Cylance Endpoint Security

セットアップガイド

Contents

Cylance Endpoint Security の要件

Cylance Endpoint Security のセットアップを開始するには、このセクションを確認し、組織の環境がソリューションの機能とコンポーネントの要件を満たしていることを確認します。

要件：Cylance コンソール

項目	要件
サポートされるブラウザー	最新バージョン： • Google Chrome（推奨） • Microsoft Edge • Mozilla Firefox メモ：Firefox を使用して管理コンソールにアクセスしている場合は、プライベートブラウザーモードを使用しないでください。また、［Firefox を閉じたときに Cookie とサイトデータを削除する］を有効にしたり、サービスワーカーを無効にしたりしないでください。これらのいずれの設定でも、コンソールの一部の画面が期待どおりにロードされない場合があります。
サポートされている言語	ブラウザを次のサポートされている言語のいずれかに設定します。 • 英語 • フランス語 • ドイツ語 • イタリア語 • 日本語 • 韓国語 • ポルトガル語 • スペイン語

要件：CylancePROTECT Desktop

CylancePROTECT Desktop の各エージェントがサポートするオペレーティングシステムについては、「Cylance Endpoint Security の互換性マトリックス」を参照してください。BlackBerry のすべての製品のサポートタイムラインを表示するには、「BlackBerry エンタープライズソフトウェアのライフサイクルリファレンスガイド」を参照してください。

次の表に、サポート対象オペレーティングシステムを、追加の要件または考慮事項とともに示します。これらの表は、サポート対象オペレーティングシステムの包括的なリストではないことに注意してください。表にオペレーティングシステムが記載されていない場合は、追加の要件も考慮事項もないということです。

Windows OS

サポートされる OS	要件
サポート対象のすべての Windows OS バージョン	• .NET Framework 4.6.2 以降 • TLS 1.2 • 仮想マシンの要件、展開ガイダンス、およびベストプラクティスについては、「付録：Windows 仮想マシンに CylancePROTECT Desktop を展開するためのベストプラクティス」を参照してください。 • CylancePROTECT Desktop は、Microsoft OneDrive からの未溶解ファイルのスキャンはサポートしていません。 • 最新の Windows セキュリティ更新プログラムがデバイスにインストールされていることを確認してから、CylancePROTECT Desktop エージェントをインストールまたはアップグレードします。
Windows 11（64 ビット）	• 大文字と小文字を区別するファイルシステムはサポートされていません。 • Windows 11 マルチセッションは現在サポートされていません。
Windows 10 （32 ビット、64 ビット）	• 大文字と小文字を区別するファイルシステムはサポートされていません。 • Windows 10 マルチセッションは現在サポートされていません。 • Windows 10 （v1809、October 2018 Update） ：統合書き込みフィルター（UWF）はサポートされていません。エージェントをインストールする前に、UWF を無効にしてください。
Windows 7 （32 ビット、64 ビット）	• Embedded Standard 7 および Embedded POSReady 7 がサポートされています。 • エージェントに必要なルート証明書をインストールします。

Windows Server 2022（64 ビット）	• Standard、Data Center、および Core エディションがサポートされています。
	• Data Center エディションでは、エージェントで以下はサポートされていません。
	  • Shielded 仮想マシン用 Hyper-V Server のロール
	  • Host Guardian Hyper-V のサポート
	  • ソフトウェア定義ネットワーク
	  • 記憶域スペースダイレクト
	• Storage Server 2022 はサポートされていません。

サポートされる OS	要件

Windows Server 2019（64 ビット）	• Standard、Data Center、および Core エディションがサポートされています。
	• Data Center エディションでは、エージェントで以下はサポートされていません。
	  • Shielded 仮想マシン用 Hyper-V Server のロール
	  • Host Guardian Hyper-V のサポート
	  • ソフトウェア定義ネットワーク
	  • 記憶域スペースダイレクト
	• Storage Server 2019 はサポートされていません。

Windows Server 2016（64 ビット）	• Standard、Data Center、Essentials および Server Core エディションがサポートされています。 • Nano Server および Storage Server はサポートされていません。
Windows Server 2012 および 2012 R2（64 ビット）	• Standard、Data Center、Essentials、Server Core、Embedded および Foundation エディションがサポートされています。 • Minimal Server Interface および Storage Server はサポートされていません。

macOS

サポートされる OS	要件

サポート対象のすべての macOS バージョン	• TLS 1.2
	• 次のルート証明書インストールされていることを確認します。ルート証明書がない場合は、エージェントが起動しないか、デバイスが管理コンソールと通信できない可能性があります。詳細については、「KB 66608」を参照してください。
	  • VeriSign Class 3 Public Primary Certification Authority - G5（VeriSign クラス 3 パブリックプライマリ認証局 - G5）
	  • Thawte Primary Root CA（Thawte プライマリルート CA）
	  • DigiCert Global Root（DigiCert グローバルルート）
	• 仮想マシンの要件、展開ガイダンス、およびベストプラクティスについては、「付録：Windows 仮想マシンに CylancePROTECT Desktop を展開するためのベストプラクティス」を参照してください。
	• 大文字と小文字を区別するボリューム形式はサポートされていません。

サポートされる **OS**	要件
macOS Sonoma（14）	• 「KB 66578」を参照してください。 • フルディスクアクセスを有効にします。フルディスクアクセスが有効になっていないと、CylancePROTECT Desktop は、ユーザーデータ保護によって保護されたファイルを処理できません。詳細については、「KB 66427」を参照してください。 • 「macOS インストールのトラブルシューティング」を参照してください。 • メモリ保護違反は、メモリのリモート割り当て、メモリのリモートマッピング、メモリへのリモート書き込み、メモリのリモートマップ解除がサポートされています。Sonoma では、その他のメモリ保護違反はサポートされていません。
macOS Monterey（12）	• 「KB 66578」を参照してください。 • フルディスクアクセスを有効にします。フルディスクアクセスが有効になっていないと、CylancePROTECT Desktop は、ユーザーデータ保護によって保護されたファイルを処理できません。詳細については、「KB66427」を参照してください。 • 「macOS インストールのトラブルシューティング」を参照してください。 • メモリ保護違反は、メモリのリモート割り当て、メモリのリモートマッピング、メモリへのリモート書き込み、メモリのリモートマップ解除がサポートされています。Monterey では、その他のメモリ保護違反はサポートされていません。
macOS Big Sur（11）	• 「KB 66578」を参照してください。 • フルディスクアクセスを有効にします。フルディスクアクセスが有効になっていないと、CylancePROTECT Desktop は、ユーザーデータ保護によって保護されたファイルを処理できません。詳細については、「KB 66427」を参照してください。 • 「macOS インストールのトラブルシューティング」を参照してください。 • メモリ保護違反は、メモリのリモート割り当て、メモリのリモートマッピング、メモリへのリモート書き込み、メモリのリモートマップ解除がサポートされています。Big Sur では、その他のメモリ保護違反はサポートされていません。

Linux OS

サポートされる OS	要件

サポート対象のすべての Linux OS バージョン	• インターネット接続が必要です。デバイスがこの要件を満たしていない場合は、代わりに CylanceON-PREM ソリューションを検討してください。
	• 「サポートされている Linux カーネルスプレッドシート」を参照してください。
	• TLS 1.2
	• 必要なパッケージ：
	  • `bzip2(x86-64)`
	  • `dbus-libs`（RHEL/CentOS 7.x または 8.x の場合、バージョン 1.10.24 以降が必要）
	  • `glibc`
	  • `gtk3`（RHEL/CentOS の場合）
	  • `libgcc`
	  • `openssl`（RHEL/CentOS 6.x の場合）
	  • `openssl-libs`（RHEL/CentOS 7.x の場合）
	  • `sqlite`
	• ルート証明書：
	  • VeriSign Class 3 Public Primary Certification Authority - G5（VeriSign クラス 3 パブリックプライマリ認証局 - G5）
	  • Thawte Primary Root CA（Thawte プライマリルート CA）
	  • DigiCert Global Root（DigiCert グローバルルート）
	• 2.1.1590 エージェントでサポートされている GNOME バージョン：
	  • 3.28
	  • 3.20
	  • 3.14
	  • 3.10
	  • 3.8
	• 仮想マシンはサポートされています。

Ubuntu 22.04 LTS（64 ビット） Ubuntu 20.04 LTS（64 ビット） Ubuntu 20.04（64 ビット） Ubuntu 18.04（64 ビット）	• Azure Ubuntu カーネルはサポートされていません。 • UEFI セキュアブートをサポートするために CylancePROTECT Desktop セキュアブート CA 証明書を使用します。詳細については、「KB 73487」を参照してください。

サポートされる OS	要件
Red Hat Enterprise Linux 9（64 ビット） Red Hat Enterprise Linux/CentOS 8（64 ビット） Red Hat Enterprise Linux/CentOS 7（64 ビット）	• UEFI セキュアブートをサポートするために CylancePROTECT Desktop セキュアブート CA 証明書を使用します。詳細については、「KB 73487」を参照してください。 • FIPS がサポートされています。FIPS を有効にする手順については、使用している OS に対応する Red Hat のドキュメントを参照してください。

CylancePROTECT Desktop とその他のウイルス対策ソフトウェアの併用

CylancePROTECT Desktop とともに、サードパーティ製のウイルス対策ソフトウェアがデバイスにインストールされている場合、これらの製品が CylancePROTECT Desktop の機能に干渉しないように、追加の設定タスクが必要とされることがあります。詳細については、「KB 66448」を参照してください。

ハードウェア要件

ハードウェアコンポーネント	要件
プロセッサ（CPU）	以下の要件も満たす 2 つ以上のプロセッサコア： • SSE2 命令セットをサポートする • x86_64 命令セットをサポートする • M1、M2、M3 など、Apple シリコンプロセッサをサポートする。Rosetta が必要 • Windows および Linux の ARM 命令セットはサポートしない
メモリ（RAM）	2GB
ディスク容量（ハードドライブ）	• 600MB • 有効になっている機能（ログレベルを詳細に設定するなど）に応じて、ディスク容量の使用率が増加する場合があります。

Windows 用 CylancePROTECT Desktop エージェントに必要なルート証明書

Windows の一部のバージョンでは、CylancePROTECT Desktop エージェントに次のルート証明書が必要です（「要件：CylancePROTECT Desktop」を参照）。ルート証明書がない場合、エージェントが起動しないか、デバイスが管理コンソールと通信できない可能性があります。ルート証明書の詳細については、「KB66608」を参照してください。

- Thawte Primary Root CA（Thawte プライマリルート CA）
- Thawte Timestamping CA（Thawte タイムスタンプ CA）
- Thawte Primary Root CA - G3（Thawte プライマリルート CA-G3）
- Microsoft Root Certificate Authority 2010（Microsoft ルート認証局 2010）
- Microsoft Root Certificate Authority 2020（Microsoft ルート認証局 2020）
- UTN-USERFirst-Object（UTN-USERFirst- オブジェクト）

- VeriSign Universal Root Certification Authority（VeriSign ユニバーサルルート認証局）
- DigiCert High Assurance EV Root CA（DigiCert 高保証 EV ルート CA）
- GlobalSign Root CA（GlobalSign ルート CA）
- USERTrust RSA Certification Authority（USERTrust RSA 認証局）
- DigiCert Assured ID Root CA（DigiCert 保証 ID ルート CA）
- VeriSign Class 3 Public Primary Certification Authority - G5（VeriSign クラス 3 パブリックプライマリ認証局 - G5）
- DigiCert Global Root CA（DigiCert グローバルルート CA）
- Starfield Class 2 Certification Authority（Starfield クラス 2 認証局）

詳細については、以下のリソースを参照してください。

- Thawte ルート証明書
- PKI リポジトリ - Microsoft PKI サービス
- 信頼された署名 (旧称 Azure Code Signing) プログラムに対する Windows サポート。詳細については、「KB 140264」を参照してください。
- DigiCert ルートおよび中間
- DigiCert 信頼された root 権限証明書
- GlobalSign ルート証明書
- Sectigo 中間証明書のダウンロードとインストール方法 - RSA
- VeriSign クラス 3 パブリックプライマリ認証局 - G5 ルート証明書

要件：CylanceOPTICS

エージェント

エージェント	要件

CylancePROTECT Desktop エージェント	• CylanceOPTICS エージェントをインストールする前に、デバイスに CylancePROTECT Desktop エージェントをインストールする必要があります。CylanceOPTICS エージェントでは、CylancePROTECT Desktop エージェントが機能している必要があります。
	• BlackBerry では、最新の機能や修正を利用できるよう、利用可能な最新バージョンの CylancePROTECT Desktop エージェントをインストールすることを推奨しています。
	• CylanceOPTICS エージェントバージョン 3.3 では 、CylancePROTECT Desktop エージェントの最小必要バージョンは 3.1.x です。CylanceOPTICS 3.3で導入された新しい Windows センサを使用する場合、Windows の CylancePROTECT Desktop エージェントに必要な最小バージョンは 3.2.x です。
	• CylanceOPTICS エージェントのバージョン 3.2 および 3.1 には、次の最小バージョンの CylancePROTECT Desktop エージェントが必要です。
	  • Windows：2.1.1578.x
	  • macOS：3.0.1000.x
	  • Linux：2.1.1590.x
	• 「CylancePROTECT Desktop 互換性マトリックス」および「CylancePROTECT Desktop の要件」を確認して、サポート対象の CylancePROTECT Desktop エージェントをインストールし、他のすべての要件を満たしていることを確認します。

エージェント	要件
CylanceOPTICS エージェント	• BlackBerry は、各デバイスに利用可能な最新バージョンの CylanceOPTICS エージェントをインストールすることをお勧めします。 • 収集したデータを CylanceOPTICS クラウドデータベースに自動保存するには、CylanceOPTICS エージェントのバージョン 3.x が必要です。以前のバージョンのエージェントは、CylanceOPTICS データをデバイスのローカルデータベースに保存します。 • エージェント 3.x では、CylanceOPTICS センサで収集されたデータは、CylanceOPTICS クラウドデータベースに送信される前にローカルにキャッシュされます。デバイスがオフラインの場合、デバイスがクラウドデータベースに接続できるまでデータがキャッシュされます。最大 1GB のデータをローカルに保存できます。アップロードする前に 1GB を超えるデータが保存されている場合は、優先度の低いデータが削除され、優先度の高いデータがキャッシュされます。 • CylanceOPTICS エージェント 2.x から 3.x にアップグレードする場合の考慮事項については、Cylance Endpoint Security のリリースノートを参照してください • バージョン 2.x から 3.x にアップグレードすると、CylanceOPTICS ローカルデータベースの全内容がバッチでクラウドデータベースにアップロードされます。 • バージョン 3.x にアップグレードした後、エージェントをバージョン 2.x にダウングレードすることはできません。バージョン 2.x をインストールする場合は、バージョン 3.x をアンインストールしてから、バージョン 2.x をインストールする必要があります。

OS のサポートと追加の要件

CylanceOPTICS がサポートするオペレーティングシステムの詳細については、「Cylance Endpoint Security の互換性マトリックス」を参照してください。BlackBerry のすべての製品のサポートタイムラインを表示するには、『BlackBerry Enterprise Software ライフサイクルリファレンスガイド』を参照してください。

次の表に、サポート対象オペレーティングシステムを、追加の要件または考慮事項とともに示します。この表は、サポート対象オペレーティングシステムの包括的なリストではないことに注意してください。表にオペレーティングシステムが記載されていない場合は、追加の要件も考慮事項もないということです。

OS	要件または考慮事項
Windows オペレーティングシステム	
Windows 8.1 Windows 7 SP1	.NetCore サポートのその他の依存関係については、この Microsoft の記事を参照してください。
macOS オペレーティングシステム	

OS	要件または考慮事項
macOS Sonoma（14.x） macOS Ventura（13.x） macOS Monterey（12.x） macOS Big Sur（11.x）	• フルディスクアクセスを有効にします。詳細については、「KB 66427」を参照してください。 • 「macOS 11.x 以降の構成要件」を参照してください。
macOS Catalina（10.15）	フルディスクアクセスを有効にします。詳細については、「KB 66427」を参照してください。
Linux オペレーティングシステム	
サポートされているすべての Linux システム	• kernel-headers と kernel-devel が必要で、実行中のカーネルとバージョンが一致する必要があります。必要なバージョンは、インストール中にパッケージマネージャで示されます。サポートされている Ubuntu システムおよび Debian システムでは、linux-headers は kernel-headers に相当します。 • eBPF、Netlink（マルチキャスト Netlink ソケットサポート 3.16 以降、または監査デーモンがアンインストールされた場合）、または Auditdsp（auditd および auditdsp プラグインを起動時に起動する）のいずれかの Linux センサスイートが必要です。CylanceOPTICS エージェントで最高のパフォーマンスを得るには、eBPF をお勧めします。eBPF が使用できない場合、エージェントは Netlink を使用して、次の最高レベルのパフォーマンスを実現しようとします。Netlink が使用できない場合、エージェントは Auditdsp の使用を試みます。使用可能なセンサスイートは、OS のバージョンによって異なります。
RHEL/CentOS 8.x RHEL/CentOS 7.x	• RHEL/CentOS 8.x では、デバイスでバージョン 3.2.1140-x 以降の CylanceOPTICS エージェントが実行されている場合を除き、ncurses-compat-libs が必要です。 • ロックダウンデバイス機能をサポートするには、Firewalld が有効で実行されている必要があります。Firewalld は、RHEL/CentOS でデフォルトで使用できます。
Amazon Linux 2	• デバイスでバージョン 3.2.1140-15000 以降の CylanceOPTICS エージェントが実行されている場合を除き、ncurses-compat-libs が必要です。 • ロックダウンデバイス機能をサポートするには、Firewalld が有効で実行されている必要があります。Firewalld は Amazon Linux 2 に手動でインストールする必要があります。

OS	要件または考慮事項
Oracle Linux サーバー UEK 8（64 ビット） Oracle Linux サーバー 8（64 ビット） Oracle Linux サーバー 7（64 ビット） Oracle Linux サーバー UEK 7（64 ビット）	• デバイスでバージョン 3.2.1140-37000 以降の CylanceOPTICS エージェントが実行されている場合を除き、ncurses-compat-libs が必要です。 • ロックダウンデバイス機能をサポートするには、Firewalld が有効で実行されている必要があります。Firewalld は、Oracle Linux でデフォルトで使用できます。
Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04	• Ubuntu 20.04 では、デバイスでバージョン 3.2.1140-x 以降の CylanceOPTICS エージェントが実行されている場合を除き、libtinfo5 が必要です。 • ロックダウンデバイス機能をサポートするには、Firewalld が有効で実行されている必要があります。Firewalld は、Ubuntu では手動でインストールする必要があります。
SUSE Enterprise Linux 15 SP4 SUSE Enterprise Linux 15 SUSE Enterprise Linux 12	• policycoreutils が必要です。 • SUSE 15.x では、kernel-default-devel がカーネルに一致する必要があります。また、デバイスでバージョン 3.2.1140-29000 以降の CylanceOPTICS エージェントが実行されている場合を除き、libncurses5 も必要です。 • SUSE 15.x でロックダウンデバイス機能をサポートするには、Firewalld が有効で実行されている必要があります。Firewalld は、SUSE 15.x でデフォルトで使用できます。ロックダウンデバイス機能は SUSE 12 ではサポートされていません。
Debian 11 Debian 10	• Debian 10 デバイスでロックダウンデバイス機能をサポートするには、iptables 1.8.5 以降が必要です。 • ロックダウンデバイス機能をサポートするには、Firewalld が有効で実行されている必要があります。Firewalld は、Debian では手動でインストールする必要があります。

他の **EDR** ソリューションとの互換性

CylanceOPTICS エージェントは、同じデバイスにインストールされている他の EDR（Endpoint Detection and Response）ソリューションと互換性がありません。CylanceOPTICS エージェントをインストールして有効にする前に、サードパーティの EDR ソリューションはすべてデバイスから削除してください。

ハードウェア

項目	要件
プロセッサ（CPU）	• 一般的な使用では、追加 CPU は 1% • 負荷の高いワークロードでは、ワークロードに応じてさらに 5〜25% の CPU バーストが必要です

項目	要件
メモリ（RAM）	エージェントには、ワークロードに応じて 0.2〜1.0GB の追加メモリが必要です。
ディスク容量（ハードドライブ）	最小 1GB • CylanceOPTICS エージェント 2.x 以前の場合、ローカルデータベースには最低 1GB が必要です。 • CylanceOPTICS 3.0 以降では、デバイスがオンライン時に CylanceOPTICS クラウドデータベースにデータをアップロードする前に、CylanceOPTICS センサデータをキャッシュするのに最低 1GB が推奨されます。

仮想マシン

CylanceOPTICS は、仮想マシンでサポートされています。要件、展開ガイダンス、およびベストプラクティスについては、「付録：Windows 仮想マシンに CylancePROTECT Desktop を展開するためのベストプラクティス」を参照してください。仮想マシンで CylanceOPTICS を使用する場合、BlackBerry は、「高度な WMI の可視性」センサを無効にして、記録されたイベントの数を減らすことをお勧めします。

要件：CylancePROTECT Mobile アプリ

項目	説明
OS	「Cylance Endpoint Security の互換性マトリックス」を参照してください。
サポートされるデバイスブラウザー	最新バージョン： • Android：Google Chrome、Samsung、Firefox、Brave • iOS：Safari
デバイス設定	• デフォルトのモバイルブラウザーで JavaScript を有効にするようユーザーに指示します。これは CylancePROTECT Mobile アプリをアクティブ化するために必要です。 • アプリをインストールした後で CylancePROTECT Mobile のバックグラウンドアクティビティを許可するよう Android ユーザーに指示します。

要件：BlackBerry Connectivity Node

ソフトウェア

項目	説明
Java Runtime Environment	JRE 17（最新の更新バージョン、64 ビット）

ハードウェア

コンポーネント	**BlackBerry Connectivity Node**
プロセッサ（CPU）	6 プロセッサコア、E5-2670（2.6 GHz）、E5-2683 v4（2.1 GHz）、または同等
メモリ（RAM）	12GB
ディスク容量（ハードドライブ）	64GB

その他の **BlackBerry Connectivity Node** 要件

- BlackBerry Connectivity Node が会社のディレクトリへのアクセスに利用できるように、構成済みのディレクトリ接続ごとに読み取り権限があるディレクトリアカウントを選択してください。
- BlackBerry Connectivity Node をホストするコンピューターで、ソフトウェアをインストールして設定できるように、権限がある Windows アカウントを使用します。
- BlackBerry Connectivity Node コンポーネントが BlackBerry Infrastructure（<*region*>.bbsecure.com、例：ca.bbsecure.com）と通信できるように、組織のファイアウォールで次のアウトバウンドポートが開いていることを確認します。
  - BlackBerry Connectivity Node をアクティブ化する場合は 443（HTTPS）
  - その他のすべてのアウトバウンド接続の場合は 3101（TCP）
- Microsoft でサポートされているバージョンの Windows Server にソフトウェアをインストールします。
- BlackBerry Connectivity Node を英語、フランス語、スペイン語、日本語、またはドイツ語のオペレーティングシステムでインストールできます。

要件：CylanceGATEWAY コネクタ

ハードウェア

コンポーネント	**CylanceGATEWAY Connector**
プロセッサ（CPU）	2 つのプロセッサコア

コンポーネント	CylanceGATEWAY Connector
メモリ（RAM）	5GB
ディスク容量（ハードドライブ）	2GB

AWS

項目	説明
インスタンスタイプ	BlackBerry では、実稼働環境で c6in または c5n のインスタンスタイプをお勧めします。

要件：CylanceGATEWAY エージェント

モバイルユーザーに対して CylanceGATEWAY 機能を有効にしている場合、ユーザーは CylancePROTECT Mobile アプリから仕事モードを有効にできます。CylancePROTECT Mobile の要件については、「要件：CylancePROTECT Mobile アプリ」を参照してください。

項目	要件
プロセッサ（CPU）	• Rosetta 2 を介した Apple シリコンデバイスを含む、すべての Apple デバイスをサポートしていること • すべての x64 ベースのプロセッサをサポートしていること • 32 ビットオペレーティングシステムをサポートしていないこと • ARM デバイスをサポートしていないこと
OS	CylanceGATEWAY エージェントがサポートするオペレーティングシステムについては、Cylance Endpoint Security compatibility matrix（Cylance Endpoint Security 互換性一覧表）を参照してください。BlackBerry のすべての製品のサポートタイムラインを表示するには、『BlackBerry Enterprise Software ライフサイクルリファレンスガイド』を参照してください。

要件：CylanceAVERT

項目	説明
CylanceAVERT エージェント	CylanceAVERT は、バンドルされたインストーラです。CylanceAVERT Microsoft Outlook プラグインや、Chrome、Firefox、Microsoft Edge のブラウザ拡張機能を備えています。
CylancePROTECT Desktop エージェント	CylancePROTECT Desktop エージェントバージョン 3.1 以降

項目	説明
OS および Microsoft Outlook のサポート	CylanceOPTICS がサポートするオペレーティングシステムや Microsoft Outlook のバージョンに関する詳細については、「Cylance Endpoint Security の互換性マトリックス」を参照してください。BlackBerry のすべての製品のサポートタイムラインを表示するには、『BlackBerry Enterprise Software ライフサイクルリファレンスガイド』を参照してください。
.NET	• Microsoft .NET 4.6.2 以降 • .NET Standard 2.0 以降
Microsoft Visual C++	Microsoft Visual C++ 2017 再頒布可能パッケージ以降

Cylance Endpoint Security ネットワーク要件

Cylance Endpoint Security エージェント

Cylance Endpoint Security デスクトップエージェントが管理コンソールと通信するには、ポート 443（HTTPS）が開いている必要があります。

このエージェントは、セキュア Web ソケット（WSS）経由で通信し、この接続を直接確立できる必要があります。次のドメインへの接続を許可するように組織のネットワークを構成します。

メモ：

- 管理コンソールは AWS によってホストされており、固定 IP アドレスはありません。HTTPS トラフィックを *.cylance.com に許可できます。cylance-optics-files-use1.s3.amazonaws.com ホスト（および他の地域の類似ホスト）の場合は、その特定のホストを許可することをお勧めします。*.amazonaws.com は他のホストにネットワークを開くことができるため、許可しないことをお勧めします。
- ドメイン api2.cylance.com は推奨されませんが、古い CylancePROTECT Desktop エージェントをサポートするために開いたままになっています。api2.cylance.com は、脅威分析とリスクスコアリングの目的で、api.cylance.com と同じ宛先に転送します。

項目	説明
北米	Cylance コンソールへのログインに必要： • login.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com

項目	説明
	CylancePROTECT Desktop が通信を必要とするドメイン： • data.cylance.com • protect.cylance.com • update.cylance.com • api.cylance.com • download.cylance.com • venueapi.cylance.com
	CylanceOPTICS が通信を必要とするドメイン： • 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
	CylanceGATEWAY エージェントが通信を必要とするドメイン： • idp.blackberry.com • quip.webapps.blackberry.com • us1.cs.blackberry.com CylanceGATEWAY Connector: deb.nodesource.com に必要 CylanceGATEWAY エージェントと CylanceGATEWAY Connector: us1.bg.blackberry.com に必要 詳細については、「KB79017」を参照してください。
北東アジア	Cylance コンソールへのログインに必要： • login-apne1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com
	CylancePROTECT Desktop が通信を必要とするドメイン： • data-apne1.cylance.com • protect-apne1.cylance.com • update-apne1.cylance.com • api.cylance.com • download.cylance.com • venueapi-apne1.cylance.com

項目	説明
	CylanceOPTICS が通信を必要とするドメイン： • 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
	CylanceGATEWAY エージェントが通信を必要とするドメイン： • idp.blackberry.com • quip.webapps.blackberry.com • jp1.cs.blackberry.com CylanceGATEWAY Connector: deb.nodesource.com に必要 CylanceGATEWAY エージェントと CylanceGATEWAY Connector: jp1.bg.blackberry.com に必要 詳細については、「KB79017」を参照してください。
東南アジア	Cylance コンソールへのログインに必要： • login-au.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com
	CylancePROTECT Desktop が通信を必要とするドメイン： • data-au.cylance.com • protect-au.cylance.com • update-au.cylance.com • api.cylance.com • download.cylance.com • venueapi-au.cylance.com
	CylanceOPTICS が通信を必要とするドメイン： • 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

項目	説明
	CylanceGATEWAY エージェントが通信を必要とするドメイン： • idp.blackberry.com • quip.webapps.blackberry.com • au1.cs.blackberry.com CylanceGATEWAY Connector: deb.nodesource.com に必要 CylanceGATEWAY エージェントと CylanceGATEWAY Connector: au1.bg.blackberry.com に必要 詳細については、「KB79017」を参照してください。
中央ヨーロッパ	Cylance コンソールへのログインに必要： • login-euc1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com
	CylancePROTECT Desktop が通信を必要とするドメイン： • data-euc1.cylance.com • protect-euc1.cylance.com • update-euc1.cylance.com • api.cylance.com • download.cylance.com • venueapi-euc1.cylance.com
	CylanceOPTICS が通信を必要とするドメイン： • 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
	CylanceGATEWAY エージェントが通信を必要とするドメイン： • idp.blackberry.com • quip.webapps.blackberry.com • eu1.cs.blackberry.com CylanceGATEWAY Connector: deb.nodesource.com に必要 CylanceGATEWAY エージェントと CylanceGATEWAY Connector: eu1.bg.blackberry.com に必要 詳細については、「KB79017」を参照してください。

項目	説明
南米	Cylance コンソールへのログインに必要： • login-sae1.cylance.com • idp.blackberry.com • cdn.cylance.com • idp.cs.cylance.com
	CylancePROTECT Desktop が通信を必要とするドメイン： • data-sae1.cylance.com • protect-sae1.cylance.com • update-sae1.cylance.com • api.cylance.com • download.cylance.com • venueapi-sae1.cylance.com
	CylanceOPTICS が通信を必要とするドメイン： • 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
	CylanceGATEWAY エージェントが通信を必要とするドメイン： • idp.blackberry.com • quip.webapps.blackberry.com • br1.cs.blackberry.com CylanceGATEWAY Connector: deb.nodesource.com に必要 CylanceGATEWAY エージェントと CylanceGATEWAY Connector: br1.bg.blackberry.com に必要 詳細については、「KB79017」を参照してください。
GovCloud	Cylance コンソールへのログインに必要： • login.us.cylance.com • idp.blackberry.com • idp.cs.cylance.com

項目	説明
	CylancePROTECT Desktop が通信を必要とするドメイン： • 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
	CylanceOPTICS が通信を必要とするドメイン： • 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 アプリ

CylancePROTECT Mobile アプリは、CylancePROTECT Mobile クラウドサービスと通信するために、次の URL への安全な直接接続が必要です。デバイスが組織の Wi-Fi ネットワークに接続されている場合、ネットワーク構成で次の接続を許可する必要があります。

- CylancePROTECT Mobile クラウドサービス：
  - 米国：https://us1.mtd.blackberry.com
  - 日本：https://jp1.mtd.blackberry.com
  - 欧州連合：https://eu1.mtd.blackberry.com
  - オーストラリア：https://au1.mtd.blackberry.com
  - SP：https://br1.mtd.blackberry.com
- 共通サービスゲートウェイ：
  - 米国：https://us1.cs.blackberry.com
  - 日本：https://jp1.cs.blackberry.com
  - 欧州連合：https://eu1.cs.blackberry.com
  - オーストラリア：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 のプロキシ要件

CylancePROTECT Desktop エージェントおよび **CylanceOPTICS** エージェントのプロキシの設定

- BlackBerry サーバーへのアウトバウンド通信にプロキシサーバーを使用するようにデバイス上の CylancePROTECT Desktop エージェントと CylanceOPTICS エージェントの両方を設定する場合は、レジストリエディターで HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop に移動し、文字列値 REG_SZ を作成します。
  - 値名 = ProxyServer
  - 値データ = *<proxyIP:port>*（例：http://123.45.67.89:8080）
- プロキシはユーザ認証無しの要求を受け入れる必要があります。SSL インスペクションはサポートされていないため、すべてのエージェントトラフィック（*.cylance.com）でバイパスする必要があります。

CylanceOPTICS エージェントのプロキシオプション

- CylanceOPTICS エージェントはプロキシ対応であり、使用可能なプロキシ設定を識別して使用するために .NET フレームワークをクエリします。レジストリで ProxyServer 値を設定した場合、CylanceOPTICS エージェントは指定されたプロキシを使用します。CylanceOPTICS エージェントはまずローカルシステムとして、次に現在ログインしているユーザーとして通信を試みます。
- CylanceOPTICS エージェントがプロキシを使用するように設定し、エージェントがクラウドサービスと通信できない場合、エージェントはプロキシをバイパスして直接接続を確立しようとします。Windows および macOS デバイスでは、このプロキシバイパスを無効にできます。CylanceOPTICS エージェントのインストール前に以下を実行してください。

プラットフォーム	手順
Windows	HKLM\SOFTWARE\Cylance\Optics\ で、文字列値 REG_SZ を作成します。 • 値名 = DisableProxyBypass • 値データ = True

macOS	• /Library/Application Support/Cylance/Desktop/registry/LocalMachine/Software/Cylance/Desktop/ で、values.xml ファイルに以下を追加します。
	`<value name="ProxyServer" type="string">http://proxy_server_IP:port</value>`
	• /Library/Application Support/Cylance/Optics/Configuration で、以下を含む ExternalConfig.xml ファイルを作成します。
	`<?xml version="1.0" encoding="utf-8"?><EnforceProxyServer>true</EnforceProxyServer>`

- CylanceOPTICS が、署名されたファイルをアーチファクトとして含む検出イベントを作成すると、Windows API からのコマンドを使用して署名または証明書を検証します。このコマンドは、OCSP サーバーに検証要求を送信します。OCSP サーバーのアドレスは、Windows によって決定されます。OCSP サーバーへの外部トラフィックの送信が試行されたとプロキシサーバーから報告された場合は、デバイスのプロキシ設定を更新して、OCSP サーバーとの接続を許可します。

Linux：プロキシサーバーを使用するための **CylancePROTECT Desktop** エージェントおよび **CylanceOPTICS** エージェントの設定

サポートされているバージョンの RHEL、CentOS、Ubuntu、Amazon Linux 2、および SUSE 15 で、認証されていないプロキシまたは認証済みのプロキシを使用するようにエージェントを設定するには、次のコマンドを使用します。エージェントをインストールする前に、これらのコマンドを使用できます。次のコマンドは、CylancePROTECT Desktop エージェントのプロキシを設定します。CylanceOPTICS エージェントのプロキシを設定するには：

- 「cylancesvc」のすべてのインスタンスを「cyoptics」に置き換えます。
- 各 http_proxy 行を複製し、「http_proxy」を「https_proxy」に置き換えます。HTTPS トラフィックは TCP 接続を使用してトンネリングされるため、ほとんどの場合、https_proxy は http_proxy と同じ値を使用します。ただし、組織で HTTPS ターミネーションプロキシサーバーを使用している場合は、https_proxy に適切な値を指定します。

認証されていないプロキシ：

```
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
```

認証済みのプロキシ：

```
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
```

管理コンソールへのログイン

アカウントを有効化すると、Cylance Endpoint Security 管理コンソールのログイン情報を記載したメールが届きます。メールのリンクをクリックしてログインページを開くか、次のページに移動します。

- 北米：https://login.cylance.com
- アジア太平洋北東部：https://login-apne1.cylance.com
- アジア太平洋南東部：https://login-au.cylance.com
- ヨーロッパ中部：https://login-euc1.cylance.com
- 南米東部：https://login-sae1.cylance.com
- **GovCloud**：https://login.us.cylance.com

メールアドレスはアカウントのログインに使用されます。パスワードを作成したら、コンソールに進むことができます。

パスワードの要件

パスワードは、以下の要件のうち 3 つを満たす必要があります。

- 小文字
- 大文字
- 特殊文字（例：* # $ %）
- 数字
- Unicode 文字/データ（例：♥☀☆）

セッションタイムアウト

セッションは、最後に成功した認証の 1 時間後にタイムアウトします。

カスタム認証

重要：カスタム認証は廃止され、近い将来削除される予定です。カスタム認証を使用して Cylance Endpoint Security にアクセスしている場合は、お使いの外部 IDP を認証方法に移行し、拡張認証を使用して Cylance コンソールにアクセスできます。拡張認証の詳細については、「強化された認証サインイン」を参照してください。お使いの外部 IDP を認証方法として設定する方法のチュートリアルについては、「カスタム認証から認証方法に外部 IDP を移行する」を参照してください。

管理コンソールには、外部 ID プロバイダー（IdP）を使用してログインします。これには、IdP で設定を構成し、X.509 証明書と IdP ログインを確認するための URL を取得する必要があります。カスタム認証は Microsoft SAML 2.0 で動作します。この機能は、OneLogin、Okta、Microsoft Azure、PingOne で動作することが確認されています。この機能にはカスタム設定もあり、Microsoft SAML 2.0 に準拠する他の IdP と連携します。

