persönliche Websites und Blogs
- Apotheke
- Philosophie und politische Interessenvertretung
- Politik
- Drücken Sie
- Berufsverband
- Berufsbezogene Netzwerke
- Öffentliche Informationen
- Immobilien
- Freizeit und Hobbys
- Referenz und Forschung
- Religion und Philosophie
- Restaurants und Speisen
- Sekte
- Shopping
- Soziale Netzwerke
- Gesellschaft
- Sport
- Empfehlungen
- Boulevardzeitungen
- Training und Tools
- Übersetzung
- Reisen

Regierung

Inhalte zum Thema Regierung. Mögliche Optionen:

- Regierung
- Regierungsgeschäft
- Rechtliche Hinweise
- Militär

Potenzielle Haftung

Inhalte zum Thema potenzielle Haftung. Mögliche Optionen:

- Prüfungsbetrug
- Urheberrechtsverletzung
- Verbrechen
- Kryptojacking
- Gefahrstoffe
- Drogen
- Extremismus
- Betrug
- Hass und Diskriminierung
- Illegal
- Marihuana
- Betäubungsmittel
- Proxy-Umgehung und Anonymisierer
- Bedenklich
- Selbstmord
- Gewalt

Produktivität

Seiten mit Themen, die sich auf die Produktivität auswirken können. Mögliche Optionen:

- Werbung und Analyse
- Chat und IM
- Unzureichender Inhalt
- Marketing und Werbung
- Produktivitätsanwendung
- Webanzeigen
- Web- und E-Mail-Marketing

Sicherheitsrisiko

Websites, die nicht schädlich sind, aber Informationen enthalten, die ein Sicherheitsrisiko darstellen könnten (z. B. Inhalte, die über Spyware informieren). Mögliche Optionen:

- Bot-Netzwerke
- Command-and-Control
- Kompromittierte Websites
- DDoS
- DNS-Tunneling
- Dynamisches DNS
- Graumarkt-Websites
- Hacking
- Malware
- Gemischter Inhalt
- Phishing
- Potenziell schädlich
- Potenziell unerwünschte Software
- Spyware
- Verdächtige Website
- Nicht autorisierter Marketplace
- Warez

Unbekannt

Website-Inhalte, die unter Umständen schädlich sein können. Mögliche Optionen:

- Verschiedenes
- Neue Domäne
- Auflösungsfehler
- Unbekannt

Bewerten der Risikostufe eines Netzwerkziels

Mithilfe der Verwaltungskonsole können Sie Risikostufen bewerten und die Kategorie und Unterkategorie eines Netzwerkziels identifizieren, so wie sie von den Cloud-Diensten von CylanceGATEWAY analysiert und festgelegt werden würden. Diese Funktion gibt Aufschluss darüber, wie CylanceGATEWAY ein Ziel klassifizieren würde, wenn der Agent versucht, darauf zuzugreifen. So können Sie Ihre ACL-Regeln (Access Control List, Zugriffssteuerungsliste) erstellen und aktualisieren, um ein Ziel zuzulassen oder zu blockieren. Ziele, die nicht als schädlich bewertet werden, geben nur die Kategorie und Unterkategorie zurück.

Bevor Sie beginnen: Sie müssen über Administratorrechte verfügen, um auf diese Funktion in der Konsole zugreifen zu können.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Schutz > Netzwerkbedrohungen**.
2. Geben Sie in das Textfeld die IP-Adresse, den FQDN oder die URL des Ziels ein.
3. Klicken Sie auf **Analysieren**.

Konfigurieren der Zugriffssteuerungsliste

CylanceGATEWAY wertet vorhandene Verbindungen zu einem Ziel alle fünf Minuten aus. Bei der Auswertung wendet CylanceGATEWAY ACL-Regeln erneut an und die bestehende Verbindung kann ggf. getrennt werden. Dies kann beispielsweise der Fall sein, wenn sich die Risikostufe des Benutzers geändert hat oder die Zielreputation seit dem Aufbau der Verbindung aktualisiert wurde.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie Ihr privates Netzwerk entsprechend den Anforderungen Ihres Unternehmens definiert haben. Anweisungen finden Sie unter Definieren eines privaten Netzwerks.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Zugriffssteuerungsliste**.
3. Wenn eine Benachrichtigung angezeigt wird, dass ein Entwurfsregelsatz in Bearbeitung ist, klicken Sie auf die Registerkarte **Entwurfsregeln**.

   Wenn Sie keinen Entwurfsregelsatz in Bearbeitung haben, wird bei jeder von Ihnen vorgenommenen Aktualisierung ein Entwurfsregelsatz erstellt.
4. Führen Sie eine der folgenden Aktionen aus:

   - Um nach einer Regel oder einem Regelentwurf zu suchen, klicken Sie auf , wählen Sie einen oder mehrere vordefinierte Geltungsbereiche und eine Bedingung aus und geben Sie die Kriterien an. Klicken Sie auf die Regel, deren Einstellungen Sie anzeigen möchten. Klicken Sie auf , um die Suche zurückzusetzen. Weitere Informationen zu Suchvorgängen finden Sie unter Durchsuchen von ACL-Regeln und Netzwerkdiensten.
   - Um am Ende der Liste eine neue Regel hinzuzufügen, klicken Sie auf **Regel hinzufügen**.
   - Um eine neue Regel über oder unter einer vorhandenen Regel hinzuzufügen, klicken Sie in die Zeile der vorhandenen Regel auf ··· und wählen Sie **Regel oben hinzufügen** oder **Regel unten hinzufügen** aus.
   - Um eine Regel zu kopieren und über oder unter einer vorhandenen Regel hinzuzufügen, klicken Sie in der Zeile der vorhandenen Regel auf ··· und wählen Sie **Regel oben kopieren** oder **Regel unten kopieren** aus.
   - Um eine vorhandene Regel zu bearbeiten, klicken Sie auf den Namen der Regel.
   - Um eine Regel zu deaktivieren, klicken Sie in der Zeile der Regel auf .
   - Um eine Regel zu aktivieren, klicken Sie in der Zeile der Regel auf .
   - Um eine Regel zu löschen, klicken Sie in der Zeile der Regel auf ··· und wählen Sie **Regel löschen** aus.
   - Um die Reihenfolge der Regeln zu ändern, klicken Sie auf **Reihenfolge** und verwenden die Pfeile, um die Regeln in der Liste nach oben oder unten zu verschieben.
   - Um eine Regel hinzuzufügen, mit der Datenverkehr an ein blockiertes bösartiges Ziel zugelassen wird, falls Benutzer Zugriff benötigen (z. B. Benutzer, die Bedrohungsanalysen durchführen), klicken Sie auf **Regel hinzufügen** mit folgenden Einstellungen. Diese Regel muss vor anderen Regeln angeordnet werden, die den Zugriff auf ein Ziel ermöglichen.

     - Aktion: Zulassen
     - Kontrollkästchen „Prüfen Sie die Zugriffsversuche anhand des Netzwerkschutzes“: Deaktivieren Sie das Kontrollkästchen.
     - Ziel: Stimmt überein mit jeder/m. Fügen Sie die Zieladresse hinzu.
     - Benutzer oder Gruppen: Stimmt überein mit jeder/m. Fügen Sie die Benutzer oder Gruppen hinzu, die Zugriff auf das Ziel benötigen.
5. Wenn Sie eine Regel hinzufügen oder bearbeiten möchten, geben Sie die ACL-Regelparameter an und klicken auf **Speichern**.

6. Klicken Sie auf **Regeln festlegen**, um Ihre Änderungen auf die Zugriffssteuerungsliste (ACL) anzuwenden.

   Sie können die Seite auch verlassen und zu einem späteren Zeitpunkt zu den Entwurfsregeln zurückkehren. Wenn Sie eine Zugriffssteuerungsliste als Entwurf festlegen, werden alle anderen Administratoren mit einer Entwurfsregelliste aufgefordert, ihren veralteten Entwurf zu löschen.

Konfigurieren des Netzwerkschutzes

Sie können auf verschiedene Weise konfigurieren, wie CylanceGATEWAY Bedrohungen erkennt und auf sie reagiert. Wenn Sie die ACL -Regeln (Access Control List) so konfigurieren, dass der Zugriff auf Ziele zugelassen wird, kann CylanceGATEWAY weiterhin den Zugriff des Benutzers auf das Ziel blockieren, wenn eine potenzielle Bedrohung erkannt wird. Sie können auch steuern, welche Informationen auf dem Bildschirm „Netzwerkereignisse“ und in der Ansicht „Warnungen“ angezeigt werden können und was an die SIEM-Lösung oder den Syslog-Server gesendet wird, falls konfiguriert. Um den zusätzlichen Netzwerkschutz zu aktivieren, stellen Sie sicher, dass für jede ACL-Regel auch der Parameter „Adressen anhand Netzwerkschutz prüfen“ ausgewählt ist. Diese Einstellung ist standardmäßig aktiviert.

- Signaturerkennung: Mithilfe der Signaturerkennung lässt sich die Erkennung tiefer Netzwerkbedrohungen über Netzwerkverbindungssignaturen aktivieren. Wenn die Signaturerkennung aktiviert ist, blockiert CylanceGATEWAY automatisch Verbindungen, bei denen Bedrohungen erkannt werden, wenn die ACL-Regel mit dem Ziel übereinstimmt, und überprüft den Netzwerkschutz. Wenn die Signaturerkennung deaktiviert ist, werden Bedrohungen protokolliert, die Verbindung wird jedoch nicht blockiert. Weitere Informationen zu einer Liste von Erkennungen und ihren Aktionen finden Sie unter Anzeigen der Netzwerkaktivität. Die Signaturerkennung ist standardmäßig aktiviert.
- Schutzmaßnahmen für das Ziel: Mithilfe der Reputation des Ziels können Sie potenziell schädliche IP-Adressen und FQDNs blockieren, die einer festgelegten Risikostufe entsprechen (niedrig, mittel oder hoch). Wenn diese Option aktiviert ist, ist die standardmäßige Risikostufe hoch. CylanceGATEWAY protokolliert und blockiert automatisch Verbindungen zu Zielen, die der festgelegten Risikostufe entsprechen, wenn das Ziel der ACL-Regel entspricht, und überprüft den Netzwerkschutz. Wenn die Schutzmaßnahmen für das Ziel deaktiviert sind, werden Bedrohungen protokolliert, die Verbindung wird jedoch nicht blockiert. Weitere Informationen zu einer Liste von Erkennungen und ihren Aktionen finden Sie unter Anzeigen der Netzwerkaktivität. Die Zielreputation ist standardmäßig aktiviert.

  Risikostufen verwenden eine Kombination aus maschinellen Lernmodellen (ML) und einer IP-Reputationsdatenbank für statische IP-Adressen, um zu bestimmen, ob ein Ziel potenzielle Bedrohungen enthalten könnte.

  - ML-Modelle: Die ML-Modelle weisen Zielen, auf die Ihre Benutzer möglicherweise zugreifen, ein Konfidenzniveau zu. Anhand der ML-Modelle wird kontinuierlich untersucht, ob ein Ziel potenzielle Bedrohungen enthalten könnte.
  - IP-Reputationsdatenbanken: Die IP-Reputationsdatenbank gibt Aufschluss über die Vertrauenswürdigkeit von IP-Adressen aus offenen und kommerziellen IP-Reputations-Feeds. CylanceGATEWAY nutzt die Reputations-Feeds, um den Risikograd einer IP-Adresse zu bestimmen. CylanceGATEWAY berücksichtigt die Anzahl der Anbieter, die ein bestimmtes Ziel für gefährlich befunden haben, und die Zuverlässigkeit der Quellen, bevor eine Risikostufe zugewiesen wird (wenn beispielsweise die Mehrheit der Quellen und IP-Reputations-Engines ein Ziel als potenzielle Bedrohung einstufen), weist CylanceGATEWAY dem Ziel eine hohe Risikostufe zu. Weitere Informationen zu Risikostufen finden Sie unter Risikoschwellenwert für Zielreputation.

  CylanceGATEWAY wendet automatisch die Kategorie „Dynamisches Risiko“ und eine Unterkategorie auf Erkennungen der IP-Reputation an, die mithilfe einer Kombination aus ML-Modellen und IP-Reputationsdatenbank als potenziell schädliche Bedrohungen identifiziert wurden. Die Datenbanken ändern sich kontinuierlich, indem Zieleinträge hinzugefügt oder entfernt werden. Sie können auf dem Bildschirm „Netzwerkereignisse“ zusätzliche Metadaten und Details für Netzwerkereignisse anzeigen, die

als dynamisches Risiko eingestuft wurden. Die Kategorie „Dynamisches Risiko“ umfasst die folgenden Unterkategorien:

• Beacon • Command-and-Control • DNS-Tunneling	• Malware • Phishing • Potenziell schädlich	• Verdächtige Website • Domain Generation Algorithm (DGA)

Risikoschwellenwert für Zielreputation

Sie können festlegen, ob das CylanceGATEWAY den Netzwerkzugriff auf potenziell schädliche Ziele basierend auf dem von Ihnen festgelegten Mindestschwellenwert blockieren soll.

Element	Beschreibung
Hoch	Diese Risikokategorie weist darauf hin, dass das Ziel zu mehr als 80 % schädlich oder bösartig ist.
Mittel	Diese Risikokategorie gibt an, dass das Ziel zu 60 bis 80 % eine Cyber-Bedrohung sein könnte.
Gering	Diese Risikokategorie gibt an, dass das Ziel zu 50 bis 60 % verdächtig ist oder potenzielle Bedrohungen enthält.

Konfigurieren der Netzwerkschutzeinstellungen

Sie können die Erkennung festlegen, die Sie aktivieren und auf dem Bildschirm Netzwerkereignisse anzeigen möchten, sowie die Informationen, die an die SIEM-Lösung oder den Syslog-Server gesendet werden. Sie können CylanceGATEWAY auch so konfigurieren, dass Benutzern eine Meldung angezeigt wird, wenn CylanceGATEWAY eine Verbindung zu einem potenziell schädlichen Ziel blockiert. Informationen zu den verfügbaren Risikostufen finden Sie unter Risikoschwellenwert für Zielreputation. Wenn Sie die Einstellungen für den Netzwerkschutz konfigurieren, erzeugt CylanceGATEWAY Warnmeldungen, die in der Ansicht „Warnungen“ angezeigt werden. Weitere Informationen finden Sie unter Verwalten von Warnungen über Cylance Endpoint Security-Dienste hinweg.

Bevor Sie beginnen: Überprüfen Sie, ob für jede ACL-Regel die Option „Zugriffsversuche anhand des Netzwerkschutzes prüfen“ ausgewählt ist. Weitere Informationen über ACLs finden Sie unter Netzwerkzugriffssteuerung.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Netzwerkschutz**.
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Geben Sie die Erkennungen an, die Sie aktivieren möchten, und geben Sie an, ob Benutzer benachrichtigt werden sollen, wenn sie aufgrund von Erkennungen blockiert werden.	**a.** Klicken Sie auf die Registerkarte **Schutz**. **b.** Wenn eine Meldung angezeigt werden soll, wenn CylanceGATEWAY eine Verbindung blockiert, wählen Sie die Option **„Blockiert"-Benachrichtigungsmeldung auf Geräten anzeigen**. **c.** Geben Sie in das Feld **Nachricht** die Meldung ein, die den Benutzern angezeigt werden soll. **d.** Um die Signaturerkennung zu aktivieren, wählen Sie **Signaturerkennung aktivieren**. Wenn diese Option aktiviert ist, werden Warnungen für blockierte Signaturerkennungen generiert und in der Ansicht „Warnungen" angezeigt. Wenn diese Option deaktiviert ist, werden keine Warnungen generiert. Weitere Informationen finden Sie unter Verwalten von Warnungen über Cylance Endpoint Security-Dienste hinweg. **e.** Um die Zielreputation zu aktivieren, wählen Sie **Zielreputation aktivieren** und die minimale Risikostufe für potenziell schädliche IP-Adressen und FQDNs aus, die blockiert werden sollen. Wenn diese Option aktiviert ist, werden Warnmeldungen generiert und basierend auf der von Ihnen festgelegten Risikostufe in der Ansicht „Warnungen" angezeigt. Wenn Sie beispielsweise die Risikostufe „Mittel und höher" auswählen, werden Warnungen mit mittlerem oder hohem Risiko in der Ansicht „Warnungen" angezeigt. Wenn diese Option deaktiviert ist, werden Warnungen, die CylanceGATEWAY als hohes Risiko einstuft, standardmäßig generiert und in der Ansicht „Warnungen" angezeigt.
Legen Sie fest, welche Erkennungen auf dem Bildschirm „Netzwerkereignisse" angezeigt werden sollen und steuern Sie sie. **Hinweis:** Wenn Sie den Datenschutz für den Datenverkehr aktivieren und die Netzwerkzugriffsversuche mit der ACL- Regel übereinstimmen, werden die Netzwerkzugriffsversuche auf dem Bildschirm „Netzwerkereignisse" nicht angezeigt.	**a.** Klicken Sie auf die Registerkarte **Bericht**. **b.** Um die Signaturerkennung für zulässige Netzwerkereignisse anzuzeigen, aktivieren Sie die Option **Zulässige Signaturerkennungsereignisse anzeigen**. Standardmäßig werden automatisch blockierte Signaturerkennungen auf dem Bildschirm „Netzwerkereignisse" angezeigt. **c.** Um die Erkennung der Zielreputation für Netzwerkereignisse anzuzeigen, die zulässig sind, aktivieren Sie **Zulässige Ziel-Reputationsereignisse anzeigen** und wählen Sie die minimale Risikostufe potenziell schädlicher IP-Adressen aus, die angezeigt werden soll. Wenn diese Option deaktiviert ist, werden Signaturereignisse als normaler zulässiger Datenverkehr erfasst. **d.** Um DNS-Tunneling-Erkennung anzuzeigen, aktivieren Sie **DNS-Tunneling-Erkennung anzeigen** und wählen Sie die minimale Risikostufe potenzieller Bedrohungen basierend auf der Analyse des DNS-Datenverkehrs vom Client zum DNS-Server aus. Die Risikostufe ist standardmäßig „Mittel". **e.** Um Zero-Day-Erkennungen anzuzeigen, aktivieren Sie die Option **Zero-Day-Erkennungen anzeigen** und wählen Sie die minimale Risikostufe für neu identifizierte schädliche Ziele aus, die zuvor nicht identifiziert wurden. Die Risikostufe ist standardmäßig „Mittel".

Aufgabe	Schritte
Legen Sie fest, welche Erkennungen in der Ansicht „Warnungen“ angezeigt und an die SIEM-Lösung oder den Syslog-Server (falls konfiguriert) gesendet werden sollen, und steuern Sie diese. **Hinweis:** Wenn Sie den Datenschutz für den Datenverkehr aktivieren und die Netzwerkzugriffsversuche mit der ACL-Regel übereinstimmen, werden die Netzwerkzugriffsversuche nicht an die SIEM-Lösung oder den Syslog-Server (falls konfiguriert) gesendet.	**a.** Klicken Sie auf die Registerkarte **Freigeben**. **b.** Um zulässige oder blockierte Netzwerkereignisse und -warnungen zu senden, bei denen eine Signatur erkannt wurde, aktivieren Sie die Option **Signaturerkennungsereignisse freigeben**. Wenn diese Option aktiviert ist, werden die blockierten Signaturerkennungen standardmäßig in der Ansicht „Warnungen“ angezeigt und an die SIEM-Lösung oder den Syslog-Server gesendet. Wählen Sie optional **Zulässige Ereignisse** aus, um zulässige Ereignisse zu senden. **c.** Um Netzwerkereignisse und -warnungen mit Zielreputationserkennung zu senden, die basierend auf der von Ihnen festgelegten oder blockierten Mindestrisikostufe zulässig waren, aktivieren Sie die Option **Zielreputationsereignisse freigeben**. Wenn diese Option aktiviert ist, werden die blockierten Zielreputationsereignisse standardmäßig in der Ansicht „Warnungen“ angezeigt und an die SIEM-Lösung oder den Syslog-Server gesendet. Wählen Sie optional **Zulässige Ereignisse** aus, um zulässige Ereignisse zu senden. **d.** Um Netzwerkereignisse und -warnungen mit DNS-Tunneling-Erkennungen auf der Grundlage der von Ihnen festgelegten Mindestrisikostufe zu senden, wählen Sie **DNS-Tunneling-Erkennungen freigeben**. Die Risikostufe ist standardmäßig „Mittel“. **e.** Um Netzwerkereignisse und -warnungen mit Zero-Day-Erkennungen auf der Grundlage der von Ihnen festgelegten Mindestrisikostufe zu senden, wählen Sie **Zero-Day-Erkennungen freigeben**. Die Risikostufe ist standardmäßig „Mittel“. **f.** Um Netzwerkereignisse zu senden, die durch ACL-Regeln blockiert sind, aktivieren Sie **Gesperrte ACL-Ereignisse freigeben**. Blockierte und zulässige ACL-Ereignisse werden nicht in der Ansicht „Warnungen“ angezeigt.