カスタム認証の使用例については、次の記事を参照してください。

- Microsoft Azure
- Okta
- OneLogin
- PingOne
- SAML 2.0 の使用

メモ：カスタム認証で Active Directory フェデレーションサービス（ADFS）は、サポートされません。

カスタム認証の設定

1. 管理コンソールのメニューから［設定］>［アプリケーション］をクリックします。
2. ［カスタム認証］チェックボックスをオンにします。設定オプションが表示されます。
3. 認証に使用するオプションを選択します。オプションの説明については、「カスタム認証の説明」を参照してください。
4. ［保存］をクリックします。

カスタム認証の説明

オプション	説明
Strong Authentication	多要素認証アクセスを提供するには、このオプションを選択します。
シングルサインオン	シングルサインオン（SSO）アクセスを提供するには、このオプションを選択します。 Strong Authentication または SSO を選択してもカスタム認証設定には影響しません。これは、すべての設定が ID プロバイダー（IdP）によって処理されるためです。
パスワードログインを許可	このオプションを選択すると、コンソールに直接ログインして SSO を使用できます。これにより、コンソールからロックアウトされずに SSO 設定をテストできます。SSO を使用してコンソールに正常にログインしたら、この機能を無効にすることをお勧めします。
プロバイダー	カスタム認証のサービスプロバイダーを選択します。
X.509証明書	X.509 証明書情報を入力します。
ログインURL	カスタム認証の URL を入力します。

カスタム認証から認証方法に外部 IDP を移行する

カスタム認証用に設定された外部 ID プロバイダー（IDP）を使用して管理コンソールにサインインする場合は、「または、外部 ID プロバイダーでサインイン」リンクをクリックして、外部 IDP 資格情報でサインインする必要があります。BlackBerry は、外部 IDP を認証方法として設定し、認証ポリシーを使用して、メインのサインイン画面から IDP 資格情報でサインインすることをお勧めします。外部 IDP を認証方法として設定すると、認証設定の詳細度と柔軟性が向上します。

メインのサインイン画面から管理コンソールにサインインするように外部 IDP を設定するには、以下のアクションを実行します。詳細については、「カスタム認証から認証方法に外部 IDP を移行する」方法を参照してください。

2023 年 12 月より前に既存の IDP を認証方法として設定した場合、ユーザーが IDP ユーザーポータルから Cylance コンソールに直接アクセスできるようにするには、「強化された認証サインイン」を参照してください。

手順	アクション
1	「SAML 認証の追加に関する考慮事項」を確認します。
2	外部 IDP で Cylance コンソールにサインインします。
3	外部 IDP を設定して、Cylance Endpoint Security と通信します。 • カスタム認証情報の記録 • 認証方法の設定
4	テナントの認証ポリシーの管理 作成した認証方法を使用するテナントのために認証ポリシーを管理します。 メモ：フェイルセーフとして、Cylance コンソールパスワードのみを使用する 1 つのユーザーポリシーを作成し、1 人の管理者に割り当てます。
5	［パスワードログインを許可］チェックボックス（［設定］ > ［アプリケーション］ > ［カスタム認証］）がオンになっていることを確認します。このオプションを選択すると、コンソールに直接ログインして SSO を使用できます。このオプションを有効にすると、コンソールからロックアウトされずに SSO 設定をテストできます。
6	メインのサインイン画面から Cylance コンソールにサインインし、外部 IDP サインイン資格情報ポリシーをテストします。
7	（オプション）カスタム認証を無効にします（［設定］ > ［アプリケーション］）。

強化された認証サインイン

管理コンソールでは、ローカルの多要素認証、より詳細な認証ポリシー、ポリシー割り当てなど、認証機能が強化されています。環境を設定して、管理者が Cylance コンソールにサインインするために完了する必要がある認証のタイプと、ユーザーが Cylance Endpoint Security アプリやエージェントをアクティブ化する前に完了する必要がある認証のタイプを指定できます。デフォルトでは、Cylance コンソールパスワードを使用して管理者は管理コンソールにアクセスし、ユーザーは Cylance Endpoint Security アプリとエージェントをアクティブ化します。2024 年 3 月以降に作成したテナントの場合、デフォルトでは管理者が、コンソールパスワードの設定後に Cylance コンソールにアクセスするためのワンタイムパスワードを入力する必要があります。

テナントの認証ポリシーを作成し、すべての管理者とユーザーがテナントで完了する必要のある認証のタイプを指定できます。Cylance コンソールサインイン、Cylance Endpoint Security アプリ、Cylance Endpoint Security デスクトップエージェントに対して作成できるテナントポリシーは 1 つだけです。ユーザーの認証ポリシーを作成し、管理者とユーザーがテナントで完了する必要がある認証のタイプを指定できます。テナントポリシーおよび認証ポリシーに追加される認証のタイプは、ポリシーで指定された順序で完了する必要があります。フェイルセーフとして、ユーザー名と強力なパスワードを使用して Cylance コンソールにアクセスする 1 人の管理者を設定できます。

メモ：これで、更新されたサインインフローが、Cylance コンソールにアクセスする唯一の方法になります。また、プレビュー期間中にコンソールに適用した認証ポリシーが有効になります。

サインインの高度な認証を設定するには、次のいずれかの操作を実行します。

Cylance コンソールへのサインインの拡張認証の設定

2024 年 3 月以前にテナントを作成した場合、ユーザーが Cylance パスワードに加えてワンタイムパスワードなどの認証方法を使用して Cylance コンソールで認証されるように設定するには、次の手順を実行します。テナントポリシーにワンタイムパスワード認証方法を追加する方法については、「管理者が Cylance コンソールにアクセスするためのワンタイムパスワード認証の追加」を参照してください。

手順	アクション
1	既存のユーザー名とパスワードを使用して Cylance コンソールにサインインします。
2	認証方法を追加します（ワンタイムパスワード、エンタープライズ認証など）。デフォルトでは、各自の環境で使用するために、ワンタイムパスワード、Cylance コンソールパスワード、およびエンタープライズ認証による認証方法が設定されます。
3	パスワードと作成した認証方法を使用する認証ポリシーを作成します（オプション）。 メモ：フェイルセーフとして、Cylance コンソールパスワードのみを使用する 1 つの認証ポリシーを作成し、1 人の管理者に割り当てます。
4	管理者とユーザーのテナントポリシーを作成します。

Cylance コンソールへのサインインのワンタイムパスワード認証の削除

2024 年 3 月以降に作成したテナントでは、ユーザーは毎回 Cylance コンソールパスワードを入力した後でワンタイムパスワードを入力してからコンソールにアクセスする必要があります。ユーザーが コンソールで認証するためのワンタイムパスワード要件を削除するには、次の手順を実行します。テナントポリシーからワンタイムパスワード認証方法を削除する方法については、「管理者が Cylance コンソールにアクセスするためのワンタイムパスワード認証の削除」を参照してください。

手順	アクション
1	既存のユーザー名とパスワードおよびワンタイムパスワードを使用して Cylance コンソールにサインインします。
2	管理コンソールのテナントポリシーからワンタイムパスワード認証方法を削除し ます。
3	Cylance コンソールにサインインし、Cylance コンソールパスワードポリシーをテストします。

SSO 用の新しい IDP SAML 認証方法と Cylance コンソールへの IDP 開始アクセスの設定

ユーザーが Cylance コンソールで認証するための新しい IDP SAML 認証方法を設定するには、次の手順を実行します。ユーザーは、IDP 資格情報を使用してサインインページからコンソールにアクセスしたり、IDP 開始 SSO を使用して IDP ユーザーポータルからコンソールにアクセスしたりできます。IDP SAML の設定方法については、「Cylance コンソールへの拡張認証および IDP 開始アクセスのための IDP SAML の設定方法」を参照して IDP を選択してください。

手順	アクション
1	IDP 環境で新しい SAML アプリケーションを作成します。
2	Cylance Endpoint Security と通信できるように IDP を設定します。
3	Cylance コンソールで認証方法を追加します。
4	パスワードと作成した認証方法を使用する認証ポリシーを作成します。 メモ：フェイルセーフとして、Cylance コンソールパスワードのみを使用する 1 つの認証ポリシーを作成し、1 人の管理者に割り当てます。
5	IDP 環境において、Cylance コンソールで生成した SSO コールバック URL を更新します。
6	メインのサインイン画面から Cylance コンソールにサインインし、外部 IDP サインイン資格情報ポリシーをテストします。
7	（オプション）カスタム認証を無効にします（［設定］ > ［アプリケーション］）。

既存の IDP SAML 認証方法の更新による、Cylance コンソールへの IDP 開始アクセスの有効化

この手順を実行するのは、IDP SAML 認証方法を 2023 年 12 月以前に作成し、IDP 開始 SSO を有効にしてユーザーが IDP ユーザーポータルからコンソールにアクセスできるようにする場合のみです。その方法については、「IDP（SAML）認証方法を更新して Cylance コンソールへの IDP 開始アクセスを有効にする方法」を参照して IDP を選択します。

手順	アクション
1	既存のユーザー名とパスワードを使用して Cylance コンソールにサインインします。
2	現在の IDP SAML 認証方法で、新しい SSO コールバック URL を生成します。

手順	アクション
3	新しく生成した SSO コールバック URL を使用して、現在の認証ポリシーを更新します。
4	IDP 環境で既存の SAML 設定を更新します。

拡張認証を使用した **Cylance Endpoint Security** 管理コンソールへのサインイン

管理者が Cylance Endpoint Security 管理コンソールにサインインするために完了する必要がある認証のタイプと、ユーザーが Cylance Endpoint Security アプリやエージェント（CylancePROTECT Mobile アプリ、CylanceGATEWAY エージェントなど）をアクティブ化するために完了する必要がある認証のタイプを指定する認証ポリシーを設定できます。Cylance Endpoint Security 管理コンソールにアクセスする前に、移行画面が一時的に表示されます。

管理コンソール（［設定］ > ［カスタム認証］）でカスタム認証用に設定されている外部 IDP でサインインする場合は、外部のサードパーティ IDP 資格情報を使用して、［または、外部 ID プロバイダーでサインイン］リンクを使用してサインインを続行する必要があります。BlackBerry では、外部 IDP 設定を認証方法として設定し、認証ポリシーを使用して、メインのサインイン画面からサードパーティ IDP 資格情報でサインインできるようにすることをお勧めします。これにより、より詳細で柔軟性のある認証構成を指定できます。外部 IDP を認証方法として設定する方法の詳細については、「カスタム認証から認証方法に外部 IDP を移行する」を参照してください。

2023 年 12 月より前に外部 IDP 設定を認証方法として設定した場合、ユーザーは、外部 IDP ユーザーポータルからシングルサインオンを使用して Cylance コンソールに直接アクセスできなくなります。この機能を有効にするには、新しい Cylance Endpoint Security シングルサインオンログイン要求を生成する必要があります。IDP から開始する Cylance コンソールへのサインインを有効にする方法の詳細については、「強化された認証サインイン」および「外部 IDP を更新して Cylance コンソールへの SSO アクセスを有効にする方法」を参照してください。

作業を始める前に： 認証ポリシーを作成し、管理者、ユーザー、および管理者やユーザーが属するグループに割り当てます。

管理コンソールにアクセスするには、次のいずれかのタスクを実行します。

アクセス	タスク	手順
メインの Cylance Endpoint Security サインイン画面	Cylance アカウントでサインインします。	**a.** メールアドレスを入力してください。 **b.** ［サインイン］をクリックします。 **c.** パスワードを入力します。 **d.** ［サインイン］をクリックします。
	認証方法として設定されている外部 ID プロバイダーでサインインします。	**a.** メールアドレスを入力してください。 **b.** ［サインイン］をクリックします。 **c.** パスワードを入力します。 **d.** ［サインイン］をクリックします。

アクセス	タスク	手順
	外部 ID プロバイダーでサインインします。	**a.** ［外部 **ID** プロバイダーでサインイン］をクリックします。 **b.** ブラウザで、メールアドレスを入力します。 **c.** ［サインイン］をクリックします。 **d.** パスワードを入力します。 **e.** ［サインイン］をクリックします。
外部 IDP ユーザーポータル	外部 ID プロバイダー資格情報を使用してシングルサインオンします。	**a.** IDP ユーザーポータルにログインします。 **b.** 割り当てられているアプリケーションをクリックします。

新しい **SSO** コールバック **URL** の生成

コピーオプションを使用して、現在の認証方法情報をコピーし、新しい SSO コールバック URL を作成できます。コピーオプションでは、コピーした認証方法を保存し、現在の SSO コールバック URL を削除し、新しい URL を生成します。

重要：このタスクを実行するのは、強化されたサインイン用に環境を設定しており、認証方法が 2023 年 12 月より前に作成されたものであり、IDP から開始するコンソールへのシングルサインオン（SSO）を有効にする場合のみです。認証方法が 2023 年 12 月より前に作成されたかどうかを確認するには、Cylance コンソールで IDP SAML 認証方法を開きます（［設定］ > ［認証］）。

- SSO コールバック URL の形式が https://login.eid.blackberry.com/_/resume/saml20/<*hash*> である場合は、これ以上のアクションは必要ありません。
- SSO コールバック URL が https://idp.blackberry.com/_/resume である場合は、次の手順を実行して、更新された URL を生成します。

作業を始める前に： IDP SAML 認証方法が 2023年12月より前に作成され、非推奨にされた SSO コールバック URL を使用しています。

1. 認証方法画面を開きます（［設定］ > ［認証］）。
2. 現在の IDP SAML 認証方法をクリックします。
3. 画面の右上隅にあるコピーアイコンをクリックします。
4. コピーした認証方法の名前を更新します。［保存］をクリックします。
5. コピーした認証方法を開きます。**SSO** コールバック **URL** を記録します。
6. 以前の IDP 認証方法を削除します。

終了したら： コピーした認証方法で現在の認証ポリシーを更新します。

新規 Cylance Endpoint Security テナントの設定

新しい Cylance Endpoint Security テナントを作成するとき、またはテナントを推奨デフォルト状態にリセットするとき、テナントには、環境を目的のセキュリティ状態に調整するために設計された事前設定済みゾーンと事前設定済みデバイスポリシーが含まれます。

新しいテナント、または推奨デフォルト状態にリセットしたテナントには、デスクトップ OS（Windows、macOS、Linux）ごとに 1 つずつ、合計 3 つの事前設定ゾーンが含まれます。これらのゾーンは、新しいデスクトップデバイスを適切な OS ゾーンに自動的に割り当てるように設定されています。事前設定ゾーンには、次に説明する段階 1 のデバイスポリシーが割り当てられます。

新しいテナントまたはリセットしたテナントには、CylancePROTECT Desktop と CylanceOPTICS の機能を制御するために、3 つの事前設定デバイスポリシーが含まれています。各事前設定ポリシーの完全な設定については、「新規 Cylance Endpoint Security テナントのデフォルト設定」を参照してください。

事前設定ポリシー	説明
段階 1	デバイスがマルウェアの脅威を待ち受けられるようにするスターター設定。詳細ポリシー設定はオフになっています。まず環境でこのポリシーを使用して、デバイスからの初期検出を監視し、適切な例外を設定します。 このポリシーのパフォーマンスと影響に満足したら、デバイスを段階 2 のポリシーに進めることができます。
段階 2	このデバイスポリシーにより、異常なマルウェア、危険なスクリプト、メモリエクスプロイトなど、さまざまな脅威を検出できます。このポリシーは少数のデバイスに割り当て、検出の量と頻度、および必要な調査レベルを測定します。これにより、ポリシー設定を調整してから、より多くのデバイスに割り当てることができます。 このポリシーのパフォーマンスに満足したら、デバイスを段階 3 のポリシーに進めることができます。
段階 3	このデバイスポリシーは段階 2 の上に構築されており、デバイスが脅威を待ち受けて、特定の予防措置を取ることができるように設定が調整されています。このデバイスポリシーは、段階 2 のポリシーで十分なテストを行った後、段階 2 のポリシーからこのポリシーに微調整を適用した後にのみ使用してください。

事前設定ゾーンおよびデバイスポリシーをテストおよび評価する際、事前設定のオプションを変更したりゾーンやポリシーのコピーや変更を行ったりして、組織の環境に最適な設定を判断するというように、必要に応じて設定を調整できます。

また、Cylance Endpoint Security には、組織のニーズに合わせて新しいテナントを簡単に設定できるオプションも用意されています。テナントの設定をエクスポートして新しいテナントにインポートしたり、新規 Cylance Endpoint Security テナントのデフォルト設定 に詳述されている推奨デフォルトにテナントをリセットしたりできます。詳細については、「Cylance Endpoint Security テナントの設定のエクスポート、インポート、リセット」を参照してください。

新規 Cylance Endpoint Security テナントのデフォルト設定

事前設定ゾーン

事前設定ゾーン	割り当てられたデバイスポリシー	デフォルトのゾーンルール
Windows ゾーン	段階 1	すべての新しい Windows デバイスをこのゾーンに移動する自動ゾーン割り当て。
Mac ゾーン	段階 1	すべての新しい macOS デバイスをこのゾーンに移動する自動ゾーン割り当て。
Linux ゾーン	段階 1	すべての新しい Linux デバイスをこのゾーンに移動する自動ゾーン割り当て。

事前設定デバイスポリシー

デバイスポリシー設定	段階 **1** のポリシー	段階 **2** のポリシー	段階 **3** のポリシー
ファイルアクション			
自動隔離（実行制御あり）：危険	オフ	オン	オン
自動隔離（実行制御あり）：異常	オフ	オフ	オン
隔離済みのファイルの自動削除を有効にする	オフ	オン	オン
自動アップロード：実行可能ファイル	オン	オン	オン
メモリアクション			
メモリ保護	オフ	オン	オン
エクスプロイテーション：スタックピボット	オフ	無視	無視
エクスプロイテーション：スタック保護	オフ	無視	無視
エクスプロイテーション：コード上書き	オフ	無視	無視
エクスプロイテーション：RAM スクレイピング	オフ	アラート	ブロック
エクスプロイテーション：悪意のあるペイロード	オフ	無視	無視

デバイスポリシー設定	段階 1 のポリシー	段階 2 のポリシー	段階 3 のポリシー
エクスプロイテーション：システムコールのモニタリング	オフ	無視	無視
エクスプロイテーション：直接システムコール	オフ	無視	無視
エクスプロイテーション：システム DLL を上書き	オフ	無視	無視
エクスプロイテーション：危険な COM オブジェクト	オフ	無視	無視
エクスプロイテーション：APC 経由のインジェクション	オフ	無視	無視
エクスプロイテーション：危険な VBA マクロ	オフ	無視	無視
プロセス注入：メモリのリモート割り当て	オフ	アラート	ブロック
プロセス注入：メモリのリモートマッピング	オフ	アラート	ブロック
プロセス注入：メモリへのリモート書き込み	オフ	アラート	ブロック
プロセス注入：メモリへの PE のリモート書き込み	オフ	アラート	ブロック
プロセス注入：リモートでのコード上書き	オフ	無視	無視
プロセス注入：メモリのリモートマッピング解除	オフ	無視	無視
プロセス注入：リモートでのスレッド作成	オフ	無視	無視
プロセス注入：リモートでの APC スケジュール	オフ	無視	無視
プロセス注入：DYLD 注入	オフ	無視	無視
プロセス注入：ドッペルゲンガー	オフ	無視	無視
プロセス注入：危険な環境変数	オフ	無視	無視
エスカレーション：LSASS 読み取り	オフ	アラート	ブロック
エスカレーション：ゼロ割り当て	オフ	アラート	ブロック
エスカレーション：他のプロセスでメモリアクセス権を変更	オフ	無視	無視
エスカレーション：子プロセスでメモリアクセス権を変更	オフ	無視	無視
エスカレーション：盗まれたシステムトークン	オフ	無視	無視

デバイスポリシー設定	段階 **1** のポリシー	段階 **2** のポリシー	段階 **3** のポリシー
エスカレーション：低整合性プロセスの開始	オフ	無視	無視
保護設定			
デバイスからのサービスシャットダウンを防止	オン	オン	オン
実行中の危険なプロセスとそのサブプロセスを強制終了	オフ	オフ	オフ
バックグラウンド脅威検出	オン	オン	オン
実行設定	繰り返し	繰り返し	繰り返し
日	10	10	10
新しいファイルを監視	オン	オン	オン
MB	150	150	150
特定のフォルダを除外	オフ	オフ	オフ
ファイルサンプルのコピー	オフ	オフ	オフ
CylanceOPTICSの設定			
CylanceOPTICS	オフ	オフ	オフ
CylanceOPTICSデスクトップ通知を有効にする	オフ	オフ	オフ
検出設定	なし	なし	なし
アプリケーション制御			
アプリケーション制御	オフ	オフ	オフ
エージェント設定			
ログファイルの自動アップロードを有効にする	オフ	オフ	オフ
デスクトップ通知を有効にする	オフ	オフ	オフ
ソフトウェアインベントリを有効化	オン	オン	オン
スクリプト制御			
スクリプト制御	オフ	オン	オン

デバイスポリシー設定	段階 1 のポリシー	段階 2 のポリシー	段階 3 のポリシー
アクティブスクリプト	オフ	アラート	ブロック危険
PowerShell スクリプト	オフ	アラート	ブロック危険
PowerShellコンソール	オフ	無効化	無効化
マクロ	オフ	無効化	無効化
Python	オフ	無効化	無効化
.NET DLR	オフ	無効化	無効化
XLM マクロ	オフ	無効化	無効化
詳細：すべてのスクリプトのスコア	オフ	オン	オン
詳細：スクリプトをクラウドにアップロード	オフ	オン	オン
詳細：疑わしいスクリプトの実行のみを警告	オフ	オン	オン
デバイスの制御			
Windows デバイス制御	オン	オン	オン
Android	フルアクセス	フルアクセス	フルアクセス
iOS	フルアクセス	フルアクセス	フルアクセス
静止画	フルアクセス	フルアクセス	フルアクセス
USB CD DVD RW	フルアクセス	フルアクセス	フルアクセス
USB ドライブ	フルアクセス	フルアクセス	フルアクセス
VMware USBパススルー	フルアクセス	フルアクセス	フルアクセス
Windows ポータブルデバイス	フルアクセス	フルアクセス	フルアクセス

Cylance Endpoint Security テナントの設定のエクスポート、インポート、リセット

新しい Cylance Endpoint Security テナントは、既存のテナントの設定をエクスポートし、新しいテナントにインポートすることで構成できます。また、新しいテナントをリセットして、推奨デフォルト設定を使用することもできます。

次の設定は、既存のテナントの設定をエクスポートするときに組み込まれ、テナント設定をインポートまたはリセットするときに変更されます。

- デバイスポリシー
- ゾーン設定
- エージェント更新設定
- グローバルセーフリストおよび隔離リスト
- Syslog 設定

メモ：エクスポート、インポート、リセットのオプションは、デバイスの登録前に新しいテナントおよびテスト設定を構成するために特別に設計されています。エクスポート機能は、既存のテナントのバックアップ設定ファイルを作成するためのものではありません。設定を新しいテナントにインポートするか、テナントをリセットすると、上記の項目の以前の設定は削除され、復元できなくなります。

1. 管理コンソールのメニューバーで、［設定］ > ［テナント設定］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
現在のテナントの設定をエクスポートします。	エクスポートされる設定には、保存したクエリで作成したゾーンおよびゾーンルールのみが含まれます。エクスポートする設定ファイルは、同じ地域の新しいテナントにのみインポートできます。エクスポートした設定ファイルは、地域が異なるテナントには無効です。 **a.** ［エクスポート］をクリックします。 **b.** .zip ファイルの名前を指定します。 **c.** ［エクスポート］をクリックします。 **d.** 新しいテナントに設定をインポートするには、次の手順を参照してください。
別のテナントからエクスポートした設定をこのテナントにインポートします。	テナント設定をインポートすると、デバイスとデバイスポリシーおよびゾーン間の関連付けを含め、テナントの現在の設定が削除されることに注意してください。削除した設定は回復できません。 **a.** ［インポート］をクリックします。 **b.** 設定 .zip ファイルを参照して選択します。 **c.** 設定フィールドに「**import**」と入力します。 **d.** ［インポート］をクリックします。 **e.** インポートを確認します。 プロセスが失敗した場合、テナントに適用された変更はすべてロールバックされます。

タスク	手順
テナントを推奨デフォルト設定にリセットします。	テナント設定をデフォルト設定にリセットすると、デバイスとデバイスポリシーおよびゾーン間の関連付けを含め、現在の設定は削除されます。削除した設定は回復できません。 **a.** ［リセット］をクリックします。 **b.** 確認フィールドに「**reset**」と入力します。 **c.** ［リセット］をクリックします。 **d.** リセットを確定します。 プロセスが失敗した場合、テナントに適用された変更はすべてロールバックされます。

インポートまたはリセットの詳細は監査ログに書き込まれます。

BlackBerry Connectivity Node のインストール

BlackBerry Connectivity Node を使用すると、Cylance Endpoint Security とオンプレミス Microsoft Active Directory または LDAP ディレクトリの間にセキュリティで保護されている接続を作成できます。Cylance Endpoint Security は Active Directory のデバイス、ユーザーおよびグループを同期できます。ディレクトリ同期によって作成されたユーザーは、CylancePROTECT Mobile アプリ、CylanceGATEWAY 、および CylanceAVERT に対して有効にすることができます。

冗長性を提供するため、BlackBerry Connectivity Node の 1 つ以上のインスタンスをインストールできます。各インスタンスは専用のコンピュータにインストールする必要があります。複数の BlackBerry Connectivity Node がある場合は、すべてを同じソフトウェアリリースにアップグレードする必要があります。最初のインスタンスをアップグレードすると、すべてのインスタンスが同じバージョンにアップグレードされるまで、ディレクトリサービスは無効になります。

1 つ以上のディレクトリ接続を設定できますが、BlackBerry Connectivity Node の複数のインスタンスがある場合は、すべてのインスタンスですべてのディレクトリ接続を同じように設定する必要があります。1 つのディレクトリ接続が見つからないか、または正しく設定されていない場合、BlackBerry Connectivity Node は、管理コンソールに無効として表示されます。

Microsoft Entra ID Active Directory と同期するために BlackBerry Connectivity Node をインストールする必要はありません。詳細については、「Cylance Endpoint Security を設定して Entra Active Directory と同期する」を参照してください。

BlackBerry Connectivity Node をインストールするには、次の操作を実行します。

手順	アクション
1	要件を確認します。
2	Java の場所の環境変数の設定。
3	BlackBerry Connectivity Node 用のインストールファイルおよびアクティベーションファイルのダウンロード。
4	BlackBerry Connectivity Node のインストールおよび設定。
5	環境に BlackBerry Connectivity Node の複数のインスタンスがある場合は、「ディレクトリ接続設定のコピー」を参照してください。
6	BlackBerry Connectivity Node インスタンスのプロキシの設定 （オプション）。

Java の場所の環境変数の設定

BlackBerry Connectivity Node のインストール先のサーバーには JRE 17 実装をインストールし、Java のホームの場所を示す環境変数を設定する必要があります。

インストールを開始すると、BlackBerry Connectivity Node は Java を検出できるか確認します。Java が見つからない場合、セットアップアプリケーションは要件パネルで停止します。ユーザーは、Java の場所を示す環境変数を設定し、Java bin フォルダが Path システム変数に含まれていることを確認する必要があります。この時点でインストーラを終了し、環境変数が作成または更新された後でのみ再起動する必要があります。

作業を始める前に： BlackBerry Connectivity Node をインストールするサーバーに、JRE 17 がインストールされていることを確認します。

1. **Windows** の［システムの詳細設定］ダイアログボックスを開きます。
2. ［環境変数］をクリックします。
3. ［システム変数］リストで、［新規］をクリックします。
4. ［変数名］フィールドに、`BB_JAVA_HOME` と入力します。
5. ［変数値］フィールドに、JRE フォルダへのパスを入力し、［**OK**］をクリックします。
6. ［システム変数］リストで、［パス］を選択し、［編集］をクリックします。
7. パスに Java bin フォルダが含まれていない場合は、［新規］をクリックして、パスに `%BB_JAVA_HOME%\bin` を追加します。
8. リスト内の %BB_JAVA_HOME%\bin エントリを十分に高い位置に移動して別のエントリで置き換えられないようにして、［**OK**］をクリックします。

終了したら： BlackBerry Connectivity Node 用のインストールファイルおよびアクティベーションファイルのダウンロード。

BlackBerry Connectivity Node 用のインストールファイルおよびアクティベーションファイルのダウンロード

作業を始める前に： Java の場所の環境変数の設定。

1. 管理コンソールのメニューバーで、［設定］ **>** ［ディレクトリ接続］をクリックします。
2. ［**Connectivity Node**］タブをクリックします。
3. ［**Connectivity Node** を追加］をクリックします。
4. ソフトウェアのダウンロードページで、［ダウンロード］をクリックします。
5. ［**UES** 用の **BlackBerry Connectivity Node**］を選択します。
6. ［ダウンロード］をクリックします。
7. BlackBerry Connectivity Node のインストールファイルをコンピューターに解凍します。

   BlackBerry Connectivity Node の複数のインスタンスをインストールする場合は、使用済みのインストールファイルをコンピューター間でコピーしないでください。各コンピューターでインストールファイルを再解凍する必要があります。
8. 管理コンソールで［アクティベーションファイルのダウンロード］をクリックします。
9. アクティベーションファイル（.txt）を保存します。

アクティベーションファイルは 60 分間有効です。アクティベーションファイルの利用前に 60 分が経過してしまった場合、新しいアクティベーションファイルをダウンロードする必要があります。最新のアクティベーションファイルのみが有効です。

終了したら： BlackBerry Connectivity Node のインストールおよび設定。

BlackBerry Connectivity Node のインストールおよび設定

作業を始める前に： BlackBerry Connectivity Node 用のインストールファイルおよびアクティベーションファイルのダウンロード。

1. 管理コンソールからダウンロードした BlackBerry Connectivity Node インストールファイル（.exe）を開きます。

   Windows メッセージが表示され、コンピューターに変更を加えるために権限が求められた場合は、［はい］をクリックします。
2. 言語を選択します。［**OK**］をクリックします。
3. ［次へ］をクリックします。
4. 国または地域を選択します。使用許諾契約書を読んで、承諾します。［次へ］をクリックします。
5. インストールプログラムは、コンピューターがインストール要件を満たしていることを確認します。［次へ］をクリックします。
6. インストールのファイルパスを変更するには、［...］をクリックし、使用するファイルパスまで移動して選択します。インストールとログフォルダの場所の作成を要求するメッセージが表示された場合は、［はい］をクリックします。［次へ］をクリックします。
7. ［サービスアカウント］ダイアログボックスにサービスアカウントのパスワードを入力します。［インストール］をクリックします。
8. インストールが完了したら、［次へ］をクリックします。

   BlackBerry Connectivity Node コンソールのアドレスが表示されます（http:/localhost:8088）。リンクをクリックし、サイトをブラウザーに保存します。
9. 言語を選択します。［次へ］をクリックします。
10. BlackBerry Connectivity Node をアクティブにすると、ポート 443（HTTPS）を介してデータが BlackBerry Infrastructure （na.bbsecure.com や eu.bbsecure.com など）に送信されます。アクティブ化後、BlackBerry Connectivity Node は、BlackBerry Infrastructure を経由する他のすべてのアウトバウンド接続にポート 3101（TCP）を使用します。次の操作のいずれかを実行します。

    - BlackBerry Connectivity Node をアクティブ化するために、デフォルト（ポート 443）以外のプロキシ設定を使用して BlackBerry Infrastructure（<地域>.bbsecure.com）に接続する場合は、「ここ」リンクをクリックして、プロキシ設定を構成し、登録プロキシの情報を入力します。このリンクは、「BlackBerry Connectivity Node の名前を入力」画面でのみ利用できます。この画面でプロキシ設定を構成せずに［次へ］をクリックした場合は、画面右上の［設定］ > ［プロキシ］をクリックすることで、アクティブ化の前にプロキシ設定を構成できます。

      メモ： プロキシは BlackBerry Infrastructure へのポート 443 にアクセスできる必要があります。BlackBerry Connectivity Node をアクティブにした後、登録プロキシ設定を変更することはできません。
    - 他のプロキシ設定を構成します。使用可能なプロキシオプションの詳細については、「BlackBerry Connectivity Node インスタンスのプロキシ設定」を参照してください。
11. ［登録名］フィールドに、BlackBerry Connectivity Node の名前を入力します。［次へ］をクリックします。

12. ［参照］をクリックします。管理コンソールからダウンロードしたアクティベーションファイルを選択します。
13. ［アクティブにする］をクリックします。

    BlackBerry Connectivity Node インスタンスをアクティブにするときに既存のサーバーグループに追加するには、組織のファイアウォールが、BlackBerry Connectivity Node をアクティブ化するために、BlackBerry Infrastructure（na.bbsecure.com または eu.bbsecure.com）を介して、ポート 443 経由で、またメイン BlackBerry Connectivity Node インスタンスとして同じ bbsecure.com 領域へ、そのサーバーからの接続を許可する必要があります。
14. ＋をクリックして、設定する会社のディレクトリのタイプを選択します。
15. 次に挙げる適切なタスクを実行して、ディレクトリを BlackBerry Connectivity Node にリンクします。

    - Microsoft Active Directory への接続
    - LDAP ディレクトリへの接続

終了したら：

- 冗長性を確保するために第 2 の BlackBerry Connectivity Node インスタンスをインストールする場合は、別のセットとして、インストールおよびアクティベーションファイルをダウンロードして、別のコンピューターでこのタスクを繰り返します。この設定は、最初のインスタンスがアクティブ化された後に行う必要があります。
- 1 つ以上のディレクトリ接続を設定できますが、複数の BlackBerry Connectivity Node がある場合は、すべてのディレクトリ接続を同じ設定にする必要があります。1 つのディレクトリ接続が見つからないか、または正しく設定されていない場合、BlackBerry Connectivity Node は、管理コンソールに無効として表示されます。この作業は、ディレクトリ接続設定を一方の BlackBerry Connectivity Node から他へコピーすることで簡単にできます。
- 設定したディレクトリ設定を変更するには、BlackBerry Connectivity Node コンソール（http:/localhost:8088）で、［全般設定］ > ［会社のディレクトリ］をクリックします。ディレクトリ接続の✎をクリックします。
- BlackBerry Connectivity Node ログを設定します。
- ディレクトリ接続は、ユーザーまたはグループが関連付けられていないのであれば、BlackBerry Connectivity Node から削除できます。BlackBerry Connectivity Node から接続を削除した場合は、削除した接続と同じ名前を使用して接続を再追加できます。

ディレクトリ接続設定のコピー

環境に BlackBerry Connectivity Node のインスタンスが複数ある場合、ディレクトリ接続の設定はすべてのノードで同一にする必要があります。この作業を容易にするため、ディレクトリ接続設定は、1 つの BlackBerry Connectivity Node からエクスポートして別のものにインポートできます。

メモ：会社のディレクトリ設定を BlackBerry Connectivity Node にインポートする前に、そのノードから既存の会社のディレクトリ接続をすべて解除する必要があります。

作業を始める前に： ディレクトリ接続設定のコピー。

1. 設定のコピー元となる BlackBerry Connectivity Node の［会社のディレクトリ接続］画面で、［**.txt** ファイルでディレクトリ接続をエクスポート］をクリックします。

   会社のディレクトリ接続に関する情報を含む .txt ファイルがコンピューターにダウンロードされます。
2. 設定のコピー先となる BlackBerry Connectivity Node の［会社のディレクトリ接続］画面で、ダウンロードした .txt ファイルを参照します。

3. ［接続をインポート］をクリックします。
   会社のディレクトリ接続が BlackBerry Connectivity Node に追加されます。

BlackBerry Connectivity Node インスタンスのプロキシの設定

データが BlackBerry Infrastructure に到達する前に、TCP プロキシサーバー（透過型または SOCKS v5）を介してデータを送信するように、BlackBerry Connectivity Node のコンポーネントを設定できます。

1. BlackBerry Connectivity Node をホストするコンピューターで、［スタート］メニューから BlackBerry Connectivity Node コンソールを開くか、ブラウザを開いて、http://localhost:8088 に移動します。
2. ［一般設定］ > ［プロキシ］をクリックします。
3. 次のタスクを実行します。

タスク	手順
SOCKS v5 プロキシサーバー（認証なし）を介して BlackBerry Infrastructure にデータを送信する。	a. ［プロキシサーバー］オプションを選択します。 b. ［**SOCKS v5** を有効にする］チェックボックスをオンにします。 c. ［**+**］をクリックします。 d. SOCKS v5 プロキシサーバーの IP アドレスまたはホスト名を入力します。［追加］をクリックします。 e. 設定する SOCKS v5 プロキシサーバーそれぞれに対して手順 3 と 4 を繰り返します。 f. ［ポート］フィールドにポート番号を入力します。 g. ［保存］をクリックします。
透過的なプロキシサーバーを介して BlackBerry Infrastructure にデータを送信する。	• ［**BlackBerry Connectivity Node**］フィールドに、プロキシサーバーの FQDN または IP アドレスおよびポート番号を入力します。

4. ［保存］をクリックします。

会社のディレクトリへのリンク

Cylance Endpoint Security を会社のディレクトリと同期するように設定して、ユーザーとグループの追加と管理を簡素化できます。Cylance Endpoint Security を会社のディレクトリに接続すると、会社のディレクトリでユーザーデータを検索してインポートすることで、ユーザーアカウントを作成できます。ディレクトリ同期によって作成されたユーザーは、CylancePROTECT Mobile アプリ、CylanceGATEWAY 、および CylanceAVERT に対して有効にすることができます。