4. Klicken Sie auf **Speichern**.

Durchsuchen von ACL-Regeln und Netzwerkdiensten

Sie können die ACL-Regeln und Netzwerkdienste durchsuchen, die Sie zu CylanceGATEWAY hinzugefügt haben. CylanceGATEWAY gibt vordefinierte Geltungsbereiche und Bedingungen für Ihre Suchkriterien an.

Bei einer Suche werden die Kriterien berücksichtigt, die Sie für einen Geltungsbereich und eine Bedingung im Suchfeld angeben, um die Suchergebnisse zurückzugeben. Wenn Sie beispielsweise die ACL-Regeln nach einer Regel durchsuchen, die „IT“ im Namen enthält (z. B. Geltungsbereich = Name, Bedingung = enthält und Suchkriterium = IT), werden alle Regeln zurückgegeben, die wie angegeben „IT“ im Regelnamen enthalten.

Hinweis: Sie können eine Suche nach den festgeschriebenen ACL-Regeln durchführen oder nach ACL-Regelentwürfen suchen. Eine Suche kann nicht sowohl die festgeschriebenen ACL-Regeln als auch die ACL-Regelentwürfe umfassen.

Wenn bei erweiterten Suchen mehrere Geltungsbereiche und Suchkriterien angegeben werden, verwendet die Suchmaschine einen UND-Operator zwischen den Suchkriterien. Alle Suchergebnisse enthalten alle angegebenen Kriterien. Wenn Sie z. B. Netzwerkdienste nach einem Dienst mit dem Namen „Beispiel“ und einem FQDN von beispiel.com durchsuchen (z. B. Geltungsbereich = Name, Bedingung = enthält, Suchkriterium = Beispiel und

Geltungsbereich = FQDN, Bedingung = enthält, Suchkriterium = beispiel.com), werden alle Regeln zurückgegeben, bei denen beide Kriterien erfüllt sind.

Groß- und Kleinschreibung müssen bei der Suche nicht beachtet werden. Wenn Sie also nach „Beispiel“ suchen, werden die gleichen Ergebnisse wie bei „beispiel“ angezeigt.

Verwenden des Quell-IP-Pinnings

CylanceGATEWAY ermöglicht das Abrufen dedizierter IP-Adressen, die Sie für das Quell-IP-Pinning verwenden können. Bei vielen SaaS-Anwendungen kann mit Quell-IP-Pinning nur der Zugriff auf Verbindungen von einem bestimmten Bereich vertrauenswürdiger IP-Adressen beschränkt werden. Ihr Unternehmen verwendet diese Methode möglicherweise bereits, um den Zugriff auf einen SaaS-Anwendungsmandanten auf die IP-Adresse zu beschränken, die von den mit dem Netzwerk Ihres Unternehmens verbundenen Geräten verwendet werden. Für Benutzer, die remote arbeiten, bedeutet dies, dass Sie den Zugriff zwischen Ihren Benutzern und Cloud-basierten Anwendungen mithilfe von Quell-IP-Pinning sichern können, ohne dass die Benutzer das VPN Ihres Unternehmens verwenden müssen. Dies kann den Datenverkehr in Ihrem Netzwerk reduzieren und die Verbindungen für Benutzer verbessern.

Wenn Sie Quell-IP-Pinning für CylanceGATEWAY aktiviert haben, zeigen die Netzwerkeinstellungen für Quell-IP-Pinning die IP-Adressen an, die BlackBerry nur für die Verwendung durch Ihr Unternehmen zugewiesen hat.

Um spezielle IP-Adressen zu erhalten, besuchen Sie support.blackberry.com/community und lesen Sie Artikel 96499.

Um Ihre zugewiesenen IP-Adressen anzuzeigen, klicken Sie in der Menüleiste auf **Einstellungen > Netzwerk**und wählen dann die Registerkarte **Quell-IP-Pinning** aus.

Konfigurieren der Gateway-Dienstoptionen

Sie konfigurieren Gateway-Dienstrichtlinien, um betriebssystemspezifische Optionen anzugeben, die steuern, wie Apps den Tunnel verwenden können, um festzulegen, ob Benutzer auf Ziele mit schlechter Reputation zugreifen können, und um Benutzer zur Überprüfung ihrer Identität zu veranlassen, bevor sie einen Tunnel einrichten können.

Parameter für die Gateway-Dienstrichtlinie

Wenn Sie CylanceGATEWAY auf Geräten konfigurieren, die mit einer EMM-Lösung wie BlackBerry UEM aktiviert werden, können Sie auch Optionen in Ihrer EMM-Lösung festlegen, die steuern, wie CylanceGATEWAY auf Geräten ausgeführt wird.

Element	Beschreibung
Allgemeine Informationen	
Name	Dies ist der Regelname.
Beschreibung	Dies ist eine kurze Beschreibung des Zwecks der Regel.
Agentenkonfiguration	

Element	Beschreibung
Ausführung von Gateway nur zulassen, wenn das Gerät von BlackBerry UEM oder Microsoft Intune verwaltet wird	Diese Einstellung legt fest, dass iOS-, Android- oder Chromebook-Geräte von BlackBerry UEM oder Microsoft Intune verwaltet werden müssen, bevor Benutzer CylanceGATEWAY verwenden können. Diese Funktion erfordert Folgendes: • BlackBerry UEM: Der BlackBerry UEM-Connector wird dem Cylance Endpoint Security-Mandanten hinzugefügt und Apps werden von BlackBerry UEM gesendet. • Intune: Der Microsoft Intune-Connector wird dem Cylance Endpoint Security-Mandanten hinzugefügt und Sie erstellen App-Konfigurationsrichtlinien, die die Gerätetypen und Intune-Benutzergruppen definieren, für die die Integration gilt. Weitere Informationen finden Sie Verbinden von Cylance Endpoint Security mit MDM-Lösungen, um zu überprüfen, ob Geräte verwaltet werden
Das Gateway darf nur auf mit MDM verwalteten Geräten Tunnel einrichten, auf denen es als verwaltetes VPN konfiguriert ist	Sie können festlegen, dass ein Gerät bei Mobile Device Management (MDM) für Ihr Unternehmen registriert ist, bei dem CylanceGATEWAY als VPN-Anbieter konfiguriert ist, bevor der CylanceGATEWAY-Arbeitsmodus einen Tunnel auf diesem Gerät erstellt. Diese Funktion wird von den folgenden Geräten unterstützt: • CylanceGATEWAY-Agent für macOS 2.7 oder höher • CylancePROTECT Mobile-App für iOS 2.14 oder höher
Gateway darf nur ausgeführt werden, wenn CylancePROTECT Desktop ebenfalls auf dem Gerät aktiviert ist	Diese Einstellung erfordert, dass CylancePROTECT Desktop für Benutzer über denselben Mandanten installiert und aktiviert wurde. Diese Funktion wird von den folgenden Geräten unterstützt: • Windows-Geräte mit CylanceGATEWAY für Windows • macOS-Geräte mit CylancePROTECT Desktop 3.0 oder höher und CylanceGATEWAY für macOS 2.0.17 oder höher. Wenn Sie diese Funktion für Geräte aktivieren, auf denen eine CylancePROTECT Desktop-Version vor 3.0 ausgeführt wird, funktioniert der Tunnel möglicherweise nicht wie erwartet.

Element	Beschreibung
Sicherheitsmodus	Sie können den Sicherheitsmodus für Ihre Benutzer aktivieren. Im Sicherheitsmodus blockiert CylanceGATEWAY den Zugriff von Anwendungen und Benutzern auf potenziell bösartige Ziele und erzwingt durch das Abfangen von DNS-Anforderungen eine Richtlinie für die zulässige Nutzung. Die CylanceGATEWAY-Clouddienste bewerten jede DNS-Abfrage anhand der konfigurierten ACL-Regeln und Netzwerkschutzeinstellungen (z. B. DNS-Tunneling und Zero-Day-Erkennung wie DGA, Phishing und Malware) und weisen den Agenten dann an, die Anfrage in Echtzeit zuzulassen oder zu blockieren. Wenn sie zulässig ist, wird die DNS-Anforderung normal über das Trägernetzwerk ausgeführt. Andernfalls setzt der CylanceGATEWAY-Agent die normale Reaktion außer Kraft, um den Zugriff zu verhindern. Wenn diese Option aktiviert ist, wird der Sicherheitsmodus automatisch aktiviert, wenn der Arbeitsmodus deaktiviert ist. Wenn diese Option für Windows-Geräte aktiviert ist, wird der Agent beim Starten in der Taskleiste minimiert. Durch die Aktivierung des Sicherheitsmodus wird der Benutzer nicht daran gehindert, den Agenten zu öffnen und den Arbeitsmodus zu aktivieren oder zu deaktivieren (wenn die Benutzerrichtlinie solche Vorgänge zulässt). Ereignisse im Sicherheitsmodus werden auf dem CylanceGATEWAY-Ereignisbildschirm und in der Ansicht „Warnungen“ angezeigt und an die SIEM-Lösung oder den Syslog-Server gesendet, sofern konfiguriert. **Hinweis:** Bei Aktivierung schützt der Sicherheitsmodus den gesamten DNS-Datenverkehr, der nicht den CylanceGATEWAY-Tunnel verwendet (z. B. lässt er zu, dass das Gateway nur auf MDM-verwalteten Geräten Tunnel einrichten kann, bei denen das Gateway als verwaltetes VPN, Per-App-Tunnel oder Split-Tunneling konfiguriert ist). Diese Funktion wird von den folgenden Geräten unterstützt: • CylanceGATEWAY-Agent für Windows 2.8 oder höher. • CylanceGATEWAY-Agent für macOS 2.7 oder höher. **Hinweis:** Diese Funktion wird nicht in Umgebungen unterstützt, die sicheres DNS mit DoT- (DNS-over-TLS) und DoH- (DNS-over-HTTPS) Protokollen verwenden. DNS-Abfragen, die mit DoT oder DoH gesendet wurden, können von CylanceGATEWAY nicht angezeigt werden. **Sicherheitsmodus und CylanceGATEWAY-Agent für macOS**: Auf macOS verwendet der CylanceGATEWAY-Agent eine Systemerweiterung, um den Sicherheitsmodus zu implementieren. Wenn Sie die Systemerweiterung „P7E3XMAM8G:com.blackberry.big3.gatewayfilter“ zu einer zulässigen Liste hinzufügen, kann sie automatisch ohne Benutzerinteraktion geladen werden, wenn der CylanceGATEWAY-Agent aktiviert wird. Andernfalls weisen Sie Ihre Benutzer an, die CylanceGATEWAY-Systemerweiterung zuzulassen, wenn sie während der Aktivierung dazu aufgefordert werden. Informationen zum Hinzufügen einer Systemerweiterung zu einer zulässigen Liste finden Sie in Ihrer macOS-Dokumentation. Weitere Anweisungen zur Aktivierung des CylanceGATEWAY-Agenten für den Sicherheitsmodus finden Sie im Benutzerhandbuch unter Aktivieren des Sicherheitsmodus im CylanceGATEWAY-Agenten. **Sicherheitsmodus und Drittanbieter-VPNs**: Wenn Ihre Umgebung für die Verwendung des Sicherheitsmodus und eines Drittanbieter-VPN konfiguriert ist, müssen Sie die DNS-Einstellungen des VPN überprüfen und ggf. anpassen, damit die DNS-Einstellungen nur die DNS-Abfragen für den Datenverkehr weiterleiten, der für die Verwendung des VPN-Tunnels definiert ist. Wenn Sie den Sicherheitsmodus aktivieren und die DNS-Einstellungen des VPN nicht überprüft werden, funktioniert das VPN möglicherweise nicht wie erwartet. Standardmäßig ist die Konfiguration für viele VPNs so konfiguriert, dass der gesamte DNS-Datenverkehr durch den VPN-Tunnel geleitet wird, wenn er aktiv ist.

Element	Beschreibung
Erzwingen der Einstellung „CylanceGATEWAY bei Anmeldung starten“	Diese Einstellung legt fest, ob der CylanceGATEWAY-Agent auf macOS- oder Windows-Geräten automatisch gestartet werden soll, wenn sich Benutzer anmelden. Diese Richtlinieneinstellung setzt die Einstellung „CylanceGATEWAY bei Anmeldung starten“ außer Kraft. BlackBerry empfiehlt, dass Sie diese Option in der Gateway-Dienstrichtlinie aktivieren. Diese Funktion wird von den folgenden Geräten unterstützt: • CylanceGATEWAY-Agent für macOS 2.7 oder höher • CylanceGATEWAY-Agent für Windows 2.7 oder höher
CylanceGATEWAY automatisch starten, wenn sich der Benutzer anmeldet	Mit dieser Einstellung wird der CylanceGATEWAY-Agent automatisch gestartet, wenn sich Benutzer beim Gerät anmelden, aber Benutzer können den Agenten weiterhin auch manuell beenden. Wenn Sie sowohl diese Einstellung als auch „Arbeitsmodus automatisch aktivieren“ für Windows-Geräte aktivieren, wird der Agent beim Starten in der Taskleiste minimiert. Diese Einstellung ist nur gültig, wenn die Einstellung „Start von CylanceGATEWAY bei Anmeldung erzwingen“ aktiviert ist.
Erzwingen der Einstellung „Arbeitsmodus automatisch aktivieren“	Diese Einstellung legt fest, ob der CylanceGATEWAY-Agent auf macOS- oder Windows-Geräten die automatische Aktivierung des Arbeitsmodus erzwingen soll, wenn der Agent startet. Diese Richtlinieneinstellung setzt die Einstellung „Arbeitsmodus automatisch aktivieren“ im Agent außer Kraft. Diese Funktion wird von den folgenden Geräten unterstützt: • CylanceGATEWAY-Agent für macOS 2.7 oder höher. • CylanceGATEWAY-Agent für Windows 2.7 oder höher
Arbeitsmodus automatisch aktivieren	Mit dieser Einstellung wird der Arbeitsmodus automatisch aktiviert, wenn der CylanceGATEWAY-Agent gestartet wird. Benutzer können den Arbeitsmodus nach dem Start des Agenten dennoch manuell aktivieren und deaktivieren. Wenn Sie sowohl diese Einstellung als auch „CylanceGATEWAY bei Benutzeranmeldung automatisch starten“ für Windows-Geräte aktivieren, wird der Agent beim Starten in der Taskleiste minimiert. Diese Einstellung ist nur gültig, wenn die Einstellung „Arbeitsmodus automatisch aktivieren“ aktiviert ist.
Tunnelverwendung	

Element	Beschreibung
Per-App-Tunnel	Diese Einstellung legt fest, welche Apps Daten durch den Tunnel an CylanceGATEWAY-Clouddienste senden können. Sie können Per-App-Tunnel entweder mit einer Liste zulässiger Apps oder einer Liste eingeschränkter Apps konfigurieren. Wenn Sie beispielsweise die Option „Zulässige Apps“ auswählen und Apps angeben, die den Tunnel verwenden können, und dann die Option auf „Eingeschränkte Apps“ ändern, können die aufgeführten Apps den Tunnel nicht verwenden. Mögliche Optionen: • Wählen Sie **Zulässige Apps** aus, um die Apps anzugeben, die den Tunnel verwenden. Alle anderen Apps können den Tunnel nicht verwenden. System-Apps und Windows-DNS verwenden immer den Tunnel. Wenn Sie diese Option auswählen, werden alle festgelegten ACL-Regeln oder Netzwerk-Zugriffskontrollrichtlinien angewendet. Weitere Informationen zu ACL-Regeln und Richtlinien für die Netzwerkzugriffskontrolle finden Sie unter Netzwerkzugriffssteuerung. • Wählen Sie **Gesperrte Apps** aus, um die Apps anzugeben, die den Tunnel nicht verwenden dürfen. Alle anderen Apps können den Tunnel verwenden. • Klicken Sie auf ⊕ und geben Sie den vollständigen Pfad oder einen Platzhalter in den Pfad für Desktop-Apps ein oder fügen Sie den Windows-Paketfamiliennamen (PFN) für Store-Apps hinzu. Es können maximal 200 App-Pfade oder PFNs kombiniert werden. Wenn Sie einen Platzhalter in den Pfad einfügen, beachten Sie Folgendes: • Sie können nur einen Platzhalter pro Pfad verwenden. Das unterstützte Format ist *\ (z. B. %ProgramFiles%*Folder_Name***Application_Name*.exe) • Platzhalter werden in den folgenden Fällen nicht unterstützt: • Wird anstelle von Umgebungsvariablen verwendet • Wird anstelle von Stammverzeichnissen im Pfad verwendet • Wird für Teil-Verzeichnisnamen verwendet (z. B. „C:\Win*\notepad.exe“) • Wird in Namen von ausführbaren Dateien verwendet (z. B. „C:\Windows *.exe“) Platzhalter werden auf Windows-Geräten unterstützt, auf denen CylanceGATEWAY-Agent für Windows 2.7 oder höher ausgeführt wird. Diese Funktion wird von den folgenden Geräten unterstützt: • CylanceGATEWAY für Windows 2.0.0.13 oder höher. • Benutzer von Android- oder Chromebook-Geräten, auf denen die CylancePROTECT Mobile-App ausgeführt wird.

Element	Beschreibung
Apps zwingen, den Tunnel zu verwenden	Diese Einstellung erfordert, dass alle Verbindungen ohne Loopback den Tunnel verwenden müssen. Wenn Sie diese Option auswählen und Split-Tunneling aktiviert haben, wird der Tunnel für den gesamten Datenverkehr verwendet. Wenn Sie diese Option auf Windows-Geräten auswählen und Split-Tunneling aktiviert haben, funktionieren Verbindungen, die den Tunnel nicht verwenden, möglicherweise nicht wie erwartet. Diese Funktion wird von den folgenden Geräten unterstützt: • Nicht verwaltete macOS-Geräte mit macOS 10.15 oder höher und CylanceGATEWAY für macOS 2.0.17 oder höher. • Nicht verwaltete iOS-Geräte mit iOS 14.0 oder höher und CylancePROTECT Mobile-App 2.4.0.1731 oder höher. • Windows-Geräte mit CylanceGATEWAY für Windows
Zulassen, dass Apps das lokale Netzwerk verwenden	Diese Einstellung ermöglicht, dass die Apps, die den Tunnel verwenden müssen, lokale Netzwerkziele erreichen können. Diese Funktion wird von den folgenden Geräten unterstützt: • Nicht verwaltete macOS-Geräte mit macOS 10.15 oder höher und CylanceGATEWAY für macOS 2.0.17 oder höher. • Nicht verwaltete iOS-Geräte mit iOS 14.2 oder höher und CylancePROTECT Mobile-App 2.4.0.1731 oder höher. • Windows-Geräte mit CylanceGATEWAY für Windows 2.5 oder höher. Diese Einstellung ist nur gültig, wenn „Apps müssen den Tunnel verwenden“ aktiviert ist.
Netzwerkverkehr von eingeschränkten Apps blockieren	Diese Einstellung verhindert alle Netzwerkverbindungen ohne Loopback von Apps, die den Tunnel nicht verwenden können. Wenn Sie diese Einstellung nicht aktivieren, können die gesperrten Apps die Standardnetzwerkverbindung verwenden. Diese Funktion wird auf Geräten unterstützt, auf denen der CylanceGATEWAY für Windows-Agent ausgeführt wird.
Zulassen, dass andere Windows-Benutzer den Tunnel verwenden	Mit dieser Einstellung können alle Benutzer, die dasselbe Windows-Gerät nutzen, den Tunnel verwenden. Wenn Sie diese Option aktivieren, gelten alle Per-App-Tunnelkriterien. Wenn Sie diese Option nicht aktivieren, werden Apps, die von anderen Windows-Benutzern ausgeführt werden, als gesperrte Apps behandelt.
Eingehende Verbindungen zulassen	Mit dieser Einstellung werden eingehende TCP-Verbindungen und UDP-Datenflüsse von Schnittstellen ohne Tunnel und ohne Loopback zugelassen. CylanceGATEWAY leitet eingehende Verbindungen nie durch den Tunnel. Diese Funktion wird auf Geräten unterstützt, auf denen der CylanceGATEWAY für Windows-Agent ausgeführt wird.
Neuauthentifizierung für den Tunnel	