会社のディレクトリにリンクするには、次の 2 つの方法があります。

- Microsoft Entra ID と同期する場合は、Cylance Endpoint Security を接続するように設定できます。
- オンプレミス Microsoft Active Directory または LDAP ディレクトリと同期する場合は、最初に BlackBerry Connectivity Node をインストールして、Cylance Endpoint Security とディレクトリの間に安全な接続を作成する必要があります。

Cylance Endpoint Security を会社のディレクトリにリンクするには、次の操作を実行します。

手順	アクション
1	オンプレミスの会社のディレクトリにリンクする場合は、BlackBerry Connectivity Node をインストールします。
2	接続するディレクトリのタイプに応じて、Entra と同期するように Cylance Endpoint Security を設定するか、Microsoft Active Directory または LDAP ディレクトリに接続します。
3	ディレクトリグループの追加。
4	オンボーディングおよびオフボーディングの設定。
5	ディレクトリ同期スケジュールの設定。

Cylance Endpoint Security を設定して Entra Active Directory と同期する

Cylance Endpoint Security を設定して Entra Active Directory と同期するには、Entra と Cylance Endpoint Security の両方を設定して接続を確立する必要があります。

1. Azure ポータルにログインします。
2. Entra Active Directory の新しいアプリ登録を作成し、適切な設定と権限を付与します。
   a) アプリの名前を追加します。
   b) アプリケーションを使用できるか、API にアクセスできるアカウントタイプを指定します。
   c) リダイレクト URI の種類として［**Web**］を選択し、URI を `http://localhost` に設定します。
   d) 次のアプリケーション権限を設定します。

- Group.Read.All（アプリケーション）
- User.Read（委任）
- User.Read.All（アプリケーション）

e) 管理者にアプリケーションの承諾を許可します。

3. アプリに割り当てた名前とアプリケーション（クライアント）ID を記録します。
4. 新しいクライアントシークレットを作成し、シークレットの［値］列に情報を記録します。

   重要：この値は、作成時にのみ使用できます。ページから移動した後は、この値にアクセスできません。値を記録しない場合は、新しい値を作成する必要があります。この値は、管理コンソールのクライアントシークレットとして使用されます。
5. 管理コンソールのメニューバーで、［設定］ > ［ディレクトリ接続］をクリックします。
6. ［新しい接続を追加］をクリックします。
7. ディレクトリ接続の［名前］と、Entra Active Directory の［ドメイン］を入力します。
8. ［クライアント **ID**］フィールドに、Entra アプリの登録で生成されたアプリケーション ID を入力します。
9. ［クライアントシークレット］フィールドに、手順 4 で Entra アプリの登録で生成されたクライアントシークレット値を入力します。
10. ［追加］をクリックします。

Microsoft Entra ID Active Directory 接続資格情報の更新

クライアントシークレットが期限切れになった場合、または Azure ポータルで変更された場合は、管理コンソールでクライアント資格情報を更新する必要があります。クライアントシークレットが期限切れになった場合または変更された場合は、［ディレクトリ接続］画面の、影響を受けるディレクトリ接続の横に が表示されます。クライアントシークレットのみを更新することも、クライアント ID とクライアントシークレットの両方を更新することも選択できます。

作業を始める前に：

- Cylance Endpoint Security を設定して Entra Active Directory と同期する でアプリケーションに割り当てた名前を記録済みであることを確認します。
- 有効なクライアントシークレットがあり、シークレットの［値］列の情報を記録済みであることを確認します。必要に応じて、新しいクライアント ID とクライアントシークレットの両方を作成できます。

1. 管理コンソールのメニューバーで、［設定］ > ［ディレクトリ接続］をクリックします。
2. 更新する Microsoft Entra ID Active Directory 接続をクリックします。
3. ［接続設定］タブをクリックします。
4. ［クライアント資格情報を更新］をクリックします。クライアントシークレットのみを更新するか、クライアント ID とクライアントシークレットの両方を更新するかを選択します。次の操作のいずれかを実行します。
   - クライアントシークレットのみを更新：Azure ポータルで記録したクライアントシークレット値を入力します。
   - クライアント ID とクライアントシークレットを更新：Azure ポータルで記録した新しいクライアント ID とクライアントシークレット値を入力します。
5. ［送信］をクリックします。
6. ［保存］をクリックします。保存に失敗すると、クライアント ID とクライアントシークレットはともに以前の値に戻ります。

Microsoft Active Directory への接続

作業を始める前に： BlackBerry Connectivity Node のインスタンスを少なくとも 1 つインストールします。

1. BlackBerry Connectivity Node コンソール（http:/localhost:8088）で、［全般設定］ > ［会社のディレクトリ］をクリックします。
2. ＋をクリックします。
3. ［**Microsoft Active Directory**］を選択します。
4. ［接続名］フィールドに、この会社のディレクトリ接続の名前を入力します。
5. ［ユーザー名］フィールドに、Microsoft Active Directory アカウントの名前を入力します。
6. ［ドメイン］フィールドに、Microsoft Active Directory をホストするドメインの FQDN を入力します。たとえば、domain.example.com などです。
7. ［パスワード］フィールドに、Microsoft Active Directory アカウントのパスワードを入力します。
8. ［ドメインコントローラー検出］ドロップダウンリストで、次のいずれかをクリックします。
   - 自動検出を使用する場合は、［自動］をクリックします。
   - ドメインコントローラーコンピューターを指定する場合は、［以下のリストから選択］をクリックします。＋をクリックして、コンピューターの FQDN を入力します。さらにコンピューターを追加するには、この手順を繰り返します。
9. ［グローバルカタログ検索ベース］フィールドに、アクセスする検索ベースを入力します（たとえば、OU=Users,DC=example,DC=com）。グローバルカタログ全体を検索するには、フィールドを空白にしておきます。
10. ［グローバルカタログ検出］ドロップダウンリストで、次のいずれかをクリックします。
    - 自動カタログ検出を使用する場合は、［自動］をクリックします。
    - カタログコンピューターを指定する場合は、［以下のリストから選択］をクリックします。＋をクリックして、コンピューターの FQDN を入力します。必要に応じてこの手順を繰り返して、さらにコンピューターを指定します。
11. リンクされている Microsoft Exchange メールボックスのサポートを有効にする場合、［リンクされた **Microsoft Exchange** メールボックスのサポート］ドロップダウンリストで、［はい］をクリックします。アクセスするフォレストごとに Microsoft Active Directory アカウントを設定するには、［アカウントフォレストのリスト］セクションで＋をクリックします。フォレスト名、ユーザーのドメイン名（ユーザーはアカウントフォレスト内の任意のドメインに属することができます）、ユーザー名、およびパスワードを指定します。
12. 会社のディレクトリからユーザーの詳細情報を同期するには、［追加のユーザーの詳細を同期］チェックボックスをオンにします。追加の詳細には、会社名とオフィスの電話番号が含まれます。
13. ［保存］をクリックします。

終了したら：

- Cylance Endpoint Security の自動オンボーディングを設定する場合は、「オンボーディングおよびオフボーディングの設定」を参照してください。
- ディレクトリ同期スケジュールを追加する場合は、「ディレクトリ同期スケジュールの設定」を参照してください。
- BlackBerry Connectivity Node のインスタンスが複数ある場合は、1 つのインスタンスから他のインスタンスにディレクトリ接続設定をコピーできます。

LDAP ディレクトリへの接続

作業を始める前に： オンプレミス LDAP ディレクトリに接続するには、まず BlackBerry Connectivity Node のインスタンスを少なくとも 1 つインストールする必要があります。

1. BlackBerry Connectivity Node コンソール（http:/localhost:8088）で、［全般設定］ > ［会社のディレクトリ］をクリックします。
2. ＋をクリックします。
3. ［**LDAP**］を選択します。
4. ［接続名］フィールドに、この会社のディレクトリ接続の名前を入力します。
5. ［**LDAP** サーバー検出］ドロップダウンリストで、次のいずれかをクリックします。自動検出を使用する場合は、［自動］をクリックします。
   - 自動検出を使用する場合は、［自動］をクリックし、［**DNS** ドメイン名］フィールドに DNS ドメイン名を入力します。
   - LDAP コンピューターを指定する場合は、［以下のリストからサーバーを選択］をクリックします。＋をクリックして、コンピューターの FQDN を入力します。さらにコンピューターを追加するには、この手順を繰り返します。
6. ［**SSL** を有効にする］ドロップダウンリストで、LDAP トラフィックに対して SSL 認証を有効にするかどうかを選択します。［はい］をクリックした場合は、［参照］をクリックして LDAP コンピューターの SSL 証明書を選択します。
7. ［**LDAP** ポート］フィールドに、LDAP コンピューターのポート番号を入力します。
8. ［認証が必須］ドロップダウンリストで、LDAP コンピュータを使用して認証する必要があるかどうかを選択します。［はい］をクリックする場合は、LDAP アカウントのユーザー名とパスワードを入力します。ユーザー名は DN 形式（たとえば、CN=Megan Ball,OU=Sales,DC=example,DC=com）にする必要があります。
9. ［検索ベース］フィールドに、アクセスする検索ベースを入力します（たとえば、OU=Users,DC=example,DC=com）。
10. ［**LDAP** ユーザー検索フィルター］フィールドに、LDAP ユーザーに対して使用するフィルターを入力します。例：(&(objectCategory=person)(objectclass=user)。Cylance Endpoint Security テナント全体で単一グループのすべてのメンバーに検索を制限する場合は、(&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)) を使用できます。
11. ［**LDAP** ユーザーの検索範囲］ドロップダウンリストで、次のいずれかをクリックします。ユーザー検索をベース DN より下のすべてのレベルに適用する場合は、［すべてのレベル］をクリックします。ベース DN の 1 レベル下にユーザー検索を制限する場合は、［**1** レベル］をクリックします。
12. ［固有 **ID**］フィールドに、各ユーザーの固有 ID の属性を入力します（たとえば、uid）。この属性は、全ユーザーに対して、不変でグローバルに固有であることが必要です。
13. ［名］フィールドに、各ユーザーの名の属性を入力します（たとえば、givenName）。
14. ［姓］フィールドに、各ユーザーの姓の属性を入力します（たとえば、sn）。
15. ［ログイン属性］フィールドに、各ユーザーのログイン属性を入力します（たとえば、cn）。
16. ［メールアドレス］フィールドに、各ユーザーのメールの属性を入力します（たとえば、mail）。
17. ［表示名］フィールドに、各ユーザーの表示名の属性を入力します（たとえば、displayName）。
18. 会社のディレクトリからユーザーの詳細情報を同期するには、［追加のユーザーの詳細を同期］チェックボックスをオンにします。追加の詳細には、会社名とオフィスの電話番号が含まれます。
19. ディレクトリにリンクされたグループを有効化するには、［ディレクトリにリンクされたグループを有効にする］チェックボックスをオンにします。

以下の情報を指定します。

- ［グループ検索ベース］フィールドに、グループ情報の検索でベース DN として使用する値を入力します。
- ［**LDAP** グループ検索フィルター］フィールドに、会社のディレクトリでグループオブジェクトを検索するのに必要な LDAP 検索フィルターを入力します。
- ［グループ固有 **ID**］フィールドに、各グループの固有 ID の属性を入力します。この属性は、不変でグローバルに一意である必要があります。
- ［グループの表示名］フィールドに、各グループの表示名の属性を入力します。
- ［グループメンバーシップの属性］フィールドに、グループメンバーシップの属性の名前を入力します。属性値は DN 形式である必要があります。
- ［テストグループ名］フィールドに、指定したグループ属性を検証するための既存のグループ名を入力します。

20. ［保存］をクリックします。

終了したら：

- Cylance Endpoint Security の自動オンボーディングを設定する場合は、「オンボーディングおよびオフボーディングの設定」を参照してください。
- ディレクトリ同期スケジュールを追加する場合は、「ディレクトリ同期スケジュールの設定」を参照してください。
- BlackBerry Connectivity Node のインスタンスが複数ある場合は、1 つのインスタンスから他のインスタンスにディレクトリ接続設定をコピーできます。

オンボーディングおよびオフボーディングの設定

オンボーディングにより、会社のディレクトリグループのユーザーメンバーシップに基づいて Cylance Endpoint Security に自動的にユーザーアカウントを追加できます。ディレクトリグループとユーザーアカウントは、同期プロセス中に CylanceGATEWAY へ追加されます。

オンボーディングを有効にする場合は、オフボーディングを設定することもできます。ユーザーがディレクトリ内で無効にされるか、オンボーディングディレクトリグループ内のすべての会社ディレクトリグループから削除されると、Cylance Endpoint Security はそのユーザーアカウントを削除し、ユーザーのデバイスからのネットワーク接続を許可しなくなります。

オフボーディング保護を使用することで、ユーザーアカウントの削除を引き延ばして、ディレクトリのレプリケーションが遅れることによる想定外の削除を回避できます。オフボーディング保護により、次の同期サイクルの 2 時間後にオフボーディングアクションが延期されます。

作業を始める前に： 接続するディレクトリのタイプに応じて、Azure Active Directory と同期するように Cylance Endpoint Security を設定するか、Microsoft Active Directory または LDAP ディレクトリに接続します。

1. 管理コンソールのメニューバーで、［設定］ **>** ［ディレクトリ接続］をクリックします。

2. ［ディレクトリ接続］リストで、オンボーディングを設定する接続をクリックします。

3. ［同期設定］タブで、［ディレクトリオンボーディング］を選択します。

4. ［同期］フィールドで、各同期プロセスで許可する変更の最大数を入力します。

デフォルトでは、制限はありません。同期する変更の数が設定した制限を超えている場合は、同期プロセスが停止します。変更には、グループに追加されたユーザー、グループから削除されたユーザー、オンボーディングされるユーザー、オフボーディングされるユーザーが含まれます。

5. ［ネストレベル］フィールドに、会社のディレクトリグループの同期するネストレベルの数を入力します。デフォルトでは、制限はありません。
6. ディレクトリグループの同期を強制するには、［同期を強制する］を選択します。

   このオプションを選択すると、グループが会社のディレクトリから削除されたときに、そのグループへのリンクが、オンボーディングディレクトリグループとディレクトリにリンクされているグループから削除されます。選択されていない場合で会社のディレクトリグループが見つからない場合、同期プロセスがキャンセルされます。
7. ユーザーがディレクトリ内のリンクされたすべてのグループから削除されたときに Cylance Endpoint Security からユーザーアカウントを削除するには、［ユーザーがすべてのオンボーディングディレクトリグループから削除されたらユーザーを削除する］を選択します。ユーザーアカウントは、リンクされたすべてのディレクトリグループから削除された後、初めて同期サイクルが発生したときに Cylance Endpoint Security から削除されます。
8. ユーザーアカウントまたはデバイスデータが Cylance Endpoint Security から予期せず削除されないようにするには、［オフボーディング保護］を選択します。

   オフボーディング保護とは、ユーザーが次の同期サイクルの 2 時間後まで Cylance Endpoint Security から削除されないことです。
9. ［保存］をクリックします。

ディレクトリ同期スケジュールの設定

スケジュールを追加すれば、Cylance Endpoint Security を組織の会社のディレクトリと自動的に同期することができます。

作業を始める前に： Microsoft Active Directory への接続 または LDAP ディレクトリへの接続。

1. 管理コンソールのメニューバーで、［設定］ > ［ディレクトリ接続］をクリックします。
2. ［ディレクトリ接続］リストで、同期スケジュールを設定する接続をクリックします。
3. ［同期スケジュール］タブで、［スケジュールを追加］をクリックします。
4. ［同期タイプ］ドロップダウンリストで、次のいずれかのオプションを選択します。
   - ［すべてのグループとユーザー］：これはデフォルト設定です。このオプションを選択して、オンボーディングが有効になっていると、同期中にユーザーに対してオンボーディングとオフボーディングが行われ、適切なディレクトリにリンクされたグループにリンクされます。オンボーディングまたはオフボーディングされていないものの、ディレクトリグループを変更したユーザーと、属性に変更を加えたユーザーが同期されます。
   - ［オンボーディンググループ］：このオプションを選択し、オンボーディングが有効になっていると、同期中にユーザーに対してオンボーディングとオフボーディングが行われ、適切なディレクトリにリンクされたグループにリンクされます。属性に変更があったユーザーは同期されます。オンボーディングまたはオフボーディングされていないものの、ディレクトリグループを変更したユーザーは同期されません。
   - ［ディレクトリにリンクされたグループ］：このオプションを選択すると、同期中にユーザーに対してオンボーディングとオフボーディングは行われません。ディレクトリグループに変更があったユーザーは適切にリンクされます。属性に変更があったユーザーは同期されます。
   - ［ユーザー属性］：このオプションを選択すると、同期中にユーザーに対してオンボーディングとオフボーディングは行われません。ディレクトリグループに変更があったユーザーは同期されません。属性に変更があったユーザーは同期されます。
5. ［繰り返し］ドロップダウンリストで、次のいずれかのオプションを選択します。

- ［間隔］：これがデフォルト設定です。このオプションを選択した場合は、同期の間隔を分単位で指定し、同期を実行できる時間と日数を指定できます
- ［**1** 日 **1** 回］：このオプションを選択すると、同期が行われる曜日と時刻を指定できます。
- ［繰り返しなし］：このオプションを選択すると、次の週に 1 回行われる同期の曜日と時刻を指定できます。

6. スケジュールの適切な日時の詳細を指定します。
7. ［送信］をクリックします。
8. ［保存］をクリックします。

会社のディレクトリとの同期

Cylance Endpoint Security は、ディレクトリ接続とはいつでも同期できます。

1. 管理コンソールのメニューバーで、［設定］ **>** ［ディレクトリ接続］をクリックします。
2. ［ディレクトリ接続］リストで、同期する接続の をクリックします。

管理者の設定

管理者ユーザーは、事前定義されたロールまたはカスタムロールを割り当てることで、管理コンソールへのアクセス方法や使用方法を制御できます。このロールベースのアクセス制御により、管理者に対して、各管理者のロールに必要な特定のコンソール機能へのアクセス権を付与できます。また、アクセス権を付与する機能を制限することもできます。

ロールと権限の詳細については、「管理者ロールの権限」を参照してください。

管理者の追加

管理者ユーザーを管理コンソールに追加して、そうしたユーザーに Cylance Endpoint Security 環境を制御および設定する権限を与えることができます。既存の管理者アカウントと新しく追加された管理者アカウントは、管理コンソールの［ユーザー］ページ（［アセット］>［ユーザー］）に表示されます。［管理者］列を追加して、各管理者アカウントの横に アイコンを表示できます。管理者ユーザーが管理コンソールで表示できる画面と、ユーザーが設定および変更できる機能は、そのユーザーに割り当てるロールによって変わります。ロールと権限の詳細については、「管理者ロールの権限」を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［管理者］をクリックします。次の操作のいずれかを実行します。

タスク	手順
新しい管理者を追加する。	a. ［ユーザーを追加］で、［メールを入力］フィールドに、ユーザーのメールアドレスを入力します。 b. ［ロールを選択］ドロップダウンリストで、ロールをクリックします。各ロールとその関連する権限については、「ロールの管理」を参照してください。 c. ゾーンマネージャーロールかユーザーロールを選択した場合は、［ゾーンを選択］ドロップダウンリストでゾーンをクリックします。 d. ［追加］をクリックします。 Cylance Endpoint Security によって、パスワードを作成するためのリンクが記載されたメールが新しい管理者ユーザーに送信されます。

タスク	手順
管理者ロールを変更する。	**a.** 管理者ユーザーをクリックします。 **b.** ドロップダウンリストで、新しいロールをクリックします。 **c.** ゾーンマネージャーまたはユーザーロールを選択した場合は、次の手順を実行します。 **1.** 新しいゾーンの作成時にユーザーに割り当てるデフォルトのゾーンロールを選択します。デフォルトは［なし］です。 **2.** ゾーンごとにユーザーのロールを調整します。 少なくとも 1 つのゾーンのゾーンマネージャーをユーザーに割り当てると、デバイスポリシーのリストの表示、インストーラのダウンロード、グローバルリストの表示など、いくつかのゾーンマネージャー機能が継承されます。ただし、ユーザーがゾーンマネージャーの機能を実行できるのは、ゾーンマネージャーロールが割り当てられているゾーンにあるデバイスのみです。同様に、ユーザーがユーザーの機能を実行できるのは、ユーザーロールが割り当てられているゾーンにあるデバイスのみです。 **d.** ポップアップウィンドウで、パスワードを入力します。 **e.** ［保存］をクリックします。

2. メニューバーで、［アセット］**>**［ユーザー］をクリックします。次の操作のいずれかを実行します。
   - 列を追加または削除するには、|||をクリックし、表示する列を選択します。
   - 列でユーザーを昇順または降順に並べ替えるには、列をクリックします。
   - 列でユーザーをフィルタリングするには、列のフィルターフィールドとアイコンを使用します。
   - 管理者アカウントのみを表示するには、⏷をクリックし、管理者オプションを **True** に設定します。

管理者ロールの権限

以下の表に、管理コンソール内のシステム定義ロールのデフォルト権限を示します。太字で表示された権限には、メイン権限が選択された後にのみ使用できる子権限があります。

ゾーンマネージャーがコンソールで表示できるデータは、管理するゾーンに限定されます。

ダッシュボード

これらの権限により、ダッシュボードページにアクセスできます。これらの権限を無効にすることはできません。ダッシュボードに表示される情報は、管理者ロールに割り当てられたロールと権限に応じて決まります。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
デバイス保護	√	√	√	√

エンドポイント検出応答

これらの権限により CylanceOPTICS の機能を管理できます。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
検出を表示	√	√		√
検出を編集	√	√		
検出を削除	√	√		
InstaQuery を表示、作成	√	√		√
InstaQueryを削除	√	√		
高度なクエリを表示、作成	√	√		√
共有のテンプレートを作成	√	√		
共有のテンプレートを削除	√			
共有のスナップショットを削除	√			
共有のエクスポートクエリを削除	√			
スケジュール済みクエリを作成	√	√		
共有のスケジュール済みクエリを編集	√			
共有のスケジュール済みクエリを削除	√			
フォーカスデータを表示、作成	√	√		√
パッケージデプロイを表示	√			√
パッケージデプロイを作成	√			
パッケージデプロイを更新	√			
パッケージデプロイを削除	√			
プレイブックの結果を表示	√			√

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
プレイブックの結果を削除	√			
パッケージを表示	√			√
パッケージを作成	√			
パッケージを削除	√			
プレイブックを表示	√			√
プレイブックを作成、編集	√			
プレイブックを削除	√			
ルールセットを表示*	√			√
ルールセットを編集*	√			
ルールセットを削除	√			
ルールを表示	√			√
カスタムルールを作成、編集	√			
カスタムルールを削除	√			
例外を表示	√			√
例外を作成、編集	√			
例外を削除	√			
ロックダウン設定を表示	√			√
ロックダウン設定を作成、編集	√			
ロックダウン設定を削除	√			

*ルールセットを表示するには、ルールセットの表示権限とルールセットの編集権限を持つ管理者ロールが必要です。

ユーザーとデバイス

これらの権限により、管理コンソールでユーザーとデバイスに対して実行できる操作を制御します。グローバル隔離のグローバルリスト権限を持っているか、これらのページからセーフリストに脅威を追加する必要があります。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
ユーザーとグループを表示	√			√
ユーザーとグループを作成	√			
ユーザーとグループを編集	√			
ユーザーとグループを削除	√			
モバイルデバイスを表示	√			√
モバイルデバイスを削除	√			
デバイスを表示	√	√	√	√
デバイスを編集	√	√		
デバイスを削除	√			
バックグラウンドスキャンを実行	√			
CylanceOPTICS デバイスのロック	√			
CylanceOPTICS デバイスのロック解除	√			
リモート応答を実行	√			
ファイルのダウンロードを許可	√			
デバイスポリシーを表示	√	√		√
デバイスポリシーを作成	√			
デバイスポリシーを編集	√			
デバイスポリシーを削除	√			
ゾーンを表示	√	√	√	√

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
ゾーンを作成	√			
ゾーンを編集	√	√		
ゾーンを削除	√			

脅威からの保護

これらの権限により、保護メニュー、CylancePROTECT Mobile のアラート、および脆弱性にアクセスできます。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
脅威からの保護を表示	√	√	√	√
Protect Mobile イベントを編集	√			
Protect Mobileポリシーを表示	√			√
Protect Mobile ポリシーを作成	√			
Protect Mobile ポリシーを編集	√			
Protect Mobile ポリシーを削除	√			

ネットワーク

これらの権限により、ネットワークアクセス制御、CylanceGATEWAY 設定、および CylanceGATEWAY アラートとイベントなどのネットワーク保護設定を管理できます。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
Gatewayサービスポリシーを表示	√			√
Gateway サービスポリシーを作成	√			

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
Gateway サービスポリシーを編集	√			
Gateway サービスポリシーを削除	√			
ネットワークアクセスコントロールを表示	√			√
ネットワークアクセスコントロールを編集	√			
Gateway設定を表示	√			√
Gateway 設定を作成	√			
Gateway 設定を編集	√			
Gateway 設定を削除	√			
Gateway レポートイベントを表示	√			√
Gateway アラートとイベントを表示	√			√

Avert

これらの権限により CylanceAVERT の機能を管理できます。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
Avert設定を表示	√			√
Avert設定を編集	√			
Avertデバイス**ID**を表示	√			√
Avertリスクスコアを表示	√			√
Avertデバイスイベントを表示	√			√
Avertポリシーを表示	√			√

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
Avertポリシーを作成	√			
Avertポリシーを編集	√			
Avertポリシーを削除	√			
Avert機密ファイルの概要を表示	√			
Avertファイルコンテンツを表示	√			
Avertファイルを削除	√			

共通

これらの権限により、管理者は Cylance Endpoint Security ソリューションの複数の機能（EMM プロバイダーとディレクトリ、モバイルデバイスと CylanceGATEWAY の登録、適応型リスクオプションとイベントなど）に影響を与えるテナントレベルの設定を管理できます。ディレクトリ接続の場合は、Microsoft Entra ID Active Directory（AD）のみを作成できます。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
EMM接続を表示	√			√
EMM接続を作成	√			
EMM接続を編集	√			
EMM接続を削除	√			
ディレクトリ接続を表示	√			√
ディレクトリ接続を作成	√			
ディレクトリ接続を編集	√			
ディレクトリ接続を削除	√			
オンプレミスディレクトリコネクタを表示	√			√
オンプレミスディレクトリコネクタを作成	√			

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
オンプレミスディレクトリコネクタを編集	√			
オンプレミスディレクトリコネクタを削除	√			
認証コントロールを表示	√			√
認証方法を作成	√			
認証方法を編集	√			
認証方法を削除	√			
登録ポリシーを表示	√			√
登録ポリシーを作成	√			
登録ポリシーを編集	√			
登録ポリシーを削除	√			
適応型リスクポリシーを表示	√			√
適応型リスクポリシーを作成	√			
適応型リスクポリシーを編集	√			
適応型リスクポリシーを削除	√			
適応型リスク設定を表示	√			√
適応型リスク設定を作成	√			
適応型リスク設定を編集	√			
適応型リスク設定を削除	√			
アラートを表示	√			√
アラートを編集	√			
アラートを削除	√			

ログ記録

これらの権限により、レポートと監査ログを表示できます。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
レポートを表示	√			√
監査ログを表示	√			√

設定

これらの権限により、管理コンソールの設定を管理できます。ユーザー管理権限とロール管理権限が関連付けられています。選択されたユーザー管理権限を持つロールが割り当てられているユーザーは、ロール管理機能にもアクセスできます。

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
アプリケーション	√	√		√
トークン管理	√			
インストーラのダウンロード	√	√		
アンインストールパスワードの管理	√			
サポートにログイン	√			
Syslog/SIEM	√			
カスタム認証	√			
脅威データレポート	√			
ユーザー管理	√			
グローバルリストを表示	√	√		√
グローバルリストを作成	√			
グローバルリストを編集	√			
グローバルリストを削除	√			

権限	管理者	ゾーンマネージャー	ユーザー	読み取り専用
エージェントの更新設定を表示	√			√
エージェントの更新設定を作成	√			
エージェントの更新設定を編集	√			
エージェントの設定を削除	√			
証明書	√	√		√
統合	√			
デバイスのライフサイクル設定を表示	√			√
デバイスのライフサイクル設定を作成	√			
デバイスのライフサイクル設定を編集	√			
デバイスのライフサイクル設定を削除	√			
アクティベーション設定を表示	√			√
アクティベーション設定を編集	√			

ロールの管理

事前定義されたロールを使用するか、カスタムロールを作成して、管理コンソールの機能への管理者アクセスを管理できます。事前定義されたロールには権限が設定されており、その権限を変更することはできません。ロールの権限に基づいて、一部のメニューオプション、ページ、および機能を使用できない場合があります。たとえば、ユーザーがゾーン機能にアクセスできない場合、ゾーンメニューオプションは表示されません。ダッシュボード画面は、すべての事前定義およびカスタムロールで使用できますが、表示されるデータには、ログインしているユーザーが管理できるゾーンのみが反映されます。

事前定義された各ロールに許可されるユーザー権限の包括的なリストについては、「管理者ロールの権限」を参照してください。カスタムロールに割り当てられたユーザーは、マイアカウントページで通知を有効にすることができません。

ロールの追加

カスタムロールはグローバルにスコープ設定され、定義された領域の関連ページおよびアクションへの完全な操作アクセス権を付与します。たとえば、カスタムロールにゾーン機能が許可された権限がある場合、そのロールに割り当てられたすべてのユーザーは、［ゾーン］または［ゾーンの詳細］ページで使用可能なすべての機能にアクセスできます。

ロールにアクセス権が選択されていない場合は、ユーザーのメニューに該当ページが表示されないか、コンソール内のどこからもそのページに移動できません。たとえば、カスタムロールの権限が脅威に対して許可され、デバイスに対して許可されていない場合、［脅威からの保護］ページがメニューに表示されますが、［デバイス］ページは表示されません。ユーザーが脅威に対する［脅威の詳細］ページを表示した場合、影響を受けるデバイスとゾーンは表示されますが、特定のデバイスの詳細のリンクをクリックしようとすると、エラーページが表示されます。

1. 管理コンソールのメニューバーで、［設定］ > ［管理者］をクリックします。
2. ［ロール］をクリックします。
3. ［新しいロールを追加］をクリックします。
4. ロールの名前を入力します。
5. このロールにアクセスを許可する機能の横にある［アクセス］チェックボックスをクリックします。セクションを展開して、その他のオプションを表示します。詳細については、「管理者ロールの権限」を参照してください。
6. ［ロールを追加］をクリックします。

終了したら：

- ロールを編集するには、既存のロールをクリックし、名前または権限を変更します。更新された名前または権限は、既存のロールに割り当てられたすべてのユーザーに適用されます。
- 事前定義されたロールまたはカスタムロールにユーザーが割り当てられている場合は、［割り当て済みユーザー］列のリンクをクリックすると、そのロールに割り当てられているユーザーのメールを表示できます。メールをクリックすると、そのユーザーの［ユーザーの詳細］ページを表示できます。
- ロールを削除するには、割り当てられているユーザーがいないロールの横にあるチェックボックスをクリックし、［削除］をクリックします。ロールにユーザーが割り当てられている場合は、このチェックボックスをオンにできません。

セッションタイムアウト制限とアイドルタイムアウト制限の設定

セッションがアクティブであれば、管理者がサインアウトするまで管理コンソールにログインしたままでいられる期間を指定できます。また、管理者がコンソールからログアウトするまでセッションをアイドル状態に維持できる期間も指定できます。

1. 管理コンソールのメニューバーで、［設定］ > ［認証］をクリックします。
2. ［設定］タブの［コンソールタイムアウト］セクションで、［セッションタイムアウト］制限を設定します。

   コンソールタイムアウト制限に達する数分前になると、カウントダウンプロンプトが管理者に表示されます。これにより管理者は、再度認証を受けて、セッションを続行することができます。管理者が［確認］をクリックして再度ログインすることによりプロンプトにアクティブに応答しなかった場合は、タイムアウト制限に達するとログアウトされます。

3. ［アイドルタイムアウト］制限を設定します。
4. ［保存］をクリックします。

ユーザーとデバイスの追加

管理コンソールにユーザーアカウントを追加して、そのユーザーに対して次の Cylance Endpoint Security サービスが有効になるようにする必要があります。

- CylancePROTECT Mobile アプリで利用できるサービス：CylancePROTECT Mobile および CylanceGATEWAY
- CylanceGATEWAY Desktop

ユーザーを追加するには、次に挙げるいずれかの方法を使用できます。

- 会社のディレクトリにリンクして、オンボーディングを有効にすると、Cylance Endpoint Security がディレクトリと同期するときにユーザーが自動的に追加されます。ディレクトリ同期スケジュールを設定して、Cylance Endpoint Security と会社のディレクトリを同期することができます。デフォルトでは、すべてのユーザーおよびグループが、毎日 30 分間隔で同期されます。
- 会社のディレクトリにリンクして、ディレクトリユーザーを個別に追加します。オンボーディングを有効にしない場合は、この方法を使用できます。
- 個々のユーザーを BlackBerry Online Account ユーザーとして追加します。

CylancePROTECT Desktop や CylanceOPTICS などの Cylance Endpoint Security のサービスを有効にするために、ユーザーアカウントを追加する必要はありません。エージェントをデバイスにインストールした後、管理コンソールでそれらのデバイスと関連データを表示および管理できます。

CylancePROTECT Mobile アプリと CylanceGATEWAY ユーザーの追加

作業を始める前に： 会社のディレクトリからユーザーを追加する場合は、「会社のディレクトリへのリンク」の手順に従います。オンボーディングを有効にすると、ディレクトリグループとユーザーアカウントは同期プロセス中に管理コンソールに追加されます。オンボーディングを有効にしないでディレクトリユーザーを個別に追加する場合や、個々のユーザーを BlackBerry Online Account ユーザーとして追加する場合は、次の手順を実行します。

1. 管理コンソールのメニューバーで、［アセット］ > ［ユーザー］をクリックします。
2. ［ユーザーを追加］をクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
ディレクトリユーザーを追加する。	a. ユーザーの名前を入力し、ドロップダウンリストから一致する結果をクリックします。 b. ユーザーグループを既に追加している場合は、必要に応じて、ユーザーを 1 つ以上のグループに追加します。

タスク	手順
BlackBerry Online Account ユーザーを追加する。	**a.** 検索フィールドをクリックし、［新しいユーザーを手動で追加］をクリックします。ディレクトリ接続を設定していない場合は、次の手順に進みます。 **b.** ユーザーの名前とメールアドレスを指定します。 **c.** ユーザーグループを既に追加している場合は、必要に応じて、ユーザーを 1 つ以上のグループに追加します。 **d.** そのユーザーで BlackBerry Online Account のパスワードリセットにアクセスし、メールアドレスを入力してパスワードを設定します。ユーザーはこのパスワードを使用して CylancePROTECT Mobile アプリをアクティブ化します。ユーザーは、アプリをアクティブ化したときに、CylancePROTECT Mobile アプリからパスワードリセットのリンクにアクセスすることもできます。

4. ［保存］をクリックします。別のユーザーを追加する場合は、［保存して新規作成］をクリックし、前の手順を繰り返します。

終了したら：

- ユーザーをグループに追加するには、［アセット］ > ［ユーザーグループ］で、［ユーザー］タブからグループを選択しグループにユーザーを追加します。オンボーディングを有効にした場合、グループメンバーシップはディレクトリから同期されます。
- 追加したユーザーに対して CylancePROTECT Mobile を有効にするには、「CylancePROTECT Mobile のセットアップ」の手順に従います。
- 追加したユーザーに対して CylanceGATEWAY を有効にするには、「CylanceGATEWAY のセットアップ」の手順に従います。
- 管理者、ユーザー、およびグループへのポリシーの割り当て。

ユーザーグループの追加

CylancePROTECT Mobile アプリと CylanceGATEWAY ユーザーに対して有効になっているユーザーのグループを作成できます。ユーザーグループは共通のプロパティを共有する関連するユーザーの集合です。グループとしてユーザーを管理した方が、同時にグループのすべてのメンバーに対してプロパティを追加、変更、または削除できるため、個々のユーザーを管理するより効率的です。ユーザーグループにポリシーを割り当てると、そのグループのすべてのメンバーにポリシーが適用されます。

ポリシーは、グループ設定ページかポリシーページからグループに割り当てることができます。ユーザーが、異なるポリシーが割り当てられている複数のグループに属している場合は、割り当てられたポリシーの最高ランクがユーザーに適用されます。

2 種類のユーザーグループを作成できます。

- ディレクトリグループは、会社のディレクトリ内のグループにリンクします。グループのメンバーシップは、ディレクトリ内のメンバーシップリストと同期します。詳細については、「オンボーディングおよびオフボーディングの設定」を参照してください。
- ローカルグループは、管理コンソールで作成および管理されます。任意のローカルユーザーまたはディレクトリユーザーをローカルグループに割り当てることができます。

ディレクトリグループの追加

自分が 1 つ以上の会社のディレクトリにリンクしオンボーディングを構成している場合、ディレクトリグループを Cylance Endpoint Security に自動的に追加できます。オンボーディングによってディレクトリグループが追加されていない場合は、ディレクトリグループを追加することもできます。

1. 管理コンソールのメニューバーで、［アセット］ > ［ユーザーグループ］をクリックします。
2. ［グループを追加］ > ［ディレクトリグループ］をクリックします。
3. ディレクトリに表示されているグループの名前を入力します。
4. 検索結果にグループ名が表示されたら、グループ名を選択します。
5. グループとネストされたグループをオンボーディングに使用できるようにするには、［ネストされたディレクトリグループ］を選択します。
6. グループにポリシーを割り当てるには、⊕ をクリックし、追加するポリシーのタイプを選択します。
7. ポリシーを選択し、［保存］をクリックします。

ローカルグループを追加

1. 管理コンソールのメニューバーで、［アセット］ > ［ユーザーグループ］をクリックします。
2. ［グループを追加］ > ［ローカルグループ］をクリックします。
3. グループの名前と説明を入力します。
4. グループにポリシーを割り当てるには、⊕ をクリックし、追加するポリシーのタイプを選択します。
5. ポリシーを選択し、［保存］をクリックします。
6. ポリシーの割り当てが完了したら、［保存］をクリックします。
7. グループにユーザーを追加するには、［ユーザーグループ］ページでグループ名をクリックし、［ユーザー］をクリックします。
8. ［ユーザーを追加］をクリックします。
9. 追加するユーザーの名前を入力して検索します。
10. 検索結果から 1 つ以上の名前を選択します。
11. ［保存］をクリックします。

ユーザーページのグループから個々のユーザーを追加および削除することもできます。

認証方法の追加

認証ポリシーに追加できるように、認証方法を追加します。認証では、認証方式を 1 つ定義するのが一般的です。たとえば、パスワード（Cylance コンソールパスワードなど）や、Active Directory、Okta、Ping Identity のような、サードパーティに接続して行う認証などが挙げられます。認証方法を認証ポリシーに追加して、管理者が Cylance コンソールにサインインするために完了する必要がある認証のタイプと、ユーザーが Cylance Endpoint Security アプリまたはエージェント（CylancePROTECT Mobile アプリ、CylanceGATEWAY など）をアクティブ化するために完了する必要がある認証のタイプを指定します。1 つの認証ポリシーに複数の認証方法を組み合わせて設定することで、複数ステップの認証を実現できます。たとえば、エンタープライズ認証とワンタイムパスワードのプロンプトを組み合わせたポリシーを設定すると、仕事用または Cylance コンソールパスワードと、ワンタイムパスワードの両方による認証をユーザーに要求できます。

作業を始める前に：

- 重要：IDP SAML 認証方法の設定前に、「強化された認証サインイン」の適切な手順を確認し、Cylance コンソールに実行したことを確認します。必要な手順が完了していない場合、サードパーティの認証方法は Cylance Endpoint Security と通信できません。詳細については、以下を参照してください。
  - IDP を設定して認証を強化し、IDP によって Cylance コンソールにアクセスする手順については、「強化された認証サインイン」を参照してください。
  - 新しい IDP SAML の設定手順については、「Cylance コンソールへの拡張認証および IDP 開始アクセスのための IDP SAML の設定方法」を参照してください。
  - 2023 年 12 月以前に作成された既存の IDP SAML のコンソールへの IDP 開始アクセスを有効にする手順については、「SSO 用の外部 IDP（SAML）認証方法を更新して Cylance コンソールにアクセスする方法」を参照してください。
- SAML 認証を追加する場合、IDP に対する署名証明書のコピーをダウンロードします。

1. メニューバーで［設定］**>**［認証］をクリックします。
2. ［認証方法を追加］をクリックします。
3. ［認証方法のタイプ］ドロップダウンリストで、次のいずれかの認証方法を選択します。

項目	説明
Entra （SAML）	プライマリサインインページでユーザーに Entra 資格情報を入力させて、Cylance コンソールへの IDP 開始アクセスを有効にする場合は、このオプションを選択します。 Entra （SAML）の設定手順の詳細については、以下を参照してください。 • 新規 Entra （SAML）の設定：拡張認証用に Entra （SAML）認証方法を設定します。 • 既存の Entra （SAML）の Entra 開始アクセスの有効化：Entra （SAML）認証方法を更新して、Cylance コンソールへの IDP 開始アクセスを有効にします。 メモ：SSO コールバック URL は、認証方法を保存すると生成され、https://login.eid.blackberry.com/_/resume/saml20/<*hash*> の形式になります。 次の手順に従います。 **a.** 認証方法の名前を入力します。 **b.** ユーザーが初めてログインするときに 1 回限りのコードでメールを検証するように要求する場合は、［検証が必要］をオンにします。コードは、テナント内のユーザーに紐づけられているメールアドレスに送信されます。 **c.** ［ログイン要求 **URL**］フィールドに、ID プロバイダーのアプリ登録シングルサインオン設定で指定されているログイン URL を入力します。たとえば Entra ポータルでは、［エンタープライズアプリケーション］ > <*Name of the newly created application*> > *application name* 設定セクション > ［ログイン URL］に移動します。 **d.** ［**IDP** 署名証明書］フィールドに、ダウンロードした署名証明書の本文（Begin Certificate 行と End Certificate 行を含む）を貼り付けます。 証明書の本文をコピーして貼り付けるときは、証明書情報の改行や形式を変更してしまわないように注意してください。 **e.** ［**SP** エンティティ **ID**］フィールドに、Entra ポータルの SAML 設定から記録した **ID**（エンティティ **ID**）を入力します。必須フィールドです。［SP エンティティ ID］の値は、IDP コンソールで記録した ID（エンティティ ID）の値と一致する必要があります。 **f.** ［詳細設定の表示］を有効にして、［メールクレーム］フィールドに、Entra ポータルで記録したクレーム名の値を貼り付けます（例：http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress）。 **g.** 他のオプション設定を指定します。 **h.** ［保存］をクリックします。 **i.** 追加した認証方法を開きます。**SSO** コールバック **URL** を記録します。この URL は、Entra ポータル > ［基本 SAML 設定］> ［返信 URL］ フィールド（アサーションコンシューマ URL）で必要です。

項目	説明
カスタム（SAML）	プライマリサインインページでユーザーにカスタム資格情報を入力させて、Cylance コンソールへの IDP 開始アクセスを有効にする場合は、このオプションを選択します。 カスタム（SAML）の設定手順の詳細については、以下を参照してください。 • 新規カスタム（SAML）の設定：拡張認証用にカスタム（SAML）認証方法を設定します。 • 既存のカスタム（SAML）のカスタム開始アクセスの有効化：カスタム（SAML）認証方法を更新して、Cylance コンソールへの IDP 開始アクセスを有効にします。 メモ：SSO コールバック URL は、認証方法を保存すると生成され、https://login.eid.blackberry.com/_/resume/saml20/<*hash*> の形式になります。 **a.** 認証方法の名前を入力します。 **b.** ユーザーが初めてログインするときに 1 回限りのコードでメールを検証するように要求する場合は、［検証が必要］をオンにします。 **c.** ［ログイン要求 **URL**］フィールドに、ID プロバイダーのシングルサインオン URL を入力します。 **d.** ［**IDP** 署名証明書］フィールドに、ダウンロードした署名証明書の本文（Begin Certificate 行と End Certificate 行を含む）を貼り付けます。 証明書の本文をコピーして貼り付けるときは、証明書情報の改行や形式を変更してしまわないように注意してください。 **e.** ［**SP** エンティティ **ID**］フィールドに、カスタム IDP ポータルで記録した対象者 URI（SP エンティティ ID）を入力します。必須フィールドです。［SP エンティティ ID］の値は、IDP コンソールで記録した対象者 URI（SP エンティティ ID）の値と一致する必要があります。 **f.** ［名前 **ID** 形式］フィールドで、IDP から要求する名前識別子形式を指定します（例：urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress）。 **g.** ［メールクレーム］フィールドに「`NameID`」と入力します。この値は、IDP コンソールで指定した NameID 形式と一致する必要があります。メールアドレスにより、正しいユーザーが管理コンソールにサインインしていることが確認されます。 **h.** 他のオプション設定を指定します。 **i.** ［保存］をクリックします。 **j.** 追加した認証方法を開きます。シングルサインオン **URL** を記録します。この URL はカスタム IDP に追加されます。

項目	説明
Cylance 管理者パスワード	ユーザーに自分の Cylance コンソールの資格情報を入力させる場合は、このオプションを選択します。次の手順に従います。 **a.** 認証方法の名前を入力します。 **b.** ［保存］をクリックします。
認証を拒否	認証ポリシーを使用して、ユーザーやユーザーグループが Cylance コンソールなどのサービスにアクセスできないようにする場合は、このオプションを選択します。ポリシー例外やアプリケーション例外を新たに追加すると、ユーザーのサブセットへのアクセスを許可できるようになります。 **a.** 認証方法の名前を入力します。 **b.** ［保存］をクリックします。
Duo MFA	ユーザーに Duo 多要素認証を使用して認証させる場合は、このオプションを選択します。 Duo を認証方法として追加する前に、認証 API アプリケーションを作成する必要があります。手順については、Duo の情報を参照してください。 次の手順に従います。 **a.** 認証方法の名前を入力します。 **b.** ［**Duo MFA** の設定］セクションで、API のホスト名、インテグレーションキー、およびシークレットキーを入力します。この情報は、組織の Duo アカウントの［アプリケーション］タブで確認できます。詳細については、Duo のマニュアルを参照してください。
エンタープライズ	ユーザーに Active Directory、LDAP、または *my*Account の資格情報を使用して認証させる場合は、このオプションを選択します。ユーザーが使用する資格情報は、コンソールのユーザーアカウントのソースとなるアカウントタイプによって異なります。次の手順に従います。 **a.** 認証方法の名前を入力します。 **b.** ［保存］をクリックします。

項目	説明
FIDO	ユーザーに FIDO2 デバイスを登録してもらい、ID を確認できるようにする場合は、このオプションを選択します。サポートされるデバイスタイプには、スマートフォン、USB セキュリティキー、Windows Hello があります。 **a.** 認証方法の名前を入力します。 **b.** ［保存］をクリックします。 FIDO が第 1 認証要素の場合は、ユーザーがデバイスの初回登録を行うときに、サインインで使用するメールアドレスにワンタイムパスワードが送信されます。FIDOがポリシーの第 2 認証要素として使用される場合は、ユーザーがデバイスの初回登録を行うときでもワンタイムパスワードは要求されません。 ユーザーアカウントから登録済みデバイスを削除する方法については、管理関連の資料の「ユーザーアカウントから登録済みの FIDO デバイスを削除する」を参照してください。
統合されたディレクトリ（Active Directory/Entra ID/LDAP）	ユーザーに Active Directory パスワードを入力させる場合は、このオプションを選択します。このオプションを選択する場合は、Cylance Endpoint Security テナントが会社のディレクトリのインスタンスと接続している必要があります。詳細については、「会社のディレクトリへのリンク」を参照してください。次の手順に従います。 **a.** 認証方法の名前を入力します。 **b.** ［保存］をクリックします。
IPアドレス	IP アドレスに基づいてユーザーのアクセスを制限する場合は、このオプションを選択します。IP アドレス認証を複数作成すると、異なるグループのアクセスを管理できるようになりますが、1 つのポリシーには、1 つの IP アドレス認証しか割り当てることができません。 コンソールの IP アドレス制限を追加または削除する手順については、「Cylance コンソールの IP アドレス制限認証方法の追加」を参照してください。 **a.** 認証方法の名前を入力します。 **b.** ［**IP** アドレス範囲］フィールドで、IP アドレス、IP 範囲、CIDR を 1 つ以上指定します。エントリはカンマで区切ります。例：IP 範囲：192.168.0.100-192.168.1.255 または CIDR：192.168.0.10/24 **c.** ［保存］をクリックします。
ローカルアカウント	ユーザーに自分の BlackBerry Online Account （*my*Account）資格情報の入力を要求する場合は、このオプションを選択します。次の手順に従います。 **a.** 認証方法の名前を入力します。 **b.** ［保存］をクリックします。

項目	説明
Okta MFA	ユーザーに Okta を使用して認証させる場合は、このオプションを選択します。次の手順に従います。 **a.** 認証方法の名前を入力します。 **b.** ［**Okta MFA** の設定］セクションで、認証 API キーと認証ドメインを入力します。 **c.** ［保存］をクリックします。
Okta （OIDC）	ユーザーに Okta を使用して認証させる場合は、このオプションを選択します。次の手順に従います。 **a.** **Okta** のドロップダウンリストで、［**OIDC**］を選択します。 **b.** 認証方法の名前を入力します。 **c.** ［アイデンティティプロバイダクライアント］セクションで、OIDC 検出ドキュメントの URL、クライアント ID、およびプライベートキー JWKS を入力します。 **d.** ［保存］をクリックします。

項目	説明
Okta （SAML）	プライマリサインインページでユーザーに Okta 資格情報を入力させて、Cylance コンソールへの IDP 開始アクセスを有効にする場合は、このオプションを選択します。 Okta （SAML）の設定手順の詳細については、以下を参照してください。 • 新規 Okta （SAML）の設定：拡張認証用に Okta （SAML）認証方法を設定します。 • 既存の Okta （SAML）の Okta 開始アクセスの有効化：Okta （SAML）認証方法を更新して、Cylance コンソールへの IDP 開始アクセスを有効にします。 メモ：SSO コールバック URL は、認証方法を保存すると生成され、https://login.eid.blackberry.com/_/resume/saml20/<*hash*> の形式になります。 **a.** **Okta** のドロップダウンリストで、［**SAML**］を選択します。 **b.** 認証方法の名前を入力します。 **c.** ユーザーが初めてログインするときに 1 回限りのコードでメールを検証するように要求する場合は、［検証が必要］をオンにします。 **d.** ［ログイン要求 **URL**］フィールドに、ID プロバイダーのシングルサインオン URL を入力します。 **e.** ［**IDP** 署名証明書］フィールドに、ダウンロードした署名証明書の本文（Begin Certificate 行と End Certificate 行を含む）を貼り付けます。 証明書の本文をコピーして貼り付けるときは、証明書情報の改行や形式を変更してしまわないように注意してください。 **f.** ［**SP** エンティティ **ID**］フィールドに、Okta ポータルで記録した対象者 URI（SP エンティティ ID）を入力します。必須フィールドです。［SP エンティティ ID］の値は、IDP コンソールで記録した対象者 URI（SP エンティティ ID）の値と一致する必要があります。 **g.** ［**IDP** エンティティ **ID**］フィールドに、Okta から記録した IdentityProvider 発行者を貼り付けます。 **h.** ［名前 **ID** 形式］フィールドで、Okta に指定した NameID 形式を選択します（例：urn:oasis:names:tc:SAML:2.0:nameid-format:persistent）。 **i.** ［メールクレーム］フィールドに「`Email`」と入力します。これは、Okta コンソールで設定した属性名と一致する必要があります。メールアドレスにより、正しいユーザーが管理コンソールにサインインしていることが確認されます。 **j.** 他のオプション設定を指定します。 **k.** ［保存］をクリックします。 **l.** 追加した認証方法を開きます。シングルサインオン URL を記録します。この URL は、Okta コンソール > ［SAML 設定］画面の次のフィールドに追加されます。 • シングルサインオン URL • 要求可能な SSO URL

項目	説明
OneLogin （OIDC）	ユーザーに OneLogin を使用して認証させる場合は、このオプションを選択します。次の手順に従います。 **a.** **OneLogin** のドロップダウンリストで、［**OIDC**］を選択します。 **b.** 認証方法の名前を入力します。 **c.** ユーザーが初めてログインするときに 1 回限りのコードでメールを検証するように要求する場合は、［検証が必要］をオンにします。 **d.** ［**OneLogin** の設定］セクションで、OIDC 検出ドキュメントの URL、クライアント ID、クライアントシークレット、および認証方法を入力します。 **e.** ［保存］をクリックします。

項目	説明
OneLogin （SAML）	プライマリサインインページでユーザーに OneLogin 資格情報を入力させて、Cylance コンソールへの IDP 開始アクセスを有効にする場合は、このオプションを選択します。 OneLogin （SAML）の設定手順の詳細については、以下を参照してください。 • 新規 OneLogin （SAML）の設定：拡張認証用に OneLogin （SAML）認証方法を設定します。 • 既存の OneLogin （SAML）の OneLogin 開始アクセスの有効化：OneLogin （SAML）認証方法を更新して、Cylance コンソールへの IDP 開始アクセスを有効にします。 メモ：SSO コールバック URL は、認証方法を保存すると生成され、https://login.eid.blackberry.com/_/resume/saml20/<*hash*> の形式になります。 **a.** 認証方法の名前を入力します。 **b.** ユーザーが初めてログインするときに 1 回限りのコードでメールを検証するように要求する場合は、［検証が必要］をオンにします。 **c.** ［ログイン要求 **URL**］フィールドに、ID プロバイダーのシングルサインオン URL を入力します。 **d.** ［**IDP** 署名証明書］フィールドに、ダウンロードした署名証明書の本文（Begin Certificate 行と End Certificate 行を含む）を貼り付けます。 証明書の本文をコピーして貼り付けるときは、証明書情報の改行や形式を変更してしまわないように注意してください。 **e.** ［**SP** エンティティ **ID**］フィールドに、OneLogin コンソールで記録した ID（エンティティ ID）を入力します。必須フィールドです。［SP エンティティ ID］の値は、IDP コンソールで記録した ID（エンティティ ID）の値と一致する必要があります。 **f.** 他のオプション設定を指定します。 **g.** ［保存］をクリックします。 **h.** 追加した認証方法を開きます。シングルサインオン URL を記録します。この URL は、OneLogin コンソールの次のフィールドに追加されます。 • ACS（コンシューマ）URL バリデータ* • ACS（コンシューマ）URL* • シングルログアウト URL

項目	説明
ワンタイムパスワード	ユーザーに、別のタイプの認証に加えてワンタイムパスワードの入力も要求する場合は、このオプションを選択します。 メモ：このオプションを選択した場合、認証ポリシーに別の認証を追加して、ワンタイムパスワードよりも高い位置付けにする必要があります。 管理者用ワンタイムパスワード認証を追加および削除する手順については、次を参照してください。 • 管理者用ワンタイムパスワード認証の追加 • 管理者用ワンタイムパスワード認証の削除 次の手順に従います。 **a.** 認証方法の名前を入力します。 **b.** ［ワンタイムパスワードの設定］セクションの最初のドロップダウンリストで、間隔を選択します。ウィンドウ内のあらゆるコードは、予期したコードから指定した更新間隔の数だけ前または後にある場合は有効です。更新間隔は 30 秒で、デフォルト設定は 1 です。 **c.** **[**ワンタイムパスワードの設定**]** セクションの 2 つ目のドロップダウンリストでは、OTP アプリのセットアップをスキップして、コード入力なしで認証できる回数を指定します。
Ping Identity （OIDC）	Ping Identity を使用してユーザーに認証してもらう場合は、このオプションを選択します。手順は次のとおりです。 **a.** ［**Ping**］のドロップダウンリストで、**[OIDC]**を選択します。 **b.** 認証方法の名前を入力します。 **c.** ［アイデンティティプロバイダクライアント］セクションで、OIDC 検出ドキュメントの URL、クライアント ID、およびプライベートキー JWKS を入力します。 **d.** ［**ID** トークンの署名アルゴリズム］のドロップダウンリストで、署名アルゴリズムを選択します。 **e.** ［保存］をクリックします。

項目	説明
Ping Identity （SAML）	プライマリサインインページでユーザーに Ping Identity 資格情報を入力させて、Cylance コンソールへの IDP 開始アクセスを有効にする場合は、このオプションを選択します。 Ping Identity （SAML）の設定手順の詳細については、以下を参照してください。 • 新規 Ping Identity （SAML）の設定：拡張認証用に Ping Identity （SAML）認証方法を設定します。 • 既存の OneLogin （SAML）の Ping Identity 開始アクセスの有効化：Ping Identity （SAML）認証方法を更新して、Cylance コンソールへの IDP 開始アクセスを有効にします。 メモ：SSO コールバック URL は、認証方法を追加すると生成され、https://login.eid.blackberry.com/_/resume/saml20/<*hash*> の形式になります。 **a.** ［**Ping Identity**］のドロップダウンリストで、**[SAML]**を選択します。 **b.** 認証方法の名前を入力します。 **c.** ユーザーが初めてログインするときに 1 回限りのコードでメールを検証するように要求する場合は、［検証が必要］をオンにします。 **d.** ［ログイン要求 **URL**］フィールドに、ID プロバイダーのシングルサインオン URL を入力します。 **e.** ［**IDP** 署名証明書］フィールドに、ダウンロードした署名証明書の本文（Begin Certificate 行と End Certificate 行を含む）を貼り付けます。 証明書の本文をコピーして貼り付けるときは、証明書情報の改行や形式を変更してしまわないように注意してください。 **f.** ［**SP** エンティティ **ID**］フィールドに、PingOne コンソールで記録したエンティティ ID を入力します。必須フィールドです。［SP エンティティ ID］の値は、IDP コンソールで記録したエンティティ ID の値と一致する必要があります。 **g.** 他のオプション設定を指定します。 **h.** ［保存］をクリックします。 **i.** 追加した認証方法を開きます。シングルサインオン URL を記録します。この URL は、次の PingOne コンソールの設定画面のフィールドに入力する必要があります。 • アサーションコンシューマサービス（ACS） • アプリケーション URL

4. ［保存］をクリックします。

終了したら： 認証ポリシーの作成。

SAML 認証の追加に関する考慮事項

SAML 認証を追加する場合、ログイン要求 URL と IDP 署名証明書の値が必要です。オプションのフィールドについては、次の点に注意してください。

メモ：外部 ID プロバイダーを設定する場合には、Cylance Endpoint Security ログイン要求 URL を追加する必要があります。URL は、https://login.eid.blackberry.com/_/resume/saml20/<*hash*> の形式である必要があります。外部 SAML 設定はシングルサインオンまたはアサーションコンシューマサービス返信 URL のリストをサポートしているため、既存の設定では、新しい URL または新しく生成した URL は 2 番目のオプションとしてリストに追加するか、元の URL を置き換えることができます。認証方法が 2023 年 12 月より前に作成したものである場合に、ユーザーがシングルサインオンを使用して Cylance コンソールにアクセスできるようにするには、更新されたログイン要求 URL を生成する必要があります。認証方法の更新の詳細については、「強化された認証サインイン」を参照してください。

項目	説明
名前 ID 形式	このフィールドを使用して、ID プロバイダーから要求するオプションの名前 ID 形式を指定できます。
フェデレーション ID のクレーム	このフィールドを使用して、システム間でアカウントをリンクするためのフェデレーション ID として使用されるクレーム値を任意で指定します。デフォルト値は NameID です。 「NameID」以外のクレームでメールアドレスを返すように IDP が設定されている場合は、このフィールドにクレームを指定する必要があります。このクレームには、一意で不変かつ永続的な値（objectGUID または UUID など）を使用する必要があります。メールアドレスのように、一意ではなく変更される可能性がある値を使用することはお勧めしません。ユーザーがログインすると、Cylance Endpoint Security はフェデレーション ID クレームの値を使用してユーザーの一意の ID を作成し、両方のシステムに ID をマッピングします。 フェデレーション ID クレームとして使用するために指定した値は、ユーザーが初めてログインしたときに外部 ID プロバイダーおよび Cylance Endpoint Security でのユーザーのリンクに使用されるため、後から変更することはできません。
Active Directory のクレーム	このフィールドを使用して、Active Directory の objectGUID をシステム間で一致させ、ユーザーを検証するために使用されるクレーム値を任意で指定できます。

項目	説明
メールのクレーム	このフィールドを使用して、システム間でメールアドレスを一致させるために使用されるクレーム値を任意で指定できます。デフォルト値は「email」です。 Cylance Endpoint Security では、すべての SAML 応答にユーザーの完全なメールアドレスが含まれ、そのメールアドレスが Cylance Endpoint Security に登録されているメールアドレスと一致していることを必要とします。「email」以外のクレームでメールアドレスを返すように IDP が設定されている場合は、このフィールドにクレームを指定する必要があります。たとえば、IDP で設定されたクレームの名前が「emailAddress」である場合は、［メールのクレーム］フィールドで「emailAddress」と設定する必要があります。これらが一致しない場合、ユーザーはサインインできません。
SP エンティティ ID	このフィールドを使用して、ID プロバイダーに送信するサービスプロバイダーエンティティ ID（発行者文字列）を任意で指定できます。 Entra SAML 認証の場合、このフィールドは必須です。入力する値は、Entra の SAML 構成の識別子（エンティティ ID）と一致する必要があります。
IDP エンティティ ID	このフィールドを使用して、ID プロバイダーエンティティ ID（IDP 発行者）を任意で指定できます。指定した場合、すべての応答でその IDP 発行者が検証されます。
許容されるクロックドリフト	このフィールドを使用して、クライアントとサーバー間の許容可能なクロックドリフトをミリ秒単位で指定できます。
署名アルゴリズム	このフィールドを使用して、署名要求に対する署名アルゴリズムを指定できます。
署名のプライベートキー	このフィールドを使用して、送信されるすべての要求の署名に使用されるオプションのプライベートキーを PEM 形式で指定できます。

カスタム認証設定を認証方法リストに移行する

既存の SAML 認証を［設定］の認証方法リストに移行して、ユーザーおよびグループまたはテナントの認証ポリシーに追加されるようにすることができます。認証方法を移行する場合、シングルサインオン URL を Cylance Endpoint Security で使用される URL に更新する必要があります。また、外部 IDP 設定の NameID クレームを更新して、ユーザーのメールアドレスではなく永続的で不変な値が返されるようにするか、フェデレーション ID のクレームとして使用できるクレームを ID プロバイダーで作成する必要があります。

設定を移行する前に、フェイルセーフとして、Cylance コンソールパスワードだけを必要とする認証ポリシーを 1 つ作成し、それを 1 人の管理者に割り当てておくとよいでしょう。

メモ：カスタム認証設定を移行する場合、外部 ID プロバイダーで、Cylance Endpoint Security ログイン要求 URL として `https://idp.blackberry.com/_/resume` を追加する必要があります。外部 SAML 設定はシングルサインオンまたはアサーションコンシューマサービス返信 URL のリストをサポートしているため、既存の設定では、新しい URL は 2 番目のオプションとしてリストに追加するか、元の URL を置き換えることができます。

SAML 認証の詳細については、「SAML 認証の追加に関する考慮事項」を参照してください。

作業を始める前に： IDP の署名証明書のコピーをダウンロードします。

1. 管理コンソールのメニューバーで、［設定］ > ［アプリケーション］をクリックします。
2. ［カスタム認証］セクションで次の手順を実行します。
   a) 次の情報をテキストファイルにコピーします。
      - プロバイダー名
      - ログインURL
   b) ［パスワードログインを許可］チェックボックスをオンにします。この設定の詳細については、「カスタム認証の説明」を参照してください。
3. メニューバーで、［設定］ > ［認証］をクリックします。
4. ［認証方法］タブで、［認証方法を追加］をクリックします。
5. ［認証方法のタイプ］ドロップダウンリストで、手順 2 でコピーしたプロバイダーに対応する SAML 認証（Entra または Okta など）をクリックするか、カスタム SAML をクリックします。
6. ［全般情報］セクションで、認証方法の名前を入力します。
7. ［**SAML** 構成］セクションで、ユーザーが初めてログインするときに 1 回限りのコードでメールを検証するように要求する場合は、［検証が必要］をオンにします。
8. ［ログイン要求 **URL**］フィールドに、ID プロバイダーのシングルサインオン URL を入力します。
9. ［**IDP** 署名証明書］フィールドに、ダウンロードした署名証明書の本文（Begin Certificate 行と End Certificate 行を含む）を貼り付けます。

   証明書の本文をコピーして貼り付けるときは、証明書情報の改行や形式を変更してしまわないように注意してください。
10. 次の操作のいずれかを実行します。

タスク	手順
外部 ID プロバイダーの NameID とメールクレームの値を更新します。	**a.** 外部 ID プロバイダーにサインインします。 **b.** Cylance Endpoint Security のシングルサインオン URLを `https://idp.blackberry.com/_/resume` に更新します。この URL は、既存の login.<*region*>.cylance.com URL に追加できます。 **c.** NameID クレームを編集して、ユーザーのメールアドレスではなく、フェデレーション ID のクレームで使用できる永続的で不変な値（objectGUID や UUID など）が返されるようにします。手順については、ID プロバイダーのドキュメントを参照してください。 **d.** ユーザーのメールアドレスを返す新しいメールクレームを作成します。

タスク	手順
外部 ID プロバイダーで新しいクレームを作成し、認証方法の設定に追加します。	**a.** 外部 ID プロバイダーにサインインします。 **b.** Cylance Endpoint Security のシングルサインオン URLを `https://idp.blackberry.com/_/resume` に更新します。この URL は、既存の login.<*region*>.cylance.com URL に追加できます。 **c.** ユーザーの永続的で不変な ID を返す新しいクレームを作成します。手順については、ID プロバイダーのドキュメントを参照してください。 **d.** Cylance 管理コンソールの［メールのクレーム］フィールドに、「`nameID`」と入力します。nameID 値では小文字の「n」を使用する必要があります。 **e.** ［フェデレーション **ID** のクレーム］フィールドに、外部 ID プロバイダーで作成した新しいクレームの名前を入力します。

11. ［保存］をクリックします。

終了したら：

- 認証ポリシーの作成。
- 認証ポリシーで SAML 認証を使用してログインする際に問題が発生した場合は、IDP から SAML 応答のサンプルをダウンロードし、クレーム名を検証できます。

テナントの認証ポリシーの管理

Cylance Endpoint Security には、デフォルトで 3 つのテナント認証ポリシーがあり、認証タイプの管理で使用されます。管理者が Cylance コンソールにサインインしたり、ユーザーが Cylance Endpoint Security アプリまたはエージェント（CylancePROTECT Mobile アプリや CylanceGATEWAY など）をアクティベートしたりするのに必要な認証になります。テナントポリシーは、ユーザーがアクセスしようとするコンソールまたはアプリで、アプリの例外ポリシーや認証ポリシーが当該のユーザーに割り当てられていない場合に適用されます。デフォルトのポリシーと認証方法は次のとおりです。

- 管理コンソール：このポリシーでは、Cylance コンソールパスワードをデフォルト認証として使用します。2024 年 3 月以降に作成されたテナントの場合、このポリシーでは Cylance コンソールパスワードとワンタイムパスワードがデフォルト認証として使用されます。Cylance Endpoint Security 管理コンソールでの認証で使用されます。
- CylanceGATEWAY ：このポリシーは、ユーザーのエンタープライズパスワードをデフォルト認証として使用します。ユーザーが CylanceGATEWAY アプリまたはデスクトップエージェントをアクティベートするときに使用されます。
- CylancePROTECT Mobile アプリ：このポリシーでは、ユーザーのエンタープライズパスワードをデフォルト認証として使用します。ユーザーがモバイルデバイスで CylancePROTECT アプリをアクティベートするときに使用されます。デスクトップエージェントの場合は適用されません。

ポリシーを編集して他のタイプの認証を追加すると、ポリシーで指定した順序での認証実施をユーザーに要求できます。たとえば、エンタープライズ認証の後にワンタイムパスワードを追加すると、ユーザーは仕事用または *my*Account の資格情報を入力してから、ワンタイムパスワードの入力をプロンプトされることになります。

作業を始める前に： 認証方法の追加。

1. メニューバーで［設定］ **>** ［認証］ **>** ［デフォルト認証］の順にクリックします。

2. 編集するポリシーをクリックします。
3. ［アプリ認証］セクションで［認証方法の追加］をクリックします。
4. ［認証方法を追加］ダイアログボックスのドロップダウンリストで、認証方法を選択します。［追加］をクリックします。

   この手順を繰り返して、ポリシーにさらに認証方法を追加します。ユーザーは、指定した順序で認証のタイプの入力を完了する必要があります。順序を変更するには、［順序の設定］をクリックし、認証方法をドラッグして希望の順序に変更してから［順序の設定］をクリックします。

   メモ：ワンタイムパスワードを認証方法として追加する場合は、エンタープライズパスワードの後に設定する必要があります。

   再度
5. ［保存］をクリックします。

認証方法をデフォルトポリシーに追加する場合、ポリシーリストのページで［デフォルト方式に戻す］をクリックすると、デフォルトの設定に戻すことができます。

認証ポリシーの作成

認証ポリシーを作成し、管理者が Cylance Endpoint Security 管理コンソールへのサインインを完了するために必要な認証のタイプと、ユーザーが Cylance Endpoint Security アプリやエージェント（CylancePROTECT Mobile、CylanceGATEWAY エージェントなど）のアクティブ化を完了するために必要な認証のタイプを指定します。ユーザーは、ポリシーで指定した順序で認証のタイプを完了する必要があります。たとえば、ワンタイムパスワードの前にエンタープライズを追加すると、ユーザーはワンタイムパスワードの入力をプロンプトされる前に自分の仕事用または *my*Account の資格情報を入力します。

ポリシーでは、アプリの例外を設定したり、特定のアプリに別の認証方法を指定したりできます。アプリの例外は、認証ポリシーよりも優先されます。テナントに設定される認証ポリシーは、次の順序で適用されます。

1. ユーザーやグループに割り当てられた認証ポリシーにおけるアプリの例外
2. ユーザーやグループに割り当てられた認証ポリシー
3. テナントアプリケーションポリシー

作業を始める前に： 認証方法の追加

1. メニューバーで、［ポリシー］ > ［ユーザーポリシー］をクリックします。
2. ［認証］タブをクリックします。
3. ［ポリシーを追加］をクリックします。
4. ポリシーの名前と説明を入力します。
5. ［認証ルール］セクションで［認証方法を追加］をクリックします。

   認証方法を 2023 年 12 月より前に作成し、Cylance Endpoint Security ログインリクエスト URL を更新して IDP 開始プロキシを有効にし、ユーザーがシングルサインオン（SSO）を使用してユーザーの IDP ポータルにログイン後、Cylance コンソールにアクセスできるようにした場合は、更新した認証方法を追加して、作成した元の認証を削除してください。詳細については、「強化された認証サインイン」を参照してください。
6. ［認証方法の追加］ダイアログボックスのドロップダウンリストで、認証方法を選択します。

   この手順を繰り返して、ポリシーにさらに認証方法を追加します。ユーザーは、ポリシーに記載されている順序で各認証時にプロンプトされます。Duo MFA をポリシーに追加する場合は、認証の第 2 要素として Duo が使用されるように、別の認証方法も追加する必要があります。順序を変更するには、［順序を設定］をクリックし、認証方法をドラッグして希望の順序に変更してから［順序を設定］を再度クリックします。

7. アプリの例外を追加する場合、［アプリの例外の管理］をクリックします。
8. ［アプリの例外の管理］ ダイアログボックスで、［使用可能なアプリ］ペインに含めるアプリを選択します。
9.  をクリックします。
10. ［保存］をクリックします。
11. ［アプリの例外の管理］セクションで、例外として追加したアプリのタブをクリックします。
12. ［認証方法を追加］をクリックします。
13. ［認証方法の追加］ダイアログボックスのドロップダウンリストから認証方法を選択します。［保存］をクリックします。

    この手順を繰り返して、アプリの例外にさらに認証方法を追加します。ユーザーは、指定した順序で認証のタイプの入力を完了する必要があります。順序を変更するには、［順序を設定］をクリックし、認証方法をドラッグして希望の順序に変更してから［順序を設定］を再度クリックします。
14. このポリシーを保存するには、［保存］をクリックします。

終了したら： 管理者、ユーザー、およびグループへのポリシーの割り当て。

管理者、ユーザー、およびグループへのポリシーの割り当て

ユーザーポリシーは、任意の数のグループ、管理者、およびユーザーに割り当てることができますが、各管理者やユーザーには、それぞれに割り当てられた各タイプのユーザーポリシーを 1 つだけ割り当てることができます。ユーザーや管理者に直接割り当てられたポリシーは、ユーザーや管理者が属するグループに割り当てられたポリシーよりも優先されます。ポリシーが管理者やユーザーに直接割り当てられておらず、管理者やユーザーが同じタイプの異なるポリシーを割り当てられた複数のグループに属している場合、割り当てられたポリシーの最高ランクが管理者やユーザーに適用されます。

管理コンソールにログインするたびに、割り当てられたポリシーが一致するまで、管理者とユーザーに割り当てられたポリシーに対してログインが評価されます。管理者やユーザーにポリシーが直接割り当てられていない場合、またはメンバーになっているグループを介してポリシーが割り当てられていない場合は、デフォルトポリシーが適用され、Cylance コンソールには Cylance パスワードを使用してのみサインインできます。強化された認証ポリシーは、次の順序で管理者およびユーザーに適用されます。

- ユーザーポリシーアプリケーションの例外
- ユーザーポリシー
- テナントアプリケーションポリシー
- デフォルトポリシー

作業を始める前に： 次のポリシータイプの 1 つ以上を作成します。

- 登録ポリシー
- CylancePROTECT Mobile ポリシー
- CylanceGATEWAY Service ポリシー
- 認証ポリシー

1. メニューバーで、［ポリシー］ > ［ユーザーポリシー］をクリックします。
2. 割り当てるポリシータイプのタブを選択します。

3. 割り当てるポリシーの名前をクリックします。
4. ［割り当て済みのユーザーとグループ］をクリックします。
5. ［ユーザーまたはグループを追加］をクリックします。
6. ［ユーザー］タブをクリックします。
7. 検索するユーザーの名前の入力を開始します。デフォルトでは、最大 50 件の検索結果が返されます。50 件を超える検索結果が返されたら、検索を絞り込みます。