Element	Beschreibung
Neuauthentifizierung für den Tunnel	Diese Einstellung legt fest, wie häufig Benutzer sich authentifizieren müssen, bevor sie einen Tunnel einrichten. Wenn Sie diese Funktion aktivieren, empfiehlt BlackBerry, dass Sie die Option „Erneute Verwendung der Authentifizierung zulassen“ festlegen, um den Zeitraum anzugeben, nach dem Benutzer sich erneut authentifizieren müssen. Diese Funktion wird von den folgenden Geräten unterstützt: • CylanceGATEWAY für macOS 2.5 oder höher. • CylanceGATEWAY für Windows 2.5 oder höher.
Erneute Verwendung der Authentifizierung zulassen	Bei Aktivierung gibt diese Einstellung einen Zeitraum an, nach dem Benutzer, die einen Tunnel authentifiziert und eingerichtet haben, erneut authentifiziert werden müssen. Der Zeitraum kann zwischen 5 Minuten und 365 Tagen nach der letzten Authentifizierung betragen. Wenn Sie beispielsweise den Zeitraum für die Zurücksetzung auf 10 Tage einstellen, müssen sich Benutzer 10 Tage nach ihrer ersten Authentifizierung erneut authentifizieren, bevor sie einen Tunnel einrichten können. Standardmäßig ist diese Einstellung deaktiviert. **Hinweis:** Wenn Sie die Option „Erneute Verwendung der Authentifizierung zulassen“ nicht aktivieren und keinen Zeitraum für die erneute Authentifizierung angeben, müssen sich Benutzer jedes Mal authentifizieren, wenn sie einen Tunnel einrichten. Diese Einstellung ist nur gültig, wenn „Neuauthentifizierung für den Tunnel“ aktiviert ist.
Übergangsfrist	Diese Einstellung ermöglicht es Benutzern, ohne Authentifizierung eine Verbindung zum Tunnel herzustellen, wenn die Verbindung zum Tunnel innerhalb von 2 Minuten nach dem Trennen der Verbindung hergestellt wird. Diese Option ist standardmäßig aktiviert, wenn Sie die Tunnel-Neuauthentifizierung aktivieren. Diese Einstellung ist nur gültig, wenn „Neuauthentifizierung für den Tunnel“ aktiviert ist.
Split-Tunneling	

Element	Beschreibung
Split-Tunneling	Mit dieser Einstellung kann CylanceGATEWAY für den Datenverkehr zu öffentlichen Zielen umgangen werden. Sie können CIDR-Adressen oder FQDNs für Ziele eingeben, die durch den Tunnel geleitet werden müssen. Für eine verbesserte Benutzererfahrung aktualisiert die Verwaltungskonsole regelmäßig die FQDN-zu-IP-Adressauflösung. **Hinweis:** FQDN-Adressen unterstützen keine Platzhalter. Wenn Sie Split-Tunneling aktivieren, umgehen Verbindungen zu zulässigen öffentlichen Zielen den Tunnel und die CylanceGATEWAY-Clouddienste, wenn Sie nicht angeben, dass Verbindungen mit diesem Ziel den Tunnel verwenden müssen. Wenn Sie Split-Tunneling aktivieren und Split-DNS nicht aktivieren, werden alle DNS-Abfragen anhand der konfigurierten ACL-Regeln ausgewertet und Netzwerkzugriffskontrollen werden angewendet, bevor der Datenverkehr an das öffentliche Ziel weitergeleitet wird. Sie können CIDR-Adressen oder FQDNs für Ziele eingeben, die durch den Tunnel geleitet werden müssen. Wenn Sie Quell-IP-Pinning verwenden, müssen alle für Quell-IP-Pinning konfigurierten Ziele den Tunnel verwenden. Wenn Sie Änderungen an Tunneling-Einstellungen oder eingehenden Verbindungen vornehmen, müssen Benutzer den Arbeitsmodus im CylanceGATEWAY-Agenten deaktivieren und aktivieren, der auf Windows- und macOS-Geräten oder in der CylancePROTECT Mobile-App auf iOS-, Android und 64-Bit-Chromebook-Geräten installiert ist, damit die Änderungen wirksam werden.
Split-DNS	Wenn diese Einstellung aktiviert ist, können DNS-Suchen für die Domänen, die in der Konfiguration Privates Netzwerk > DNS > Forward-Lookup-Zone aufgeführt sind, über den Tunnel durchgeführt werden, in dem Netzwerkzugriffskontrollen angewendet werden. Alle anderen DNS-Suchen werden über das lokale DNS durchgeführt. Wenn Sie den Sicherheitsmodus aktiviert haben, wird der DNS-Datenverkehr, der den Gateway-Tunnel nicht verwendet, durch den Sicherheitsmodus geschützt. Split-DNS ist standardmäßig deaktiviert. Android- und 64-Bit-Chromebook-Geräte unterstützen kein Split-DNS-Tunneling und verwenden den Tunnel, auf den Zugriffskontrollen angewendet werden. Diese Einstellung ist nur gültig, wenn „Split-Tunneling“ aktiviert ist.

Konfigurieren der Gateway-Dienstoptionen

1. Klicken Sie in der Menüleiste auf **Richtlinien > Benutzerrichtlinie**.
2. Klicken Sie auf die Registerkarte **Gateway-Dienst**.
3. Klicken Sie auf **Richtlinie hinzufügen**.
4. Geben Sie die Richtlinienparameter für den Gateway-Dienst an.
5. Klicken Sie auf **Hinzufügen**.
6. Wenn Sie Änderungen an Tunneling-Einstellungen oder eingehenden Verbindungen vorgenommen haben, müssen Benutzer den Arbeitsmodus im CylanceGATEWAY-Agenten deaktivieren und aktivieren, der auf Windows- und macOS-Geräten installiert ist, oder in der CylancePROTECT Mobile-App auf iOS-, Android- und Chromebook-Geräten, damit die Änderungen wirksam werden.

Wenn Sie fertig sind:

- Weisen Sie die Richtlinie Benutzern und Gruppen zu.

- Gegebenenfalls weisen Sie den Richtlinien einen Rang zu.

Festlegen der Verwendung des CylanceGATEWAY-Tunnels durch mit einer EMM-Lösung aktivierte Geräte

CylanceGATEWAY ist eine Cloud-native Lösung, die Zero-Trust-Netzwerkzugriff (Zero Trust Network Access, ZTNA) gestützt auf künstliche Intelligenz (KI) bietet. Wenn CylanceGATEWAY auf einem Gerät aktiviert ist, erkennt das Gerät CylanceGATEWAY als VPN-Anbieter, der ein Zero-Trust-Netzwerkzugriffsprofil erstellt. Wenn Sie Geräte mit BlackBerry UEM oder einer anderen EMM-Lösung aktiviert haben, können sich die VPN-Optionen, die Sie in Ihrer EMM-Lösung festgelegt haben, auf die Funktionsweise von CylanceGATEWAY auf dem Gerät auswirken.

Für iOS-Geräte können Sie Ihr BlackBerry UEM oder eine andere EMM-Lösung verwenden, um Per-App-VPN einzurichten und festzulegen, welche Apps Daten durch den CylanceGATEWAY-Tunnel senden. Geräte müssen aktiviert werden, um VPN- und App-Verwaltung zu ermöglichen. Weitere Informationen finden Sie unter:

- Festlegen, welche Apps CylanceGATEWAY auf iOS-Geräten verwenden sollen
- Festlegen, welche Apps CylanceGATEWAY auf iOS-Geräten in einer Microsoft Intune-Umgebung verwenden sollen

Für Android-Geräte können Sie BlackBerry UEM oder eine andere EMM-Lösung verwenden, um die durchgängige Aktivierung von CylanceGATEWAY zu erzwingen und zu verhindern, dass Benutzer die VPN-Konfiguration im Arbeitsprofil ändern. Weitere Informationen finden Sie unter:

- Festlegen von CylanceGATEWAY-Optionen auf Android Enterprise-Geräten
- Festlegen der CylanceGATEWAY-Optionen auf Android Enterprise-Geräten in Ihrer Microsoft Intune-Umgebung

Festlegen, welche Apps CylanceGATEWAY auf iOS-Geräten verwenden sollen

Wenn Ihr Unternehmen Geräte mit einer EMM-Lösung verwaltet, die die Per-App-VPN-Konfiguration unterstützt, können Sie iOS-Geräte so konfigurieren, dass CylanceGATEWAY als VPN-Anbieter erkannt wird, und mithilfe einer Per-App-VPN-Konfiguration festlegen, welche Apps Daten über den CylanceGATEWAY-Tunnel senden.

Zum Einrichten von Per-App-Tunneloptionen müssen Sie über Berechtigungen für die VPN- und App-Verwaltung auf iOS-Geräten verfügen, die mit Ihrer EMM-Lösung aktiviert werden. Um festzulegen, welche Apps den CylanceGATEWAY-Tunnel in BlackBerry UEM verwenden, führen Sie die folgenden Schritte aus:

1. Fügen Sie in der UEM-Verwaltungskonsole die Apps hinzu, die Daten über CylanceGATEWAY an UEM senden sollen, und weisen Sie sie Benutzern zu.

   Nur Apps, die Benutzern zugewiesen sind, verwenden den CylanceGATEWAY-Tunnel. Der Standardbrowser und die CylancePROTECT Mobile-App dürfen nicht Benutzern zugewiesen werden, da das Gerät ansonsten keinen Tunnel mit CylanceGATEWAY einrichten kann.

   Bei Geräten mit den Aktivierungsarten „Privatsphäre des Benutzers“ und „Benutzerdatenschutz - Benutzerregistrierung“ verwenden nur zugewiesene interne Apps und Apps, die über das Apple Volume Purchase Program lizenziert sind, den Tunnel.
2. Erstellen Sie ein Aktivierungsprofil, das eine der folgenden Aktivierungsarten zuweist:
   - MDM-Steuerelemente
   - Benutzerdatenschutz - Benutzerregistrierung
   - Privatsphäre des Benutzers mit aktivierter VPN- und App-Verwaltung
3. Erstellen Sie ein VPN-Profil und nehmen Sie die folgenden Einstellungen vor:

Einstellung	Beschreibung
Verbindungstyp	Benutzerdefiniert

Einstellung	Beschreibung
VPN-Bundle-ID	com.blackberry.protect
Server	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest. Der Wert muss 127.0.0.1 lauten.
Authentifizierungstyp	Kennwort
Kennwort	Dieses Feld leer lassen
Per App VPN aktivieren	Ausgewählt
Domäneneinstellungen	Geben Sie die Domänen an, die eine Verbindung über den CylanceGATEWAY-Tunnel herstellen können. Wenn Sie eine Domäne angeben, verwenden zugewiesene Apps den Tunnel nur für Verbindungen zur angegebenen Domäne. Sie können Domänen für Safari, Kalender, Kontakte, Mail und in der Datei apple-app-site-association aufgelistete Domänen angeben. Sie können auch Domänen angeben, die den Tunnel überhaupt nicht verwenden. Wenn Sie bei Geräten mit den Aktivierungsarten „Privatsphäre des Benutzers“ und „Benutzerdatenschutz - Benutzerregistrierung“ eine Domäne angeben, die nicht der im Feld **Server** angegebenen Root-Domäne untergeordnet ist, ignoriert das Gerät das gesamte VPN-Profil und nicht nur die ungültige Domäne.
Zulassen, dass Apps automatisch eine Verbindung herstellen	Wählen Sie diese Option aus, um festzulegen, dass die App die Verbindung automatisch starten kann. **Hinweis:** Verbindungen über den CylanceGATEWAY-Tunnel können nur gestartet werden, wenn CylanceGATEWAY in der CylancePROTECT Mobile-App auf dem Gerät aktiviert ist.
Datenverkehrs-Tunneling	IP-Schicht

4. Weisen Sie Benutzern Profile zu und bitten Sie die Benutzer, Geräte zu aktivieren.

Festlegen, welche Apps CylanceGATEWAY auf iOS-Geräten in einer Microsoft Intune-Umgebung verwenden sollen

Sie können iOS-Geräte so konfigurieren, dass CylanceGATEWAY als VPN-Anbieter erkannt wird, und Per-App-VPN konfigurieren, um festzulegen, welche Apps Daten durch den CylanceGATEWAY-Tunnel senden. Unter Microsoft Intune können Sie Einstellungen vornehmen, die Auswirkungen auf CylanceGATEWAY haben.

Zum Einrichten von Per-App-Tunneloptionen müssen Sie über Berechtigungen für die VPN- und App-Verwaltung auf iOS-Geräten verfügen, die mit Intune aktiviert werden. Um festzulegen, welche Apps den CylanceGATEWAY-Tunnel in Intune verwenden, führen Sie die folgenden Schritte aus:

1. Fügen Sie im Admin Center von Microsoft Intune die Apps hinzu, die Sie über CylanceGATEWAY an Intune senden möchten, und weisen Sie sie Benutzern zu.

   Nur Apps, die Benutzern zugewiesen sind, verwenden den CylanceGATEWAY-Tunnel. Der Standardbrowser und die CylancePROTECT Mobile-App dürfen nicht Benutzern zugewiesen werden, da das Gerät ansonsten keinen Tunnel mit CylanceGATEWAY einrichten kann.
2. Erstellen Sie ein VPN-Profil und nehmen Sie die folgenden Einstellungen vor: Weitere Informationen zu den iOS- und iPadOS-Einstellungen finden Sie unter Hinzufügen von VPN-Einstellungen auf iOS- und iPadOS-Geräten.

Einstellung	Beschreibung
Verbindungstyp	Benutzerdefiniertes VPN
VPN-Serveradresse	Der Wert muss 127.0.0.1 lauten. Dieser Wert wird von CylanceGATEWAY nicht verwendet.
Authentifizierungsmethode	Benutzername und Kennwort
Split-Tunneling	Deaktivieren
VPN-ID	Bei iOS-Geräten geben Sie com.blackberry.protect ein Bei macOS-Geräten geben Sie com.blackberry.big ein
	• Schlüssel: *key* • Wert: *value* Microsoft Intune erfordert ein benutzerdefiniertes Attribut. CylanceGATEWAY verwendet diese Einstellung nicht. Sie können ein beliebiges Attribut eingeben.
Automatisches VPN	Per-App-VPN
Anbietertyp	Pakettunnel
Safari-URLs	Geben Sie die Domänen an, die eine Verbindung über den CylanceGATEWAY-Tunnel herstellen können. Intune unterstützt keine Platzhalter in Domänen, sie sind impliziert. Wenn Sie beispielsweise „org“ eingeben, bedeutet das „*.org“. **Hinweis:** Verbindungen über den CylanceGATEWAY-Tunnel können nur gestartet werden, wenn CylanceGATEWAY in der CylancePROTECT Mobile-App auf dem Gerät aktiviert ist. Wenn Sie blackberry.com als verwaltetes Safari-VPN angeben, werden neu aktivierte CylancePROTECT Mobile-Apps an der Aktivierung gehindert.

3. Falls erforderlich, lassen Sie Benutzer die CylancePROTECT Mobile-App aktivieren.

Festlegen von CylanceGATEWAY-Optionen auf Android Enterprise-Geräten

Für Android-Geräte können Sie festlegen, welche Apps Daten über den CylanceGATEWAY-Tunnel senden, indem Sie die CylanceGATEWAY-Dienstrichtlinie verwenden. Wenn Ihr Unternehmen Android Enterprise-Geräte mit einer EMM-Lösung wie BlackBerry UEM verwaltet, können Sie Einstellungen in Ihrem EMM-Anbieter konfigurieren, die Auswirkungen auf CylanceGATEWAY haben.

Sie können die IT-Richtlinie in BlackBerry UEM verwenden, um anzugeben, ob CylanceGATEWAY immer auf Geräten aktiviert ist und ob Benutzer VPN-Konfigurationen im Arbeitsprofil auf dem Gerät ändern können. Weitere Informationen zu den UEM-IT-Richtlinienregeln sind in der UEM-IT-Richtlinienreferenz zu finden.

1. Erstellen oder bearbeiten Sie in der UEM-Verwaltungskonsole eine IT-Richtlinie.
2. Führen Sie eine der folgenden Aktionen aus:

a) Um die durchgängige Aktivierung von CylanceGATEWAY zu erzwingen, legen Sie die folgenden IT-Richtlinienregeln für das Android-Arbeitsprofil fest.

IT-Richtlinienregel	Beschreibung
VPN-Verbindung dauerhaft erzwingen	Ausgewählt
Verwendung von BlackBerry Secure Connect Plus für eine VPN-Verbindung	Nicht ausgewählt
Paket-ID VPN-App	com.blackberry.protect
Verwendung von VPN für geschäftliche Anwendungen erzwingen	Nicht ausgewählt. Wenn diese Option ausgewählt ist, kann die CylancePROTECT Mobile-App nicht auf dem Gerät aktiviert werden.
Von VPN ausgenommene geschäftliche Anwendungen	Wenn die Regel „Verwendung von VPN für geschäftliche Anwendungen erzwingen“ ausgewählt ist, • müssen Sie `com.android.chrome` eingeben, damit der Chrome-Browser auf das Netzwerk zugreifen kann, und die CylancePROTECT Mobile-App auf dem Gerät aktivieren, bevor die Verbindung zum VPN hergestellt wird. Diese Regel gilt nur für Geräte mit Android 10.0.0 und höher. • Wenn Sie `com.android.protect` eingeben, kann die CylancePROTECT Mobile-App nur dann ohne VPN auf das Netzwerk zugreifen, wenn keine Verbindung zum VPN besteht.

b) Damit Geräte Daten durch den CylanceGATEWAY-Tunnel senden können, wenn die Option **VPN-Verbindung dauerhaft erzwingen** nicht ausgewählt ist, wählen Sie **Benutzerkonfiguriertes VPN im geschäftlichen Bereich zulassen** aus.

Wenn weder **VPN-Verbindung dauerhaft erzwingen** noch **Benutzerkonfiguriertes VPN im geschäftlichen Bereich zulassen** ausgewählt ist, lässt es das Gerät nicht zu, dass geschäftliche Apps Daten durch den Tunnel senden.

3. Weisen Sie die IT-Richtlinie Benutzern zu.

Festlegen von CylanceGATEWAY-Optionen auf Chromebook-Geräten

Für 64-Bit-Chromebook-Geräte können Sie festlegen, welche Apps Daten über den CylanceGATEWAY-Tunnel senden, indem Sie die CylanceGATEWAY-Dienstrichtlinie verwenden. Wenn Ihr Unternehmen Chrome OS Enterprise-Geräte über eine Google-Domäne verwaltet, können Sie erzwingen, dass CylanceGATEWAY immer aktiviert ist, und verhindern, dass Benutzer die VPN-Konfiguration in der CylancePROTECT Mobile-App ändern. Anweisungen hierzu finden Sie auf der Seite https://support.google.com/ unter „Virtuelle private Netzwerke einrichten (Android-VPN-App)“. Sie können die Verwaltung von Chromebook Enterprise-Geräten auch auf Ihren EMM-Anbieter erweitern, z. B. BlackBerry UEM. Weitere Informationen finden Sie unter Erweitern der Verwaltung von Chrome OS-Geräten auf BlackBerry UEM.

Festlegen der CylanceGATEWAY-Optionen auf Android Enterprise-Geräten in Ihrer Microsoft Intune-Umgebung

Bei Android-Geräten können Sie festlegen, welche Apps Daten über den CylanceGATEWAY-Tunnel senden, indem Sie die Gateway-Richtlinie verwenden. Unter Microsoft Intune können Sie Einstellungen vornehmen, die Auswirkungen auf CylanceGATEWAY haben.

Über die Konfigurationsrichtlinie können Sie angeben, ob CylanceGATEWAY immer auf Geräten aktiviert ist und ob Benutzer VPN-Konfigurationen im Geräteprofil ändern können. Weitere Informationen zu den Einstellungen des Konfigurationsprofils finden Sie unter Android Enterprise-Geräteeinstellungen zur Konfiguration von VPN.

1. Erstellen Sie im Admin Center von Microsoft Intune ein Konfigurationsprofil. Nehmen Sie die folgenden Einstellungen vor:
   - Plattform: Android Enterprise
   - Profiltyp: Geräteeinschränkungen
2. Legen Sie die folgenden Regeln für das Konfigurationsprofil fest.

Einstellung	Beschreibung
Always-on-VPN	Aktivieren
VPN-Client	Benutzerdefiniert
Paket-ID	com.blackberry.protect
Sperrmodus	Nicht konfiguriert. Wenn diese Option ausgewählt ist, wird die CylancePROTECT Mobile-App möglicherweise nicht aktiviert.

3. Weisen Sie die Konfigurationsrichtlinie Benutzern zu.
4. Weisen Sie die CylancePROTECT Mobile-App Benutzern zu.

Verbinden von Cylance Endpoint Security mit MDM-Lösungen, um zu überprüfen, ob Geräte verwaltet werden

Sie können Cylance Endpoint Security mit BlackBerry UEM oder Microsoft Intune verbinden, damit Cylance Endpoint Security überprüfen kann, ob iOS- und Android-Geräte verwaltet werden.

Nachdem Sie die Verbindung zu UEM hergestellt haben, können Sie die iOS- und Android-Geräte, Benutzer und Gruppen konfigurieren, für die die Integration gilt. Bei UEM stellen Sie sicher, dass Benutzer mit einer unterstützten Aktivierungsart aktiviert sind und verwalten die Verteilung der CylancePROTECT Mobile-App mithilfe der in der UEM-Verwaltungskonsole verfügbaren Benutzer- und Gruppenverwaltungsfunktionen.

Beachten Sie, dass alle von BlackBerry UEM verwalteten Geräte, die diese Funktion verwenden sollen, über die App CylancePROTECT Mobile verfügen müssen, die von der BlackBerry UEM-Instanz bereitgestellt wird.

Wenn Sie bei Intune-Integrationen eine Verbindung zwischen Cylance Endpoint Security und Intune herstellen, erstellen Sie App-Konfigurationsrichtlinien, die die Gerätetypen und Intune-Benutzergruppen definieren, für die die Integration gilt. Beachten Sie, dass alle von Intune verwalteten Geräte, die diese Funktion verwenden sollen, in einer App-Konfigurationsrichtlinie auf der Cylance-Konsole unter Assets > Benutzergruppen enthalten sein müssen.

Auf der Cylance-Konsole erstellen und weisen Sie die Gateway-Dienstrichtlinie zu, die die Ausführung des Gateways nur dann zulässt, wenn das Gerät von BlackBerry UEM oder Intune verwaltet wird. Wenn der Benutzer

versucht, auf ein Netzwerkziel auf einem MDM-verwalteten Gerät zuzugreifen, wird der Netzwerkdatenverkehr durch den sicheren Tunnel gesendet, sofern das Ziel zulässig ist.

Führen Sie die folgenden Aktionen aus, um Cylance Endpoint Security mit BlackBerry UEM zu verbinden:

Schritt	Aktion
1	Überprüfen Sie die Voraussetzungen.
2	Verknüpfen Sie sich mit Ihrem Unternehmensverzeichnis. • Unter Cylance Endpoint Security, siehe Verknüpfung mit Ihrem Unternehmensverzeichnis. • Unter BlackBerry UEM, siehe Herstellen einer Verbindung zu Unternehmensverzeichnissen.
3	Installieren und konfigurieren Sie den BlackBerry Connectivity Node. • Unter Cylance Endpoint Security, siehe Installieren oder Aktualisieren des BlackBerry Connectivity Node. • Unter BlackBerry UEM, siehe Installieren einer BlackBerry Connectivity Node-Instanz.
4	Hinzufügen eines BlackBerry UEM-Connectors.
5	Mit BlackBerry UEM die CylancePROTECT Mobile-App auf Geräten installieren.

Führen Sie die folgenden Aktionen aus, um Cylance Endpoint Security mit Intune zu verbinden:

Schritt	Aktion
1	Überprüfen Sie die Voraussetzungen.
2	Cylance Endpoint Security mit Intune verbinden.

Voraussetzungen: Überprüfen, ob Geräte mit MDM verwaltet werden

- BlackBerry UEM
  - BlackBerry UEM Cloud oder die lokale UEM-Version 12.15 oder höher werden unterstützt.
  - Stellen Sie sicher, dass Sie über eine gültige BlackBerry UEM-SRP-ID und einen Authentifizierungsschlüssel für Ihre BlackBerry UEM Cloud- und BlackBerry UEM-Instanzen verfügen. Sie können die SRP-IDs und Authentifizierungsschlüssel für Ihre UEM-Instanzen in *my*Account unter „Organisation > Dienste > UEM“ anzeigen.
  - Der Cylance Endpoint Security-Mandant und die UEM-Domäne Ihres Unternehmens müssen dieselbe Unternehmens-ID aufweisen.
  - Bei lokalen BlackBerry UEM-Umgebungen müssen Sie Verbindungen von BlackBerry UEM-Connector zulassen. Wenn Sie keine Verbindungen über den BlackBerry UEM-Connector zulassen, wird beim Versuch,

Ihre Mandanteninformationen zu speichern, die Fehlermeldung „Die UEM-Verbindungsanfrage ist ungültig“ angezeigt und Sie können die Informationen nicht speichern. Anweisungen zur Aktivierung des BlackBerry UEM-Connectors finden Sie unter support.blackberry.com/community in Artikel 97480. Standardmäßig ist diese Option in BlackBerry UEM Cloud-Umgebungen aktiviert.
  - Die Benutzerkonten müssen die gleichen Active Directory- oder Entra ID-Konten auf der Cylance-Konsole verwenden.
  - Cylance Endpoint Security unterstützt die Verbindung zu einer UEM-Domäne.
  - Sie müssen Mit BlackBerry UEM die CylancePROTECT Mobile-App auf Geräten installieren. Die App muss von UEM aus verteilt werden, da sie App-Konfigurationen erfordert, die nicht vorhanden sind, wenn Benutzer die App aus dem App Store oder aus Google Play herunterladen und installieren.
  - Die Voraussetzungen für iOS -Geräte finden Sie unter Voraussetzungen: Überprüfen, ob iOS-Geräte von UEM verwaltet werden.
  - Die Voraussetzungen für Android-Geräte finden Sie unter Voraussetzungen: Überprüfen, ob Android-Geräte von UEM verwaltet werden
- Microsoft Intune
  - Das Cylance Endpoint Security-Administratorkonto, mit dem Sie die Verbindung zu Intune herstellen, muss über eine Intune-Lizenz verfügen.
  - Cylance Endpoint Security unterstützt die Verbindung zu einer Intune-Instanz.
  - Beachten Sie, dass alle Intune-verwalteten Geräte, die diese Funktion verwenden sollen, in einer App-Konfigurationsrichtlinie auf der Cylance-Konsole enthalten sein müssen. Weitere Informationen finden Sie unter Cylance Endpoint Security mit Intune verbinden.

Voraussetzungen: Überprüfen, ob iOS-Geräte von UEM verwaltet werden

Die iOS-Geräte müssen mit einer der folgenden Aktivierungsarten aktiviert werden*:

- MDM-Steuerelemente
- Privatsphäre des Benutzers
- Privatsphäre des Benutzers – Benutzerregistrierung

Wenn Ihre Benutzer mit der Aktivierungsart „Privatsphäre des Benutzers“ aktiviert sind, führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Mit Cylance Endpoint Security das Per-App-VPN verwalten	1. Deaktivieren Sie in der Aktivierungsart „Privatsphäre des Benutzers“ das Kontrollkästchen **VPN-Verwaltung zulassen** und aktivieren Sie das Kontrollkästchen **App-Verwaltung zulassen**. 2. In der Cylance Endpoint Security-Konsole konfigurieren Sie die Gateway-Dienstoptionen.
Mit UEM das Per-App-VPN verwalten	1. Aktivieren Sie in der Aktivierungsart „Privatsphäre des Benutzers“ die Kontrollkästchen **VPN-Verwaltung zulassen** und **App-Verwaltung zulassen**. 2. Erstellen Sie ein benutzerdefiniertes VPN-Profil. Geben Sie im Feld **VPN-Bundle-ID** die Bundle-ID CylancePROTECT Mobile ein, `com.blackberry.protect`. 3. In der Cylance Endpoint Security-Konsole konfigurieren Sie die Gateway-Dienstoptionen.

*Wenn Sie ein Gerät in der UEM-Instanz deaktivieren möchten, verwenden Sie den Befehl „Nur geschäftliche Daten löschen“, um geschäftliche Daten (z. B. die IT-Richtlinie, Profile, Apps und Zertifikate) auf dem Gerät zu löschen. Wenn Sie den Befehl „Gerät entfernen“ auswählen, wird das Gerät aus Ihrer UEM-Instanz entfernt, aber

Daten und Profile werden nicht entfernt und das Gerät empfängt möglicherweise weiterhin E-Mails und andere geschäftliche Daten. BlackBerry empfiehlt, den Befehl „Gerät entfernen“ nur dann zu verwenden, wenn ein Gerät unwiederbringlich verloren gegangen ist oder beschädigt wurde und nicht zu erwarten ist, dass es den Server erneut kontaktiert. Weitere Informationen zu Befehlen, die Sie an Geräte senden können, finden Sie unter Befehle für iOS-Geräte in der BlackBerry UEM-Dokumentation.

Voraussetzungen: Überprüfen, ob Android-Geräte von UEM verwaltet werden

Android-Geräte müssen mit einer der folgenden Aktivierungsarten aktiviert werden:

- Geschäftlich und persönlich – Privatsphäre des Benutzers (Android Enterprise mit geschäftlichem Profil)
- Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät)
- Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil)
- Nur geschäftlicher Bereich (Samsung Knox)
- Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)
- Geschäftlich und persönlich – Privatsphäre des Benutzers (Samsung Knox)

Hinzufügen eines BlackBerry UEM-Connectors

Standardmäßig werden auf der Seite „Connector“ Name, Verbindungstyp und Verbindungsstatus für den BlackBerry UEM-Connector angezeigt, der derzeit in Ihrer Umgebung verwendet wird. Ihr Cylance Endpoint Security-Mandant unterstützt eine Verbindung zu einer UEM-Domäne.

Bevor Sie beginnen: Überprüfen Sie die Voraussetzungen für BlackBerry UEM-Connector.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Connectors**.
2. Klicken Sie auf **Connector hinzufügen** und wählen Sie **BlackBerry UEM** aus der Dropdown-Liste aus.
3. Geben Sie auf dem Bildschirm **Mandanteninformationen** die SRP-ID des BlackBerry UEM-Mandanten und den Authentifizierungsschlüssel ein.
4. Klicken Sie auf **Speichern**.

Mit BlackBerry UEM die CylancePROTECT Mobile-App auf Geräten installieren

Über UEM können Sie die CylancePROTECT Mobile-App auf Geräten installieren. Die App muss von UEM aus verteilt werden, da sie App-Konfigurationen erfordert, die nicht vorhanden sind, wenn Benutzer die App von der BlackBerry-Website, aus dem App Store oder von Google Play herunterladen und installieren.

Hinweis:

Beachten Sie die folgenden Funktionseinschränkungen, wenn Sie UEM zum Installieren der CylancePROTECT Mobile-App auf Geräten verwenden:

- Bei Geräten mit den Android Enterprise-Aktivierungsarten „Privatsphäre des Benutzers“ oder „Vollständige Kontrolle“ wird das Scannen von SMS-Nachrichten nicht unterstützt.
- Bei Geräten mit Android Enterprise-Aktivierungsarten wird die Erkennung der Bildschirmsperre nicht unterstützt.

Bevor Sie beginnen: Lesen Sie Voraussetzungen: Überprüfen, ob Geräte mit MDM verwaltet werden.

1. Befolgen Sie die Anweisungen in der UEM-Dokumentation für Administratoren, um die CylancePROTECT Mobile-App zur App-Liste hinzuzufügen:
   - Hinzufügen einer iOS-App zur App-Liste
   - Hinzufügen einer Android-App zu einer App-Liste

   Legen Sie die folgenden App-Konfigurationseinstellungen fest:

OS	Konfigurationseinstellungen für die App
iOS	• Name der App-Konfiguration: *name* • Schlüssel: uemperimeterid • Wert: %perimeterid%
Android	Name: *name* Die folgenden Einstellungen sind bereits ausgefüllt: • Benutzer-ID: userid • UEM-Perimeter-ID: %perimeterid%

2. Zuweisen der CylancePROTECT-App zu Benutzern oder Gruppen.
3. Verfügbarkeit der CylancePROTECT-App als erforderlich festlegen.

Wenn Sie fertig sind:

- Teilen Sie den Benutzer mit, dass sie die CylancePROTECT Mobile-App mithilfe der Informationen aktivieren müssen, die sie in ihrer Aktivierungs-E-Mail erhalten haben. Cylance Endpoint Security sendet die Aktivierungs-E-Mail nachdem Sie eine Registrierungsrichtlinie zugewiesen haben.
- Befolgen Sie die Anweisungen für Verbinden von Cylance Endpoint Security mit MDM-Lösungen, um zu überprüfen, ob Geräte verwaltet werden.

Cylance Endpoint Security mit Intune verbinden

Bevor Sie beginnen:

Das Cylance Endpoint Security-Administratorkonto, mit dem Sie die Verbindung zu Intune herstellen, muss über eine Intune-Lizenz verfügen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Connectors**.
2. Klicken Sie auf **Connector hinzufügen** und wählen Sie **Microsoft Intune** aus der Dropdown-Liste aus.
3. Geben Sie Ihre Entra-Mandanten-ID ein. Klicken Sie auf **Weiter**.
4. Geben Sie Ihre Administratorzugangsdaten für Entra an.
5. Aktivieren Sie auf dem Bildschirm **App-Konfigurationsrichtlinien** die Betriebssystemplattformen, für die die Intune-Integration gelten soll, und führen Sie die folgenden Schritte für die jeweilige Plattform aus. Beachten Sie, dass alle Intune-verwalteten Geräte, die diese Funktion verwenden sollen, in einer App-Konfigurationsrichtlinie enthalten sein müssen. Wenn Sie die App-Konfigurationsrichtlinien später erstellen möchten, klicken Sie auf **Abbrechen**.
   a) Optional können Sie den Namen der Richtlinie ändern. Ändern Sie die Ziel-App nicht.
   b) Wenn Sie möchten, dass die Richtlinie für alle Gruppen der Intune-Instanz gilt, aktivieren Sie **Alle Gruppen**.
   c) Wenn Sie möchten, dass die Richtlinie für bestimmte Gruppen der Intune-Instanz gilt, klicken Sie auf ⊕. Suchen Sie nach Gruppen, wählen Sie sie aus und klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern**. Wenn Sie eine App-Konfigurationsrichtlinie für Android hinzugefügt haben, befolgen Sie die angezeigten Aufforderungen zur Administratorzustimmung.

Die von Ihnen erstellten App-Konfigurationsrichtlinien sind im Intune Admin Center sichtbar.

Wenn Sie fertig sind:

- Bitten Sie den Intune-Administrator Ihres Unternehmens, den MTD-Connector für CylancePROTECT Mobile im Intune Admin Center zu bearbeiten und die folgenden Optionen zu aktivieren. Zur Genehmigung des Connectors führen Sie die folgenden Schritte aus:

1. Melden Sie sich beim Intune Admin Center an.
2. Klicken Sie auf **Mandantenverwaltung > Connector und Token**.
3. Klicken Sie im Abschnitt **Plattformübergreifend** auf **Schutz vor mobilen Bedrohungen**.
4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie im Dropdown-Menü **Connector für den Schutz vor mobilen Bedrohungen auswählen** die Option **CylancePROTECT Mobile** aus.
6. Klicken Sie auf **Erstellen**.

- Wenn Sie App-Konfigurationsrichtlinien zu einem späteren Zeitpunkt hinzufügen möchten oder zusätzliche Richtlinien hinzufügen möchten, klicken Sie unter **Einstellungen > Connectors** auf **App-Konfiguration generieren** für die Intune-Verbindung.
- Wenn Sie auch Cylance Endpoint Security mit Intune verbinden möchten, um die Risikostufen von Geräten zu verwalten, siehe Integration von Cylance Endpoint Security mit Microsoft Intune, um auf mobile Bedrohungen zu reagieren.

Installieren des CylanceGATEWAY-Agenten

Der CylanceGATEWAY-Agent schützt die Windows 10-, Windows 11- und macOS-Geräte der Benutzer, indem Sie Verbindungen zu Internetzielen blockieren können, mit denen die Geräte nicht kommunizieren sollen, selbst wenn das Gerät nicht mit Ihrem Netzwerk verbunden ist. BlackBerry pflegt eine ständig wachsende Liste unsicherer Internetziele, zu denen die Verbindungsaufnahme der Endpunkte blockiert werden kann. Wenn Ihr Unternehmen auch Benutzer daran hindern möchte, bestimmte Websites zu besuchen, die nicht Ihren Standards für die zulässige Nutzung entsprechen, können Sie Richtlinien erstellen, um zusätzliche Ziele festzulegen, auf die kein Benutzer zugreifen kann bzw. bestimmte Benutzer oder Gruppen nicht zugreifen können.

Der CylanceGATEWAY-Agent ist auf Benutzergeräten installiert, damit Benutzer sicher auf Netzwerkressourcen zugreifen können und ihr Gerät vor verdächtigen und potenziell schädlichen Netzwerkaktivitäten geschützt ist. Wenn der CylanceGATEWAY-Agent installiert und der Arbeitsmodus aktiviert ist, stellt CylanceGATEWAY sichere Verbindungen zwischen dem Gerät des Benutzers und dem Netzwerk Ihres Unternehmens sowie dem öffentlichen Internet her, analysiert Ihre Netzwerkaktivität und wendet die von Ihnen verwalteten Netzwerkzugriffsrichtlinien an. Wenn Sie den Sicherheitsmodus für macOS- und Windows-Geräte aktivieren, erweitert CylanceGATEWAY die Mandanten-ACL-Regeln und den Endpunktschutz für Geräte, wenn der Arbeitsmodus nicht aktiviert ist, um sicherzustellen, dass Geräte immer vor Netzwerkdatenverkehr geschützt sind, der den Tunnel nicht verwendet.

Wenn Sie eine neue Installation des CylanceGATEWAY-Agenten bereitstellen, müssen die Geräte der Benutzer neu gestartet werden und die Benutzer müssen den Installationsvorgang manuell abschließen und den Arbeitsmodus aktivieren oder den Sicherheitsmodus aktivieren. Wenn Sie ein Upgrade des CylanceGATEWAY-Agenten bereitstellen, müssen die Geräte der Benutzer neu gestartet werden, damit das Upgrade abgeschlossen werden kann. Während des Upgrades behält der CylanceGATEWAY-Agent alle Konfigurationen bei. Es sind keine weiteren Maßnahmen durch die Benutzer erforderlich.

Wenn die Installation des CylanceGATEWAY-Agenten von Enterprise-Geräteverwaltungs-Tools (z. B. Microsoft System Center Configuration Manager (SCCM) oder einem anderen Bereitstellungstool) gesteuert wird, können Sie die Parameter customDomain einfügen, um die Benutzerinteraktion bei Aktivierung des Agenten zu minimieren. Sie können den benutzerdefinierten Domänennamen aus dem Feld „Name der benutzerdefinierten Domäne“ unter „Einstellungen > Anwendung“ abrufen. Sie können die Parameter für Windows-Geräte über die Befehlszeile und für macOS-Geräte über eine verwaltete App-Konfiguration oder MCX-App-Einstellungen bereitstellen. Sie können Benutzer auch anweisen, den CylanceGATEWAY-Agenten manuell herunterzuladen und zu installieren, um den Arbeitsmodus zu aktivieren oder den Sicherheitsmodus zu aktivieren.

- Geben Sie für macOS-Geräte den folgenden Wert an, um den Namen der benutzerdefinierten Domäne festzulegen, der verwendet werden soll, wenn Benutzer den CylanceGATEWAY-Agenten 2.9 oder höher aktivieren:

  ```
  <dict>
    <key>customDomain</key>
    <string>Your_custom_domain_name</string>
  </dict>
  ```

- Geben Sie für Windows-Geräte den folgenden Befehl an, um den Namen der benutzerdefinierten Domäne festzulegen, der verwendet werden soll, wenn Benutzer den CylanceGATEWAY-Agenten 2.9 oder höher aktivieren:

  `CylanceGATEWAY-<version>.exe /v"CUSTOM_DOMAIN=<your_custom_domain_name>"`

  Informationen zum Festlegen des Namens der benutzerdefinierten Domäne für eine automatische Installation finden Sie unter Durchführen einer Installation im Hintergrund und ein Upgrade des CylanceGATEWAY-Agenten.

Durchführen einer Installation im Hintergrund und ein Upgrade des CylanceGATEWAY-Agenten

Sie können den CylanceGATEWAY-Agent für Benutzer bereitstellen. Wenn es sich bei der Bereitstellung um eine Neuinstallation handelt, müssen Benutzer ihr Gerät neu starten, den Installationsvorgang manuell abschließen und den Arbeitsmodus aktivieren oder den Sicherheitsmodus aktivieren. Bei neuen Bereitstellungen können Sie den Namen der benutzerdefinierten Domäne angeben, den Sie aus dem Feld „Namen der benutzerdefinierten Domäne“ unter „Einstellungen > Anwendung“ erhalten haben. Wenn es sich bei der Bereitstellung um ein Upgrade handelt, müssen Benutzer ihre Geräte neu starten, damit das Upgrade abgeschlossen werden kann. Die Konfigurationen des CylanceGATEWAY-Agenten werden beibehalten und es sind keine weiteren Maßnahmen seitens der Benutzer erforderlich.

Bevor Sie beginnen: Laden Sie eine Kopie des CylanceGATEWAY-Agenten für Windows von der BlackBerry-Website herunter und speichern Sie sie auf Ihrem Computer.