   管理者アカウントは、ユーザーリストに アイコンとともに表示されます。シナリオによっては、管理者アカウントと Active Directory ユーザーアカウントという 2 つのユーザーアカウントが 1 人のユーザーに対して表示される場合があります。
8. 検索結果から 1 つ以上の名前を選択します。［追加］をクリックします。

   また、［ユーザー設定ページ］でポリシーをユーザーに割り当てることもできます。
9. ［ユーザーグループ］タブをクリックします。
10. 検索して追加するユーザーグループの名前の入力を開始します。デフォルトでは、最大 50 件の検索結果が返されます。50 件を超える検索結果が返されたら、検索を絞り込みます。
11. 検索結果から 1 つ以上の名前を選択します。［追加］をクリックします。

    ポリシーは、［グループ設定ページ］でグループに割り当てることもできます。
12. ユーザーまたはグループからポリシーの割り当てを解除するには、ポリシーの割り当てを解除するユーザーおよびグループを選択し、［削除］をクリックします。

ポリシーをランク付け

個々のユーザーおよびユーザーグループにポリシーを割り当てることができます。個々のユーザーにポリシーを割り当てると、ユーザーが属するグループに割り当てたポリシーよりも優先されます。ポリシーがユーザーに直接割り当てられておらず、ユーザーが所属する複数のグループに別々のポリシーが割り当てられている場合、割り当てられたポリシーの最高ランクのものがユーザーに適用されます。

ポリシーをランク付けする前に、目標とポリシーの割り当て先グループに基づいて戦略を決定する必要があります。たとえば、特定の部門グループに適用されるネットワークアクセス制御ポリシーを最高ランクにし、より制限の厳しいポリシーをそれより下にランク付けします。または、最も制限の厳しいポリシーを最高ランクにすることもできます。

1. メニューバーで、［ポリシー］ > ［ユーザープロファイル］をクリックします。
2. 割り当てるポリシータイプのタブを選択します。
3. ［ランク付け］をクリックします。
4. リスト内のポリシーの順序を変更するには、ポリシーの をリスト内の新しい位置にドラッグします。
5. ［保存］をクリックします。

CylancePROTECT Mobile および CylanceGATEWAY ユーザーの登録

ユーザーがモバイルデバイス上の CylancePROTECT Mobile アプリと Windows および macOS デバイス上の CylanceGATEWAY エージェントをアクティブ化できるように、登録ポリシーをユーザーに割り当てます。

登録ポリシーには、モバイルデバイス用とデスクトップデバイス用に個別の設定が含まれます。サポートされるデバイスタイプを指定できます。また、ユーザーに送信するメールメッセージとして、アクティベーション手順と、アクティベーションプロセスの開始に必要となるパスワードまたは QR Code が記載されたテキストを指定できます。アクティベーションパスワードまたは QR Code の有効日数は、［設定］ > ［アクティベーション］で指定できます。この設定は、すべての登録ポリシーに適用されます。

ユーザーが CylancePROTECT Mobile アプリまたは CylanceGATEWAY エージェントをアクティブ化する前に、ユーザーに次のポリシーを割り当てる必要があります。

ユーザーのタイプ	必要なポリシー
CylancePROTECT Mobile アプリユーザー、CylanceGATEWAY サポートなし	• 登録ポリシー • CylancePROTECT Mobile ポリシー
CylancePROTECT Mobile アプリユーザー、CylanceGATEWAY サポートのみあり	• 登録ポリシー • Gateway サービスポリシー
CylancePROTECT Mobile アプリユーザー、CylancePROTECT Mobile と CylanceGATEWAY の両方のサポートあり	• 登録ポリシー • CylancePROTECT Mobile ポリシー • Gateway サービスポリシー
CylanceGATEWAY エージェントを使用するデスクトップユーザー	• 登録ポリシー • Gateway サービスポリシー

メモ：CylanceGATEWAY エージェントは、セキュア Web ソケット（WSS）経由で通信するため、この接続を直接確立できる必要があります。適切なドメインへの接続を許可するように組織のネットワークを設定する必要があります。たとえば、CylanceGATEWAY エージェントがアクティブ化され、定期的に認証されるようにするには、idp.blackberry.com およびお住まいの地域のドメインへのアクセスを許可する必要があります。ご使用の環境で認証プロキシを使用している場合は、プロキシサーバー上のトラフィックを許可する必要があります。適切なドメインが許可されていないと、CylanceGATEWAY エージェントはブラウザを開いて認証プロセスを完了することができません。CylanceGATEWAY で許可する必要のあるドメインの詳細については、support.blackberry.com/community にアクセスして、記事 79017 を参照してください。Cylance Endpoint Security のネットワーク要件の詳細については、「Cylance Endpoint Security ネットワーク要件」を参照してください。

登録ポリシーの作成

1. 管理コンソールのメニューバーで、［ポリシー］ > ［ユーザーポリシー］をクリックします。
2. ［登録］タブをクリックします。

3. ［ポリシーを追加］をクリックします。
4. ポリシーの名前と説明を入力します。
5. CylancePROTECT Mobile アプリを使用してモバイルデバイスユーザーの登録オプションを設定するには、次の操作を実行します。
   a) ［モバイル］をクリックします。
   b) ユーザーが登録できるデバイスタイプを制限するには、［許可されたプラットフォーム］で［**iOS**］または［**Android**］をオフにします。
   c) ［**UES Mobile** ウェルカムメール］で、ユーザーに送信されるメールメッセージの件名を確認し、必要に応じて更新します。
   d) 必要に応じてメッセージの本文を更新し、組織固有の情報を提供します。
      メールメッセージでは変数を使用できます。
6. Windows および macOS デバイスで CylanceGATEWAY エージェントの登録オプションを設定するには、次の操作を実行します。
   a) ［**Gateway Desktop**］をクリックします。
   b) ユーザーが登録できるデバイスタイプを制限するには、［許可されたプラットフォーム］で［**Windows**］または［**macOS**］をオフにします。
   c) ［ウェルカムメール］で、ユーザーに送信されるメールメッセージの件名を確認し、必要に応じて更新します。
   d) 必要に応じてメッセージの本文を更新し、組織固有の情報を提供します。
      メールメッセージでは変数を使用できます。ユーザーは、最初のサインインページの［カスタムドメイン］フィールドに {{CustomDomain}} の値を入力する必要があります。変数を使用して値を挿入するか、［設定］ > ［アプリケーション］の［会社］フィールドで値を検索できます。
7. ［追加］をクリックします。

終了したら： ポリシーをユーザーおよびグループに割り当てます。

サポートされている登録メールの変数

登録ポリシーで指定するメールメッセージのテキストでは、次の変数を使用できます。

変数	説明
{{UserDisplayName}}	ユーザーページやユーザーがオンボーディングしたディレクトリに表示されるユーザーの表示名。
{{FullUserName}}	ユーザーページやユーザーがオンボーディングしたディレクトリに表示される完全なユーザー名。
{{UserName}}	ユーザーページやユーザーがオンボーディングしたディレクトリに表示されるユーザー名。
{{UserEmailAddress}}	ユーザーページやユーザーがオンボーディングしたディレクトリに表示されるユーザーのメールアドレス。
{{CustomDomain}}	組織の Cylance Endpoint Security の会社ドメイン名。この値は、［会社］フィールドの［設定］ > ［アプリケーション］に表示されます。

変数	説明
{{EnrollmentQRCode}}	モバイルデバイスの CylancePROTECT Mobile アプリのアクティベーションを簡素化するため、Cylance Endpoint Security によって生成される QR コード。この変数は、モバイルデバイスユーザーに送信されるメールメッセージでのみ使用できます。
{{EnrollmentPasscode}}	Cylance Endpoint Security によって生成されるアクティベーションパスワード
{{EnrollmentPasscodeExpiry}}	アクティベーションパスワードと QR コードの有効期限が切れる日付。アクティベーションパスワードや QR コードの有効日数は、［設定］ > ［アクティベーション］で設定できます。

CylancePROTECT Desktop および CylanceOPTICS を管理するためのゾーンの設定

ゾーンを使用して、CylancePROTECT Desktop および CylanceOPTICS デバイスをグループ化して管理できます。デバイスのグループ化は、地域（アジアやヨーロッパなど）、職務（営業担当者や IT スタッフなど）、または組織で必要な任意の基準に基づいて行うことができます。

デバイスポリシーをゾーンに割り当て、そのデバイスポリシーをゾーンに属する CylancePROTECT Desktop および CylanceOPTICS デバイスに適用できます。ドメイン名、IP アドレス範囲、オペレーティングシステムなど、保存済みクエリで指定した条件に基づいてデバイスをゾーンに追加するゾーンルールを追加することもできます。新しいデバイスは、ゾーンルールの条件に一致する場合、ゾーンに自動的に追加されます。

デフォルトでは、ゾーンに自動的に追加されるデバイスはゾーンルールに従います。ゾーンルールで自動デバイス削除オプションを選択している場合、ゾーンルールに従うデバイスは、ゾーンルールの基準を満たさなくなると、ゾーンから自動的に削除されます。ゾーンルールを無視するデバイスを手動で追加して、ゾーンから自動的に削除されないようにすることもできます。ゾーンを管理するときに、デバイスがゾーンルールに従うか無視するかを変更できます。

ゾーンマネージャーの役割を持つ管理者ユーザーは、デバイスにエージェントをインストールできますが、デフォルトゾーン（ゾーン化されていない）へのアクセス権がないため、ゾーンにデバイスを割り当てることはできません。

新しい Cylance Endpoint Security テナントを作成するとき、またはテナントを推奨デフォルト状態にリセットするとき、BlackBerry は環境を目的のセキュリティ状態に調整するために設計された事前設定済みゾーンと事前設定済みデバイスポリシーを提供します。詳細については、「新規 Cylance Endpoint Security テナントの設定」を参照してください。

ゾーンの追加と設定

作業を始める前に： ゾーンルールをゾーンに追加する場合は、［アセット］ > ［デバイス］画面からクエリを作成して保存する必要があります。保存済みクエリの結果にあるデバイスのリストは、ゾーンに自動的に追加されるデバイスを示します。

1. 管理コンソールのメニューバーで、［ゾーン］をクリックします。
2. ［新しいゾーンを追加］をクリックします。
3. ［ゾーン名］フィールドに、ゾーンの名前を入力します。
4. ［ポリシー］ドロップダウンリストで、ゾーンに関連付けるデバイスポリシーをクリックします。
5. ［値］フィールドで、ゾーンの適切な優先度レベルをクリックします。この設定は、ゾーンやデバイスの管理には影響しません。
6. ［保存］をクリックします。
7. ゾーンリストで、作成したゾーンの名前をクリックします。
8. 次の操作のいずれかを実行します。

タスク	手順
ゾーンルールを追加して、デバイスを自動的に追加します。	ゾーンルールを追加するには、保存済みクエリが必要です。 **a.** ［ルールを作成］をクリックします。 **b.** 保存済みクエリを選択します。検索パラメータが表示されます。 **c.** ゾーンに関連付けられているデバイスポリシーを自動的に適用する場合は、［ゾーンに追加されたデバイスにゾーンポリシーを適用する］を選択します。 **d.** ゾーンルールの条件に一致しないデバイスをゾーンから自動的に削除する場合は、［このゾーンからデバイスを自動的に削除する］を選択します。これは、ゾーンルールに従うデバイスにのみ影響します。 **e.** ［保存］をクリックします。
デバイスをゾーンに手動で追加します。	デバイスをゾーンに手動で追加すると、デバイスはデフォルトでゾーンルールを無視します。ゾーンルールを無視するデバイスは、ゾーンルールの条件に一致しない場合でもゾーンに残ります。 **a.** ［デバイス］タブで、［デバイスをゾーンに追加］をクリックします。 **b.** 追加するデバイスを選択します。フィルターを適用してデバイスを検索できます。 **c.** 選択したデバイスにゾーンデバイスポリシーを適用する場合は、［選択したデバイスにゾーンポリシーを適用］チェックボックスをオンにします。 **d.** ［保存］をクリックします。
ゾーンデバイスポリシーをゾーン内のすべてのユーザーに適用します。	このアクションにより、現在デバイスに割り当てられているすべてのデバイスポリシーが、現在ゾーンに割り当てられているデバイスポリシーに置き換えられます。 **a.** ［このゾーン内のすべてのデバイスに適用］チェックボックスをオンにします。 **b.** ［保存］をクリックします。
ゾーンルールに従うか無視するようにデバイスを設定します。	ゾーン内のデバイスのリストでは、ゾーンルールに従うデバイスをゾーンルール列から識別できます。ゾーンルールに従うデバイスは、ゾーンからの自動削除の対象となります。ゾーンルールを無視するデバイスは、ゾーンに残ります（手動で削除しない限り）。 **a.** ［デバイス］タブで、1 つ以上のデバイスを選択します。 **b.** ［ゾーンルールに従う］または［ゾーンルールを無視する］をクリックします。 **c.** ［はい］をクリックします。

タスク	手順
別のゾーンにデバイスをコピーします。	**a.** ［デバイス］タブで、1 つ以上のデバイスを選択します。 **b.** ［デバイスをコピー］をクリックします。 **c.** 1 つ以上のゾーンを選択します。 **d.** ［保存］をクリックします。
ゾーンからデバイスを削除します。	**a.** ［デバイス］タブで、1 つ以上のデバイスを選択します。 **b.** ［デバイスをゾーンから削除］をクリックします。 **c.** ［はい］をクリックします。

CylancePROTECT Desktop のセットアップ

手順	アクション
1	CylancePROTECT Desktop の要件を確認します。
2	デバイスポリシーを作成して構成します。 • 新しいテナントには、事前設定ゾーンとデバイスポリシーが含まれているため、環境を目的のセキュリティ状態に合わせて簡単に調整できます。 • デバイスポリシーの作成とテストに関する推奨事項を確認します。 • ゾーン管理に関する推奨事項を確認します。
3	CylancePROTECT Desktop エージェントをデバイスにインストールします。 • Windows 用 CylancePROTECT Desktop エージェントのインストール • macOS 用の CylancePROTECT Desktop エージェントのインストール • Linux 用の CylancePROTECT Desktop エージェントのインストール
4	CylancePROTECT Desktop および CylanceOPTICS エージェントの更新の管理。

CylancePROTECT Desktop の展開のテスト

デバイスに CylancePROTECT Desktop エージェントを展開する前に、テスト環境内の他のアプリケーションとの動作をテストして、組織で使用されているアプリケーションが期待どおりに実行および動作することを確認できるようにする必要があります。たとえば、エージェントが一部のアプリケーションの適切な実行をブロックしていることが判明した場合は、実行できるように除外を設定することができます。

新しい Cylance Endpoint Security テナントを作成するとき、またはテナントを推奨デフォルト状態にリセットするとき、BlackBerry は環境を目的のセキュリティ状態に調整するために設計された事前設定済みゾーンと事前設定済みデバイスポリシーを提供します。詳細については、「新規 Cylance Endpoint Security テナントの設定」を参照してください。

エージェントをテストする場合は、組織で使用されているアプリケーションを搭載したテストシステムにインストールして、実際の環境を正確に再現していることを確認します。

エージェントをテストするには、次の手順を実行します。

1. テストポリシーの作成
2. テストゾーンの作成

デバイスポリシーには、エージェントの設定が含まれており、脅威が発生したときに何をするかを指定します。ゾーンを使用すると、地理的な場所、ビジネスユニット、オペレーティングシステム、またはその他のグループプロパティごとにシステムをグループ化できます。ゾーンルールは、設定した基準（オペレーティングシステム、IP アドレス範囲、その他の基準など）に基づいて、システムをゾーンに自動割り当てするのに役立ちます。ポリシーとゾーンをテストして、これらの機能を理解し、組織内でこれらの機能を使用する方法を計画するのに役立てる必要があります。

CylancePROTECT Desktop テストポリシーの作成

段階的なアプローチで CylancePROTECT Desktop のポリシー機能を実装し、パフォーマンスと運用に影響を与えないようにする必要があります。デフォルトでは、デバイスポリシーを作成しても、ポリシー機能は有効にならないため、手動で有効にする必要があります。各自の環境に記録される脅威の種類と CylancePROTECT Desktop エージェントの動作を理解すると、徐々に多くのポリシー機能を有効にすることができます。

組織で使用されているアプリケーションを搭載したデバイスで、デバイスポリシーをテストすることをお勧めします。デバイスポリシーのテストに使用するデバイスは、クリーンなマシンではなく、実稼働環境のデバイスを正確に表していることが重要です。これは、CylancePROTECT Desktop エージェントを介してポリシーが適用されたときに、アプリケーションが正しく実行できることを保証するためです。たとえば、実稼働環境で使用しているデバイスのうち、ユーザーが日常業務に必要とするすべてのアプリケーション（独自仕様およびカスタム）を含むサブセットを選択します。

エージェントは実行制御とプロセス監視を使用して、実行中のプロセスのみを分析します。これには、起動時に実行され、自動実行に設定され、ユーザーが手動で実行するすべてのファイルが含まれます。エージェントは、管理コンソールにのみアラートを送信します。デフォルトでは、ブロックまたは隔離されたファイルはありません。

1. 管理コンソールで、［ポリシー］ > ［デバイスポリシー］ > ［新しいポリシーを追加］をクリックします。
2. ［ポリシー名］フィールドに、テストポリシーの名前を入力します。
3. ［自動アップロード］を有効にすると、疑わしいファイルを分析して CylancePROTECT クラウドサービスに送信し、詳細に分析できます。
   a) ［ファイルアクション］タブの［自動アップロード］セクションで、使用可能なすべてのファイルタイプを選択します。
   b) ［作成］をクリックして、初期テストポリシーを作成します。
   c) テストに使用する CylancePROTECT Desktop エンドポイントに初期テストポリシーを割り当てます。
   d) テストポリシーを割り当てたデバイスは 1 日以上稼働させ、デバイスで通常使用されるアプリケーションとプロセスが実行され、分析されるようにします。このテストの実行以外で監視する必要があるデバイスで定期的（週 1 回など）に実行する必須のアプリケーションを検討することをお勧めします。
   e) ポリシーのテスト中にコンソールの［保護］ > ［脅威］画面に移動して、CylancePROTECT が脅威（異常または危険）と見なすアプリケーションとプロセスのリストを確認し、エンドポイントで実行を許可するアプリケーションとプロセスを特定します。脅威をクリックすると、その脅威の詳細が表示され、悪意のあるファイルをダウンロードして脅威を独自に調査できます。悪意のあるファイルは変更されませんが、ファイル拡張子なしで SHA256 ハッシュを使用して名前が変更されるため、誤ってそのファイルが検出されることはありません。元のファイル拡張子を含むように名前を変更すると、悪意のあるファイルが実行されるおそれがあります。個人情報は、コンソールやその他のテナントまたは組織と共有されません。
   f) ［ポリシー］ > ［デバイスポリシー］に移動し、デバイスポリシーを編集して、このポリシーが割り当てられているエンドポイントで特定のアプリケーションやプロセスを実行できるようにします。［ファイルアクション］タブの［ポリシーセーフリスト］]セクションにファイルを追加できます。

      また、特定のデバイスまたは組織内のすべてのデバイスにあるファイルを隔離または放棄することもできます。詳細については、「CylancePROTECT Desktop のセーフリストと危険リストの管理」を参照してください。
4. デバイスポリシーを編集して、バックグラウンド脅威検出スキャンを有効にし、ディスクにある、休止中の脅威と思われる実行可能ファイルを分析します。
   a) ［保護設定］タブで、［バックグラウンド脅威検出］設定を有効にし、［1 回実行］オプションを選択します。ソリューションの予測機能のために定期にスキャン行う必要はありませんが、コンプライアンス目的などで［定期的に実行］を選択して有効にすることもできます。

b) ［新しいファイルを監視］設定を有効にします。この設定は、デバイスのパフォーマンスに悪影響を及ぼすおそれがあります。フォルダの除外を追加すると、影響が軽減される場合があります。
c) 特定のフォルダをバックグラウンド脅威検出から除外するには、［特定のフォルダを除外（サブフォルダを含む）］を選択し、除外するフォルダを指定します。指定したフォルダ内のファイルの実行を許可するには、［実行を許可］を選択します。こうしたフィールドの詳細については、「保護設定」を参照してください。
d) ［保存］をクリックしてポリシーを保存します。
e) ポリシーを再度テストし、ユーザーが使用する必要があるアプリケーションが実行を許可されていることを確認します。バックグラウンド脅威検出スキャンには、システムの使用状況と分析が必要なファイルの数に応じて、最大 1 週間かかることがあります。必要に応じて、ポリシーセーフリスト、グローバルセーフリストにファイルを追加するか、個々のデバイスについてファイルを放棄します。保護設定でファイルを含むフォルダを除外することもできます。

5. デバイスポリシーを編集して、システムで実行されている危険なプロセスは強制終了させます。たとえば、実行可能ファイル（.exe または .msi）で脅威が検出され、危険と見なされた場合は、この設定により、実行中のプロセスおよびそのサブプロセスが強制終了されます。
   a) ［保護設定］タブで、［実行中の危険なプロセスとそのサブプロセスを強制終了］設定を有効にします。
6. ポリシーを編集して、危険なファイルや異常なファイルの自動隔離設定を有効にします。
   a) ［ファイルアクション］タブの［危険］テーブル列で、［実行可能ファイル］の横にある［自動隔離］設定を有効にして、危険なファイルをデバイスの隔離フォルダに自動的に移動します。危険なファイルにはマルウェア属性が設定されており、マルウェアである可能性があります。
   b) ［異常］で、［自動隔離］を有効にして、異常なファイルをデバイスの隔離フォルダに自動的に移動します。異常なファイルにはマルウェア属性がいくつか設定されていますが、危険なファイルよりは少ないため、マルウェアである可能性は低くなります。
7. ポリシーを編集してメモリ保護設定を有効にし、メモリエクスプロイト、プロセスの注入、エスカレーションを処理します。
   a) デバイスポリシーの［メモリアクション］タブで［メモリ保護］を有効にし、違反タイプを［アラート］に設定します。違反タイプがアラートに設定されているときにそのタイプの脅威が検出された場合、エージェントはコンソールに情報を送信しますが、デバイスメモリで実行されているプロセスをブロックしたり終了したりすることはありません。
   b) ポリシーのテスト中にコンソールの［保護］>［メモリ保護］画面に移動して、脅威である可能性のあるプロセスのメモリ保護アラートのリストを確認します。
   c) 日常的な業務に使用しても安全であると判断したプロセスがある場合は、実行を許可するプロセスに対して除外を追加します。デバイスポリシーの［メモリアクション］タブで［除外を追加］をクリックし、ファイルへの相対パスを指定します。
   d) 実行を許可するプロセスの除外を指定した後、すべての違反タイプについてアクションを［ブロック］に設定します。違反タイプがブロックされると、エージェントはコンソールに情報を送信し、悪意のあるプロセスがメモリ内で実行されないようにブロックします。悪意のあるプロセスを呼び出したアプリケーションは、引き続き実行できます。
8. ポリシーを編集して、デバイス制御設定を有効にします。この例では、すべてのデバイスタイプへのアクセスをブロックし、例外を許可する方法を示しますが、逆にすべてのデバイスタイプへのフルアクセスを許可し、例外をブロックすることも可能です。
   a) デバイスポリシーの［デバイス制御］タブで、［デバイス制御］ポリシーを有効にします。
   b) 各 USB デバイスタイプのアクセスレベルを［フルアクセス］に設定します。
   c) ポリシーを保存します。
   d) テストデバイスに USB デバイスを挿入します。

e) 管理コンソールで［保護］**>**［外部デバイス］の順に選択し、許可するデバイスのベンダー ID、製品 ID、およびシリアル番号を確認します。メーカーによっては、製品に固有のシリアル番号を使用しません。複数の製品に同じシリアル番号を使用しているメーカーもあります。
f) デバイスポリシーの［デバイス制御］タブの［外部ストレージの除外リスト］セクションで、［デバイスを追加］をクリックして、許可するデバイスを追加します。
g) テストが完了した後で、各デバイスタイプのアクセスレベルを［ブロック］に設定します。必要に応じて除外を追加できます。

9. ポリシーを編集して、スクリプト制御設定を有効にします。推奨されるテスト期間は 1〜3 週間です。
a) デバイスポリシーの［スクリプト制御］タブで、［スクリプト制御］ポリシーを有効にします。
b) 各スクリプトタイプのポリシーを［アラート］に設定します。スクリプト制御で警告が設定されている時間が長いほど、組織で使用されている実行頻度の低いスクリプトを検索する可能性が高くなります。

メモ：Active Directory 設定をスクリプトで管理している場合は、スクリプト制御設定を有効にすると大量のイベントが発生する可能性があります。

c) ［保護］**>**［スクリプト制御］に移動し、許可するデバイスで実行されたスクリプトを識別します。
d) デバイスポリシーの［スクリプト制御］タブの［ファイル、スクリプト、またはプロセスを除外］セクションで、［除外を追加］をクリックし、許可するスクリプトの相対プロセスパスを指定します（例：`\Cases\AllowedScripts`）。
e) 実行を許可するスクリプトの除外を追加した後で、各スクリプトタイプのポリシーを［ブロック］に設定します。

除外とそれを使用するタイミング

次の表では、各タイプの除外を説明し、それらを適切に使用するタイミングと方法に関して一般的なガイダンスを示します。

除外タイプ	説明と例
ポリシーセーフリスト（ファイルアクション）	ポリシーセーフリストは、デバイスポリシーの［ファイルアクション］タブで指定します。 デバイスにデバイスポリシーが割り当てられている場合、デバイスはポリシーセーフリストで指定されたファイルを実行できます。ポリシーセーフリストは特定のデバイスのポリシーレベルで適用されますが、グローバルセーフリストまたは隔離リストはすべてのデバイスのグローバルレベルで適用されます。ポリシーセーフリストは、グローバル隔離リストよりも優先されます。ポリシーセーフリストに追加されたファイルは、そのファイルがグローバル隔離リストに登録されている場合でも、ポリシーが割り当てられているすべてのデバイスで実行できます。グローバル隔離リストは、すべてのデバイスでファイルの実行をブロックします。 例：PSEXEC などの権限の昇格ツールを頻繁に使用して日常業務を行っているとします。他のユーザーに同じ権限を持たせず、自社の日常業務に影響を与えることなく、そのようなツールを使用できないようにしたいと考えています。これを行うには、グローバル隔離リストに PSEXEC を追加し、ポリシーセーフリストに同じファイルハッシュを追加します。次に、PSEXEC をセーフリストに追加した特定のデバイスポリシーに、ユーザーと他の許可ユーザーのみが割り当てられていることを確認します。結果的に、デバイスポリシーに割り当てられていないすべてのユーザーは PSEXEC を隔離していますが、デバイスポリシーに割り当てられているユーザーは使用できることになります。

除外タイプ	説明と例
実行可能ファイルまたはマクロファイルを除外（メモリ保護）	［メモリ保護］が有効になっている場合、メモリ保護ポリシーの除外は、デバイスポリシーの［メモリアクション］タブで指定します。 メモリ保護の除外を指定すると、エージェントは特定アプリケーションからの特定タイプの違反を無視するようになります。言い換えると、アプリケーションが特定タイプの違反を引き起こすアクションを実行しても、アプリケーションのブロックまたは終了を回避できます。 メモリ保護が有効になっている場合、エージェントはアプリケーションプロセスを監視し、プロセスが実行する特定のアクションをチェックしています。エージェントが監視している特定のアクション（LSASS 読み取りなど）をプロセスが実行する場合、エージェントはデバイスポリシーに従ってそのアクションに応答します。偽陽性のイベントが発生し、メモリ保護によって、アプリケーションによるアクションがブロックされたり、アプリケーションが完全に終了されたりする場合もあります。このような状況では、メモリ保護の除外を指定できます。特定のアプリケーションを特定の違反タイプから除外すると、ブロックまたは終了せずに、意図したとおりにアプリケーションを実行できます。 例：デフォルトの場合、組織では、全アプリケーションの全メモリ保護違反がブロックされます。担当者は Test.exe を頻繁に使用しており、LSASS 読み取り違反にのみ、正当な理由があると理解しています。このような場合、エージェントが Test.exe からの LSASS 読み取り違反のみを無視するように除外を追加できます。他のタイプの違反が発生した場合、エージェントは Test.exe をブロックします。 メモリ保護の除外では、相対パス（ドライブ文字は不要）を使用し、実行可能ファイルのレベルまで指定できます。例: • `\Application\Subfolder\Test.exe` • `\Subfolder\executable` メモ：実行可能ファイルのレベルでは、相対パスなしで除外を指定することは推奨されません。たとえば、`\Test.exe` に対して除外が設定されている場合、同じ名前の悪意のあるファイルは、デバイス上の任意のフォルダから実行できます。

除外タイプ	説明と例
特定のフォルダを除外（保護設定）	［バックグラウンド脅威検出］が有効になっている場合、バックグラウンド脅威検出の除外は、デバイスポリシーの［保護設定］タブで指定します。これは、ディレクトリセーフリストと呼ばれます。ディレクトリを除外すると、スキャンの実行時に、そのディレクトリ内のすべてのファイル（サブフォルダを含む）が無視されます。 ［実行を許可］を選択すると、エージェントは除外ディレクトリから起動された実行可能ファイルをすべて無視します。 例：組織内のアプリケーション開発者は、コンパイル時に生成される一時ファイルを格納するために、特定のディレクトリ（C:\DevFiles\Temp など）を使用します。エージェントは、これらのファイルをスキャンし、検出されたさまざまな特性により安全でないと判断した場合、それ以降、これらのファイルを隔離することになります。開発者は、一時ディレクトリを許可する要求を送信します。このような場合、C:\DevFiles\Temp ディレクトリを追加すると、一時ファイルは無視され、開発者は作業を実行できるようになります。
フォルダの除外（スクリプト制御）	［スクリプト制御］が有効になっている場合、スクリプト制御ポリシーの除外は、デバイスポリシーの［スクリプト制御］タブで指定します。指定したディレクトリでスクリプトを実行できるようにする場合は、除外を追加できます。スクリプト制御除外を追加する場合は、相対パスを指定します。サブフォルダも除外に含まれます。 例：IT 管理者は、C:\Scripts\Subfolder\Test にあるスクリプトを実行しようとしています。IT 管理者がスクリプトを実行しようとするたびに、スクリプトはスクリプト制御によってブロックされます。スクリプトを実行可能にするには、スクリプト制御ポリシーの除外として、次のいずれかの相対パスを追加できます。 • \Scripts\Subfolder\Test • \Subfolder\Test\ • \Scripts\Subfolder\ • \Scripts\ • \Subfolder\ • \Test\

デバイスポリシーを使用した CylancePROTECT Desktop デバイスの管理

デバイスポリシーは、CylancePROTECT Desktop エージェントが検出した疑わしいファイルやマルウェアをどのように処理するかを定義します。実行制御は、すべてのデバイスポリシーでデフォルトで有効になっています。安全でないファイルまたは異常なファイルの実行が試行されると、エージェントが管理コンソールに警告を送信できるようになります。また、エージェントはインストールされると、実行中のすべてのプロセスとモジュールを分析し、すでにアクティブな脅威が存在するかどうかを判断します。各デバイスに 1 つのデバイスポリシーが

割り当てられます。デバイスに他のポリシーが割り当てられていない場合は、デフォルトポリシーが割り当てられます。

デバイスポリシーは、次のような使い方ができます。

- 安全でないファイルや異常なファイルを自動的に隔離し、デバイス上で実行できないようにします。ファイルに危険または異常があることを示す脅威スコアがある場合でも組織が安全と見なすファイルのポリシーセーフリストを定義できます。
- メモリ保護設定を有効にして、プロセスの注入やエスカレーションを含むメモリエクスプロイトを防止します。実行可能ファイルとマクロファイルの除外を追加して、実行を許可することができます。
- CylancePROTECT サービスのシャットダウンの防止、実行中の安全でないプロセスやサブプロセスの強制終了、および休止中の脅威である可能性があるファイルを分析するバックグラウンド脅威検出の実行などの保護設定を有効にします。
- CylanceOPTICS 設定を有効にして構成します。
- アプリケーション制御機能を有効にして、新しいアプリケーションの実行を制限し、すでにインストールされているアプリケーションに対する更新や変更をブロックします。
- ログファイルの自動アップロードやデスクトップ通知などのエージェントの設定を有効にします。
- スクリプト制御設定を有効にして、悪意のあるスクリプトがデバイス上で実行されないようにします。組織が安全であると判断した特定のスクリプトを実行できるよう、除外を追加できます。
- デバイス制御設定を有効にして、USB 大容量ストレージデバイス（USB フラッシュドライブ、外付けハードドライブ、スマートフォンなど）がデバイスに接続されないようします。

デバイスポリシーの作成と管理

デバイスポリシーを使用して、CylancePROTECT Desktop および CylanceOPTICS エージェントの機能を制御できます。組織内のグループのさまざまなニーズを満たすために、異なるデバイスポリシーを作成できます。

1. 管理コンソールのメニューバーで、［ポリシー］ > ［デバイスポリシー］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
新しいデバイスポリシーの追加	**a.** ［新しいポリシーを追加］をクリックします。 **b.** ［ポリシー名］フィールドに、デバイスポリシーの名前を入力します。 **c.** デバイスポリシー設定を選択します。 **d.** ［作成］をクリックします。
デバイスポリシーの編集	**a.** 編集するデバイスポリシーの名前をクリックします。 **b.** デバイスポリシー設定を更新します。 **c.** ［保存］をクリックします。
デバイスポリシーのコピー	**a.** コピーするデバイスポリシーの名前をクリックします。 **b.** ［ポリシー名］フィールドで、デバイスポリシーの名前を変更します。 **c.** 必要に応じて、デバイスポリシー設定を更新します。 **d.** ［名前を付けて保存］をクリックします。

タスク	手順
デバイスポリシー設定	デバイスポリシー設定の詳細については、次のセクションを参照してください。 • ファイルアクション • メモリアクション • 保護設定 • アプリケーション制御 • エージェント設定 • スクリプト制御 • デバイスの制御 • CylanceOPTICS の設定
ゾーン内のデバイスに対するデバイスポリシーの自動割り当て	ゾーンの設定時にデバイスポリシーを指定しておくと、デバイスがゾーンに追加されたときに、自動的にデバイスポリシーをデバイスに割り当てることができます。詳細については、「ゾーンの追加と設定」を参照してください。
デバイスポリシーをデバイスに手動で割り当てます。	**a.** 管理コンソールのメニューバーで、［アセット］ > ［デバイス］をクリックします。 **b.** デバイスポリシーを割り当てるデバイスを選択します。 **c.** ［ポリシーを割り当て］をクリックします。 **d.** 割り当てるデバイスポリシーを選択します。 **e.** ［保存］をクリックします。

ファイルアクション

次の設定は、デバイスポリシーの［ファイルアクション］タブで指定します。これらの設定により、危険または異常と判断する脅威が検出されたファイルを CylancePROTECT Desktop エージェントがどのように処理するかを指定します。

オプション	説明

自動隔離（実行制御あり）	この設定では、安全でないファイルまたは異常なファイルを自動的に隔離して実行を防ぐかどうかを指定します。異常なファイルを隔離したい場合は、最初に安全でないファイルの隔離オプションを選択しておく必要があります。安全でないファイルには、マルウェアの属性が非常に多く含まれており、異常なファイルよりもマルウェアの可能性が高くなっています。
	
	ファイルが隔離されると、次の処理が行われます。
	• ファイル名が変更されて `.quarantine` 拡張子が追加されます。
	• ファイルが元の場所から次のいずれかの隔離ディレクトリに移動されます。
	  • **Windows** デバイスの場合：`C:\ProgramData\Cylance\Desktop\q`
	  • **macOS** デバイスの場合：`/Library/Application Support/Cylance/Desktop/q`
	  • **Linux** デバイスの場合：`/opt/cylance/desktop/q`
	• ユーザーがファイルを操作できないように、ファイルのアクセス制御リスト（ACL）が変更されます。
	
	マルウェアの中には、他のディレクトリにファイルを作成するよう設計されているものもあり、この試みは成功するまで継続されます。このようなファイルを削除する代わりに、CylancePROTECT Desktop はマルウェアを変更してこれらが再作成されないようにすることで、その実行を阻止します。

隔離済みのファイルの自動削除を有効にする	この設定では、指定日数の経過後に隔離ファイルを自動的に削除するかどうかを指定します。たとえば、ファイルを 14 日間隔離した後に削除するように設定できます。日数の範囲は 14〜365 です。 ファイルが削除されると、次の処理が行われます。 • 検証や監査を行う目的で、アクションがエージェントログファイルに取り込まれるようにします。 • エージェント UI の隔離リストからファイルが削除されます。
自動アップロード	使用可能なすべてのファイルタイプに対して［自動アップロード］が有効になっていることを確認します。CylancePROTECT クラウドサービスで分析したことのないファイルをエージェントが検出した場合、分析のためにファイルをアップロードするように要求されます。 CylancePROTECT Desktop がアップロードして分析するのは、Portable Executable（PE）、Executable and Linkable Format（ELF）、Mach Object ファイル形式（Mach-O）ファイルなどの不明なファイルのみです。同じ不明ファイルが組織内の複数のデバイスで検出された場合、CylancePROTECT Desktop はデバイスごとに 1 つのファイルではなく、1 つのデバイスからのみ 1 つのファイルをアップロードして分析します。

オプション	説明
ポリシーセーフリスト	安全であると思われるファイルをポリシーセーフリストに追加することで、それらの実行を可能にします。ポリシーセーフリストは、グローバルセーフリストやグローバル隔離リストよりも優先されます。たとえばポリシーセーフリストに追加されたファイルは、そのファイルがグローバル隔離リストに登録されている場合でも、ポリシーが割り当てられているデバイスで実行できます。グローバル隔離リストは、すべてのデバイスでファイルの実行をブロックします。

ポリシーセーフリストへのファイルの追加

ポリシーセーフリストにファイルを追加すると、脅威スコアが危険または異常であることを示している場合でも、そのポリシー内のすべてのエージェントがそのファイルを安全と見なすようにすることができます。ポリシーセーフリストの詳細については、「除外とそれを使用するタイミング」を参照してください。

作業を始める前に：［保護］ > ［脅威］画面から除外するファイルの SHA256 値を取得します。

1. 管理コンソールのメニューバーで、［ポリシー］ > ［デバイスポリシー］をクリックします。
2. ポリシーの名前をクリックして編集するか、［新しいポリシーを追加］をクリックします。
3. ［ファイルアクション］タブの［ポリシーセーフリスト］セクションで、［ファイルを追加］をクリックします。
4. 除外するファイルの SHA256 値を指定します。
5. 必要に応じて、MD5 値とファイル名を指定します。
6. カテゴリを選択し、このファイルを除外する理由を入力します。
7. ［送信］をクリックします。

メモリアクション

次の設定は、デバイスポリシーの［メモリアクション］タブで指定します。［メモリ保護］を有効にして、プロセスの注入やエスカレーションなど、CylancePROTECT Desktop エージェントによるメモリエクスプロイトの処理方法を指定できます。実行可能ファイルを除外リストに追加して、このポリシーが適用されたときにこれらのファイルを実行できるようにすることもできます。

オプション	説明
メモリ保護	この設定では、このポリシーでメモリ保護設定を有効にするかどうかを指定します。有効にすると、エージェントは潜在的な脅威であるさまざまなタイプのプロセスの呼び出しを検出し、選択した設定に従って各タイプを処理します。 • 無視：エージェントはアクションを実行しません。 • アラート：エージェントは違反をログに記録してそのインシデントを管理コンソールに報告します。 • ブロック：エージェントは違反をログに記録してそのインシデントを管理コンソールに報告し、プロセスの呼び出しをブロックします。呼び出しを行ったアプリケーションは、引き続き実行できます。 • 停止：エージェントは違反をログに記録してそのインシデントを管理コンソールに報告し、プロセスの呼び出しをブロックして、呼び出したアプリケーションを終了します。

オプション	説明
実行可能ファイルを除外	この設定では、無視するファイルの相対パスを指定します。この除外リストにファイルを追加すると、このポリシーが割り当てられているデバイス上でファイルを実行またはインストールできるようになります。 ファイルの相対パスと無視する違反タイプを指定します。Windows デバイスでは、絶対ファイルパスを指定することもできます。相対パスが同じである他の実行可能ファイルも除外される可能性があるため、短縮された相対パスは注意して使用してください。 除外を適用した後、そのプロセスのすべてのインスタンスを終了して、ドライバがそのプロセスに注入できないようにする必要があります。 **Windows の例** • 相対パス： `\Application\Subfolder\application.exe` • 絶対パス： `C:\Application\Subfolder\application.exe` **Linux の例** • 相対パス： `/opt/application/executable` • ダイナミックライブラリファイルの相対パス： `/executable.dylib` **macOS の例** • 相対パス（スペースなし）： `/Applications/SampleApplication.app/Contents/MacOS/executable` • 相対パス（スペースあり）： `/Applications/Sample Application.app/Contents/MacOS/executable` • ダイナミックライブラリファイルの相対パス： `/executable.dylib` メモリ保護の除外にワイルドカードを使用することもできます。詳細については、「メモリ保護の除外におけるワイルドカード」を参照してください。 メモ：無視する違反タイプを 1 つも追加せずに除外を保存すると、メモリ保護イベントとスクリプト制御イベントの両方に除外が適用されます。無視する違反タイプを 1 つ以上追加すると、除外はメモリ保護にのみ適用されます。

オプション	説明
特定の違反タイプを無視	除外を追加する場合は、このチェックボックスをオンにすると、次のいずれかまたはすべての項目に基づいてファイル違反が無視されます。 • 違反タイプのカテゴリ（エクスプロイト、プロセスの注入、エスカレーションなど） • 各カテゴリの個々の違反タイプ（スタックピボット、メモリのリモート割り当て、ゼロ割り当てなど） メモリ保護ポリシーに除外を追加する際に、ポリシーをメモリ保護違反のみに適用してスクリプト制御違反に適用しない場合は、無視する違反タイプを 1 つ以上指定します。無視する違反タイプを選択しない場合、警告メッセージが表示され、メモリ保護ポリシーとスクリプト制御ポリシーの両方に除外が適用されます。 既存のメモリ保護ポリシーの場合： • ［特定の違反タイプを無視］除外設定がオンになっていても、スクリプト制御ポリシーが無効になっている場合には、アクションは必要ありません。 • ［特定の違反タイプを無視］除外設定がオフになっており、ポリシーをメモリ保護違反のみに適用してスクリプト制御には適用しないようにする場合は、この設定をオンにして、無視する違反タイプを 1 つ以上指定する必要があります。 既存のポリシーを編集して除外を追加した場合、違反タイプを変更するまで［特定の違反タイプを無視］チェックボックスは表示されません（ブロックから終了または警告への変更など）。 無視する特定の違反タイプが設定されているファイルごとに、詳細情報の表示、設定の編集、または削除を行うことができます。
DLL 除外として扱う	サードパーティ DLL の除外を追加する場合は、この設定を選択します。たとえば、CylancePROTECT Desktop for Windows に加えてサードパーティのセキュリティ製品を実行している場合は、CylancePROTECT がその製品に関する特定の違反を無視するように、適切な .dll ファイルの除外を追加できます。この機能は、［悪意のあるペイロード］および［システム DLL を上書き］違反タイプのみをサポートしています。 DLL 除外を指定する場合、次のルールが適用されます。 • デバイスポリシーで、［**DLL** 除外として扱う］オプションを選択する必要があります。 • Windows デバイスでは、デバイスで CylancePROTECT Desktop エージェントバージョン 3.1.1001 以降を実行している必要があります。 • 指定するファイルパスは、.dll ファイルへのフルパス、直接のパスである必要があります。ワイルドカードは許可されていません。 • .dll ファイルは、CylancePROTECT Desktop がインストールされているデバイスで信頼済み証明書を使用して署名されている必要があります。それ以外の場合、除外されません。 DLL 除外のサポートに関する詳細については、support.blackberry.com にアクセスして KB 108909 を参照してください。

メモリ保護違反のタイプ

悪用違反タイプ

違反タイプ	説明	サポートされる **OS**
スタックピボット	スレッドのスタックが別のスタックに置き換えられました。通常、システムはスレッドに 1 つのスタックのみを割り当てます。攻撃者は別のスタックを使用して、データ実行防止（DEP）によってブロックされない方法で実行を制御する可能性があります。	Windows macOS* Linux
スタック保護	スレッドのスタックのメモリ保護が変更され、実行権限が有効になりました。スタックメモリは実行可能であってはなりません。実行権限が有効になったということは、攻撃者が悪用の一環としてスタックメモリに格納された悪意のあるコードの実行準備をしている可能性があることを意味します。この試みは、本来であればデータ実行防止（DEP）によってブロックされます。	Windows macOS* Linux
コードの上書き	プロセスのメモリに存在するコードが、データ実行防止（DEP）を回避する可能性のある手法で変更されています。	Windows
RAMスクレイピング	プロセスが、別のプロセスから有効な磁気ストライプトラックデータを読み取ろうとしています。通常、この違反は販売時システム（POS）に関連付けられます。	Windows
悪意のあるペイロード	悪用に関連する汎用シェルコードとペイロード検出が検出されました。 このメモリ保護違反タイプは、DLL 除外をサポートしています。	Windows
エージェント **2.1.1580** 以降で使用可能な違反タイプ		
システムコールのモニタリング	アプリケーションまたはオペレーティングシステムへのシステムコールが検出されました。	Windows
直接システムコール	悪意のあるコードを他のプロセスにサイレント注入しようとしたことが検出されました。この違反タイプはブロックできません。	Windows
システム **DLL** を上書き	システム DLL を上書きしようとしたことが検出されました。 このメモリ保護違反タイプは、DLL 除外をサポートしています。	Windows
危険な **COM** オブジェクト	コンポーネントオブジェクトモデル（COM）オブジェクトへの参照を持つ悪意のあるコードが検出されました。	Windows

違反タイプ	説明	サポートされる **OS**
APC 経由のインジェクション	プロセスが非同期プロシージャコール（APC）を使用しているか、リモートスレッドを開始して `LoadLibrary` などの関数を呼び出し、任意のコードをターゲットプロセスに注入するプロセスです。 このポリシーが［アラート］に設定されている場合は、Windows デバイス上のアプリケーションに対して実行される有効なインジェクションと悪意のあるインジェクションの両方に関するアラートが表示されることがあります。このアラートは、インジェクションを受けたアプリケーションを報告しますが、アラートの原因となった実行可能なソースはユーザーが特定する必要があります。インジェクションが有効か悪意があるかを判断する際に役立つ可能性のある必須データを収集する方法については、support.blackberry.com にアクセスして「KB 92422」を参照してください。 このポリシーが［ブロック］または［停止］に設定されている場合は、報告されたアプリケーションが有効であっても、デバイスで実行されないようにします。これにより、ユーザーの日常の活動が中断されることがあります。	Windows
エージェント **3.0.1000** 以降で使用可能な違反タイプ		
危険な **VBA** マクロ	危険な実装を含むマクロが検出されました。 この設定は、エージェントバージョン 2.1.1580 以降を実行しているデバイスを悪意のあるマクロから保護します。メモリ保護ポリシーでの除外指定は、エージェントバージョン 3.0 以降でサポートされています。 エージェントバージョン 2.1.1578 以前を実行しているデバイスを悪意のあるマクロから保護するには、スクリプト制御ポリシーとその除外を有効にして設定します。	Windows

* macOS Catalina 以前のバージョンでのみサポートされています。

プロセスの注入違反タイプ

違反タイプ	説明	サポートされる **OS**
リモートでのメモリ割り当て	プロセスが別のプロセスでメモリを割り当てました。ほとんどの割り当ては同じプロセス内でのみ行われます。これは、システム上の悪意のあるものを強化するために、コードまたはデータを別のプロセスに注入しようとしたことを示している可能性があります。	Windows macOS

違反タイプ	説明	サポートされる **OS**
リモートでのメモリマッピング	プロセスがコードやデータを別のプロセスに導入しました。これは、別のプロセスでコードの実行を開始しようとしたことを示しており、悪意のあるものを強化する可能性があります。	macOS
リモートでのメモリ書き込み	プロセスが別のプロセスでメモリを変更しました。これは通常、以前に割り当てられたメモリにコードまたはデータを格納しようとしたことを示している可能性があります（「`OutOfProcessAllocation`」を参照）。ただし、攻撃者が悪意のある目的で実行を迂回するために、既存のメモリを上書きしようとしていることも考えられます。	Windows macOS
リモートでのメモリへの **PE** 書き込み	プロセスが別のプロセスでメモリを変更して、実行可能イメージを格納しました。一般的に、最初にコードをディスクに書き込んでいない状態で、攻撃者がそのコードを実行しようとしていることを示しています。	Windows
リモートでのコード上書き	プロセスが別のプロセスで実行可能メモリを変更しました。通常の状況では、特に別のプロセスによって実行可能メモリが変更されることはありません。これは通常、別のプロセスで実行を迂回しようとしたことを示しています。	Windows
リモートでのメモリマッピング解除	プロセスが別のプロセスのメモリから Windows 実行可能ファイルを削除しました。これは、実行を迂回するために、実行可能イメージを変更されたコピーに置き換える意図を示している可能性があります。	Windows macOS
リモートでのスレッド作成	プロセスが別のプロセスに新しいスレッドを作成しました。プロセスのスレッドは通常、同じプロセスによってのみ作成されます。この方法は通常、攻撃者が別のプロセスに侵入した悪意のあるものをアクティブ化するために使用されます。	Windows macOS*
リモートでの**APC**スケジュール	プロセスによって、別のプロセスのスレッドの実行が迂回されました。一般的に攻撃者はこの方法を使用して、別のプロセスに侵入した悪意のあるものをアクティブ化します。	Windows
DYLDインジェクション	起動されたプロセスに共有ライブラリが注入される原因となる環境変数が設定されました。攻撃者は、Safari などのアプリケーションのリストを変更したり、アプリケーションを bash スクリプトで置き換えたりすることがあります。これにより、アプリケーションの起動時にモジュールが自動的に読み込まれます。	macOS* Linux
エージェント **2.1.1580** 以降で使用可能な違反タイプ		

違反タイプ	説明	サポートされる **OS**
ドッペルゲンガー	ファイルシステムにまだ書き込まれていないファイルから、悪意のある新しいプロセスが開始されました。ファイル書き込みトランザクションは通常、プロセスの開始後にロールバックされるため（これにより悪意のあるファイルがディスクにコミットされないようにします）、ディスク上のファイルをスキャンしようとすると、修正されていない良性ファイルのみが表示されます。	Windows
危険な環境変数	悪意のあるコードにアタッチされている可能性のある環境変数が検出されました。	Windows

* macOS Catalina 以前のバージョンでのみサポートされています。

昇格違反タイプ

違反タイプ	説明	サポートされる **OS**
LSASS読取り	Windows ローカルセキュリティ権限プロセスに属するメモリに、ユーザーのパスワードを取得しようとしたことを示す方法でアクセスがありました。	Windows
ゼロ割り当て	ヌルページが割り当てられました。メモリ領域は通常は予約済みですが、特定の状況では割り当てることができます。攻撃では、通常はカーネル内の既知のヌルデリファレンスエクスプロイトを利用して、権限の昇格を設定します。	Windows macOS*
エージェント **2.1.1580** 以降で使用可能な違反タイプ		
他のプロセスでメモリアクセス権を変更	違反しているプロセスが、別のプロセス内でメモリアクセス権限を変更しました。これは通常、コードを別のプロセスに注入し、メモリアクセス権限を変更してメモリを実行可能な状態にするために行われます。	Windows
子プロセスでメモリアクセス権を変更	違反しているプロセスが子プロセスを作成し、その子プロセスのメモリアクセス権限を変更しました。	Windows
盗まれたシステムトークン	アクセストークンが変更され、ユーザーがセキュリティアクセス制御を回避できるようになりました。	Windows
低整合性プロセスの開始	整合性レベルが低いプロセスが実行されるように設定されました。	Windows

* macOS Catalina 以前のバージョンでのみサポートされています。

メモリ保護の除外におけるワイルドカード

メモリ保護の除外には、「^ & ' @ { } [ ] , $ = !」の特殊文字を含めることができます（すべての OS）。- # ( ) % .+ ~ _*

Windows デバイスでは、任意の文字値の後にコロンが続く（C: など）場合もサポートされています。

現時点では、アスタリスク（*）のエスケープはサポートされていません。たとえば、ファイル名にアスタリスクが含まれているファイルを除外するのに使用することはできません。

DLL 除外を追加する場合は、ワイルドカードを使用できません。

ワイルドカード	説明
*	これは、プラットフォーム固有のファイルパス区切り文字を除く、0 文字以上に一致します。ファイルパス区切り文字は、Windows デバイスでは「\」、Linux および macOS では「/」です。
**	これは絶対パス内の 0 以上のディレクトリに一致し、ドライブ、ディレクトリ、および子ディレクトリを除外するために使用します。（例：`C:\MyApp\''\**\''`）。 ** ワイルドカードを使用する場合は、次の規則に従ってください。 • ** は、**\ など、必ずファイルパス区切り文字とともに使用してください /**/ • パターン **\ は、Windows デバイスのパターンの先頭にある場合にのみ有効です。すべてのドライブ内のすべてのディレクトリと一致します。 • パス内では、**\ や /**/ は複数回使用でき、制限はありません。

メモ：通常のワイルドカードでは、3 つのアスタリスク「***」が有効で、1 つのアスタリスク「*」に相当します。ただし、3 つのアスタリスクは、誤字を見逃す原因となる可能性があるため、除外対象にはなりません。たとえば、「C:***.exe」というパターンの場合、「C:***.exe」と入力したつもりが、「\」を 1 つ入力し忘れた可能性があります。「***」を 1 つの「*」として扱うと、意図した動作とは異なる動作を引き起こす可能性があります。

Windows でメモリ保護の除外に使用するワイルドカードの例

次の例は、`C:\Application\TestApp\MyApp\program.exe` のパスに格納されている実行可能ファイルの除外に基づいています。

	例

有効な除外パスの例	ワイルドカードを使用しないで相対パスで除外する場合：
	`\Application\TestApp\MyApp\program.exe`
	C:\Application の「**MyApp**」ディレクトリにある **program.exe** を除外する場合：
	`C:\Application\**\MyApp\program.exe`
	C:\Application の「**MyApp**」ディレクトリにあるあらゆる **.exe** ファイルを除外する場合：
	`C:\Application\**\MyApp\*.exe`
	C:\Application の「**MyApp**」ディレクトリにあるあらゆる実行可能ファイル（ファイル拡張子を問わない）を除外する場合：
	`C:\Application\**\MyApp\*`
	C:\Application\TestApp のいずれかの子ディレクトリにある **program.exe** を除外する場合：
	`C:\Application\TestApp\**\program.exe`
	C: ドライブの **\Application\TestApp\MyApp** にある **program.exe** を除外する場合：
	`C:\**\Application\TestApp\MyApp\program.exe`
	C: ドライブの **\Application\TestApp\MyApp** にあるあらゆる実行可能ファイルを除外する場合：
	`C:\**\Application\TestApp\MyApp\*.exe`
	C: ドライブの **\Application\TestApp\MyApp** にあるあらゆる実行可能ファイル（拡張子を問わない）を除外する場合：
	`C:\**\Application\TestApp\MyApp\*`

	例
除外でのアスタリスクの不適切な使い方	フォルダ名またはファイル名の文字と一致させるには、アスタリスク（*）を１つだけ使用してください。二重アスタリスク（**）はディレクトリパスと一致させるために予約されており、除外の最後に使用することはできません。 以下は C:\Application\TestApp\MyApp\program.exe を除外する場合の例のリストです。 • 不適切：C:\Application\TestApp\MyApp**.exe • 不適切：C:\Application**\MyApp\program.exe • 適切：C:\Application\TestApp\MyApp*.exe • 適切：C:\Application\TestApp**.exe • 適切：C:\Application**\program.exe
推奨されない除外	ドライブ文字の直後に二重アスタリスク（**）を使用しないでください。例: `C:\**\program.exe` この例では、program.exe は C: ドライブ内の任意のフォルダから実行できます。この除外は厳密には間違っていませんが、ドライブにある任意のディレクトリ（子ディレクトリを含む）内のすべてを除外することになります。

macOS でのメモリ保護の除外で使用されるワイルドカードの例

次の例は、パス/Application/TestApp/MyApp/program.dmgに格納されている実行可能ファイルを除外するためのものです。

種類	説明

除外の適切な使い方	**program.dmg** が「**MyApp**」子ディレクトリの下にある限り、**program.dmg** を除外します。
	`/Application/**/MyApp/program.dmg`
	「**MyApp**」子ディレクトリの下にある限り、**.dmg** を含むすべての実行可能ファイルを除外します。
	`/Application/**/MyApp/*.dmg`
	実行可能ファイルが「**MyApp**」子ディレクトリの下にある限り、それらをすべて除外します。
	`/Application/**/MyApp/ *`
	program.dmg が「**TestApp**」ディレクトリの子ディレクトリにある限り、それらをすべて除外します。
	`/Application/TestApp/**/program.dmg`

種類	説明
除外でのアスタリスクの不適切な使い方	フォルダ名またはファイル名の文字と一致させるには、アスタリスク（*）を 1 つだけ使用してください。二重アスタリスク（**）はディレクトリパスと一致させるために予約されており、除外の最後に使用することはできません。 次に示すのは、`/Application/TestApp/MyApp/program.dmg` を除外するコンテキストでのサンプルリストです。 • ◦ 不適切：/Application/TestApp/MyApp/pro**am.dmg ◦ 適切：/Application/TestApp/MyApp/progra*.dmg ◦ • ◦ 不適切：/Application/** ◦ 適切：/Application/**/*
推奨されない除外	除外の先頭には二重アスタリスク（**）を使用しないでください。例: `/**/program.dmg` この例では、`program.dmg` はドライブ内の任意のフォルダから実行できます。この除外は厳密には間違っていませんが、ドライブにある任意のディレクトリ（子ディレクトリを含む）内のすべてを除外することになります。

保護設定

CylancePROTECT Desktop は、悪意のあるプロセスの実行を常に監視し、危険または異常なものの実行が試行されたときにコンソールに通知します。CylancePROTECT Desktop エージェントを設定するには、デバイスポリシーの［保護設定］タブにある下記設定から行います。

オプション	説明
デバイスからのサービスシャットダウンを防止	このオプションを選択すると、デバイスユーザーは CylancePROTECT Desktop エージェントのサービスまたは次のバージョンの CylanceOPTICS エージェントのサービスを停止できなくなります。 • Windows 用 CylanceOPTICS エージェント 3.1 以降、CylancePROTECT Desktop 3.0 以降搭載 • macOS 用 CylanceOPTICS エージェント 3.3 以降、CylancePROTECT Desktop 3.1 以降搭載 この設定を有効にすると、macOS ユーザーは、デバイスプロパティの自己保護レベルが［ローカル管理者］に設定されている場合にのみ、サービスを停止できるようになります（［アセット］ > ［デバイス］ > デバイスをクリック）。この設定が有効になっている限り、Windows ユーザーはエージェントサービスを停止できません。 バージョン 3.1 以降の CylancePROTECT Desktop エージェントは、Microsoft の Antimalware Protected Process Light（AM-PPL）テクノロジを使用した信頼できるサービスとして実行され、エージェントのシャットダウンを防止することもできます。この機能を使用するには、デバイスが Windows 10 1709 以降、または Windows Server 2019 以降を実行している必要があります。

オプション	説明
実行中の危険なプロセスとそのサブプロセスを強制終了	この設定を選択すると、脅威が検出されたときの状態に関係なく、エージェントはプロセスと子プロセス（.exe や .dll）を終了します。これにより、デバイス上で実行されている可能性のある悪意のあるプロセスを詳細に制御できます。 ファイルは、自動隔離、手動隔離、またはグローバル隔離リストを使用して隔離する必要があります。この機能は、ファイルを隔離する前に有効にする必要があります。この機能が有効になっていても、ファイルが隔離または自動隔離されていない場合、プロセスは引き続き実行されます。 例：あるファイルの実行が許可されていたときに、それを隔離することにしたとします。この設定を有効にすると、ファイルが隔離され、子プロセスとともにプロセスが終了します。この設定を無効にすると、ファイルは隔離されますが、ファイルの実行が許可されているため、ファイルによって開始されたプロセスは引き続き実行される可能性があります。

オプション	説明

バックグラウンド脅威検出	ディスク全体のスキャンを実行して、ディスク上に潜伏している脅威を検出して分析します。フルディスクスキャンは、システムリソースの使用を少なくすることで、エンドユーザーへの影響を最小限に抑えるように設計されています。バックグラウンド脅威検出スキャンには、システムの使用状況と分析が必要なシステム上のファイルの数に応じて、最大 1 週間かかることがあります。最新のバックグラウンドスキャンが完了した日時がコンソールに記録されます。
	
	スキャンは、インストール時にのみ 1 回実行するか、指定した繰り返し間隔で実行するかを選択できます。デフォルトのスキャン間隔は 10 日です。検出モデルへの大幅なアップグレード（新しいオペレーティングシステムの追加など）も、フルディスクスキャンをトリガーします。スキャンの実行頻度を増やすと、デバイスのパフォーマンスに影響を与える可能性があることに注意してください。
	
	［バックグラウンド脅威検出］設定を［**1** 回実行］に設定し、［新しいファイルの監視］を有効にして、ディスク上の新しいファイルや更新ファイルを監視することをお勧めします。新しいファイルや更新ファイルを監視する場合、既存ファイルを一度すべてスキャンする必要があります。予測的な性質を備えた技術のため、ディスク全体を定期的にスキャンする必要はありませんが、コンプライアンスの理由で実装していても問題ありません（PCI コンプライアンスなど）。
	
	メモ：同じ VM ホストの複数の VM デバイスでバックグラウンド脅威検出スキャンを同時に実行すると、デバイスのパフォーマンスに影響します。この機能を VM デバイスに対して段階的に有効にして、同時に実行されるスキャンの数を制限することを検討してください。
	
	スキャンを手動で実行するには、次のいずれかのコマンドを使用します。
	
	• Windows デバイスの場合：
	
	`C:\Program Files\Cylance\Desktop\CylanceSvc.exe / backgroundscan`
	
	• macOS デバイスの場合：
	
	`/Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -background-scan`
	
	• Linux デバイスの場合：
	
	`/opt/cylance/desktop/Cylance -b`
	`/opt/cylance/desktop/Cylance --start-bg-scan`

オプション	説明
新しいファイルを監視	この設定では、エージェントが新しいファイルや変更ファイルをスキャンおよび分析して、潜伏している脅威を確認することができます。脅威が検出された場合、ファイルは実行の有無問わず隔離されます。この設定は、バックグラウンド脅威検出（1 回実行）と併せて有効にすることをお勧めします。 自動隔離（実行制御）モードでは、実行時に危険なファイルや異常なファイルをブロックします。したがって、スキャン中にエージェントが脅威を検出したときに悪意のあるファイルを隔離する場合を除き、［自動隔離］モードが有効になっている場合は、［新しいファイルの監視］を有効にする必要はありません。 この設定は、パフォーマンスに影響する可能性があります。ディスク処理やメッセージ処理を監視して、パフォーマンスに変化がないか確認することをお勧めします。特定のフォルダを除外すると、パフォーマンスが向上する場合があります。また、エージェントが特定のフォルダやファイルをスキャンまたは分析する対象から外すことができます。
スキャンする最大アーカイブファイルサイズを設定	エージェントがスキャンするアーカイブファイルの最大サイズを指定します。この設定は、［バックグラウンド脅威検出］と［新しいファイルの監視］の設定に適用されます。アーカイブファイルをスキャンしない場合は、ファイルサイズを 0 MB にします。

オプション	説明
特定のフォルダを除外	この設定では、フォルダやサブフォルダを指定して、［バックグラウンド脅威検出］や［新しいファイルの監視］の機能によるスキャン対象から除外することができます。 Windows では、絶対パス（ドライブ文字を使用）を使用します。（例：`C:\Test`）。 macOS の場合は、ルートからの絶対パスを使用します。ドライブ文字は使用しません。（例：`/Applications/SampleApplication.app`）。 Linux の場合は、ルートからの絶対パスを使用します。ドライブ文字は使用しません。（例：`/opt/application`）。 **Windows** の例： `C:\Test` **macOS** の例（スペースなし）： `/Applications/SampleApplication.app` **macOS** の例（スペースあり）： `/Applications/Sample\ Application.app` **Linux** の例： `/opt/application/` ワイルドカード * は、フォルダの除外にも対応しています。詳細については、「保護設定のフォルダの除外におけるワイルドカード」を参照してください。 除外は以前の設定には影響しません。エージェントの初回インストール後、［バックグラウンド脅威検出］および［新しいファイルの監視］の機能では、設定された除外リストに従ってファイルを無視します。最初の検出または有害判定の後に除外を追加しても、既に検出または有害判定を受けたファイルが改めて除外されることはありません。以前に検出または有害判定を受けたファイルは、ローカルで撤回されるかグローバルセーフリストに追加されるまで、この状態のままになります。 たとえば、新しいファイルの監視で C:\Windows\ccmcache\test.exe という名前のファイルが有害判定された後で、C:\Windows\ccmcache\ が［保護設定］タブに追加された場合、有害判定されたファイルは、そのフォルダが除外として追加されても、有害のままになります。この場合、ローカルで有害判定を解除するか、ファイルをグローバルセーフリストに追加するまで、ファイルは有害と見なされます。
実行を許可	ファイルは、［特定のフォルダを除外］で指定されている場合も含め、どのフォルダから実行されようと、実行制御/自動隔離の対象になります。［実行を許可］設定を有効にすると、［特定のフォルダを除外］リストで指定したフォルダからファイルを実行できます。この設定は、最初や最後の入力項目だけでなく、リスト内のすべてのフォルダに適用されます。 これらのフォルダにドロップされたファイルや脅威は実行が許可されるので、デバイスや組織が侵害されるおそれがあります。不正なファイルを除外フォルダに追加しないように十分に注意してください。

オプション	説明
ファイルサンプルのコピー（マルウェア）	共有ネットワークドライブを指定して、バックグラウンド脅威検出で検出されたファイルサンプルのコピーを保存したり、新しいファイルを監視したり、実行制御を実施したりします。これにより、CylancePROTECT Desktop が危険または異常と見なしたファイルを独自に分析できます。 • CIFS/SMB ネットワーク共有がサポートされています。 • ネットワーク共有の場所を 1 つ指定します。完全修飾パスを使用する必要があります。例：`\\server_name\shared_folder` • 条件を満たすファイルはすべて、重複も含めてネットワーク共有にコピーされます。一意性テストは実行されません。 • ファイルは圧縮処理されます。 • ファイルはパスワードで保護されます。パスワードは「infected」です。

保護設定のフォルダの除外におけるワイルドカード

［保護設定］タブでフォルダの除外を指定する場合、アスタリスク（*）がすべてのオペレーティングシステムのワイルドカードとして使用できます。

文字	意味
*	アスタリスクを使用してフォルダを除外したり、フォルダ名のプレフィックスやサフィックスを示したりします。 • アスタリスクは、プラットフォーム固有のパス区切り文字（「\」）以外の 1 文字以上の文字列にマッチします。 • 除外パスでは、複数のワイルドカードを使用できます。 • 現時点では、「*」のエスケープはサポートされていません。たとえば、フォルダ名にアスタリスク「*」が含まれているフォルダは、除外できません。 • 以前のフォルダ除外機能は、引き続き適用されます。つまり、除外は子フォルダにも適用されます。

文字	意味

フォルダ除外の例：	以下は、`C:\Application\TestFolder1\MyApp\program.exe` を除外する例です。
	フォルダ除外におけるワイルドカードの適切な使用例
	• ワイルドカードを使用していない除外。
	`C:\Application\TestFolder1\MyApp\`
	• ワイルドカードで「MyApp」フォルダの親フォルダを示しています。
	C:\Application*\MyApp\
	• エージェントが照合するフォルダ名にプレフィックス（この場合「Test」）があることをワイルドカードで示しています。
	C:\Application*Folder1\MyApp\
	• エージェントが照合するフォルダ名にサフィックス（この場合「1」）があることをワイルドカードで示しています。
	C:\Application\TestFolder*\MyApp\
	• エージェントが照合するフォルダ名にプレフィックス（この場合「Test」）とサフィックス（この場合「1」）があることをワイルドカードで示しています。
	C:\Application*Folder*\MyApp\
	• C:ドライブの「Application」以下にあるフォルダをすべて除外することをワイルドカードで示しています。
	C:\Application*\
	• 全ドライブの「Application」以下にあるフォルダをすべて除外することをワイルドカードで示しています。
	\Application\
	フォルダ除外におけるワイルドカードの不適切な使用例
	• `C:\Application\TestFolder1\MyApp\*.exe`
	実行可能ファイルのファイル名にワイルドカードを使用することはできません。ワイルドカードは、フォルダ名またはディレクトリ名に対してのみ使用できます。
	• C:\Application**
	ダブルアスタリスク（**）は、フォルダの除外ではサポートされていません。ダブルではなく、シングルアスタリスク（*）を使用します。
	推奨されないフォルダ除外
	`C:\*`
	この除外は有効なエントリですが、C: ドライブ全体のあらゆるディレクトリ（子ディレクトリを含む）が対象となり、実際にすべて除外されることになります。

アプリケーション制御

アプリケーション制御とは、Windows デバイスおよび Linux デバイスで、ユーザーがデバイス上の実行可能ファイルに対する変更を制限できるようにするオプションの設定です。アプリケーション制御が有効になる前にデバ

イス上にあったアプリケーションのみを実行できます。アプリケーション制御は通常、セットアップ後に変更されない固定機能デバイス（POS デバイスなど）で使用されます。

アプリケーション制御を有効にすると、アプリケーションの追加やデバイス上のアプリケーションへの変更を試行しても拒否されます。つまり、アプリケーションを Web ブラウザからダウンロードしたり、別のデバイスやコンピュータ（外部ドライブや共有ドライブなど）からコピーしたりすることはできません。

アプリケーション制御の主な目的は次のとおりです。

- リモートドライブまたは外部ドライブからの実行可能ファイルの実行を拒否します。
- ローカルドライブでの新しい実行可能ファイルの作成を拒否します。
- ローカルドライブ上の既存のファイルに対する変更を拒否します。

アプリケーション制御を使用する場合は、次の点に留意してください。

- アプリケーション制御が有効になっている場合、CylancePROTECT Desktop および CylanceOPTICS エージェントの更新プロセスは無効になります。
- アプリケーション制御が有効になっている場合、CylancePROTECT Desktop エージェントや CylanceOPTICS エージェントを削除することはできません。
- アプリケーション制御を使用するシステム上で CylanceOPTICS を実行することは推奨されません。アプリケーション制御が有効になっていると、CylanceOPTICS はアプリケーション制御の制限により正しく機能しません。
- アプリケーション制御が有効になっている場合、リモートドライブまたは外部ドライブ上のすべての実行可能ファイルの実行が拒否されます。本番環境が停止したりネットワークアクティビティが過剰になったりしないよう、アプリケーション制御ではリモートドライブまたは外部ドライブへのファイル転送は監視しません。
- 「Linux デバイスでアプリケーション制御を使用する際の考慮事項」を参照してください。

アプリケーション制御設定

オプション	説明
アプリケーション制御	この設定では、アプリケーション制御を有効にするかどうかを指定します。アプリケーション制御を有効にすると、次の推奨設定が自動的に適用されます。 • ［ファイルアクション］タブでは、危険なファイルと異常なファイルの両方に対して、［自動隔離（実行制御あり）］設定が選択されます。 • ［メモリアクション］タブでは、［メモリ保護］設定が選択されます。すべてのメモリ保護違反タイプは［停止］に設定されます。 • ［保護設定］タブでは、［新しいファイルを監視］設定が選択されます。 これらの設定を変更する場合は、指定のタブから選択を解除します。
ウィンドウを変更	この設定を有効にすると、アプリケーション制御が一時的に無効になり、新しいアプリケーションの編集および実行、またはエージェントの更新を含む更新の実行が可能になります。必要な変更を行ったら、このチェックボックスをオフにして変更ウィンドウを閉じ、アプリケーション制御を再度有効にします。 この設定を使用してアプリケーション制御を一時的に無効にすると、フォルダの除外などの変更は保持されます。［アプリケーション制御］設定を無効にすると、設定はデフォルトにリセットされます。

オプション	説明
フォルダの除外(サブフォルダを含む)	この設定では、アプリケーション制御が有効になっている場合にアプリケーションの変更や追加を許可するフォルダの絶対パスを指定します。この設定は、Windows エージェント 1410 以降を実行しているデバイスに適用されます。 例：`C:\Program Files\Microsoft SQL Server` フォルダの除外は、ローカルの内蔵ドライブでのみ使用できます。リムーバブルドライブまたはリモートドライブの除外はサポートされていません。

アプリケーション制御アクティビティの表示

デバイスのアプリケーション制御アクティビティは、［脅威と活動］セクションの［デバイスの詳細］ページで確認できます。

Linux デバイスでアプリケーション制御を使用する際の考慮事項

Linux デバイスのデバイスポリシーでアプリケーション制御を有効にする前に、次の点に注意してください。

- アプリケーション制御ポリシーのフォルダ除外は Linux エージェントではサポートされていません。
- アプリケーション制御を有効にすると、ローカルファイルシステム上のすべての実行可能ファイルのインベントリが作成されます。ファイルの実行は、インベントリ内のファイルに制限されます。
- 実行可能ファイルは、アプリケーション制御を有効にした後でもデバイスに追加できますが、実行することはできません。アプリケーション制御が有効になっている場合は、インベントリにあるアプリケーションのみ実行できます。
- アプリケーション制御が有効になっている Linux デバイスで更新を許可すると、問題が発生する可能性があります。

エージェント設定

エージェント設定を使用すれば、ファイルが隔離されたときなどにデスクトップ通知をデバイスに表示できます。このページからコンソールにエージェントログファイルをアップロードすることもできます。