1. Öffnen Sie eine Eingabeaufforderung und führen Sie sie als Administrator aus.
2. Navigieren Sie zu dem Ort, an dem Sie die CylanceGATEWAY-Agenten gespeichert haben. Führen Sie eine der folgenden Aufgaben aus: In diesem Beispiel verwenden wir CylanceGATEWAY-Agent Version 2.7.0.19.
   - Um eine Installation im Hintergrund oder ein Upgrade durchzuführen, ohne die Geräte des Benutzers neu zu starten, geben Sie Folgendes ein:

     `.\CylanceGATEWAY-2.7.0.19.exe /s /v" REBOOT=Suppress /qn"`
   - Um eine Installation im Hintergrund oder ein Upgrade durchzuführen und die Geräte des Benutzers sofort neu zu starten, geben Sie Folgendes ein: `.\CylanceGATEWAY-2.7.0.19.exe /s /v" /qn"`
   - Um eine Installation im Hintergrund oder ein Upgrade durchzuführen und eine Installationsprotokolldatei namens GWInstall zu erstellen, geben Sie Folgendes ein:

     `.\CylanceGATEWAY-2.7.0.19.exe /s /v" REBOOT=Suppress /qn /l*v .\GWInstall.log"`
   - Um eine neue Installation durchzuführen und den Namen der benutzerdefinierten Domäne anzugeben, geben Sie Folgendes ein:

     `.\CylanceGATEWAY-<2.9.x.x>.exe /s /v" CUSTOM_DOMAIN=<your_custom_domain_name> /qn"`

     Für diese Funktion ist der CylanceGATEWAY Agent für Windows 2.9 oder höher erforderlich.
3. Weisen Sie Ihre Benutzer ggf. an, ihre Geräte neu zu starten und den Anweisungen auf dem Bildschirm zu folgen.

Einrichten von CylanceAVERT

Element	Beschreibung
1	Überprüfen der Softwareanforderungen.
2	Definieren vertraulicher Inhalte
3	Installieren von CylanceAVERT
4	Erstellen von Richtlinien zum Informationsschutz
5	Zuweisen von Richtlinien zu Administratoren, Benutzern und Gruppen

Installieren des CylanceAVERT-Agenten

Sie können CylanceAVERT von der Seite „Downloads“ im BlackBerry-Portal myAccount herunterladen und installieren.

Sie können CylanceAVERT im Hintergrund über SCCM oder JAMF für Benutzer installieren. Dazu müssen Sie den Befehlszeilenparameter `IAgreetoBBSLA=true` angeben, um den Endbenutzer-Lizenzvertrag (EULA) zu akzeptieren. Die EULA wird dem Benutzer nicht angezeigt. Nach der Installation von CylanceAVERT im Hintergrundmodus muss das System neu gestartet werden.

Hinweis: Vor der Installation von CylanceAVERT im Hintergrundmodus müssen Sie die Lizenzvereinbarung für die BlackBerry-Lösung lesen, einschließlich der Datenschutzhinweise von BlackBerry. Sie können die Anwendung nur installieren, wenn Sie die Bedingungen der Lizenzvereinbarung für die BlackBerry-Lösung auf die oben angegebene Weise akzeptieren. **Wenn Sie die Bedingungen der Lizenzvereinbarung für die BlackBerry-Lösung nicht akzeptieren, dürfen Sie CylanceAVERT nicht installieren oder verwenden.**

Nachdem der CylanceAVERT-Agent installiert wurde, kann der Benutzer Sicherheitsbenachrichtigungen für die potenzielle unbefugte Freigabe sensibler Unternehmensdaten erhalten, wenn er E-Mails sendet, Dateien über USB überträgt und Dateien auf eine Website hochlädt.

Wenn sich ein Benutzer, der nicht zu Cylance Endpoint Security hinzugefügt wurde, bei einem Desktop anmeldet, auf dem CylanceAVERT installiert ist, wird der Benutzer automatisch mit allen auf ihn angewendeten Richtlinien zu Cylance Endpoint Security hinzugefügt. Hierfür ist eine Verbindung zu Active Directory oder zum BlackBerry Connectivity Node-Verzeichnis erforderlich. Wenn Sie eine BlackBerry Connectivity Node-Verzeichnisverbindung für die Benutzerverwaltung verwenden, müssen Sie BlackBerry Connectivity Node Version 2.12.1 oder höher verwenden. Weitere Informationen finden Sie unter Installieren von BlackBerry Connectivity Node und Verknüpfung mit Ihrem Unternehmensverzeichnis im Cylance Endpoint Security-Einrichtungshandbuch.

Hinweis: Wenn ein Benutzer die CylanceAVERT-App über die Windows-Taskleiste beendet, erhält er keine Windows-Benachrichtigung, wenn ein Exfiltrationsereignis eintritt.

Installieren von CylanceAVERT

CylanceAVERT erfordert CylancePROTECT Desktop Version 3.1 oder höher.

Hinweis: CylanceAVERT kann auf einem Computer mit CylancePERSONA nicht installiert werden.

1. Doppelklicken Sie auf dem Gerät auf das Installationsprogramm des CylanceAVERT-Agent.
2. Befolgen Sie die Installationsschritte.

Wenn Sie fertig sind:

- Sie können wie folgt überprüfen, ob der CylanceAVERT-Agent installiert ist:
  - Das CylanceAVERT-Symbol wird in der Taskleiste angezeigt.
  - Der CylanceAVERT-Benutzer wird in der Konsole in der Benutzerliste auf der Seite „Assets“ angezeigt.
  - Überprüfen Sie im Windows Task-Manager, ob der CylanceAVERT-Prozess ausgeführt wird.
- Um den Agenten zu deinstallieren, verwenden Sie die Windows-Einstellungen.

Hinweis: Nach der Installation von CylanceAVERT verhindert das Browser-Plug-in das Hochladen von Dateien auf ungesicherte Websites (nicht-SSL). BlackBerry empfiehlt, dass Sie nicht versuchen, Dateien auf Nicht-SSL-Websites hochzuladen.

Definieren sensibler Inhalte mithilfe von Einstellungen zum Informationsschutz

Mit den Informationsschutz-Einstellungen können Sie die Datentypen angeben, nach denen CylanceAVERT in sensiblen Dateien sucht, die gesammelten Nachweise, die als vertrauenswürdig geltenden E-Mail- und Browser-Domänen und die E-Mail-Adressen, an die Sie Benachrichtigungen über ein Exfiltrationsereignis senden möchten.

Verwalten von Nachweissammlungen

Sie können anpassen, wie Daten-Exfiltrationsereignisse in CylanceAVERT erfasst werden. Mithilfe der Datenerfassungseinstellungen können Sie die Nachweise konfigurieren, die während eines Daten-Exfiltrationsereignisses zu Auditzwecken erfasst werden sollen. Die Konfiguration der Datenerfassungseinstellungen ermöglicht es Ihnen, Entscheidungen zu treffen, z. B. zum Aufnehmen von Dateisegmenten des Exfiltrationsereignisses, Speichern vollständiger Kopien der Dateien, die an dem Exfiltrationsereignis beteiligt sind, Verwalten von Uploads in den Nachweisordner, Auswählen von Zeiten für das Hochladen von Dateien und Angeben der Aufbewahrungsfristen für Datennachweise.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Datenschutz**.
2. Klicken Sie auf die Registerkarte **Datenerfassung**.
3. Führen Sie einen der folgenden Schritte aus, um die Einstellungen für den Datenschutz zu konfigurieren:

Element	Schritte
Dateisegmente	Klicken Sie auf **Dateisegmente generieren**, um die Erfassung von Dateisegmenten ein- oder auszuschalten. Wenn **Dateisegmente generieren** aktiviert ist, wird ein Dateisegment des Daten-Exfiltrationsereignisses in den Ereignisdetails gespeichert. Standardmäßig ist **Dateisegmente generieren** deaktiviert.

Element	Schritte
Sammlung von Nachweisdateien	• Klicken Sie auf **Sammlung von Nachweisdateien aktivieren**, um die Erfassung von Nachweisdateien ein- oder auszuschalten. Standardmäßig ist die Option **Sammlung von Nachweisdateien aktivieren** deaktiviert. Wenn die Option **Sammlung von Nachweisdateien aktivieren** markiert ist, wird eine vollständige Kopie der Dateien, die an einem Daten-Exfiltrationsereignis beteiligt sind, in den Ereignisdetails gespeichert. Weitere Informationen finden Sie unter Anzeigen von CylanceAVERT-Ereignisdetails. • Klicken Sie auf das Textfeld **Festplattenspeicher** und geben Sie einen Wert für den maximalen freien Speicherplatz an, den Sie zum Zwischenspeichern von Nachweisdateien auf Remote-Geräten oder dem Nachweisordner zuweisen können. Standardmäßig ist **Festplattenspeicher** auf 10 % eingestellt.
Dateiupload	Klicken Sie auf das Dropdown-Menü **Methode für Dateiupload** und wählen Sie eine Methode aus. Wenn Sie **Direkt** auswählen, können Geräte in Ihrem Netzwerk Dateien direkt in Ihren Nachweisordner hochladen. Wenn der direkte Zugriff auf Ihren Nachweisordner blockiert ist (z. B. durch Ihre Firewall), lädt BlackBerry die Dateien durch Auswahl von **BlackBerry Proxy Service** über seine Cloud hoch. Standardmäßig ist **Direkt** ausgewählt.
Aufbewahrung von Nachweisdateien	Klicken Sie auf das Dropdown-Menü **Datenaufbewahrung** und wählen Sie aus, wie lange Nachweisdateien in Ihrem Nachweisordner gespeichert werden sollen. Die Werte für den Zeitraum, für den Nachweisdateien gespeichert werden können, sind 30, 60 oder 90 Tage. Standardmäßig ist die **Datenaufbewahrung** auf 30 Tage eingestellt.

Hinzufügen zulässiger und vertrauenswürdiger Domänen

Sie geben Domänen an, um Browser- und E-Mail-Adressen aufzulisten, auf die Sie Dateien sicher hochladen können. Nachdem Sie Domänen hinzugefügt haben, müssen Sie sie für die Verwendung in den Informationsschutzrichtlinien aktivieren. Wenn Sie eine zulässige Domäne für eine Richtlinie angeben und sie auf Uploads sensibler Dateien gescannt wird, löst diese Domäne keine Richtlinienverletzungen aus. Dazu muss die Domäne anhand eines hinzugefügten Zertifikats validiert worden und als vertrauenswürdige Domäne eingestuft worden sein. Wenn Sie keine Domänen in den Einstellungen zum Informationsschutz angeben oder keine Domänen zur Verwendung in Ihren Richtlinien hinzufügen, werden alle Domänen als nicht vertrauenswürdig behandelt.

Hinweis:

- Alle Domänen von USB-Geräten werden als nicht vertrauenswürdig betrachtet.
- Nachdem Sie eine zulässige Domäne angegeben haben, werden alle Subdomänen als zulässig betrachtet, wenn deren vertrauenswürdige Zertifikate ebenfalls hinzugefügt wurden.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie ein vertrauenswürdiges Zertifikat hochgeladen haben. Damit eine Domäne als vertrauenswürdig gilt, muss ein vertrauenswürdiges Zertifikat hochgeladen werden. Wenn kein vertrauenswürdiges Zertifikat hochgeladen und die zulässige Domäne in einer Richtlinie verwendet wird, wird dennoch ein Exfiltrationsereignis ausgelöst. Weitere Informationen finden Sie unter Prüfen von Domänen mithilfe vertrauenswürdiger Zertifikate.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Datenschutz**.
2. Klicken Sie auf die Registerkarte **Zulässige Domänen**.
3. Um eine neue Browserdomäne hinzuzufügen, klicken Sie auf die Schaltfläche **Neue Domäne hinzufügen**.

4. Geben Sie im Dialogfeld **Zulässige Domäne hinzufügen** einen Namen und eine Beschreibung für die Domäne in die Textfelder ein. Platzhalterzeichen werden im Feld „Domänenname“ nicht unterstützt.
5. Aktivieren Sie optional die Möglichkeit, diese Domäne in einer Richtlinie zu verwenden.
6. Um zu prüfen, ob diese Domäne ein vorhandenes vertrauenswürdiges Zertifikat verwendet, klicken Sie auf **Überprüfen**. Wenn Sie kein Zertifikat hochgeladen haben, fügen Sie das Zertifikat jetzt hinzu. Anweisungen finden Sie unter Prüfen von Domänen mithilfe vertrauenswürdiger Zertifikate.
7. Klicken Sie auf **Hinzufügen**.
8. Wenn Sie eine neue E-Mail-Domäne hinzufügen möchten, geben Sie die Domäne im Abschnitt **Zulässige E-Mail-Domänen** ein und trennen Sie sie durch ein Komma von den zuvor eingegebenen Domänen.

Wenn Sie fertig sind:

Um eine zulässige Domäne zu löschen, klicken Sie in der Liste **Zulässige Domänen** auf das Kontrollkästchen neben der Domäne, die Sie löschen möchten, und klicken Sie auf **Löschen**.

Verwenden von Vorlagen zum Gruppieren von Datentypen

Sie können Vorlagen verwenden, um sensible Datentypen zu gruppieren, die Ihr Unternehmen in einer Richtlinie verwenden soll.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Informationsschutz**.
2. Klicken Sie auf die Registerkarte **Vorlagen**.
3. Um eine vordefinierte Vorlage hinzuzufügen, klicken Sie auf **Vordefinierte hinzufügen**, wählen Sie die vordefinierten Vorlagen aus der Liste aus und klicken Sie auf **Hinzufügen**.
4. Um eine eigene Vorlage zu erstellen, klicken Sie auf **Benutzerdefinierte erstellen**.
5. Geben Sie auf der Seite **Neue Vorlage hinzufügen** im Abschnitt **Allgemeine Informationen** den Vorlagennamen ein und wählen Sie die Region aus der Dropdown-Liste aus.
6. Wählen Sie im Dropdown-Menü **Region** die Region aus, für die die Vorlage verwendet werden soll. Wenn Sie beispielsweise eine Vorlage mit den Datentypen „Canadian Health Card“ (Kanadische Krankenversicherungskarte) und „Canadian Sin Number“ (Kanadische Sozialversicherungsnummer) erstellen, wählen Sie „Kanada“ als Region aus.
7. Wählen Sie im Dropdown-Menü **Informationstyp** den Informationstyp aus, der Ihrer Vorlage entspricht. Werte sind benutzerdefinierte, gesundheitsbezogene, personenbezogene und Finanzdaten.
8. Wählen Sie im Abschnitt **Conditions Builder** den Datentyp aus der Dropdown-Liste aus und geben Sie dann die Mindestanzahl an Vorkommen an, die erforderlich sind, um die Richtlinienverletzung auszulösen. Um der Gruppe einen weiteren Datentyp hinzuzufügen, klicken Sie auf **Element hinzufügen**.
   - Um der Gruppe einen weiteren Datentyp hinzuzufügen, klicken Sie auf **Element hinzufügen**.
   - Um eine weitere Bedingungsgruppe hinzuzufügen, klicken Sie auf **Gruppe hinzufügen**.
9. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

Nachdem Ihre Vorlage hinzugefügt wurde, können Sie sie zu einer Informationsschutzrichtlinie hinzufügen. Weitere Informationen finden Sie im Abschnitt Verwalten von Richtlinien zum Schutz von Informationen.

Um eine Vorlage zu entfernen, gehen Sie in der Spalte **Aktionen** neben der Vorlage, die Sie entfernen möchten, wie folgt vor:

- Um eine vordefinierte Vorlage zu entfernen, klicken Sie auf ⊗. Klicken Sie im Bestätigungsdialogfeld auf **Entfernen**.
- Um eine benutzerdefinierte Vorlage zu löschen, klicken Sie auf 🗑. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**.

Wenn eine Vorlage aus Ihrer Liste entfernt wird, steht sie nicht mehr für die Verwendung in einer Informationsschutzrichtlinie zur Verfügung.

Um eine benutzerdefinierte Vorlage zu bearbeiten, klicken Sie auf die Vorlage in der Liste und bearbeiten Sie die Informationen in den Feldern. Vordefinierte Vorlagen können nicht bearbeitet werden. Weitere Informationen finden Sie in den Schritte 4 bis 7.

Um eine Vorlage zu kopieren, klicken Sie in der Spalte „Aktionen“ der zu kopierenden Vorlage auf  .

Festlegen sensibler Datentypen

Datentypen stehen für die sensiblen Daten, nach denen CylanceAVERT sucht. Sie können Datentypen in den Einstellungen zum Informationsschutz festlegen und an die Anforderungen Ihres Unternehmens anpassen. Die für Datentypen verfügbaren Suchmethoden sind Schlüsselwörter oder reguläre Ausdrücke.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Datenschutz**.
2. Klicken Sie auf die Registerkarte **Datentypen**.
3. Klicken Sie auf **Benutzerdefinierten Datentyp hinzufügen**.

   Hinweis: Sie können auch vordefinierte Datentypen zu Ihrer Liste hinzufügen, wodurch der Datentyp in einer Informationsschutzrichtlinie verwendet werden kann. Um einen vordefinierten Datentyp zu einer Liste hinzuzufügen, klicken Sie auf **Vordefinierten Datentyp hinzufügen**, wählen Sie die vordefinierten Datentypen aus, die Sie der Liste hinzufügen möchten, und klicken Sie auf **Hinzufügen**.
4. Legen Sie auf der Seite **Benutzerdefinierten Datentyp hinzufügen** einen Namen und eine Beschreibung für den neuen Datentyp fest.
5. Wählen Sie in der Dropdown-Liste **Region** die Region aus, für die der Datentyp verwendet werden soll. Wenn Sie beispielsweise nach einer kanadischen Führerscheinnummer suchen, wählen Sie Kanada als Region aus.
6. Wählen Sie im Dropdown-Menü **Informationstyp** den Informationstyp aus, der Ihrem Datentyp entspricht. Werte sind benutzerdefinierte, gesundheitsbezogene, personenbezogene und Finanzdaten.
7. Wählen Sie im Dropdown-Menü **Suchmethode** die Suchmethode aus, die Sie verwenden möchten. Werte sind Schlüsselwörter, Ausdruck oder Schlüsselwort-Wörterbuch. Ein Schlüsselwort-Wörterbuch ist eine Textdatei, in der mehrere Schlüsselwörter angegeben sind. Um ein Schlüsselwort-Wörterbuch zu erstellen, müssen Sie eine Textdatei erstellen, in der jedes Schlüsselwort in eine neue Zeile geschrieben wird.
8. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie **Schlüsselwörter** als Suchmethode ausgewählt haben, geben Sie die Schlüsselwörter, nach denen gesucht werden soll, in das Feld **Schlüsselwörter** ein. Sie können mehrere Schlüsselwörter durch Kommas trennen.
     - Wählen Sie **Genaue Übereinstimmung**, wenn Sie die Datei als vertraulich betrachten möchten, wenn die Schlüsselwörter genau übereinstimmen. Wenn diese Option ausgewählt ist, werden Schlüsselwörter nicht gefunden, wenn sie Teil einer größeren Textzeichenfolge sind. Wenn Sie beispielsweise „vertraulich“ als Schlüsselwort angeben, wird „Vertraulichkeit“ nicht zu einer Übereinstimmung führen.
     - Wählen Sie **Groß-/Kleinschreibung erzwingen**, wenn Sie die Datei als vertraulich betrachten möchten, wenn die Schlüsselwörter genau übereinstimmen. Bei Auswahl dieser Option wird die Groß-/Kleinschreibung von Text erzwungen. Wenn Sie beispielsweise „vertraulich“ als Schlüsselwort angeben, wird „VERTRAULICH“ nicht zu einer Übereinstimmung führen.
   - Wenn Sie **Regulärer Ausdruck (RegEx)** als Suchmethode ausgewählt haben, geben Sie den regulären Ausdruck, nach dem Sie suchen möchten, in das Feld **Regex** ein.

     Hinweis: Wenn Sie einen regulären Ausdruck verwenden möchten, sollten Sie Folgendes beachten:

     - Der reguläre Ausdruck muss der .NET-Ausdruckssprache entsprechen.
     - Sie können den Regex mit gängigen Tools wie Regex101 oder Regex Storm validieren.
   - Wenn Sie **Schlüsselwort-Wörterbuch** auswählen, führen Sie die folgenden Schritte aus:

- Wählen Sie **Genaue Übereinstimmung**, wenn Sie die Datei als vertraulich betrachten möchten, wenn die Schlüsselwörter genau übereinstimmen. Wenn diese Option ausgewählt ist, werden Schlüsselwörter nicht gefunden, wenn sie Teil einer größeren Textzeichenfolge sind. Wenn Sie beispielsweise „vertraulich“ als Schlüsselwort in Ihrem Schlüsselwort-Wörterbuch angeben, wird „Vertraulichkeit“ nicht zu einer Übereinstimmung führen.
- Wählen Sie **Groß-/Kleinschreibung erzwingen**, wenn Sie die Datei als vertraulich betrachten möchten, wenn die Schlüsselwörter genau übereinstimmen. Bei Auswahl dieser Option wird die Groß-/Kleinschreibung von Text erzwungen. Wenn Sie beispielsweise „vertraulich“ als Schlüsselwort in Ihrem Schlüsselwort-Wörterbuch angeben, wird „VERTRAULICH“ nicht zu einer Übereinstimmung führen.
- Klicken Sie auf **Schlüsselwort-Wörterbuch hochladen** und wählen Sie Ihr Wörterbuch aus. Sie können nur ein Schlüsselwort-Wörterbuch pro Datentyp hochladen.

Hinweis: Die folgenden Einschränkungen gelten für ein Schlüsselwort-Wörterbuch:

- Die Gesamtgröße aller Schlüsselwort-Wörterbücher auf einem Mandanten darf 1,5 MB nicht überschreiten.
- Ein einzelnes Schlüsselwort im Schlüsselwort-Wörterbuch darf nicht länger als 1024 Zeichen sein.
- Pro Mandant darf ein Schlüsselwort-Wörterbuch maximal 1000 Datenelemente enthalten.

9. Klicken Sie auf **Erstellen**.

Wenn Sie fertig sind:

- Ein benutzerdefinierter Datentyp kann gelöscht werden. Um einen benutzerdefinierten Datentyp zu löschen, klicken Sie in der Spalte **Aktionen** auf . Klicken Sie im Bestätigungs-Popup auf **Löschen**.
  Hinweis: Wenn der Datentyp in einer Richtlinie verwendet wird, wird das Popup-Fenster **Datentyp wird verwendet** angezeigt und Sie können ihn erst löschen, wenn er entfernt wurde.
- Ein vordefinierter Datentyp kann aus Ihrer Liste entfernt, aber nicht gelöscht werden. Um einen vordefinierten Datentyp aus Ihrer Liste zu entfernen, klicken Sie in der Spalte **Aktionen** auf . Klicken Sie im Bestätigungs-Popupfenster auf **Entfernen**. Sie können einen vordefinierten Datentyp erneut zu Ihrer Liste hinzufügen, indem Sie auf **Vordefinierten Datentyp hinzufügen** klicken und den Datentyp aus der Liste auswählen.
  Hinweis: Wenn der Datentyp in einer Richtlinie verwendet wird, wird das Popup-Fenster **Datentyp wird verwendet** angezeigt und Sie können ihn erst löschen, wenn er entfernt wurde.
- Ein vorhandenes Schlüsselwort-Wörterbuch kann heruntergeladen werden. Wenn ein aktualisiertes Schlüsselwort-Wörterbuch hochgeladen wird, wird der Endpunkt erneut gescannt und die Richtlinien werden ausgewertet. Derzeit werden vorhandene Ereignisse weiterhin vom vorherigen Datentyp ausgewertet.

Prüfen von Domänen mithilfe vertrauenswürdiger Zertifikate

Mit vertrauenswürdigen Zertifikaten können Sie die zulässigen Browserdomänen überprüfen, die in den Einstellungen zum Informationsschutz hinzugefügt wurden. Wenn ein vertrauenswürdiges Zertifikat fehlt und die zulässige Domäne in einer Richtlinie verwendet wird, wird ein Exfiltrationsereignis ausgelöst. Weitere Informationen zu zulässigen Domänen finden Sie unter Hinzufügen zulässiger und vertrauenswürdiger Domänen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Datenschutz**.
2. Klicken Sie auf die Registerkarte **Vertrauenswürdige Zertifikate**.
3. Klicken Sie auf **Zertifikat hinzufügen**.
4. Laden Sie eine Stamm- oder Zwischenzertifikat (.pem) hoch. Klicken Sie auf **Dateien durchsuchen**, um nach einer lokalen .pem-Datei auf Ihrem Gerät zu suchen, und klicken Sie dann auf **Hinzufügen**.

Senden von Benachrichtigungen an eine angegebene E-Mail-Adresse

Sie können E-Mail-Adressen angeben, an die Benachrichtigungen gesendet werden sollen, wenn ein Daten-Exfiltrationsereignis auftritt oder wenn der Nachweisordner die Speicherkapazität erreicht. Nur Cylance Endpoint Security-Administratoren können Ereignisdetails anzeigen, aber jeder Benutzer kann Benachrichtigungen erhalten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Datenschutz**.
2. Klicken Sie auf die Registerkarte **Benachrichtigungen**.
3. Aktivieren Sie die Option **Informationsschutz-Ereignisbenachrichtigungen aktivieren**, um das Senden von E-Mail-Benachrichtigungen für CylanceAVERT-Ereignisse an bestimmte E-Mail-Empfänger zu aktivieren.
4. Geben Sie in das Feld **Empfänger eingeben** die E-Mail-Adressen der Empfänger von CylanceAVERT-Ereignisbenachrichtigungen ein. Sie können mehrere E-Mail-Adresseinträge durch ein Komma trennen.
5. Aktivieren Sie die Option **Benachrichtigungen zum Nachweisordner-Speicher aktivieren**, um das Senden von E-Mail-Benachrichtigungen zur Speicherkapazität des Nachweisordners an bestimmte E-Mail-Empfänger zu aktivieren.
6. Geben Sie in das Textfeld **E-Mail-Empfänger** die E-Mail-Adressen ein, die Benachrichtigungen über die Speicherkapazität des Nachweisordners erhalten sollen. Sie können mehrere E-Mail-Adresseinträge durch ein Komma trennen.

Verwalten von Richtlinien zum Schutz von Informationen

Mit den Richtlinien zum Informationsschutz können Sie organisatorische oder regulatorische Richtlinien erstellen, die ausgelöst werden, wenn bestimmte Bedingungen erfüllt sind. Sie können Bedingungen mithilfe einer Vorlage oder über den Conditions Builder hinzufügen. Die Richtlinien zum Schutz von Informationen sind kumulativ und werden nicht wie andere Cylance Endpoint Security-Richtlinien klassifiziert. Wenn der Benutzer unbekannt ist oder ihm keine Richtlinien zugewiesen wurden, werden alle Richtlinien auf den Benutzer angewendet.

Die Richtlinien zum Schutz von Informationen können regulatorischer oder organisatorischer Art sein. Je nach Richtlinientyp wird eine andere Abstimmungslogik angewendet.

- Wenn einem Benutzer mehrere regulatorische Richtlinienarten zugewiesen sind, werden die Richtlinien für den Benutzer konsolidiert und die restriktivsten Regeln und Behebungsmaßnahmen werden angewendet.
- Wenn einem Benutzer mehrere organisatorische Richtlinienarten zugewiesen sind, werden die Richtlinien für den Benutzer konsolidiert und die am wenigsten restriktiven Regeln und Behebungsmaßnahmen werden angewendet.

Hinweis: Mindestens eine Richtlinie zum Informationsschutz ist erforderlich. Wenn Sie versuchen, die Richtlinie zum Informationsschutz zu löschen, erhalten Sie eine Fehlermeldung, dass eine Richtlinie erforderlich ist.

Best Practices für die Richtlinienkonsolidierung

CylanceAVERT bietet zwei Arten der Richtlinienkonformität, die in einer Informationsschutzrichtlinie verwendet werden können.

Die regulatorische Konformität bezieht sich auf einen festen Satz sensibler Daten, die zum Schutz sensibler Informationen im Zusammenhang mit Branchen- oder behördlichen Vorschriften verwendet werden. Regulatorische Daten sind Daten, die sich im Laufe der Zeit nicht ändern. Bei den vordefinierten Datentypen in den CylanceAVERT-Einstellungen handelt es sich ausschließlich um regulatorische Datentypen, die Ihnen von BlackBerry zur Verfügung gestellt werden, um die Produkteinrichtung zu beschleunigen und zu vereinfachen. Sie können Ihre eigenen regulatorischen Datentypen und Vorlagen zur Verwendung in einer Richtlinie erstellen, die alle regulatorischen Daten enthält, die Ihr Unternehmen benötigt. Anstatt beispielsweise die von BlackBerry bereitgestellte Vorlage zu verwenden, können Sie z. B. eine regulatorische Richtlinie erstellen, die eine kanadische SIN-Nummer, PHIN, Gesundheitsservice-Nummer, Führerschein-, Bankkonto- und Reisepassnummer in einer

einzigen Richtlinie enthält. CylanceAVERT verwendet reguläre Ausdrücke oder Schlüsselwortabgleiche, um festzustellen, ob eine Datei relevante regulatorische Informationen enthält, die in der Richtlinie angegeben sind.

Organisatorische Konformität bezieht sich auf eine unbestimmte Reihe von Daten, bei denen sich der Inhalt und die Personen, die auf die Daten zugreifen können, je nach Unternehmenssituation ständig ändern. Daher sollte die organisatorische Konformität zum Schutz sensibler Daten eingesetzt werden, die Informationen über das geistige Eigentum des Unternehmens oder andere für Ihr Unternehmen relevante Informationen enthalten.

Es besteht die Möglichkeit, dass mehrere Richtlinien auf dieselbe vertrauliche Datei angewendet werden, wobei sich die Richtlinien in den zu ergreifenden Behebungsmaßnahmen widersprechen können, wenn eine sensible Datei erkannt wird. In diesem Fall wendet CylanceAVERT für diese Richtlinien eine Abstimmung der Behebungsmaßnahmen an.

Wenn Richtlinienkollisionen auftreten, wendet CylanceAVERT automatisch diese Abstimmung an. Die Abstimmungsaktion unterscheidet sich, je nachdem ob die Datei gegen eine regulatorische, eine organisatorische oder gegen beide Richtlinien verstößt. Wenn eine Datei nur als „organisatorisch“ klassifiziert wird, wird die am wenigsten restriktive Behebungsaktion angewendet. Wenn eine Datei als regulatorisch und/oder organisatorisch eingestuft wird, werden die restriktivsten Aktionen angewendet. Wenn eine Datei beispielsweise einer organisatorischen Richtlinie unterliegt, die festlegt, dass die Datei vertraulich ist, wenn sie 2 Mal das Wort „vertraulich“ enthält, und einer zweiten Unternehmensrichtlinie, die die Vertraulichkeit auf der Grundlage von 3 Vorkommen des Wortes festlegt, wird die Datei bei 3 Vorkommen des Worts als sensibel eingestuft (am wenigsten restriktiv). Wenn es sich jedoch bei einer oder beiden dieser Richtlinien um regulatorische Richtlinien handelt, würde die Datei bei 2 Vorkommen als sensibel eingestuft (am stärksten restriktiv).

Richtlinie zum Informationsschutz erstellen

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Benutzerrichtlinie**.
2. Klicken Sie auf die Registerkarte **Informationsschutz**.
3. Klicken Sie auf **Richtlinie hinzufügen**.
4. Geben Sie im Abschnitt **Allgemeine Informationen** Folgendes ein:
   - Geben Sie im Feld **Richtlinienname** einen Namen für die Richtlinie ein.
   - Geben Sie im Feld **Beschreibung** eine Beschreibung der Richtlinie ein.
   - Wählen Sie im Dropdown-Menü **Richtlinientyp** den Typ der Richtlinie aus, die Sie erstellen möchten. Mögliche Werte für den Richtlinientyp sind „regulatorisch“ oder „organisatorisch“.
     - Ein regulatorischer Richtlinientyp bezieht sich auf einen festen Satz sensibler Daten, die durch eine Vorschrift definiert werden, die sich nicht zwangsläufig im Laufe der Zeit ändert (z. B. PCI, HIPAA usw.).
     - Ein organisatorischer Richtlinientyp bezieht sich auf firmeneigene Daten, bei denen sich die Zielgruppe, die Zugriff auf die Daten erhält, ständig ändern kann. Daher sollten organisatorische Daten als Datenelemente klassifiziert werden (z. B. Dateitypen, Stichwörter, Dateierstellende, Rolle der Dateierstellenden usw.).
5. Konfigurieren Sie im Abschnitt **Bedingungen** die Bedingungen, die eine Richtlinienverletzung auslösen. Verwenden Sie dazu eine der folgenden Optionen:

Bedingung	Beschreibung
Bedingungen mithilfe einer Vorlage hinzufügen	**a.** Klicken Sie auf **Aus Vorlage hinzufügen**. **b.** Klicken Sie auf das Kontrollkästchen für die Vorlagen, die Sie Ihrer Richtlinie hinzufügen möchten. **Hinweis:** Sie können die Vorlagenliste mithilfe der Suchleiste filtern.

Bedingung	Beschreibung
Bedingungen mit Conditions Builder hinzufügen	**Hinweis:** Der Conditions Builder besteht aus **Und**- und **Oder**-Anweisungsgruppen. Sie müssen eine Kombination aus diesen Anweisungsgruppen verwenden, um zu bestimmen, wann eine Richtlinie ausgelöst wird. **a.** Wählen Sie im Abschnitt **Und**-Bedingungen die Bedingungen aus der Dropdown-Liste aus und geben Sie dann die Mindestanzahl an Vorkommen aus dem numerischen Dropdown-Menü an, die zum Auslösen der Bedingung erforderlich sind. • Wenn Sie Ihrer aktuellen Anweisungsgruppe ein weiteres Element hinzufügen möchten, klicken Sie auf **Element hinzufügen**. • Wenn Sie eine weitere Ausweisgruppe hinzufügen möchten, klicken Sie auf **Gruppe hinzufügen**. • Wenn Sie eine Anweisungsgruppe löschen möchten, klicken Sie auf **Gruppe löschen**. **b.** Wählen Sie im Abschnitt **Oder**-Bedingungen die Bedingungen aus der Dropdown-Liste aus und geben Sie dann die Mindestanzahl an Vorkommen aus dem numerischen Dropdown-Menü an, die zum Auslösen der Bedingung erforderlich ist.

6. Klicken Sie im Abschnitt **Zulässige Domänen** auf ⊕ und wählen Sie dann die Browserdomäne aus der Liste aus, die Sie für Ihre Richtlinie zulassen möchten.
7. Wählen Sie im Abschnitt **Zulässige E-Mail-Domänen** aus, welche E-Mail-Empfänger in den Einstellungen zum Informationsschutz für Ihre Richtlinie zugelassen werden sollen.
8. Wählen Sie im Abschnitt **Aktionen** aus den Dropdown-Listen die Aktion aus, die für Webbrowser-, USB- und E-Mail-Exfiltrationsereignisse durchgeführt werden soll. Wählen Sie aus den folgenden Aktionen:

   - Melden: Diese Option meldet die Datenexfiltration oder Richtlinienverletzung an die Cylance Endpoint Security-Konsole, die auf der Seite „Avert-Ereignisse“ (Avert > Ereignisse) angezeigt werden kann, erstellt eine Benachrichtigung in der Ansicht „Benachrichtigungen“ und sendet die Ereignisse an die SIEM-Lösung oder den Syslog-Server, sofern konfiguriert. Darüber hinaus wird eine E-Mail an die im Bildschirm „Benachrichtigungen“ (Einstellungen > Informationsschutz) angegebenen E-Mail-Empfänger gesendet.
   - Melden und mitteilen: Diese Option meldet die Datenextraktion oder Richtlinienverletzung an die Cylance Endpoint Security-Konsole und zeigt das Badge für Datenexfiltration oder Richtlinienverletzung sowie die Mitteilung in der Taskleiste des Endpunkts für den Benutzer an.
   - Melden, mitteilen und warnen: Diese Option meldet die Datenexfiltration oder Richtlinienverletzung an die Cylance Endpoint Security-Konsole, zeigt ein Badge und eine Mitteilung in der Taskleiste an und fügt eine Windows-Mitteilung im Endpunkt sowie eine Popup-Nachricht für den Benutzer hinzu, bevor die Datenexfiltration oder Richtlinienverletzung auftritt. Wenn ein Benutzer z. B. Microsoft Outlook verwendet, fängt der CylanceAVERT-Agent die E-Mail ab und zeigt eine Benachrichtigung im E-Mail-Editor sowie eine Warnung an den Benutzer an, bevor die sensiblen Daten gesendet werden.
9. Klicken Sie auf **Hinzufügen**.

   Hinweis: Wenn einem Benutzer Richtlinien zugewiesen werden und diese Richtlinien dann entfernt werden, wird der Benutzer aus CylanceAVERT gelöscht.

Wenn Sie fertig sind:

Führen Sie eine der folgenden Aktionen aus:

- Sie können Benutzern oder Benutzergruppen eine Richtlinie zuweisen. Weitere Informationen finden Sie unter CylanceAVERT-Benutzerdetails anzeigen.

- Um eine Richtlinie für den Informationsschutz zu löschen, aktivieren Sie das Kontrollkästchen neben der Richtlinie in der Liste, und klicken Sie dann auf **Löschen**.
- Um eine Richtlinie für den Informationsschutz zu bearbeiten, klicken Sie auf die Richtlinie in der Liste, nehmen Sie eine Änderung an der Richtlinie vor, und klicken Sie dann auf **Speichern**.

Verwalten von Updates für die CylancePROTECT Desktop- und CylanceOPTICS-Agenten

Sie können Aktualisierungsregeln verwenden, um Updates der CylancePROTECT Desktop- und CylanceOPTICS-Agenten auf Geräten zu verwalten. Mit Aktualisierungsregeln können Sie Cylance Endpoint Security so konfigurieren, dass automatisch Updates auf eine bestimmte Version oder die neueste verfügbare Version übertragen werden, oder Sie können automatische Updates deaktivieren, sodass Sie die Softwareverteilung mit der von Ihrem Unternehmen bevorzugten Methode verwalten können. Zonen sind Aktualisierungsregeln zugeordnet, sodass Geräte und Benutzer, die Teil dieser Zonen sind, entsprechend Aktualisierungen erhalten (auch als zonenbasierte Aktualisierung bezeichnet). Standardmäßig sind die Test-, Pilot- und Produktionsaktualisierungsregeln verfügbar, Sie können jedoch auch zusätzliche Aktualisierungsregeln hinzufügen, um Agenten-Aktualisierungen entsprechend den Anforderungen Ihres Unternehmens zu verwalten.

Die Agentenversion auf dem Gerät wird immer auf die Version aktualisiert, die in der Aktualisierungsregel angegeben ist. Sie können Aktualisierungsregeln verwenden, um eine niedrigere Version eines Agenten zu installieren, auch wenn das Gerät bereits eine neuere Version verwendet.

Wenn der Linux-Treiber auf einem Gerät zuvor manuell aktualisiert wurde, wird der Treiber nicht automatisch im Rahmen der Agenten-Aktualisierung aktualisiert. Dadurch wird verhindert, dass das automatisierte System eine Aktion eines Administrators überschreibt.

Beim Testen von Agenten-Aktualisierungen sollten Sie Folgendes berücksichtigen:

- BlackBerry empfiehlt, dass Sie Agenten-Aktualisierungsregeln mit Aktualisierungsregeln und Zonen testen, die zu Testzwecken erstellt wurden (z. B. mit den Test- und Pilot-Aktualisierungsregeln), bevor Sie andere Aktualisierungsregeln verwenden, die Sie für die Produktionsbereitstellung hinzugefügt haben. Beim Testen von Aktualisierungen sollten Sie Geräte verwenden, die für Test- und Bewertungszwecke reserviert sind.
- Erstellen Sie Zonen für das Testen von Agenten-Aktualisierungen und fügen Sie Geräte hinzu, die für Tests reserviert sind. Ordnen Sie die von Ihnen erstellten Zonen den Test- und Pilot-Aktualisierungsregeln zu. Weitere Informationen zum Erstellen von Zonen finden Sie unter Einrichten von Zonen für die Verwaltung von CylancePROTECT Desktop und CylanceOPTICS.
- Stellen Sie sicher, dass sich alle Testgeräte in einer Zone befinden, die Sie testen. Die Produktionsaktualisierungsregel gilt für alle Geräte, die sich nicht in einer Zone befinden, der eine andere Aktualisierungsregel zugeordnet ist.

Hinweis: Wenn der Speicherschutz, die Skriptsteuerung und/oder die Gerätesteuerung in der Geräterichtlinie aktiviert sind, wird ein Neustart des Geräts nach der Installation oder Aktualisierung des Agenten empfohlen, ist aber nicht unbedingt erforderlich. Ein Neustart stellt sicher, dass alle neuen Richtlinieneinstellungen vollständig wirksam wurden.