オプション	説明
ログファイルの自動アップロードを有効にする	コンソールのエージェントログがログファイルをアップロードし、コンソールで表示できるようにします。アップロードされたログファイルは30日間保存されます。 このオプションを有効にすると、［デバイス］タブからこのポリシーに割り当てられたデバイスを選択したとき、［エージェントログ］タブが表示されます。ログファイル名は、ログの日付になります。
デスクトップ通知を有効にする	エージェント通知ポップアップは、各デバイスで設定することも、コンソールのポリシーレベルで設定することもできます。デバイスレベルでエージェント通知ポップアップを有効または無効にすると、コンソール設定よりも優先されます。ログファイルを記録するデバイスがこのポリシーに割り当てられていることを確認します。 エージェント UI では、CylanceUI が再起動されるか、デバイスが再起動されると、［イベント］タブがクリアされます。

オプション	説明
ソフトウェアインベントリを有効化	この設定では、エージェントがデバイスにインストールされているアプリケーションのリストを管理コンソールにレポートするかどうかを指定します。この機能を使用すると、管理者は、デバイスにインストールされている脆弱性の原因となりうるアプリケーションを識別し、脆弱性に対するアクションに優先順位を付け、それに応じて管理していくことができます。 この機能には、Windows バージョン 3.2 の CylancePROTECT Desktop が必要です。 テナントに登録されているデバイスにインストール済みのすべてのアプリケーションのリストは、［アセット］ > ［インストール済みアプリケーション］画面から表示でき、アプリケーションごとに、それがインストールされているデバイスのリストが表示されます。個々のデバイスにインストールされているアプリケーションのリストは、［アセット］ > ［デバイス］ > ［デバイスの詳細］ > ［インストール済みアプリケーション］画面から表示することもできます。

スクリプト制御

スクリプト制御は、悪意のあるスクリプトの実行をブロックすることで Windows デバイスを保護します。スクリプトの実行を許可する場合は、ワイルドカードを使用していくつかの方法で除外を追加できます。たとえば、スクリプトの実行をブロックし、除外リストに追加されたスクリプトのみを実行できるようにポリシーを設定することができます。

項目	説明
アクション	スクリプトのタイプごとに、次のいずれかのアクションを選択できます。 • 無効：このアクションでは、すべてのスクリプトを実行できますが、コンソールにはレポートしません。この設定は推奨されません。 • アラート：このアクションでは、すべてのスクリプトを実行してコンソールにレポートできます。環境内で実行されているスクリプトをすべて監視する場合に使用する設定です。この設定は、許可またはブロックするスクリプトを決定する初期展開で推奨されます。 • ブロック：このアクションでは、すべてのスクリプトの実行をブロックし、コンソールにレポートします。除外リストに追加されたファイルのみを実行できます。アラートモードでの脅威の検証および監視後に使用する設定です。 Active Script および PowerShell スクリプトの設定では、次の設定を使用できます。 • 危険なスクリプトをブロック：スクリプトがまだ除外リストにない場合、CylancePROTECT は Cylance クラウドサービスからスクリプトの脅威スコアを取得し、危険な脅威スコアを受け取った場合、スクリプトの実行がブロックされます。危険なファイルはマルウェアに非常に類似しています。スコアのない異常なスクリプトはコンソールに通知されますが、ブロックされません。 • 異常なスクリプトと危険なスクリプトをブロック：スクリプトが除外リストにない場合、CylancePROTECT は Cylance クラウドサービスからスクリプトの脅威スコアを取得し、異常または危険な脅威スコアを受け取った場合、スクリプトの実行がブロックされます。危険なファイルはマルウェアに非常に類似しています。異常なファイルにはマルウェアに類似した属性がありますが、危険なファイルよりマルウェアである可能性は低くなります。スコアのないスクリプトはコンソールに通知されますが、ブロックされません。 ［保護］ > ［スクリプト制御］の画面で、スクリプト制御アラートを検索したり、イベントをブロックしたりすることができます。
アクティブスクリプト	この設定では、Active Scripts の実行またはブロックを制御します。Active Script には、VBScript や Jscript が含まれます スクリプト制御を強化するには、［危険なスクリプトをブロック］または［異常なスクリプトと危険なスクリプトをブロック］のいずれかの設定を使用します。これらの設定には、CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。デバイスがそれ以前のエージェントを実行している場合、スクリプトはデフォルトでブロックされます。

項目	説明
PowerShell スクリプト	この設定では、PowerShell スクリプトの実行またはブロックを制御します。 スクリプト制御を強化するには、［危険なスクリプトをブロック］または［異常なスクリプトと危険なスクリプトをブロック］のいずれかの設定を使用します。これらの設定には、CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。デバイスがそれ以前のエージェントを実行している場合、スクリプトはデフォルトでブロックされます。
PowerShellコンソール	この設定では、PowerShell コンソールの実行または起動のブロックを制御します。PowerShell コンソールをブロックすると、PowerShell コンソールの対話モードでの使用を防止することで、セキュリティが強化されます。 PowerShell コンソールのアラートモードには、CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。スクリプトを実行し、検出されたイベントを管理コンソールにレポートできます。アラートモードをサポートしていないエージェントの場合、PowerShell コンソールの使用はデフォルトで許可され、アラートは生成されません。 PowerShell コンソールを起動するスクリプトを使用していて、PowerShell コンソールがブロックされている場合、スクリプトは失敗します。可能であれば、PowerShell コンソールではなく PowerShell スクリプトを呼び出すようにスクリプトを変更することをお勧めします。これは、`-file` スイッチを使用して実行できます。コンソールを起動せずに PowerShell スクリプトを実行するための基本的なコマンド：`Powershell.exe -file [script name]`

項目	説明
マクロ（2.1.1578 以前）	この設定では、Microsoft Office のマクロに対してアラートを出すかブロックするかを制御します。マクロは Visual Basic for Applications（VBA）を使用して、Microsoft Office ドキュメント（通常、Microsoft Office、Excel、PowerPoint）内にコードを埋め込むことができます。マクロの主な目的は、スプレッドシート内のデータの操作や文書内のテキストの書式設定など、ルーチン操作を簡略化することです。ただし、マルウェア作成者はマクロを使用してコマンドを実行し、システムを攻撃できます。マクロでシステムを操作しようとすると、悪意のあるアクションが実行されていると見なされます。エージェントは、Microsoft Office 製品外に影響を与えるマクロから発生する悪意のあるアクションを探します。 次の点に留意してください。 • スクリプト制御のマクロ機能は、2.1.1578 以前のバージョンのエージェントで動作します。これより新しいエージェントの場合は、メモリ保護ポリシーの危険な **VBA** マクロ違反タイプを使用します。 • スクリプト制御用に作成されたマクロ除外は、危険な **VBA** マクロ違反タイプのメモリ保護除外に追加する必要があります。 • Microsoft Office 2013 以降、マクロはデフォルトで無効になっています。ほとんどの場合、Microsoft Officeドキュメントのコンテンツを表示するのにマクロを有効にする必要はありません。マクロは、信頼するユーザーから受け取ったドキュメントで、有効にする正当な理由がある場合のみ有効にします。それ以外の場合は、マクロは常に無効にする必要があります。
Python	この設定では、Python スクリプト（バージョン 2.7 および 3.0～3.8）の実行またはブロックを制御します。この設定は、2.1.1580 以降のエージェントで有効です。
.NET DLR	この設定では、NET DLR スクリプトの実行またはブロックを制御します。この設定は、2.1.1580 以降のエージェントで有効です。
XLM マクロ（プレビュー）	メモ：XLM マクロ機能は現在、プレビューモードで提供されているため、予想外の動作が発生する可能性があります。 この設定では、CylancePROTECT Desktop での Excel 4.0（XLM）マクロの実行またはブロックを制御します。マクロが有効化され実行されると、Microsoft AMSI インターフェイスがエージェントと連携して、デバイスポリシーに従ってマクロの実行を許可するかブロックするかを判断します。 この機能の使用条件は次のとおりです。 • Microsoft Windows 10 以降 • CylancePROTECT Desktop エージェントバージョン 3.1 • VBA マクロは Excel の［ファイル］ **>** ［トラストセンター］ **>** ［**Excel** トラストセンター］ **>** ［マクロ設定］ のメニューで無効にする必要があります。

項目	説明
詳細設定	次の詳細設定はスクリプトのスコアリングを促進し、スクリプト制御に役立ちます。 • すべてのスクリプトをスコアリング：この設定では、スクリプト制御の設定に関係なく、すべてのスクリプトがスコアリングされます。デフォルトでは、スクリプト制御の設定が［アラート］または［ブロック］に設定されている場合、スクリプトはスコアなしのままになります。 • スクリプトをクラウドにアップロード：この設定では、スクリプトのコピーを CylancePROTECT クラウドサービスにアップロードして脅威の分析とスコアリングを行うかどうかを指定します。このオプションが選択されていない場合、CylancePROTECT はハッシュの詳細を使用してスクリプトのスコア取得を試行します。 • 疑わしいスクリプト実行についてのみアラート：スクリプトがスコアリングされ、脅威が検出されなかった場合、この設定では、スクリプトの実行を管理コンソールにレポートしないことを指定します。このオプションが選択されていない場合、脅威を検出できなくても、すべてのスクリプトの実行を管理コンソールにレポートします。

項目	説明
ファイル、スクリプト、プロセスの除外	スクリプト制御が「プロック」になっている場合でも、フォルダを指定しておくことで、アラートを生成することなく、当該のフォルダ（およびサブフォルダ）内のスクリプトを実行できるようにすることができます。また、プロセスの除外を追加することで、特定のアプリケーションのスクリプトを適切に実行して、それ以外のものをブロックするようにすることもできます。たとえば、IT 部門が特定のツールを使用して常にスクリプトを実行する場合は、当該ツールでのプロセスを除外として追加することで、特定のツールによるスクリプトの実行が可能になります。 フォルダまたはサブフォルダの相対パスを指定します。フォルダパスは、ローカルドライブ、マッピングされたネットワークドライブ、または UNC（Universal Naming Convention）パスとして使用できます。 フォルダとスクリプトの除外 • フォルダの除外には、スクリプトやマクロのファイル名を含めることはできません。これらのエントリは無効となり、エージェントでは無視されます。 • 特定のスクリプトを除外する場合は、ワイルドカードを使用する必要があります。ワイルドカードで特定のスクリプトを除外する方法について、詳しくは スクリプト制御の除外におけるワイルドカード を参照してください。 • 「everyone」のグループに書き込み権限が付与されると、組織内外の誰もがスクリプトをフォルダやサブフォルダにドロップして、書き込むことができるようになります。CylancePROTECT Desktop では、継続的にスクリプトに関するアラートを送信したりブロックしたりすることになります。書き込み権限は、直接の親フォルダだけでなく、あらゆるすべての親フォルダに適用されます。 プロセスの除外 • プロセスの除外を使用するには、エージェントのバージョンが 2.1.1580 以降である必要があります。 • プロセス除外の実行可能ファイルは、実行制御により隔離されるため、実行がブロックされる可能性があります。実行可能ファイルが隔離されている場合は、ファイルを［ファイルアクション］タブの［ポリシーセーフリスト］に追加する必要があります。 • プロセス除外では、引き続きスクリプトの実行が許可され、指定したフォルダからの実行が制限されなくなります。

スクリプト制御の除外におけるワイルドカード

［スクリプト制御］タブで除外を指定する場合は、アスタリスク（*）をワイルドカードとして使用できます。

スクリプト制御の除外でワイルドカードを使用すると、コンソールに表示されるアラートの数が減り、除外パスとファイル名に一致する特定のスクリプトをユーザーが実行できるようになります。たとえば、ディレクトリパスでワイルドカードを使用するときに、特定のスクリプトの名前全体を使用して、そのスクリプトを除外するこ

とができます。また、ファイル自体の名前の一部としてワイルドカードを使用すると、類似する名前を共有しているスクリプトのグループを照合することもできます。

除外にワイルドカードを使用すると柔軟性が得られますが、除外対象が多すぎる場合には、セキュリティのスタンスを下げることもあります。たとえば /windows/temp など、フォルダ全体を除外しないでください。代わりに、除外するスクリプトのファイル名全体または一部を指定する際に、ワイルドカードを使用します（例：/windows/temp/myscript*.vbs）。

次の表に、スクリプト制御の除外のルールを示します。

項目	説明
サポートされているワイルドカード文字	スクリプト制御の除外のワイルドカードとしてサポートされているのはアスタリスク（*）のみです。 ワイルドカードは 1 つ以上の文字を表します。
UNIX 形式のスラッシュ	ワイルドカードを使用している場合、除外では UNIX 形式のスラッシュを使用する必要があります（Windows システムでも同様）。 例: /windows/system*/*
フォルダの除外	フォルダを除外する場合は、除外を（ファイルではなく）フォルダとして区別するため、パスの最後にワイルドカードを使用する必要があります。 例: • /windows/system32/* • /windows/*/test/* • /windows/system32/test*/*

ファイルの除外	ファイルを除外する場合は、除外を（フォルダではなく）ファイルとして区別するため、除外はファイル拡張子で終了する必要があります。例:
	• /windows/system32/*.vbs
	• /windows/system32/script*.vbs
	• /windows/system32/*/script.vbs
	• 各ワイルドカードは 1 つのフォルダレベルのみを表します。除外で表すフォルダのレベルは、除外しようとしているファイルのレベルと一致する必要があります。
	  • たとえば、/folder/*/script.vbs は \folder\test\script.vbs と一致しますが、\folder\test\001\script.vbs とは一致しません。この場合は、/folder/*/001/script.vbs または /folder/*/*/script.vbs のいずれかが必要です。
	  • ワイルドカードは、スクリプトが存在するレベルごとに保持される必要があります。
	  • 1 レベルに 2 つ以上のワイルドカードを使用することはできません。たとえば、/folder/*file*.ext は使用できません。

項目	説明
プロセスの除外	ワイルドカードによるプロセスの除外には、フォルダではなくプロセスの除外として区別するためにファイル拡張子が必要です。 ディレクトリに関係なくプロセスを指定する方法については、次の例を参照してください。 • `/my*.exe`（ローカルドライブ） • `//my*.exe`（ネットワークドライブ） 特定のディレクトリ内のプロセスを指定する方法については、次の例を参照してください。 • `/directory/child/my*.exe`（ローカルドライブ） • `//directory/child/my*.exe`（ネットワークドライブ）
除外における完全一致と部分一致の例	ワイルドカードでは、完全除外と部分除外がサポートされます。 • `/folder/*/script.vbs` • `/folder/test*/script.vbs`
絶対パス	絶対パスは、スクリプト制御の除外ではサポートされていません。
相対パス	共通の相対パスを区別できる場合は、ワイルドカードで UNC（汎用名前付け規則）のパスを除外できます。 たとえば、「DC01」から「DC24」などのパスでデバイス名を使用する場合は、次のようにします。 `/dc*/path/to/script/*`
ネットワークパス	ネットワークパスは除外することができます。例: • `//hostname/application/*` • `//host*/application/*` • `//*name/*/application/*` • `//hostname/*`

スクリプト制御の除外の例

特定のディレクトリの場所から実行される動的スクリプト、または複数の異なるユーザーフォルダから実行されるスクリプトに除外を追加するには、スクリプト制御の除外にワイルドカードを使用します。たとえば、例外パスにトークン「*」を使用すると、バリアントを確実にカバーできます。

次の表は、除外される一致と除外されない不一致を含む除外の例を示しています。

除外の例	一致	不一致
`/users/*/temp/*`	• `\users\john\temp` • `\users\jane\temp`	• `\users\folder\john\temp` • `\users\folder\jane\temp` フォルダレベルの数が一致しないため、これらのフォルダは除外されません。

除外の例	一致	不一致
`/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` ワイルドカードは 1 つ以上の文字を表すため、これらのフォルダは除外されません。
`//*example.local/sysvol/script*.vbs`	`\\ad.example.local\sysvol\script1.vbs`	`\\ad.example.local\sysvol\script.vbs` ワイルドカードは 1 つ以上の文字を表すため、このスクリプトは除外されません。
`/users/*/*/*.vbs`	• `/users/john/temp/script.vbs` • `/users/john/temp/anotherscript.vbs`	• `/users/john/temp1/temp2/script.vbs` フォルダレベルの数が一致しないため、このスクリプトは除外されません。

プロセスの除外

スクリプト制御の除外リストにはプロセスを追加することができます。この機能は、スクリプトを呼び出す特定のプロセスを除外する場合に便利です。たとえば、SCCM を除外して、一時ディレクトリで PowerShell スクリプトを起動するようにできます。ここでのプロセスとは、スクリプトインタープリタを呼び出してスクリプトを実行するあらゆるプロセスのことです。

- 次の例では、myfile.exe プロセスがインタープリタ（PowerShell.exe など）を呼び出してスクリプトを実行できるようにしています。
  - /windows/*/myfile.exe
- 次の例では、myprocess.exe を除外リストに追加して、フォルダパスに関係なく実行できるようにしています。
  - `\myprocess.exe`（ローカル Windows ドライブ上）
  - `\\myprocess.exe`（ネットワーク Windows ドライブ上）
- 次の例では、myprocess.exe を除外リストに追加して、特定のフォルダパスからのみ実行できるようにしています。
  - `\directory\child\myprocess.exe`（ローカル Windows ドライブ上）
  - `\\directory\child\myprocess.exe`（ネットワーク Windows ドライブ上）

メモ：

- 絶対パスは、除外に対してサポートされていません。
- 親要素はサポートされていません。
- 実行可能ファイル（exe）が除外に追加されると、/[CySc_process]/ が自動的に除外に追加されます。上記の除外例を追加した場合、結果は次のようになります。/[CySc_process]//windows/*/myfile.exe

スクリプト制御の除外の代替オプション

スクリプトを除外する代替法として、グローバルセーフリストを使用する方法や、証明書を追加する方法があります。

- CylancePROTECT Desktop のグローバル隔離リストまたはグローバルセーフリストへのファイルの追加
  - この方法は SHA256 ハッシュ値を必要とし、またこの値が変更されないことを前提としています。ハッシュ値は、スクリプトの更新、またはスクリプトの設計により行われた変更によって変化します。したがってこの方法では、スクリプトまたはマクロが頻繁に更新される場合や、プログラムによって変更される場合（新しい日付や時刻を追加する場合、システム要求を作成する場合、データを取得する場合など）には、その維持に必要な管理作業が増えます。CylancePROTECT Desktop エージェントが管理コンソールにスクリプトを報告するたびに、SHA256 ハッシュ値を報告する必要があります。ハッシュ値が変更されるたびにエージェントが新しい値を報告し、ユーザーがグローバルセーフリストにその新しい値を追加する必要があります。ハッシュ値を生成できない場合（スクリプトが正常に実行されない、ファイルが存在しない、権限の問題があるなど）には、スクリプトがコンソールに報告されると汎用ハッシュが使用されます。
  - 以下の SHA256 ハッシュ値は、スクリプトに対してハッシュを生成できない場合に CylancePROTECT Desktop エージェントが使用する汎用ハッシュです。この値をグローバルセーフリストに追加しようとすると、エージェントの機能に起因するエラーメッセージが表示されます。
    - `FE9B64DEFD8BF214C7490AA7F35B495A79A95E81F8943EE279DC99998D3D3440`
  - 以下の SHA256 ハッシュ値は、PowerShell ワンライナーが使用され、スクリプトに対してハッシュを生成できない場合に CylancePROTECT Desktop エージェントが使用する汎用ハッシュです。この値をグローバルセーフリストに追加しようとすると、エージェントの機能に起因するエラーメッセージが表示されます。
    - `FE9B64DEFD8BF214C7490BB7F35B495A79A95E81F8943EE279DC99998D3D3440`
- CylancePROTECT Desktop グローバルセーフリストへの証明書の追加
  - この方法では、有効なコード署名証明書をコンソールに送信する必要があり、PowerShell および Active Script でのみ使用できます（マクロでは使用できません）。

デバイスの制御

デバイスの制御では、組織内のデバイスに接続する USB 大容量ストレージデバイスを制御することで、デバイスを保護します。デバイス制御を有効にすると、USB フラッシュドライブ、外部ハードドライブ、スマートフォンなどの USB 大容量ストレージデバイスへのフルアクセス、読み取り専用、ブロックを制御できるようになります。ポリシーの一環で除外を使用することで、特定の大容量ストレージデバイスのアクセスレベルをベンダー ID、製品 ID、シリアル番号で定義することもできます。たとえば、すべての USB 大容量ストレージデバイスをブロックしているときに、除外を作成して一部の許可されたデバイスのみにフルアクセスできるようにすることができます。

- デバイス制御は、エージェントバージョン 2.1.1410 以降を実行している Windows デバイス、およびエージェントバージョン 3.3.1000 以降を実行している macOS デバイスで使用できます。
- デバイス制御により、マウスやキーボードなどの USB 周辺機器に影響が及ぶことはありません。たとえば、すべての USB 大容量ストレージデバイスタイプをブロックするポリシーを作成しても、USB キーボードは使用できます。
- SD カードのデバイス制御は現時点ではサポートされていません。ただし、USB カードリーダーデバイスと併用すると、デバイス制御で USB デバイスが検出される場合があります。

デバイス制御が有効な場合、適用のポリシーアクション（フルアクセス、読み取り専用、ブロック）に準じて、挿入されたすべての USB 大容量ストレージデバイスがログに記録されます。ポリシーアクションが「読み取り

専用」または「ブロック」で、デバイスでのデスクトップ通知が有効の場合、USB 大容量ストレージデバイスが接続されると、デバイスにてポップアップ通知が表示されます。デバイス制御イベントのログは、コンソールの［保護］**>**［外部デバイス］の画面で確認できます。

デバイス制御の設定	説明
Windows デバイス制御	この設定では Windows デバイスのデバイス制御をオンにして、USB デバイスタイプごとに適用するポリシーを選択できます。 Windows と macOS の両方の OS プラットフォームでデバイス制御が有効になっている場合、除外リストは両方のデバイス間で共有されます。
macOS デバイス制御	この設定では macOS デバイスのデバイス制御をオンにして、USB デバイスタイプごとに適用するポリシーを選択できます。 Windows と macOS の両方の OS プラットフォームでデバイス制御が有効になっている場合、除外リストは両方のデバイス間で共有されます。

デバイス制御のポリシーアクション	説明
ブロック	この設定では、デバイスが外部 USB ストレージデバイスにアクセスできないようにします。
読み取り専用	この設定では、読み取り専用で外部 USB ストレージデバイスにアクセスできるようにします。読み取り専用アクセスでは、デバイスで外部 USB デバイスのコンテンツを表示できますが、USB デバイスへの書き込みや削除のアクセスは許可されません。 次の USB デバイスタイプは、Windows デバイスでのみ読み取り専用アクセスに設定できます。 • 静止画 • USB CD/DVD RW • USB ドライブ • VMware USB パススルー • Windows ポータブルデバイス 除外を追加する場合、この設定は Windows デバイスにのみ適用され、macOS デバイスでは無視されます。
フルアクセス	この設定では、外部 USB ストレージデバイスにアクセスして読み取り、書き込み、削除ができるようになります。

サポートされる **USB** デバイスタイプ	説明	エージェントプラットフォーム
Android	Android OS を実行するポータブルデバイス（スマートフォンやタブレットなど）です。 Android デバイスが接続されると、デバイスタイプが Android、静止画像、Windows ポータブルデバイスとして識別される場合があります。Android デバイスをブロックする場合は、静止画および Windows ポータブルデバイスもブロックすることを検討してください。	Windows
iOS	iOS を実行している Apple ポータブルデバイス（iPhone や iPad など）です。 一部の iOS デバイスは、デバイスの制御が有効になっているときは充電されず、デバイスの電源がオフになっていない限りブロックするように設定されます。Apple には、デバイスの機能に、iOS デバイスのブロック機能のために必要とされる充電機能を備えています。Apple 以外のデバイスは、この方法で充電機能をバンドルしておらず、影響を受けません。	Windows
静止画	デバイスタイプには、スキャナ、デジタルカメラ、フレームキャプチャ付きマルチモードビデオカメラ、フレームグラバーなどが挙げられます。 メモ：エージェントでは、Canon カメラを静止画像デバイスとしてではなく、Windows ポータブルデバイスとして認識します。	Windows
USB CD DVD RW	USB 光学式ドライブ。	Windows、macOS
USB ドライブ	USB ハードドライブまたは USB フラッシュドライブ。	Windows、macOS
VMware USB パススルー	VMware 仮想マシンクライアントです。USB デバイスをホストに接続します。	Windows
Windows ポータブルデバイス	スマートフォン、デジタルカメラ、ポータブルメディアプレーヤーなど、Microsoft Windows ポータブルデバイス（WPD）ドライバ技術を使用するポータブルデバイスです。	Windows

外部ストレージの除外の追加

特定のストレージデバイスのアクセス権限を指定する場合は、外部 USB 大容量ストレージデバイスの除外を追加できます。デバイス制御ポリシーに除外対象を追加する場合は、デバイスのベンダー ID が必要です。製品 ID とシリアル番号はオプションであり、除外対象をより具体的に設定する場合にも使用できます。各除外対象に正し

い情報を使用するには、デバイス制御を有効にしてデバイスを挿入し、コンソールでそのログエントリを検索します（［保護］ > ［外部デバイス］）。

外部ストレージの除外を追加する場合は、次の点に留意してください。

- すべてのメーカーが製品にシリアル番号を使用しているわけではありません。一部のメーカーでは、複数の製品に同じシリアル番号を使用しています。
- 外部ストレージの除外は編集できません。必要に応じて新しい除外対象を追加し、不要になった除外対象を削除します。
- 各デバイス制御ポリシーの除外対象の数は 5000 までに制限されています。この制限に達すると、［デバイスを追加］ボタンは無効になります。
- Windows と macOS の両方の OS プラットフォームでデバイス制御が有効になっている場合、除外リストは両方のデバイス間で共有されます。

1. コンソールで、［設定］ > ［デバイスポリシー］に移動します。
2. 新しいポリシーを作成するか、既存のポリシーを編集します。
3. ［デバイス制御］タブをクリックして、デバイス制御がオンになっていて設定されていることを確認します。
4. ［外部ストレージの除外リスト］セクションで、［デバイスを追加］をクリックします。
5. ［ベンダー **ID**］を入力します。
6. 除外対象を絞り込むには、［製品 **ID**］と［シリアル番号］を含めます（オプション）。除外を説明するコメントを追加することもできます。
7. ［アクセス］フィールドで、割り当てるアクセスレベルを選択します。
   - フルアクセス
   - 読み取り専用

     この設定は Windows デバイスにのみ適用され、macOS デバイスでは無視されます。
   - ブロック
8. ［送信］をクリックします。
9. ポリシーを保存（または作成）します。

デバイス制御除外の一括インポート

管理者は、.csv ファイルを使用してデバイス制御除外を一括でインポートすることができます（ファイルあたり最大 500 個の除外）。フォーマット要件の詳細およびサンプルテンプレートのダウンロードについては、support.blackberry.com にアクセスして「KB 65484」を参照してください。

デバイス制御除外の **.csv** テンプレートのダウンロード

1. デバイスポリシーの［デバイス制御］タブで、［デバイス制御］を有効にします。
2. ［除外をインポート］をクリックします。
3. ［テンプレートをダウンロード］をクリックして、ファイルを保存します。
4. 形式の要件に従ってテンプレートを変更します。

デバイス制御除外を含む **.csv** ファイルのインポート

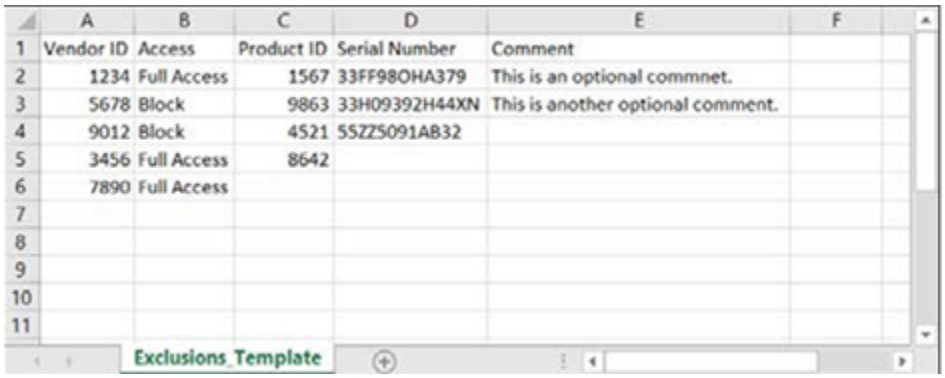
1. デバイスポリシーの［デバイス制御］タブで、［デバイス制御］を有効にします。

2. ［除外をインポート］をクリックします。
3. ［インポートする **.csv** ファイルを参照］をクリックして、インポートする .csv ファイルを選択します。
4. ［アップロード］をクリックします。

.csv ファイルの形式要件

- .csv ファイルのみが承諾されます。
- .csv ファイルには列のヘッダー情報が必要です。インポート機能は、.csv ファイルの最初の行を無視します。除外がインポートファイルの最初の行にあると、インポートされません。列見出しは次の順序で並べる必要があります：
  - ベンダーID
  - アクセス
  - 製品ID
  - シリアル番号
  - Comment
- 各除外には［ベンダー ID］と［アクセス］のフィールドが必要です。
- ［製品 ID］、［シリアル番号］、［Comment］のフィールドは任意です。
- ［アクセス］列には、フルアクセス、読み取り専用、ブロックのいずれかの値が必要で、英語の値のみが受け入れられます。
- ［コメント］列は、カンマ（,）をサポートしていません。

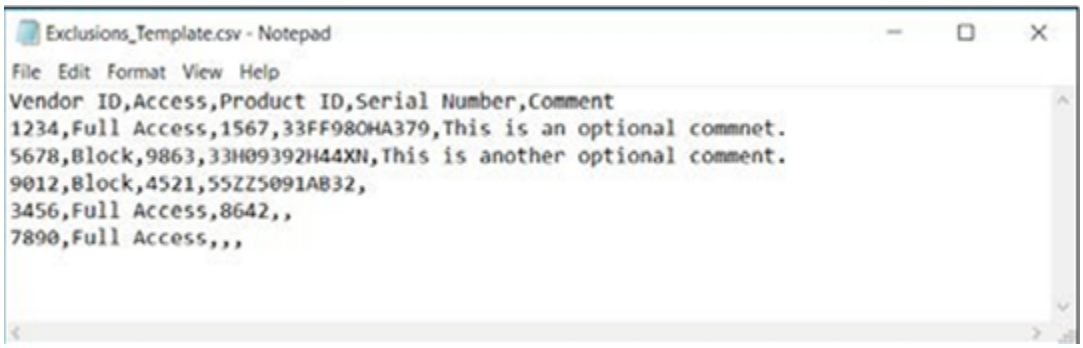
例：スプレッドシートを使用した一括インポート



	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

例：テキストエディタを使用した一括インポート



Exclusions_Template.csv - Notepad

File Edit Format View Help

```
Vendor ID,Access,Product ID,Serial Number,Comment
1234,Full Access,1567,33FF98OHA379,This is an optional commnet.
5678,Block,9863,33H09392H44XN,This is another optional comment.
9012,Block,4521,55ZZ5091AB32,
3456,Full Access,8642,,
7890,Full Access,,,
```

制限事項

- .csv ファイルごとの除外の最大数は 500 です。500 個以上の除外を含むファイルをインポートしようとすると、エラーメッセージが表示されます。
- ポリシーごとの除外の最大数は 5000 です。この数を超えると、警告メッセージが表示されます。
- 使用するデバイスの言語設定が英語でないと、Microsoft Excel でテンプレートをインポートおよび編集するときに、オプションを UTF-8 およびカンマ区切りで設定しなければならない場合があります。オプションを変更せずにファイルを開くと、認識できない文字が表示される場合があります。

Windows 用 CylancePROTECT Desktop エージェントのインストール

CylancePROTECT Desktop は、デバイスに影響を与える前に、マルウェアを検出してブロックします。BlackBerry は、マルウェアの識別に数学的アプローチを使用し、事後署名、信頼ベースのシステム、サンドボックスなどの代わりに機械学習技術を使用します。このアプローチは、新しいマルウェア、ウイルス、ボット、および将来のバリアントを無用にします。CylancePROTECT Desktop は OS 層およびメモリ層におけるマルウェアのファイル実行の可能性を分析して、悪意のあるペイロードの配信を防止します。

エージェントは、個別のデバイスにインストールすることも、インストールパラメーターを使用して展開ツールで環境全体に展開することもできます。

Windows エージェントのインストール

作業を始める前に：

- 管理コンソールから CylancePROTECT Desktop インストールファイルをダウンロードします。［設定］ > ［展開］をクリックします。［製品］ドロップダウンリストから［**CylancePROTECT**］を選択し、ターゲットオペレーティングシステム、エージェントバージョン、およびファイルタイプを設定します。［ダウンロード］をクリックします。
- 管理コンソールで［設定］ > ［アプリケーション］からインストールトークンをコピーします。

1. CylancePROTECT Desktop インストーラをダブルクリックします。
2. ［CylancePROTECT Desktop セットアップ］ウィンドウで［インストール］をクリックします。
3. インストールトークンを入力し、［次へ］をクリックします。
4. 必要に応じて、保存先フォルダを変更します。
5. ［**OK**］をクリックしてインストールを開始します。
6. ［完了］をクリックしてインストールを完了します。CylancePROTECT Desktop を起動するチェックボックスがオンになっていることを確認します。

終了したら： デバイスポリシーで、メモリ保護、スクリプト制御、デバイス制御のいずれかまたはすべてが有効になっている場合は、エージェントのインストールまたはアップグレード後にデバイスを再起動することをお勧めしますが、厳密には必要ありません。再起動すると、新しいポリシー設定が完全に有効になります。

Windows のインストールパラメーター

エージェントは、GPO、Microsoft System Center Configuration Manager（SCCM）、MSIEXEC、およびその他のサードパーティ製ツールを使用して、対話型または非対話型でインストールできます。MSI を以下のパラメーターでカスタマイズするか、コマンドラインからパラメーターを指定することができます。

パラメーター	値	説明
PIDKEY	*<Installation Token>*	このパラメーターは、インストールトークンを自動的に入力します。
LAUNCHAPP	0 または 1	0：この値は、実行時にシステムトレイアイコンとスタートメニューフォルダを非表示にします。 1：この値は、実行時にシステムトレイアイコンとスタートメニューフォルダを表示します。 値が入力されていない場合、デフォルト値は 1 です。
SELFPROTECTIONLEVEL	1 または 2	1：この値を指定すると、ローカル管理者がレジストリとサービスを変更できるようになります。 2：この値を指定すると、システム管理者のみがレジストリとサービスを変更できるようになります。 値が入力されていない場合、デフォルト値は 2 です。
APPFOLDER	*<Target Installation Folder>*	このパラメーターは、エージェントのインストールディレクトリを指定します。デフォルトの場所は C:\Program Files\Cylance\Desktop です。

パラメーター	値	説明

REGWSC	0 または 1	0：この値は、CylancePROTECT Desktop がアンチウイルスプログラムとして Windows に登録されないことを示します。CylancePROTECT Desktop と Windows Defender をデバイス上で同時に実行することができます。
		
		1：この値は、CylancePROTECT Desktop がアンチウイルスプログラムとして Windows に登録されていることを示します。
		
		値が入力されていない場合、デフォルト値は 1 です。
		
		上記のコマンドは、Windows Server 2016 および 2019 には影響しません。Windows Server 2016 および 2019 に CylancePROTECT Desktop をインストールした後で、Windows Defender を無効にするには、次のレジストリ値を設定します。
		
		`HKLM\SOFTWARE\Policies\Microsoft \Windows Defender\DisableAntiSpyware`
		
		`REG_DWORD`
		
		`Value = 1`
		
		Windows Defender サブキーが存在しない場合は、手動で作成する必要があります。
		
		グループポリシー設定を使用して Windows Defender を管理する方法の詳細については、「グループポリシー設定を使用して Microsoft Defender ウイルス対策を管理する」を参照してください。

VENUEZONE	"*<Zone_Name>*"	このパラメーターを使用して、デバイスを追加するゾーンの名前を指定します。その名前のゾーンが見つからない場合は、指定した名前のゾーンが作成されます。 ゾーン名には、空白、タブ、復帰改行、等号、改行文字、またはその他の非表示の文字を含めることはできません。

パラメーター	値	説明
VDI	<X>	マスターイメージに CylancePROTECT Desktop をインストールする場合は、インストールパラメーター VDI=<*X*> を使用します。ここで、<*X*> はドメインに接続されていないマシンまたはイメージの総数（マスターイメージを含む）の「カウンタ」です。<*X*> の値によって、エージェントがデフォルトのエージェントフィンガープリントメカニズムではなく、VDI フィンガープリントを使用して仮想マシンの識別を開始するタイミングが決まります。 VDI パラメーターはカウンタ「X」を使用し、遅延効果があります。一方、AD パラメーターはインストール時にすぐに使用されます。 詳細については、「仮想マシンで CylancePROTECT Desktop を使用するための要件と考慮事項」を参照してください。
AD	1	このパラメーターには、エージェントバージョン 1520 以降が必要です。 最初のインストール時に、ドメインに接続されたマスターイメージで Active Directory（AD）パラメーターを使用します。ドメインに接続されたマスターイメージにインストールすると、すぐにマスターイメージ上の VDI フィンガープリントが使用され、その後ワークステーションのプールが作成されます。 AD フィンガープリントは、VDI=<*X*> インストールパラメーターよりも優先されます。詳細については、「仮想マシンで CylancePROTECT Desktop を使用するための要件と考慮事項」を参照してください。
PROXY_SERVER	<*ip_address*>:<*port_ number*>	このパラメーターは、エージェントが通信する必要があるプロキシサーバーの IP アドレスを指定します。プロキシサーバーの設定は、デバイスのレジストリに追加されます。エージェントログファイルでは、プロキシサーバーの情報を確認できます。