So funktionieren Aktualisierungsregeln mit Zonen

- Geräte werden Zonen entweder durch Zonenregeln oder durch manuelle Zuweisung zugeordnet.
- Geräte können mehreren Zonen zugeordnet werden.
- Zonen werden Aktualisierungsregeln zugewiesen. Geräte, die diesen Zonen zugewiesen sind, folgen den Aktualisierungsregeln.
- Aktualisierungsregeln sind nicht spezifisch für eine Betriebssystemplattform, Sie können jedoch Zonen erstellen, um die Aktualisierungen von Geräten mit bestimmten Betriebssystemplattformen zu verwalten. Wenn die in der Aktualisierungsregel angegebene Agentenversion für eine Plattform nicht verfügbar ist, erhält das Gerät das Update, sobald es für die Plattform verfügbar ist.
- Aktualisierungsregeln wird eine Rangfolge zugewiesen. Wenn ein Gerät mehreren Zonen zugeordnet ist, für die unterschiedliche Aktualisierungsregeln gelten, wird die Aktualisierungsregel mit der höchsten Rangfolge angewendet, die eine Aktualisierung des Agenten verlangt (automatische Aktualisierung oder bestimmte

Version). Wenn sich ein Gerät in mindestens einer Zone mit einer Aktualisierungsregel befindet, die ein Update verlangt, wird der Agent auf dem Gerät entsprechend aktualisiert. Die Aktualisierungsregel für die Produktion hat den niedrigsten Rang und gilt für Geräte, die sich nicht in einer Zone mit einer Aktualisierungsregel befinden, sowie für Geräte in Zonen, in denen keine der Regeln eine Aktualisierung für den Agenten verlangen.

Beispiele für Aktualisierungsregeln

Die folgenden Beispiele veranschaulichen Aktualisierungsregeln, denen Zonen zugewiesen sind, die speziell für zonenbasierte Aktualisierungen erstellt wurden.

Beispiel für eine Aktualisierungsregel	Zugewiesene Zonen
Windows Server – Test	• Windows Server – Aktualisierungszone „US Test“ • Windows Server – Aktualisierungszone „Europa Test“
Windows Server – Pilot	• Windows Server – Aktualisierungszone „US Pilot“ • Windows Server – Aktualisierungszone „Europa Pilot“
Windows Server – Produktion	• Windows Server – Aktualisierungszone „US Produktion“ • Windows Server – Aktualisierungszone „Europa Produktion“

Verwalten von Updates für die CylancePROTECT Desktop- und CylanceOPTICS-Agenten

Bevor Sie beginnen: Sie müssen Zonen mit Geräten erstellen, die für das Testen von Agent-Updates reserviert sind. Sie verknüpfen diese Zonen mit den Test- und Pilot-Aktualisierungsregeln. Sie können eigene Aktualisierungsregeln zum Testen oder für die Produktionsbereitstellung hinzufügen. Weitere Informationen zum Erstellen von Zonen finden Sie unter Einrichten von Zonen für die Verwaltung von CylancePROTECT Desktop und CylanceOPTICS.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Aktualisieren**.
2. Erstellen Sie ggf. eine Aktualisierungsregel. Sie können beispielsweise eine Regel zum Testen von Agent-Updates erstellen.
   a) Klicken Sie auf **Neue Regel hinzufügen**.
   b) Geben Sie einen Namen für die Regel ein.
   c) Klicken Sie auf **Senden**.
3. Klicken Sie auf eine Aktualisierungsregel. Klicken Sie beispielsweise auf **Testen**.
4. Erweitern Sie **Zonen** und wählen Sie die Zonen aus, die Sie dieser Aktualisierungsregel zuweisen möchten.
5. Erweitern Sie **Agent** und wählen Sie eine Aktualisierungsoption aus.

   Hinweis: Wenn Sie die Agentenversion auf einem Gerät nicht aktualisieren möchten, verwenden Sie die Einstellung **Nicht aktualisieren**. Sie müssen außerdem darauf achten, dass sich das Gerät nicht in einer anderen Zone mit einer anderen Aktualisierungsregel (einschließlich der Produktionsregel) befindet, die eine Aktualisierung des Agenten angibt (automatische Aktualisierung oder bestimmte Version). Wenn sich ein Gerät in einer Zone mit einer Aktualisierungsregel befindet, die ein Update verlangt, wird sie aktualisiert. Wenn ein Gerät mehreren Aktualisierungsregeln zugeordnet ist, die eine Aktualisierung verlangen, wird der Agent gemäß der Regel mit der höchsten Rangfolge aktualisiert.

6. Aktivieren Sie das Kontrollkästchen **Linux-Treiber automatisch aktualisieren**, damit der Agent automatisch auf den neuesten Treiber zur Unterstützung des neuesten Linux-Kernels aktualisiert wird. Für die Funktion „Linux-Treiber automatisch aktualisieren“ ist der CylancePROTECT Desktop-Agent Version 3.1.1000 oder höher und die Agent-Treiberversion 3.1.1000 oder höher erforderlich.
7. Erweitern Sie **CylanceOPTICS** und wählen Sie eine Aktualisierungsoption aus.

   Sie können „Automatisch aktualisieren“ nur auswählen, wenn Sie den CylancePROTECT Desktop-Agenten für die Verwendung von „Automatisch aktualisieren“ konfiguriert haben.
8. Wiederholen Sie die Schritte 2 bis 7 für die **Pilotaktualisierungsregel** oder eine Regel, die Sie für Pilottests erstellt haben.
9. Wiederholen Sie die Schritte 2 bis 7 für die **Produktionsaktualisierungsregel** oder eine Regel, die Sie für die Produktion erstellt haben. Der standardmäßigen **Produktionsaktualisierungsregel** werden keine Zonen zugewiesen, weil sie für alle Geräte gilt, die sich in keiner Zone mit Aktualisierungsregel befinden.

   Wenn der CylancePROTECT Desktop-Agent in der Produktionsaktualisierungsregel auf „Automatisch aktualisieren“ eingestellt ist, sind die Test- und Pilotregeln nicht verfügbar. Die von Ihnen erstellten Aktualisierungsregeln sind von der Konfiguration der Produktionsaktualisierungsregel nicht betroffen.
10. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Wenn Sie Aktualisierungsregeln hinzugefügt haben, klicken Sie auf die Pfeile neben den Regeln, um die Rangordnung festzulegen. Die Regeln am Anfang der Liste haben Vorrang vor den Regeln, die weiter unten in der Liste stehen. Die Test-, Pilot- und Produktionsregeln befinden sich immer am Ende der Liste. Sie können ihre Rangordnung nicht ändern. Die Aktualisierungsregel für die Produktion gilt für Geräte, die sich nicht in einer Zone mit einer Aktualisierungsregel befinden, sowie für Geräte in Zonen, in denen keine der Regeln eine Aktualisierung für den Agenten verlangen.
- Um eine Aktualisierung des CylancePROTECT Desktop-Agenten auf einem Gerät vor dem stündlichen Intervall auszulösen, klicken Sie auf dem Gerät mit der rechten Maustaste auf das Symbol CylancePROTECT Desktop in der Taskleiste und dann auf **Nach Updates suchen**. Starten Sie den Cylance-Dienst neu oder führen Sie den folgenden Befehl aus dem Cylance-Verzeichnis aus:

  ```
  CylanceUI.exe–update
  ```
- Wenn der Speicherschutz, die Skriptsteuerung und/oder die Gerätesteuerung in der Geräterichtlinie aktiviert sind, wird ein Neustart des Geräts nach der Installation oder Aktualisierung des Agenten empfohlen, ist aber nicht unbedingt erforderlich. Ein Neustart stellt sicher, dass alle neuen Richtlinieneinstellungen vollständig wirksam wurden.

Verbinden von Cylance Endpoint Security mit externen Diensten

Cylance Endpoint Security unterstützt verschiedene Connectoren, mit denen Sie Daten und Funktionen in Dienste von Drittanbietern und andere BlackBerry-Produkte integrieren können. Ein Cylance Endpoint Security-Mandant kann eine Verbindung zu mehreren externen Diensten herstellen.

Cylance Endpoint Security unterstützt die folgenden Connectoren:

Connector	Beschreibung
BlackBerry UEM	Mit dem BlackBerry UEM Connector kann CylanceGATEWAY überprüfen, ob Android- und iOS-Geräte von UEM verwaltet werden. Weitere Informationen finden Sie unter Verbinden von Cylance Endpoint Security mit MDM-Lösungen, um zu überprüfen, ob Geräte verwaltet werden.
Microsoft Intune	Der Microsoft Intune-Connector ermöglicht es Cylance Endpoint Security, die Risikostufe der Mobilgeräte Ihres Unternehmens an Intune zu melden. Die Geräterisikostufe wird auf der Grundlage der Erkennung mobiler Bedrohungen durch die CylancePROTECT Mobile-App auf von Intune-verwalteten Geräten berechnet. Intune kann Risikominderungsmaßnahmen auf Basis der Geräterisikostufe ausführen. Weitere Informationen finden Sie unter Integration von Cylance Endpoint Security mit Microsoft Intune, um auf mobile Bedrohungen zu reagieren.
Okta	Mit dem Okta Connector können Sie die Anmeldungs- und Zugriffsdaten von Okta-Diensten erfassen und die verknüpften Informationen in der Ansicht „Warnungen“ in der Cylance-Konsole anzeigen lassen. Weitere Informationen finden Sie unter Integrieren von Cylance Endpoint Security mit Okta.
Mimecast	Der Mimecast-Connector ermöglicht Ihnen die Integration von Risikobewertungsdaten für E-Mail-Anhänge von Mimecast-Diensten und die Anzeige der verknüpften Informationen in der Ansicht „Warnungen“ in der Cylance Konsole. Weitere Informationen finden Sie unter Integrieren von Cylance Endpoint Security mit Mimecast.

Integrieren von Cylance Endpoint Security mit Okta

Sie können eine Okta-Verbindung zu Ihrer Cylance-Konsole hinzufügen, um Okta-Warnhinweise in der Ansicht „Warnungen“ anzuzeigen. In der Ansicht „Warnungen“ können Administratoren Okta-Autorisierungs- und Zugriffswarnungen über eine einheitliche Schnittstelle anzeigen. Der Okta-Connector verwendet die Okta-Ereignis-API, um die Ereignistelemetrie in der Ansicht „Warnungen“ anzuzeigen. Die Okta-Benutzeranomalie-Ereignisse, die in der Ansicht „Warnungen“ zusammengefasst werden, umfassen verdächtige Benutzeranmeldeversuche und blockierte Sicherheitsanfragen. Durch das Zusammenfassen von Okta-Ereignissen in diesen Kategorien erhalten Sie bessere Einblicke in Anmeldeversuche von Dritten, fehlerhafte Anmeldungen durch Benutzer und Anmeldeversuche von verdächtigen Quell-IP-Adressen.

In der Ansicht „Warnungen“ werden Anfragen von verbotenen IP-Adressen in der gesamten Benutzerbasis Ihres Unternehmens zusammengefasst, um Einblicke in mögliche Muster oder Kampagnen zu erhalten. Die aufgestellten Daten können auch Informationen über das Quellgerät des Zugriffsversuchs enthalten, sodass Sie feststellen können, ob die Anfrage von einem Menschen oder einer Maschine gestellt wurde.

Weitere Informationen zum Konfigurieren der Erstellung von Warnungen über Okta, die in der Ansicht „Warnungen“ angezeigt werden können, finden Sie in den folgenden Ressourcen:

- Okta Hilfezentrum: Konfigurieren von Kennwortrichtlinien
- Okta Hilfezentrum: Netzwerkzonen in Blockierlisten aufnehmen

Weitere Informationen zur Ansicht „Warnungen“ finden Sie unter Verwalten von Warnungen über Cylance Endpoint Security-Dienste hinweg in der Dokumentation für Administratoren.

Voraussetzungen für das Hinzufügen eines Okta-Connectors

Bevor Sie eine Okta-Verbindung für Cylance Endpoint Security konfigurieren können, müssen Sie einige Aufgaben mit dem Okta-Dienst abschließen.

Schritt	Element	Beschreibung
1	Okta-Basis-URL dokumentieren	Sie müssen die Okta-Basis-URL für Ihre Umgebung dokumentieren, um sie bei der Konfiguration des Okta-Connector zu verwenden. Die Okta-Basis-URL ist die Produktions-URL Ihres Okta-Servers. Weitere Informationen zum Auffinden Ihrer Okta-Basis-URL finden Sie unter Suchen Ihrer Okta-Domäne in der Okta-Dokumentation.
2	Einen Okta-Administrator erstellen	Sie müssen einen Okta-Administrator erstellen, um die Okta-API nutzen zu können. BlackBerry empfiehlt die Erstellung eines dedizierten Benutzers, der mit dem API-Token in Schritt 3 verknüpft ist. Dieser Schritt wird empfohlen, weil er bei der Überprüfung von Arbeitsabläufen hilft und gewährleistet, dass andere Okta-Benutzer nicht über Token verfügen, die für Sicherheitsarbeitsabläufe erstellt und verwendet werden. Weitere Informationen zum Erstellen eines Okta-Administrators finden Sie unter Erstellen einer Administratorrollenzuweisung mithilfe eines Administrators in der Okta-Dokumentation.
3	Ein Okta-API-Token erstellen	Sie müssen ein Okta-API-Token erstellen, um Anforderungen an die Okta-API zu authentifizieren. Weitere Informationen zur Erstellung eines Okta-API-Token finden Sie unter API-Tokenverwaltung in der Okta-Dokumentation.

Befolgen Sie nach Abschluss dieser Schritte die Anweisungen unter Hinzufügen und Konfigurieren eines Okta-Connector.

Hinzufügen und Konfigurieren eines Okta-Connector

Bevor Sie beginnen: Lesen Sie Voraussetzungen für das Hinzufügen eines Okta-Connectors.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Connectors**.
2. Klicken Sie auf **Connector hinzufügen > Okta**.
3. Geben Sie im Abschnitt **Allgemeine Informationen** einen Namen für den Connector ein.
4. Geben Sie im Abschnitt **Okta-Konfiguration** die Okta-Service-API-URL, das Okta-API-Token und die Abfragehäufigkeit an.

   Hinweis: BlackBerry empfiehlt, die Abfragehäufigkeit auf dem Standardwert zu belassen, es sei denn, Sie haben eine bestimmte Ratenlimitanforderung für Ihr Unternehmen.
5. Klicken Sie auf **Verbindung testen**.
6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Lassen Sie Warnungen in der Ansicht „Warnungen“ anzeigen und verwalten Sie sie dort. Weitere Informationen finden Sie unter Verwalten von Warnungen über Cylance Endpoint Security-Dienste hinweg in der Dokumentation für Administratoren.

Integrieren von Cylance Endpoint Security mit Mimecast

Sie können eine Mimecast-Verbindung zu Ihrer Cylance-Konsole hinzufügen. Mimecast-Anhangschutz analysiert alle E-Mail-Anhänge, die Ihre Benutzer erhalten, und kann Anhänge auf Grundlage der von Ihnen konfigurierten Richtlinie verarbeiten.

In der Ansicht „Warnungen“ können Administratoren Informationen von Mimecast zu den Risiken von Anhängen über eine einheitliche Schnittstelle anzeigen. Mimecast zeigt die durch den Mimecast-Anhangschutzdienst gelieferte Telemetrie für Anhangrisiken an. Die Aktion, die Mimecast auf den Dateianhang anwendet, wird in der Spalte „Reaktion“ der Ansicht „Warnungen“ angezeigt. Wenn Mimecast eine Warnung als schädlich kategorisiert, wird der Warnung in der Ansicht „Warnungen“ eine hohe Priorität zugewiesen. Wenn Mimecast eine Warnung als unsicher oder unbekannt kategorisiert, wird der Warnung eine mittlere Priorität zugewiesen. Alarme, denen von Mimecast eine niedrige Priorität zugewiesen wird, werden nicht in der Ansicht „Warnungen“ angezeigt.

In der Ansicht „Warnungen“ wird der Anhang-Hash zur Gruppierung von Warnungen verwendet, was bedeutet, dass eine ähnliche Warnung über mehrere Benutzer in Ihrem Unternehmen hinweg für dieselbe Bedrohung gruppiert werden kann. Über den Link „Erkennungsdetails“ können Sie auf das Dashboard von Mimecast Attachment Protection zugreifen, um Bedrohungen zu untersuchen und zu beheben.

Weitere Informationen zur Ansicht „Warnungen“ finden Sie unter Verwalten von Warnungen über Cylance Endpoint Security-Dienste hinweg in der Dokumentation für Administratoren.

Voraussetzungen für das Hinzufügen eines Mimecast-Connectors

Bevor Sie eine Mimecast-Verbindung für Cylance Endpoint Security konfigurieren können, müssen Sie einige Aufgaben mit dem Mimecast-Dienst abschließen.

Schritt	Aufgabe	Details
1	Erstellen eines Mimecast-Kontos	Administratoren müssen ein neues Konto für alle Dienstnutzer erstellen. Weitere Informationen finden Sie unter Erstellen/Bearbeiten von Mimecast-Benutzern in der Mimecast-Dokumentation.

Schritt	Aufgabe	Details
2	Hinzufügen einer API-Anwendung	Geben Sie die Details und Einstellungen Ihrer API-Anwendung an. Stellen Sie bei der Konfiguration der API-Anwendung sicher, dass „Dienstanwendung“ ausgewählt ist. Dies ist erforderlich, um sicherzustellen, dass API-Schlüssel nicht ablaufen. Wenn diese Option nicht ausgewählt ist, geht die Konnektivität des Mimecast-Connectors verloren, wenn der Schlüssel abläuft. Informationen zum Hinzufügen einer API-Anwendung in Mimecast finden Sie unter Hinzufügen einer API-Anwendung in der Anleitung „Verwalten von API-Anwendungen von Mimecast“.
3	Erstellen von Schlüsseln zur Benutzerzuordnung	Sie müssen Schlüssel zur Benutzerzuordnung erstellen, um Mimecast mit Cylance Endpoint Security zu verbinden. Informationen zum Erstellen von Schlüsseln zur Benutzerzuordnung finden Sie unter Erstellen von Schlüsseln zur Benutzerzuordnung in der Anleitung „Verwalten von API-Anwendungen von Mimecast“.
4	Informieren der Benutzer über die Mimecast-Konfiguration	Es wird empfohlen, dass Sie Ihre Benutzer über die Mimecast-Konfiguration informieren. Sie können die vorkonfigurierten E-Mail-Vorlagen von Mimecast herunterladen.
5	Konfigurieren von Definitionen und Richtlinien für den Anhangschutz	Konfigurieren Sie die Definitionen und Richtlinien für den Anhangschutz, die Mimecast verwendet, wenn eine unsichere E-Mail erkannt wird. Weitere Informationen finden Sie unter Konfiguration des Anhangschutzes in der Mimecast-Dokumentation.
6	Aktivieren und Konfigurieren von Benachrichtigungen	Stellen Sie sicher, dass Sie Benachrichtigungen für alle API-Benutzer für Benachrichtigungsdaten aktiviert und konfiguriert haben, damit sie in der Ansicht „Warnungen“ verfügbar sind. Weitere Informationen finden Sie unter Konfiguration des Anhangschutzes in der Mimecast-Dokumentation.

Schritt	Aufgabe	Details
7	Verzeichnisdienste aktivieren	Stellen Sie sicher, dass Sie die Mimecast-Verzeichnisdienste aktiviert haben, damit die Mimecast-Benutzerinformationen (E-Mail-Adresse) mit den Benutzerdaten korrelieren, die in Ihrem Entra- oder Active Directory-Dienst gespeichert sind. Diese Konfiguration ermöglicht auch die Korrelation mit Ihren Geräten und den Gerätedaten, die mit den Benutzern in Ihren Verzeichnisdiensten verknüpft sind. Weitere Informationen zum Aktivieren von Verzeichnisdiensten finden Sie unter Verzeichnissynchronisierung in der Mimecast-Dokumentation.

Befolgen Sie nach Abschluss dieser Schritte die Anweisungen unter Hinzufügen und Konfigurieren eines Mimecast-Connectors.

Hinzufügen und Konfigurieren eines Mimecast-Connectors

Bevor Sie beginnen: Lesen Sie Voraussetzungen für das Hinzufügen eines Mimecast-Connectors.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Connectors**.
2. Klicken Sie auf **Connector hinzufügen > Mimecast**.
3. Geben Sie im Abschnitt **Allgemeine Informationen** einen Namen für den Connector ein.
4. Geben Sie im Abschnitt **Mimecast-Konfiguration** die erforderlichen Informationen an, geben Sie eine Abfragehäufigkeit an und wählen Sie eine Basis-URL aus.

   Weitere Informationen zur Mimecast-Schlüsselgenerierung finden Sie unter Verwalten von API-Anwendungen in der Mimecast-Dokumentation.
5. Klicken Sie auf die Umschaltfläche, um die Abfrage zu aktivieren.
6. Klicken Sie auf **Verbindung testen**.
7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Lassen Sie Warnungen in der Ansicht „Warnungen“ anzeigen und verwalten Sie sie dort. Weitere Informationen finden Sie unter Verwalten von Warnungen über Cylance Endpoint Security-Dienste hinweg in der Dokumentation für Administratoren.

Anhang: Best Practices für die Bereitstellung von CylancePROTECT Desktop auf virtuellen Maschinen unter Windows

Sie können sowohl physische als auch virtuelle Maschinen mit CylancePROTECT Desktop schützen. In diesem Abschnitt werden die bewährten Verfahren für die Bereitstellung des CylancePROTECT Desktop-Agenten auf Windows-basierten Virtual Desktop Infrastructure (VDI)-Arbeitsstationen erläutert.

CylancePROTECT Desktop ist gut als Gast-Betriebssystemkomponente geeignet, da es wenig IOPS erfordert und pro Gast wenig arbeitsspeicherintensiv ist. Die Vorbereitung und Bereitstellung des CylancePROTECT Desktop-Agenten in virtuellen Umgebungen hat Ähnlichkeiten mit der Bereitstellung auf physischen Maschinen. Die Bereitstellungsschritte und Best Practices in diesem Abschnitt stellen sicher, dass der Agent in einer virtuellen Umgebung mit weniger zugewiesenen Ressourcen effizient arbeitet, und helfen Ihnen, ein Golden Image ohne unsichere oder anormale Dateien zu erstellen. Nachdem das Golden Image gründlich überprüft wurde, können Produktions-VDI-Images daraus geklont werden.

Anforderungen und Überlegungen für die Verwendung von CylancePROTECT Desktop auf virtuellen Maschinen

Element	Anforderungen oder Überlegungen
Unterstützte Virtualisierungstechnologien für Unternehmen	• Microsoft Hyper-V • Citrix XenDesktop • VMware Horizon/View • VMware Workstation • VMware Fusion

Element	Anforderungen oder Überlegungen
Nicht persistente virtuelle Maschinen	Eine nicht persistente VM wird gelöscht, wenn die Sitzung beendet wird, und durch dasselbe Golden Image ersetzt. Wenn eine neue VM erstellt wird, registriert der CylancePROTECT Desktop-Agent die VM bei der Verwaltungskonsole, was dazu führt, dass Geräte für denselben Endpunkt doppelt registriert werden (ältere Registrierungen werden als doppelte Offline-Gerätedatensätze behandelt, die nie wieder online verwendet werden). Verwenden Sie einen der folgenden Installationsparameter, wenn Sie den CylancePROTECT Desktop -Agenten auf dem Gold Image installieren, um eine doppelte Registrierung desselben VM-Geräts zu vermeiden: • `VDI=<X>`: Der Wert für $<X>$ ist ein Zähler, der bestimmt, wann der Agent die virtuelle Maschine mithilfe von VDI-Fingerprinting anstelle des standardmäßigen Agent-Fingerprinting-Mechanismus identifizieren soll. Doppelte Geräte werden nicht registriert, wenn der Agent VDI-Fingerprinting verwendet. • Beispiel: Sie installieren den Agenten auf einem Golden Image mit dem Parameter `VDI=2`. Sie verwenden das Golden Image, um ein übergeordnetes Image zu erstellen. Anschließend verwenden Sie das übergeordnete Image zum Erstellen eines Workstation-Image. Der Agent beginnt mit der Verwendung von VDI-Fingerprinting für das Workstation-Image, da das Golden Image und das übergeordnete Image den Zählwert von 2 erfüllen. • `AD=1`: Dieser Parameter funktioniert genauso wie `VDI=<X>`, es gibt jedoch keinen Zähler, der definiert, wann der Agent mit der Verwendung von VDI-Fingerprinting beginnt. Der Agent verwendet VDI-Fingerprinting auf dem Golden Image und für alle Images, die Sie aus dem Golden Image erstellen. Dieser Parameter wird für das EXE-Format der einheitlichen CylancePROTECT Desktop- und CylanceOPTICS-Installationsprogramme nicht unterstützt.
Funktionen für Speicherschutz und Skriptsteuerung	Beachten Sie Folgendes, bevor Sie die Funktionen für Speicherschutz- und Skriptsteuerung in einer VDI-Umgebung aktivieren: • Beide Funktionen verwenden Process Injection, um unerwünschten oder nicht autorisierten Code zu identifizieren und zu blockieren. Plug-ins, Tools oder DLLs können in virtualisierten Umgebungen negative Auswirkungen haben. Sie sollten daher den Speicherschutz und die Optionen zur Skriptsteuerung testen, bevor Sie diese auf Produktions-Workstations bereitstellen. • Es wird empfohlen, den Speicherschutz im „Nur Warnung“-Modus zu testen und anschließend entsprechend strengere Änderungen an der Geräterichtlinie vornehmen. Wenn das System instabil wird, können Sie den Speicherschutz deaktivieren. • Wenn Systemkonflikte oder -instabilitäten auftreten, können Sie als Sicherheitsmaßnahme den Kompatibilitätsmodus für den Speicherschutz aktivieren. • Siehe Bekannte Inkompatibilitäten für Speicherschutz und Skriptsteuerung v2 in Protect 1580 und höher.

Element	Anforderungen oder Überlegungen
Option zum Deaktivieren der Agent-UI	Sie haben die Möglichkeit, die CylancePROTECT Desktop Agent-UI zu deaktivieren, um Systemressourcen zu schonen. Weitere Informationen finden Sie unter Windows-Installationsparameter.
Bekannte Probleme	Informationen zu den Problemen, die beim Ausführen des CylancePROTECT Desktop-Agenten in einer virtuellen Umgebung gemeldet wurden, finden Sie unter VDI Trending Issues.

Bereitstellen von CylancePROTECT Desktop auf virtuellen Maschinen

Bevor Sie beginnen: Lesen Sie Anforderungen und Überlegungen für die Verwendung von CylancePROTECT Desktop auf virtuellen Maschinen.

1. Erstellen Sie eine Geräterichtlinie, mit der Sie das Golden Image für die VDI vorbereiten. Konfigurieren Sie die folgenden Optionen in der Richtlinie:

Geräterichtlinien-Kategorie	Optionen
Dateiaktionen	Aktivieren Sie **Automatische Quarantäne mit Ausführungssteuerung** für unsichere und anormale Dateitypen.
Schutzeinstellungen	• Aktivieren Sie **Bedrohungserkennung im Hintergrund** (**Einmal ausführen**). • Aktvieren Sie **Auf neue Dateien überwachen**.

2. Bereiten Sie das VDI-Golden-Image vor.
   a) Installieren Sie den CylancePROTECT Desktop-Agent auf dem Golden Image. Verwenden Sie beispielsweise den folgenden Installationsbefehl und die folgenden Parameter:

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

   b) Wenden Sie die in Schritt 1 erstellte Geräterichtlinie auf das Golden Image an.

   Warten Sie, bis der Scan „Bedrohungserkennung im Hintergrund“ abgeschlossen ist. Der Scan kann je nach Größe des Datenträgers und der Aktivität auf dem Image während des Scans mehrere Stunden dauern.
   c) Überprüfen Sie die Ergebnisse des Scans zur Bedrohungserkennung im Hintergrund und fügen Sie, falls erforderlich, auf dem Golden Image erkannte Binärdateien zu den Quarantäne- oder Sicherheitslisten von CylancePROTECT Desktop hinzu.
3. Löschen Sie auf dem Golden Image die Fingerabdruckwerte aus der Registrierung.
   a) Beenden Sie den CylanceSvc-Dienst. Lesen Sie auf support.blackberry.com den Artikel KB 107236.
   b) Verwenden Sie das lokale Administratorkonto, übernehmen Sie den Registrierungsschlüssel, und geben Sie der folgenden Registrierung die Berechtigungen für den Vollzugriff: `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`
   c) Sichern oder exportieren Sie die oben gezeigte Registrierung.
   d) Entfernen Sie die Registrierungsschlüssel FP, FPMask und FPVersion.
4. Erstellen Sie das Golden Image.

5. Erstellen Sie eine Geräterichtlinie, die für VDI-Produktions-Arbeitsstationen vorgesehen ist. BlackBerry empfiehlt die Verwendung der folgenden Optionen in der Richtlinie zusätzlich zu den Optionen, die Sie für Ihre Produktions-Workstations aktivieren möchten:

Geräterichtlinien-Kategorie	Optionen
Dateiaktionen	• Aktivieren Sie **Automatische Quarantäne mit Ausführungssteuerung** für unsichere und anormale Dateitypen. • Aktivieren Sie **Automatisches Hochladen**.
Schutzeinstellungen	• Aktvieren Sie **Auf neue Dateien überwachen**. • Deaktivieren Sie **Bedrohungserkennung im Hintergrund**.

6. Stellen Sie das Golden Image bereit, und klonen Sie es auf Produktions-Workstations. Jedes geklonte Image muss eine eindeutige UUID oder ID haben, die sich vom Golden Image unterscheidet.
7. Wenden Sie die Komponentenrichtlinie aus Schritt 5 auf die Produktions-Workstations an.

Wenn Sie fertig sind: Setzen Sie für die geklonten Geräte zonenbasierte Agent-Aktualisierungen auf **Nicht aktualisieren** oder auf eine bestimmte Version des Agenten. Updates sollten über das Golden Image gesteuert werden. Siehe Aktualisieren von CylancePROTECT Desktop auf geklonten Geräten.

Aktualisieren von CylancePROTECT Desktop auf geklonten Geräten

Bevor Sie beginnen: Bereitstellen von CylancePROTECT Desktop auf virtuellen Maschinen.

1. Aktualisieren Sie den CylancePROTECT Desktop-Agenten auf dem Golden Image.
2. Wenn zusätzliche Aktualisierungen oder Dateien auf das Golden Image angewendet werden, wenden Sie die Geräterichtlinie für die VDI-Vorbereitung auf das Golden Image an, und warten Sie, bis der Scan zur Bedrohungserkennung im Hintergrund abgeschlossen ist.
3. Überprüfen Sie die Ergebnisse des Scans zur Bedrohungserkennung im Hintergrund und fügen Sie, falls erforderlich, auf dem Golden Image erkannte Binärdateien zu den Quarantäne- oder Sicherheitslisten von CylancePROTECT Desktop hinzu.
4. Wenden Sie die Richtlinie für Produktionsgeräte auf das Golden Image an.
5. Versiegeln Sie das Golden Image wieder.
6. Überprüfen Sie, ob die Agent-Aktualisierung auf die geklonten Geräte propagiert wurde.

Rechtliche Hinweise

Patente, sofern zutreffend, zu finden unter: www.blackberry.com/patents.

Dieses Dokument und alle Dokumente, die per Verweis in dieses Dokument mit einbezogen werden, z. B. alle über die BlackBerry-Webseite erhältlichen Dokumente, werden ohne Mängelgewähr und je nach Verfügbarkeit bereitgestellt. Die entsprechenden Dokumente werden ohne ausdrückliche Billigung, Gewährleistung oder Garantie seitens BlackBerry Limited und seinen angegliederten Unternehmen („BlackBerry“) bereitgestellt. BlackBerry übernimmt keine Verantwortung für eventuelle typografische, technische oder anderweitige Ungenauigkeiten sowie für Fehler und Auslassungen in den genannten Dokumenten. Die BlackBerry-Technologie ist in dieser Dokumentation teilweise in verallgemeinerter Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von BlackBerry zu schützen. BlackBerry behält sich das Recht vor, die in diesem Dokument enthaltenen Informationen von Zeit zu Zeit zu ändern. BlackBerry ist jedoch nicht verpflichtet, die Benutzer über diese Änderungen, Updates, Verbesserungen oder Zusätze rechtzeitig bzw. überhaupt in Kenntnis zu setzen.

Diese Dokumentation enthält möglicherweise Verweise auf Informationsquellen, Hardware oder Software, Produkte oder Dienste, einschließlich Komponenten und Inhalte wie urheberrechtlich geschützte Inhalte und/oder Websites von Drittanbietern (nachfolgend „Drittprodukte und -dienste“ genannt). BlackBerry hat keinen Einfluss auf und übernimmt keine Haftung für Drittprodukte und -dienste, dies gilt u. a. für Inhalt, Genauigkeit, Einhaltung der Urheberrechtsgesetze, Kompatibilität, Leistung, Zuverlässigkeit, Rechtmäßigkeit, Angemessenheit, Links oder andere Aspekte der Drittprodukte und -dienste. Der Einschluss eines Verweises auf Drittprodukte und -dienste in dieser Dokumentation impliziert in keiner Weise eine besondere Empfehlung der Drittprodukte und -dienste oder des Drittanbieters durch BlackBerry.

SOFERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN HINSICHTLICH DER HALTBARKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER VERWENDUNGSZWECK, MARKTGÄNGIGKEIT, MARKTGÄNGIGEN QUALITÄT, NICHTVERLETZUNG VON RECHTEN DRITTER, ZUFRIEDENSTELLENDEN QUALITÄT ODER DES EIGENTUMSRECHTS ABGELEHNT. DIES GILT AUCH FÜR ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, DIE SICH AUS EINEM GESETZ, EINER GEPFLOGENHEIT, CHANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDEN LEISTUNG VON SOFTWARE, HARDWARE, DIENSTEN ODER DRITTPRODUKTEN UND -DIENSTEN STEHEN, AUF DIE HIER VERWIESEN WIRD. MÖGLICHERWEISE GELTEN FÜR SIE ZUDEM ANDERE LANDESSPEZIFISCHE RECHTE. IN MANCHEN RECHTSGEBIETEN IST DER AUSSCHLUSS ODER DIE EINSCHRÄNKUNG KONKLUDENTER GEWÄHRLEISTUNGEN UND BEDINGUNGEN NICHT ZULÄSSIG. IN DEM GESETZLICH ZULÄSSIGEN UMFANG WERDEN SÄMTLICHE KONKLUDENTEN GEWÄHRLEISTUNGEN ODER BEDINGUNGEN IM ZUSAMMENHANG MIT DER DOKUMENTATION, DIE EINGESCHRÄNKT WERDEN KÖNNEN, SOFERN SIE NICHT WIE OBEN DARGELEGT AUSGESCHLOSSEN WERDEN KÖNNEN, HIERMIT AUF 90 TAGE AB DATUM DES ERWERBS DER DOKUMENTATION ODER DES ARTIKELS, AUF DEN SICH DIE FORDERUNG BEZIEHT, BESCHRÄNKT.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS HAFTET BLACKBERRY UNTER KEINEN UMSTÄNDEN FÜR SCHÄDEN JEGLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEGLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTE UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE,

VERSCHÄRFTEN SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIREKTE, KONKRETE, STRAFE EINSCHLIESSENDE SCHÄDEN, FOLGESCHÄDEN ODER SCHÄDEN, FÜR DIE ANSPRUCH AUF KOMPENSATORISCHEN SCHADENERSATZ BESTEHT, SCHÄDEN WEGEN ENTGANGENEN GEWINNEN ODER EINKOMMEN, NICHTREALISIERUNG ERWARTETER EINSPARUNGEN, BETRIEBSUNTERBRECHUNGEN, VERLUST GESCHÄFTLICHER DATEN, ENTGANGENE GESCHÄFTSCHANCEN ODER BESCHÄDIGUNG BZW. VERLUST VON DATEN, DAS UNVERMÖGEN, DATEN ZU ÜBERTRAGEN ODER ZU EMPFANGEN, PROBLEME IM ZUSAMMENHANG MIT ANWENDUNGEN, DIE IN VERBINDUNG MIT BLACKBERRY-PRODUKTEN UND -DIENSTEN VERWENDET WERDEN, KOSTEN VON AUSFALLZEITEN, NICHTVERWENDBARKEIT VON BLACKBERRY-PRODUKTEN UND -DIENSTEN ODER TEILEN DAVON BZW. VON MOBILFUNKDIENSTEN, KOSTEN VON ERSATZGÜTERN, DECKUNG, EINRICHTUNGEN ODER DIENSTEN, KAPITAL- ODER ANDERE VERMÖGENSSCHÄDEN, UNABHÄNGIG DAVON, OB SCHÄDEN DIESER ART ABZUSEHEN ODER NICHT ABZUSEHEN WAREN, UND AUCH DANN, WENN BLACKBERRY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS ÜBERNIMMT BLACKBERRY KEINERLEI VERANTWORTUNG, VERPFLICHTUNG ODER HAFTUNG, SEI SIE VERTRAGLICHER, DELIKTRECHTLICHER ODER ANDERWEITIGER NATUR, EINSCHLIESSLICH DER HAFTUNG FÜR FAHRLÄSSIGKEIT UND DER DELIKTSHAFTUNG.

DIE IN DIESEM DOKUMENT GENANNTEN EINSCHRÄNKUNGEN, AUSSCHLÜSSE UND HAFTUNGSAUSSCHLÜSSE GELTEN (A) UNGEACHTET DER VON IHNEN ANGEFÜHRTEN KLAGEGRÜNDE, FORDERUNGEN ODER KLAGEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF VERTRAGSBRUCH, FAHRLÄSSIGKEIT, ZIVILRECHTLICHER DELIKTE, DELIKTSHAFTUNG ODER SONSTIGE RECHTSTHEORIE UND SIND AUCH NACH EINEM WESENTLICHEN VERSTOSS BZW. EINEM FEHLENDEN GRUNDLEGENDEN ZWECK DIESER VEREINBARUNG ODER EINES DARIN ENTHALTENEN RECHTSBEHELFS WIRKSAM; UND GELTEN (B) FÜR BLACKBERRY UND DIE ZUGEHÖRIGEN UNTERNEHMEN, RECHTSNACHFOLGER, BEVOLLMÄCHTIGTEN, VERTRETER, LIEFERANTEN (EINSCHLIESSLICH MOBILFUNKANBIETERN), AUTORISIERTE BLACKBERRY-DISTRIBUTOREN (EBENFALLS EINSCHLIESSLICH MOBILFUNKANBIETERN) UND DIE JEWEILIGEN FÜHRUNGSKRÄFTE, ANGESTELLTEN UND UNABHÄNGIGEN AUFTRAGNEHMER.

ZUSÄTZLICH ZU DEN OBEN GENANNTEN EINSCHRÄNKUNGEN UND AUSSCHLÜSSEN HAFTEN DIE FÜHRUNGSKRÄFTE, ANGESTELLTEN, VERTRETER, DISTRIBUTOREN, LIEFERANTEN, UNABHÄNGIGEN AUFTRAGNEHMER VON BLACKBERRY ODER BLACKBERRY ANGEHÖRENDEN UNTERNEHMEN IN KEINER WEISE IM ZUSAMMENHANG MIT DER DOKUMENTATION.

Bevor Sie Drittprodukte bzw. -dienste abonnieren, installieren oder verwenden, müssen Sie sicherstellen, dass Ihr Mobilfunkanbieter sich mit der Unterstützung aller zugehörigen Funktionen einverstanden erklärt hat. Einige Mobilfunkanbieter bieten möglicherweise keine Internet-Browsing-Funktion in Zusammenhang mit einem Abonnement für den BlackBerry® Internet Service an. Erkundigen Sie sich bei Ihrem Dienstanbieter bezüglich Verfügbarkeit, Roaming-Vereinbarungen, Mobilfunktarifen und Funktionen. Für die Installation oder Verwendung von Drittprodukten und -diensten mit den Produkten und Diensten von BlackBerry sind u. U. Patent-, Marken-, Urheberrechts- oder sonstige Lizenzen erforderlich, damit die Rechte Dritter nicht verletzt werden. Es liegt in Ihrer Verantwortung, zu entscheiden, ob Sie Drittprodukte und -dienste verwenden möchten, und festzustellen, ob hierfür Lizenzen erforderlich sind. Für den Erwerb etwaiger Lizenzen sind Sie verantwortlich. Installieren oder verwenden Sie Drittprodukte und -dienste erst nach dem Erwerb aller erforderlichen Lizenzen. Alle Drittprodukte und -dienste, die Sie mit Produkten und Diensten von BlackBerry erhalten, werden lediglich zu Ihrem Vorteil, OHNE MÄNGELGEWÄHR und ohne ausdrückliche oder stillschweigende Bedingung, Billigung, Garantie, Zusicherung oder Gewährleistung jedweder Art von BlackBerry bereitgestellt. BlackBerry übernimmt in diesem Zusammenhang keinerlei Haftung. Die Verwendung von Drittprodukten und -diensten unterliegt Ihrer Zustimmung zu den Bedingungen separater Lizenzen und anderer geltender Vereinbarungen mit Dritten, sofern sie nicht ausdrücklich von einer Lizenz oder anderen Vereinbarung mit BlackBerry abgedeckt wird.

Die Nutzungsbedingungen für BlackBerry-Produkte und -Dienste werden in einer entsprechenden separaten Lizenz oder anderen Vereinbarung mit BlackBerry dargelegt. KEINE PASSAGE IN DIESEM DOKUMENT IST DAZU VORGESEHEN, BELIEBIGE SCHRIFTLICHE VEREINBARUNGEN ODER GARANTIEN, DIE VON BLACKBERRY FÜR TEILE VON BELIEBIGEN BLACKBERRY-PRODUKTEN ODER -DIENSTLEISTUNGEN AN ANDERER STELLE ALS IN DIESER DOKUMENTATION ANGEGEBEN WURDEN, ZU ERSETZEN.

BlackBerry Enterprise Software enthält bestimmte Softwarekomponenten von Drittanbietern. Die mit der Software verbundenen Lizenz- und Copyright-Informationen finden Sie unter: http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

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

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

Veröffentlicht in Kanada