パラメーター	値	説明
AWS	1	このパラメーターには、エージェントバージョン 1500 以降が必要です。 このパラメーターを使用して、Amazon EC2 インスタンス ID を取得し、この ID をデバイス名に含めると、Amazon Cloud ホストの識別に役立ちます。 デバイス名は変更され、ホスト名とインスタンス ID が含まれるようになります。たとえば、デバイス名が ABC-DE-12345678 であり、AWS EC2 ID が i-0a1b2cd34efg56789 である場合、完全なデバイス名は ABC-DE-123456789_i-0a1b2cd34efg56789 になります。 この機能は Amazon EC2 インスタンス ID 専用です。
PROTECTTEMPPATH	1	このパラメーターには、エージェントバージョン 1480 以降が必要です。 このパラメーターを使用して、CylanceDesktopArchive および CylanceDesktopRemoteFile フォルダの場所を、Cylance ProgramData フォルダに変更します。 詳細については、KB 66457「Changing the location of the CylanceDesktopArchive and CylanceDesktopRemoteFile folders（CylanceDesktopArchive および CylanceDesktopRemoteFile フォルダの場所の変更）」を参照してください。

例：**PIDKEY**、**APPFOLDER**、および **LAUNCHAPP** パラメーター

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

この例では、インストールはサイレントで実行され、インストールログは C:\temp フォルダに保存されます。このフォルダの作成が必要になる場合があります。エージェントの実行中は、システムトレイアイコンとスタートメニューの Cylance フォルダが非表示になります。実行可能なコマンドラインオプションの詳細については、https://docs.microsoft.com/en-us/windows/win32/msi/command-line-options を参照してください。

例：**PIDKEY**、**VDI**、および **LAUNCHAPP** パラメーター

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

この例では、VDI の 2 は、ワークステーションのプールが作成される前に、ドメインに接続されていないマシンまたはイメージの総数（マスターイメージと追加イメージまたは親イメージ）です。

例：**PIDKEY**、**AD**、および **LAUNCHAPP** パラメーター

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

この例では、AD パラメーターは、マスターイメージと作成されたワークステーションのプールで、VDI フィンガープリントをただちに使用します。グループポリシーを使用して展開するために MSI インストールファイルを編集する方法については、KB 66391「Editing the MSI Installer using Orca（Orca を使用した MSI インストーラの編集）」を参照してください。

macOS 用の CylancePROTECT Desktop エージェントのインストール

CylancePROTECT Desktop は、デバイスに影響を与える前に、マルウェアを検出してブロックします。BlackBerry は、マルウェアの識別に数学的アプローチを使用し、事後署名、信頼ベースのシステム、サンドボックスなどの代わりに機械学習技術を使用します。このアプローチは、新しいマルウェア、ウイルス、ボット、および将来のバリアントを無用にします。CylancePROTECT Desktop は OS 層およびメモリ層におけるマルウェアのファイル実行の可能性を分析して、悪意のあるペイロードの配信を防止します。

エージェントは、個別のデバイスにインストールすることも、インストールパラメーターを使用して展開ツールで環境全体に展開することもできます。

macOS 用 CylancePROTECT Desktop エージェントのインストール

作業を始める前に：

- 管理コンソールから CylancePROTECT Desktop インストールファイルをダウンロードします。［設定］ > ［展開］をクリックします。［製品］ドロップダウンリストから［**CylancePROTECT**］を選択し、ターゲットオペレーティングシステム、エージェントバージョン、およびファイルタイプを設定します。［ダウンロード］をクリックします。
- 管理コンソールで［設定］ > ［アプリケーション］からインストールトークンをコピーします。

1. CylancePROTECT Desktop インストールファイル（.dmg または .pkg）をダブルクリックして、インストーラをマウントします。
2. CylancePROTECT Desktop ユーザーインタフェイスで  をダブルクリックしてインストールを開始します。
3. ［続行］をクリックして、OS とハードウェアが要件を満たしていることを確認します。
4. ［続行］をクリックします。
5. インストールトークンを入力します。
6. ［続行］をクリックします。
7. 必要に応じて、インストール場所を変更します。
8. ［インストール］をクリックします。
9. 資格情報を入力します。
10. ［ソフトウェアをインストール］をクリックします。
11. 概要画面で、［閉じる］をクリックします。
12. ［**OK**］ > ［完了］をクリックします。

13. macOS Catalina に CylancePROTECT Desktop をインストールする場合は、CylanceUI で通知を表示する許可を求めるメッセージが表示されます。［許可する］をクリックします。

macOS 以降の CylancePROTECT Desktop 構成要件

CylancePROTECT Desktop エージェントのバージョン 2.1 以降を、macOS を実行しているデバイスにインストールする場合は、次の構成要件に注意してください。要件は、デバイスが MDM ソリューション（Jamf Pro など）で管理されているかどうかによって異なります。

MDM で管理されているデバイス

以下の情報は、MDM ソリューションとして Jamf Pro を使用していますが、他の MDM ソリューションにも適用されます。

要件	手順
全般設定	構成プロファイルを作成し、［一般］タブで次の設定を指定します。 • プロファイルの名前と説明を指定します。 • レベル：コンピュータレベル • 配布方法：自動インストール
CylancePROTECT カーネル拡張機能を有効にします。（macOS 10 のみ）	承認されたカーネル拡張機能のオプションで次の設定を行います。 • 表示名：Cylance • チーム ID：6ENJ69K633 • ［範囲］タブで、構成プロファイルの範囲が CylancePROTECT Desktop および CylanceOPTICS を実行する macOS 10 デバイスに適用されるよう指定されていることを確認します
CylancePROTECT システム拡張機能を有効にします。（macOS 11+）	システム拡張機能のオプションで次の設定を行います。 • 表示名：CylanceSystemExtension • システム拡張機能のタイプ：使用可能なシステム拡張機能 • チーム識別子：6ENJ69K633 • 使用可能なシステム拡張機能：com.cylance.CylanceEndpointSecurity.extension

要件	手順
CylancePROTECT エージェントおよびシステム拡張のフルディスクアクセスを有効にします。	プライバシー環境設定ポリシー制御のオプションで次の設定を行います。 App Access 構成を追加し、次の設定を指定します。 • 識別子：com.cylance.Agent • 識別子のタイプ：バンドル ID • コード要件： このトピックの HTML バージョンからコード要件をコピーします。コード要件は 1 行にしておく必要があり、追加のスペースや改行を含めないようにしてください。 • **SystemPolicyAllFiles** サービスを追加し、**Allow** に設定します。 別の App Access 構成を追加し、次の設定を指定します。 • 識別子：com.cylance.CylanceEndpointSecurity.extension • 識別子のタイプ：バンドル ID • コード要件： このトピックの HTML バージョンからコード要件をコピーします。コード要件は 1 行にしておく必要があり、追加のスペースや改行を含めないようにしてください。 • **SystemPolicyAllFiles** サービスを追加し、**Allow** に設定します。
通知	構成プロファイルの［通知］タブでは、次の設定が推奨されます。 • 重要アラート：有効 • 通知：有効 • バナーアラートタイプ：持続 • ロック画面の通知：表示 • 通知センターの通知：表示 • バッジアプリアイコン：表示 • 通知のサウンド再生：有効
Scope	［範囲］タブで次を設定します。 • 構成プロファイルの範囲指定について、CylancePROTECT Desktop を実行する macOS デバイスに適用されることを確認します。
インストール後に再起動します。	上記の設定手順を完了したら、CylancePROTECT Desktop エージェントをインストールし、デバイスを再起動します。

MDM で管理されていないデバイス

MDM 管理がされていないデバイスでは、デバイスへの macOS エージェントのインストール後、「CylanceES システム拡張機能」を承認するように求めるプロンプトがユーザーに表示されます。プロンプトの指示に従って、システム拡張を有効にし、ディスクへのフルアクセスを許可します。ユーザーは「CylanceUI」からの通知をタップして、通知設定を構成することもできます。

1. ［セキュリティ環境設定を開く］をクリックします。［システム環境設定］ > ［セキュリティとプライバシー］ > ［一般］タブが開きます。
2. 必要に応じてロックをクリックして変更を認証し、［許可する］をクリックします。
3. 「アプリケーション **'CylanceES'** のシステムソフトウェアのロードがブロックされました」というメッセージの横にある［許可する］をクリックして、機能拡張を承認します。
4. フルディスクアクセスを有効にするには、デバイスで［システム環境設定］ > ［セキュリティとプライバシー］ > ［プライバシー］タブに移動します。
5. 必要に応じてロックをクリックして変更を認証し、［許可する］をクリックします。
6. 下にスクロールして［フルディスクアクセス］をクリックします。
7. ［**CylanceEsExtension**］を選択します。
8. ［システム環境設定］ > ［通知］ > ［**CylanceUI**］タブで、エージェントへの通知を許可します。

コマンドラインを使用した **macOS** エージェントのインストールコマンド

コマンドラインを使用して macOS エージェントをインストールする場合は、インストールパラメーターを含めた `cyagent_ install_token` ファイルを作成する必要があります。このファイルには、インストールトークンおよび設定可能なその他のオプションパラメーターが含まれます。

次のセクションでは、コマンドラインからのファイルの作成例を説明していますが、テキストエディタからファイルを作成して、各パラメーターを個別の行に記述することもできます。ファイルは、インストールパッケージと同じフォルダにある必要があります。

インストールトークンのみを使用した **macOS** エージェントのインストール

次のコマンド例をターミナルで使用すると、インストールトークンを使用して `cyagent_ install_token` ファイルを作成し、エージェントをインストールすることができます。.dmg インストーラを使用する場合は、コマンドのファイル拡張子を適宜変更します。

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

以下は、インストールトークンを使用しない場合のインストールコマンドです。

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

パラメーター指定を使用した **macOS** エージェントのインストール

次のコマンド例をターミナルで使用すると、`cyagent_ install_token` ファイルの作成を指定パラメーターを用いて行い、エージェントをインストールすることができます。.dmg インストーラを使用する場合は、コマンドのファイル拡張子を適宜変更します。

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

インストールパラメーター

CylancePROTECT Desktop エージェントは、ターミナルのコマンドラインオプションを使用してインストールできます。

パラメーター	値	説明
`InstallToken`	<インストールトークン>	インストールトークンは、エージェントをインストールするときに必要です。これは管理コンソールで［設定］**>**［アプリケーション］をクリックすることで確認できます。
`NoCylanceUI`		このパラメーターは、起動時にシステムトレイを非表示にします。
`SelfProtectionLevel`	1 または 2	1：この値を指定すると、ローカル管理者のみがレジストリとサービスを変更できるようになります。 2：この値を指定すると、システム管理者のみがレジストリとサービスを変更できるようになります。 値が指定されていない場合、デフォルト値は 2 です。
`LogLevel`	0、1、2、または 3	0：この値は、エラーメッセージのみログに記録されることを示しています。 1：この値は、エラーおよび警告メッセージがログに記録されることを示しています。 2：この値は、エラー、警告、情報メッセージがログに記録されることを示しています。 3：この値は、すべてのメッセージを記録する詳細ログを有効にします。詳細ログファイルのサイズは非常に大きくなる可能性があるので注意してください。BlackBerry では、トラブルシューティング中、詳細ログをオンにして、トラブルシューティングが完了したら 2 に戻すことをお勧めします。 値が指定されていない場合、デフォルト値は 2 です。
`VenueZone`	<ゾーン名>	このパラメーターを使用して、既存のゾーンまたは作成するゾーンにデバイスを追加します。ゾーンが存在しない場合は、入力された名前を使用してゾーンが作成されます。 ゾーン名には、タブ、復帰、改行、等号、空白、その他の不可視文字は使用できません。 このパラメーターには、エージェントバージョン 1380 以降が必要です。

パラメーター	値	説明
ProxyServer	<*IP* アドレス>:<ポート番号>	これにより、プロキシサーバーの設定がデバイスのレジストリに追加されます。プロキシサーバー情報は、エージェントログファイルで確認できます。 このパラメーターには、エージェントバージョン 1470 以降が必要です。

macOS インストールのトラブルシューティング

以下の表に、macOS インストールをトラブルシューティングするために実行できるアクションの概要を示します。

問題	アクション

インストールトークンとインストーラの詳細ログを使用したトラブルシューティング	次のコマンドを入力し、「YOURINSTALLTOKEN」は管理コンソールの［設定］ > ［アプリケーション］タブにあるインストールトークンで置き換えます。
	`echo YOURINSTALLTOKEN >cyagent_install_token`
	`sudo installer -verboseR -dumplog -pkg CylancePROTECT.pkg -target /`
	echo コマンドは、cyagent_install_token ファイルを出力します。このファイルは、1 行につき 1 つのインストールオプションが記述されたテキストファイルです。このファイルは、CylancePROTECT.pkg インストールパッケージと同じフォルダにある必要があります。
	macOS Catalina 端末を使用して CylancePROTECT Desktop エージェントをインストールすると、DYLD 警告が表示されることがあります。この警告は、CylancePROTECT Desktop ではなくオペレーティングシステムによって生成されたものであるため、インストールには影響しません。

macOS エージェントサービスの開始または停止	エージェントサービスを開始するには、次のコマンドを実行します。 `sudo launchctl load /Library/launchdaemons/com.cylance.agent_service.plist` エージェントサービスを停止するには、次のコマンドを実行します。 `sudo launchctl load /Library/launchdaemons/com.cylance.agent_service.plist`

問題	アクション
macOS Big Sur でのエンドポイントセキュリティシステム拡張のサポート	BlackBerry では、CylancePROTECT Desktop システム拡張機能の承認とフルディスクアクセスを含む構成プロファイルの展開には MDM を使用することをお勧めします。デフォルトでは、macOS Big Sur オペレーティングシステムを新たにインストールしたシステムへの MDM プロファイルのリモートサイレントインストールは、サポートされていません。 ユーザー操作を行わずにリモートの macOS システムに構成プロファイルをインストールするには（サイレントインストール）、Apple Mobile Device Management（MDM）が必要です。macOS Big Sur にアップグレードする前に、デバイスを MDM ベンダーに登録する必要があります。アップグレード前に登録しなかったデバイスでは、管理者権限でのユーザー操作が必要です。 リモートサイレントインストールをサポートするには、次の手順を実行します。 1. macOS Catalina をインストールします。 2. MDM プロファイルを適用します。 3. 構成プロファイルをデバイスにダウンロードします。 4. デバイスを macOS Big Sur にアップグレードします。 サポートされている CylancePROTECT Desktop エージェントのバージョンと拡張タイプは次のとおりです。 • バージョン 1570 以前の CylancePROTECT Desktop エージェントには、Catalina 以前の macOS でサポートされているカーネル拡張機能が含まれています。 • バージョン 1580 以降の CylancePROTECT Desktop エージェントには、Catalina 以前の macOS でサポートされているカーネル拡張機能と、Big Sur 以降の macOS でサポートされているエンドポイントセキュリティシステム拡張機能が含まれています。

Linux 用の CylancePROTECT Desktop エージェントのインストール

エージェントは、各システムに直接インストールするか、Ansible、SCCM、cloud-init などのシステム管理ソフトウェアを使用してインストールすることができます。エージェントをインストールする際には、インストールパラメーターを使用してインストール設定を行います。

ターゲットデバイスがシステム要件を満たし、ソフトウェアをインストールするための適切な権限を持っていることを確認します。

- CylancePROTECT Desktop の要件を確認します。
- Linux エージェントをインストールするには、root 権限が必要です。
- Linux エージェントインストール用の設定ファイルの作成

Linux デバイスに CylancePROTECT Desktop エージェントをインストールした後、システム上の最新のカーネルをサポートするように Linux ドライバを最新の状態に保ってください。更新されたドライバパッケージは、定期的にリリースされ、エージェントリリースとは独立してリリースされます。詳細については、「Linux ドライバの更新」を参照してください。

Linux エージェントインストールパッケージ

エージェントバージョン 2.1.1590 以降の CylancePROTECT Desktop エージェント、エージェント UI、およびドライバパッケージは 1 つの圧縮された .tgz ファイルに含まれています。

Debian パッケージ	コンポーネント
cylance-protect-driver	独自のドライバ
cylance-protect-open-driver	オープンなドライバ
cylance-protect	CylancePROTECT Desktop エージェント/サービス
cylance-protect-ui	CylancePROTECT Desktop UI

RPM パッケージ	コンポーネント
CylancePROTECTDriver	独自のドライバ
CylancePROTECTOpenDriver	オープンなドライバ
CylancePROTECT	CylancePROTECT Desktop エージェント/サービス
CylancePROTECTUI	CylancePROTECT Desktop UI

Linux インストールの前提条件

エージェントは、各システムに直接インストールするか、Ansible、SCCM、cloud-init などのシステム管理ソフトウェアを使用してインストールすることができます。エージェントをインストールする際には、インストールパラメーターを使用してインストール設定を行います。

ターゲットデバイスがシステム要件を満たし、ソフトウェアをインストールするための適切な資格情報を持っていることを確認します。

- CylancePROTECT Desktop の要件
- Linux エージェントをインストールするには、root 権限が必要です。

Linux エージェントインストール用の設定ファイルの作成

CylancePROTECT Desktop エージェントを Linux デバイスにインストールする前に、Cylance Endpoint Security テナントへのデバイスの登録とローカルエージェント設定の定義に使用する設定ファイルを作成する必要があります。この設定ファイルは、エージェントのインストール後にデバイスから削除されます。

CylancePROTECT Desktop の `config_defaults.txt` では、行末にラインフィードのみを含める必要があります。DOS/Windows コンピューターでファイルを作成すると、行末にはキャリッジリターンとラインフィードが含まれます。config_defaults.txt ファイルを適切な形式に変換する方法については、support.blackberry.com/community にアクセスして記事 65749 を参照してください。

1. `/opt/cylance/` ディレクトリに `config_defaults.txt` ファイルを作成します。

2. 次の情報を使用してこのファイルを編集します。

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

- *YOUR_INSTALL_TOKEN* を管理コンソールで取得されるインストールトークンに置き換えます。
- *ZONE_NAME* をデバイスの追加先のゾーン名に置き換えます。指定したゾーンがコンソールに存在しない場合は、自動的に作成されます。

パラメーター	説明
InstallToken	これは必須フィールドです。デバイスを登録する Cylance Endpoint Security テナントを指定します。管理コンソールの［設定］ > ［アプリケーション］メニューのインストールトークンを使用します。
SelfProtectionLevel	この設定は、Cylance サービスとフォルダへのアクセスのレベルを制限します。 • 1 : [ローカル管理者]のみがレジストリとサービスを変更できます。 • 2 : [システム管理者]のみがレジストリとサービスを変更できます。 デフォルト設定は［2］です。
LogLevel	この設定は、デバッグログに収集される情報のレベルを指定します。 • 0 : エラー • 1 : 警告 • 2 : 情報 • 3 : 詳細 デフォルト設定は［2］です。詳細ログを選択すると、ログファイルのサイズが急速に大きくなります。
VenueZone	この設定は、デバイスを追加するゾーンを指定します。 • 指定したゾーン名がコンソールに存在しない場合は、指定した名前を使用してゾーンが作成されます。 • ゾーン名またはデバイス名の先頭または末尾にホワイトスペースがある場合（「 Hello」や「Hello 」など）、デバイス登録時にホワイトスペースは削除されます。タブ、キャリッジリターン、改行、その他の不可視文字は使用できません。 • ゾーン名に等号（=）を含めることはできません。たとえば、「Hello=World」は使用できません。

パラメーター	説明
UiMode	この設定は、システム起動時のエージェントユーザーインターフェイスのモードを指定します。 • 1：最小限のユーザーインターフェイス • 2：フルユーザーインターフェース デフォルト設定は［2］です。
AWS	この設定は、エージェントを Amazon Web Services ホスト上で実行することを指定します。デフォルトでは、デバイスのホスト名がデバイス名として管理コンソールで使用されます。この設定を有効にすると、エージェントはホストからインスタンス ID を取得し、ホスト名にインスタンス ID を加えてコンソールのデバイス名フィールドに保存できます。この設定により、Amazon Web Services ホスト上の各エージェントが固有のデバイス名を管理コンソールに報告します。 1：エージェントがインスタンス ID を取得できるようにします。 デバイス名は変更され、ホスト名 + インスタンス ID が含まれるようになります。インスタンス ID は、「i-」プレフィックスで示されます。 ABC-DE-123456789_i- 0a1b2cd34efg56789 では、デバイス名が ABCDE-12345678、AWS EC2 ID が i-0a1b2cd34efg56789 です。

Linux エージェントの自動インストール

作業を始める前に：

- CylancePROTECT Desktop の要件を確認します。
- 管理コンソールから CylancePROTECT Desktop インストールファイルをダウンロードします。［設定］ > ［展開］をクリックします。［製品］ドロップダウンリストから［**CylancePROTECT**］を選択し、ターゲットオペレーティングシステム、エージェントバージョン、およびファイルタイプを設定します。［ダウンロード］をクリックします。
- 管理コンソールで［設定］ > ［アプリケーション］からインストールトークンをコピーします。
- ルート権限があることを確認します。

1. Linux エージェントインストール用の設定ファイルの作成。
2. 次のコマンドを指定順で実行して、ドライバとエージェントをインストールします。.tgz ファイルから抽出したファイルを使用して、*<version>* の値を決定します。

Linux ディストリビューション	コマンド
• Red Hat Enterprise Linux • CentOS • Amazon Linux • Oracle	次のコマンドを実行して、ドライバとエージェントをインストールします。 **a.** `yum install CylancePROTECTOpenDriver-<version>.rpm CylancePROTECTDriver-<version>.rpm` **b.** `yum install CylancePROTECT.<version>.rpm CylancePROTECTUI.<version>.rpm`
SUSE Linux Enterprise Server	次のコマンドを実行して、ドライバとエージェントをインストールします。 **a.** `zypper install CylancePROTECTOpenDriver-<version>.rpm CylancePROTECTDriver-<version>.rpm` **b.** `zypper install CylancePROTECT.<version>.rpm CylancePROTECTUI.<version>.rpm`

終了したら：

- インストール後にエージェント UI が自動的に起動しない場合（CentOS、SUSE、Ubuntu デバイスなどで）、CylancePROTECT UI を表示するには GNOME シェルを再起動する必要があります。「UI の手動起動」を参照してください。

Linux エージェントの手動インストール

作業を始める前に：

- CylancePROTECT Desktop の要件を確認します。
- 管理コンソールから CylancePROTECT Desktop インストールファイルをダウンロードします。［設定］ > ［展開］をクリックします。［製品］ドロップダウンリストから［**CylancePROTECT**］を選択し、ターゲットオペレーティングシステム、エージェントバージョン、およびファイルタイプを設定します。［ダウンロード］をクリックします。
- 管理コンソールで［設定］ > ［アプリケーション］からインストールトークンをコピーします。
- ルート権限があることを確認します。

1. Linux エージェントインストール用の設定ファイルの作成。
2. 次のコマンドを指定順で実行して、ドライバとエージェントをインストールします。.tgz ファイルから抽出したファイルを使用して、*<version>* の値を決定します。

Linux ディストリビューション	コマンド

• Red Hat Enterprise Linux または CentOS
• Amazon Linux
• Oracle
• SUSE Linux Enterprise Server
	a. 次のコマンドを使用して、オープンドライバをインストールします。
	`rpm -ivh CylancePROTECTOpenDriver-<version>.rpm`
	b. 次のコマンドを使用して、エージェントドライバをインストールします。
	`rpm -ivh CylancePROTECTDriver-<version>.rpm`
	c. 次のコマンドを使用して、エージェントをインストールします。
	`rpm -ivh CylancePROTECT.<version>.rpm`
	d. 次のコマンドを使用して、エージェント UIをインストールします。*
	`rpm -ivh CylancePROTECTUI.<version>.rpm`
	* SUSE Linux Enterprise Server を実行しているデバイスの場合は、エージェント UI をインストールする前に Gnome 3 ライブラリ（libgtk-3-0）をインストールする必要がある場合があります。必要に応じて、次のコマンドを使用します：`zypper install libgtk-3-0`

• Ubuntu
• Debian
	a. 次のコマンドを使用して、オープンドライバをインストールします。
	`dpkg -i cylance-protect-open-driver_<version>.deb`
	b. 次のコマンドを使用して、エージェントドライバをインストールします。
	`dpkg -i cylance-protect-driver_<version>.deb`
	c. 次のコマンドを使用して、エージェントをインストールします。
	`dpkg -i cylance-protect.version.deb`
	d. 次のコマンドを使用して、エージェント ID をインストールします。
	`dpkg -i cylance-protect-ui.version.deb`

終了したら：

インストール後にエージェント UI が自動的に起動しない場合（CentOS、SUSE、Ubuntu デバイスなどで）、CylancePROTECT UI を表示するには GNOME シェルを再起動する必要があります。「UI の手動起動」を参照してください。

Linux ドライバの更新

サポートされている各 Linux カーネルには、CylancePROTECT Desktop エージェントをデバイス上で実行できるように、サポートされているドライバが必要です。デバイス上の Linux カーネルをアップグレードする際は、デバイスが対応のドライバを実行していることを必ず確認してください。最新のカーネルにアップグレードすると、デバイスが最新の OS セキュリティ更新プログラムを受信できるようになります。また、最新のエージェントとドライバを使用することで、CylancePROTECT で確実に保護されるようになります。

Linux ドライバを最新の状態に保つには、次のオプションがあります。

シナリオ	操作
Linux カーネルのアップグレード時に、ドライブの更新が利用可能になると直ちに自動更新します。	• デバイスがバージョン 3.1 以降のエージェントおよびドライバ 3.1 以降を実行していることを確認します。 • 更新ルールで［Linux ドライバを自動更新］機能を有効にします。
Linux カーネルのアップグレード時にドライバを手動更新します。	• Linux カーネルをアップグレードするたびに、管理コンソールでドライバパッケージが入手できるようになったら、ドライバパッケージを手動でダウンロードする必要があります。使用している Linux カーネルに必要なドライバの最小バージョンを確認するには、「サポートされている Linux ドライバとカーネル」のスプレッドシートを参照してください。 • エージェントとドライバを更新するには、パッケージマネージャまたは同様のツールとメソッドを使用します。 • エージェントを手動で更新することを選択した場合、BlackBerry では、ゾーンベースのエージェントの更新設定を、これらのデバイスでは［更新しない］に変更することをお勧めします。 ヒント：3.1.1100 ドライバは、エージェント 2.1.1590 以降と互換性があります。バージョン 2.1.1590 以降のエージェントを実行しているデバイスにドライバをインストールすると、エージェント 3.1 にアップグレードした際に［Linux ドライバを自動更新］機能を利用できるようになります。

Linux ドライバの自動更新

デバイス上の Linux カーネルをアップグレードする際は、デバイスが対応のドライバを実行していることを必ず確認してください。デバイスで実行している CylancePROTECT Desktop エージェントのバージョンが 3.1 以降の場合は、Linux ドライバの自動更新機能を有効化できます。これにより、カーネルが更新されて利用可能なカーネルがシステム上で検出されたときに、エージェントがドライバを自動的に更新できるようになります。最新のカーネルにアップグレードすると、デバイスが最新の OS セキュリティ更新プログラムを受信できるようになります。また、最新のエージェントとドライバを使用することで、CylancePROTECT で確実に保護されるようになります。

1. 管理コンソールのメニューバーで、［設定］ > ［更新］の順にクリックします。
2. Linux デバイスの更新の管理に使用する更新ルールをクリックします。作成が必要な場合は、「CylancePROTECT Desktop および CylanceOPTICS エージェントの更新の管理」を参照してください。
3. ［エージェント］セクションを展開します。
4. ［**Linux** ドライバの自動更新］オプションを選択します。
5. ［保存］をクリックします。

Linux ドライバの手動更新

Linux デバイス上のカーネルをアップグレードする際には、デバイスがそのカーネルをサポートするドライバを実行していることを確認する必要があります。Linux ディストリビューションがカーネル更新プログラムをリリースすると、BlackBerry は更新された Linux ドライバパッケージを作成し、管理コンソールから入手できるようにします。ドライバアップデートパッケージは、エージェントリリースに含まれているバージョンよりも新しいバージョンがある場合にのみ入手可能になります。

BlackBerry では、エージェントをバージョン 3.1 以降にアップグレードすることをお勧めします。このバージョン以降では、更新されたカーネルが検出された後、入手可能になり次第、エージェントが Linux ドライバを自動更新できるようにする機能が有効になります。バージョン 3.0 または 2.1.1590 のエージェントを実行している場合、または［Linux ドライバを自動更新］機能を使用しないという選択をした場合は、Linux カーネルのサポートされているドライバを手動でインストールする必要があります。組織のツールやメソッドを使用して、互換性のあるドライバをデバイスに展開できます。

作業を始める前に：

- ルート権限または sudo 権限があることを確認します。
- デバイスで Linux カーネルをサポートするために必要な最小ドライババージョンを確認します。

1. 管理コンソールのメニューバーで、［設定］ > ［展開］をクリックします。
2. ［製品］リストで、［**CylancePROTECT** ドライバ］を選択します。
3. ［**OS**］リストで、ドライバをダウンロードするオペレーティングシステムを選択します。
4. ［バージョン］リストで、ドライバのバージョンを選択します。
5. ［形式］リストで、ドライバの形式を選択します。
6. ［ダウンロード］をクリックします。
7. RPM パッケージをアップグレードするには、次のいずれかのコマンドを入力します。
   両方のドライバを同じコマンドラインに貼り付け、xx をパッケージのバージョン番号に置き換えます。

ディストリビューション	コマンド
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`

ディストリビューション	コマンド

サポート対象の 32 ビット Ubuntu および Xubuntu ディストリビューション	• 次のコマンドを使用して依存関係をインストールします。
	`apt-get update -y && apt-get install`
	• 次のコマンドを使用して、CylancePROTECT Desktop ドライバ DEB パッケージをインストールします。
	`dpkg -i cylance-protect-open-driver_xx_i386_32.deb`
	`dpkg -i cylance-protect-driver_xx_i386_32.deb`

サポート対象の 64 ビット Ubuntu、Xubuntu、および Debian ディストリビューション	• 次のコマンドを使用して依存関係をインストールします。
	`apt-get update -y && apt-get install`
	• 次のコマンドを使用して、CylancePROTECT Desktop ドライバ DEB パッケージをインストールします。
	`dpkg -i cylance-protect-open-driver_`*`xx`*`_amd64.deb`
	`dpkg -i cylance-protect-driver_`*`xx`*`_amd64.deb`

8. 次のコマンドを使用してサービスを再起動します：`systemctl start cylancesvc`。

エージェントの Linux コマンド

CylancePROTECT Desktop エージェントの Linux コマンドのリストを表示するには、次を使用します。

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

コマンドの使用例： `cylance <option>`

オプション	説明
-r, --register=<*token*>	提供されたトークンを使用して、エージェントをコンソールに登録します
-s, --status	エージェントの更新を確認します
-b, --start-bg-scan	バックグラウンド脅威検出スキャンを開始します
-B, --stop-bg-scan	バックグラウンド脅威検出スキャンを停止します
-d, --scan-dir=<*dir*>	ディレクトリをスキャンします
-l, --getloglevel	現在のロギングレベルを取得します
-L, --setloglevel=<*level*>	ロギングレベルを設定して、デバッグログに収集する情報のレベルを指定します

オプション	説明
-P, --getpolicytime	ポリシーの更新時刻を取得します
-p, --checkpolicy	ポリシーの更新を確認します
-t, --threats	脅威のリストを表示します
-q, --quarantine=<*id*>	ハッシュ ID を指定してファイルを隔離します
-w, --waive=<*id*>	ハッシュ ID を指定してファイルを保留します
-v, --version	このツールのバージョンを表示します
-h, --help	コマンドのリストを表示します

Linux エージェントインストールのトラブルシューティング

以下の表に、Linux エージェントのインストールをトラブルシューティングするために実行できるアクションの概要を示します。

タスクまたはエラー	アクション

エージェントサービスの開始または停止	Linux デバイスで Cylance サービスを開始または停止するには、次のコマンドを使用します。
	• Cylance サービスを開始する場合：
	`systemctl start cylancesvc`
	• Cylance サービスを停止する場合：
	`systemctl stop cylancesvc`

カーネルドライバがロードされているかどうかの確認	カーネルドライバがロードされているかどうかを確認するには、次のコマンドを入力します。
	`lsmod | grep CyProtectDrv`
	カーネルモジュールがロードされている場合、コマンドは次のように出力します。
	`CyProtectDrv 210706  0CyProtectDrvOpen 16384 1 CyProtectDrv`
	カーネルモジュールがロードされていない場合、出力は返されません。

タスクまたはエラー	アクション

カーネルドライバのロードおよびアンロード	CylancePROTECT Desktop Linux エージェント 2.1.1590 以降では、CyProtectDrv と CyProtectDrvOpen の 2 つのドライバが一緒にロードおよびアンロードされます。以前のバージョンのエージェントでは、CyProtectDrv ドライバのみがロードされていました。
	カーネルドライバをロードするには、次のいずれかのコマンドを入力します。
	• SUSE Linux ディストリビューションの場合：
	`modprobe --allow-unsupported cyprotect`
	--allow-unsupported フラグを使用しない場合は、/etc/modprobe.d/10-unsupported-modules.conf を編集し、'allow_unsupported_modules' を '1' に変更します。
	• その他の全 Linux ディストリビューションの場合：
	`modprobe cyprotect`

Linux UI の手動起動	インストール後にエージェント UI が自動的に起動されなかった場合は、「UI の手動起動」を参照してください。
エラー：Multilib バージョンの問題検出	デバイスにパッケージをインストールするときに「エラー：Multilib バージョンの問題検出」が発生する場合は、「エラー：Multilib バージョンの問題が見つかりました」を参照してください。

UI の手動起動

（CentOS、Ubuntu、および SUSE デバイスなどでは）インストール後にエージェント UI が自動的に起動しない場合があります。これを手動で起動するには、GNOME Shell Extension を再起動するか、ログアウトしてから再度ログインします。

GNOME Shell Extension を再起動する前に、GNOME Tweak Tool をインストールする必要があります。デフォルトでは、Ubuntu に GNOME Tweak Tool が含まれていないことがあります。

1. GNOME Tweak Tool をインストールする必要がある場合は、次のコマンドを実行します。

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

2. GNOME Shell Extension を再起動するには、Alt+F2 キーを押し、ダイアログボックスに「r」と入力して ENTER キーを押します。
CylanceUI アイコンが表示されない場合は、Tweak Tool から GNOME Shell Extension を手動で有効にします。GNOME Tweak Tool を起動するには、ターミナルに「gnome-tweaks」と入力します。GNOME Tweak Tool で、［**Extensions**］タブに移動し、CylanceUI を有効にします。

エラー：**Multilib** バージョンの問題が見つかりました

Red Hat Enterprise Linux または CentOS を実行しているデバイスへのパッケージのインストール時に「エラー：Multilib バージョンの問題が見つかりました」が発生した場合、これは通常、32 ビットライブラリと

ともに、対応する 64 ビットライブラリをインストールまたはアップグレードする必要があることを意味します。multilib バージョンのチェックは問題があることを示しているのみです。

たとえば、エラーが sqlite ライブラリに関連する場合：

- 別のパッケージで必要な依存関係が欠落している sqlite のアップグレードがあります。 Yum は、異なるアーキテクチャの古いバージョンの sqlite をインストールして、この問題を解決しようとします。その他のアーキテクチャを除外すると、yum により、パッケージの依存関係が欠落しているなど、問題の根本原因が表示されます。問題の根本原因を含むエラーメッセージを表示するには、--exclude sqlite.otherarch でアップグレードを再試行できます。
- 複数の sqlite アーキテクチャがインストールされていますが、yum ではこれらのアーキテクチャのうち 1 つのアップグレードしか確認できません。片方のアーキテクチャしか必要としない場合は、アーキテクチャ更新が欠落している sqlite を削除し、エラーが解決されたかどうかを確認できます。
- 既にインストールされているバージョンの sqlite が重複しています。「yum check」を使用してこのエラーを表示できます。
- 一致する sqlite ライブラリをインストールまたはアップグレードするには、次のコマンドを使用します。

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

  エラーが dbus-libs、openssl、または libgcc ライブラリに関連する場合は、このコマンドで sqlite を適切なライブラリに置き換えます。

CylancePROTECT Desktop および CylanceOPTICS エージェントの削除時にユーザーにパスワードの入力を要求する

Windows および macOS の CylancePROTECT Desktop エージェント、Windows の CylanceOPTICS エージェントバージョン 3.1 以降と、macOS の CylanceOPTICS エージェントバージョン 3.3 以降をアンインストールする際に、ユーザーにパスワードの入力を要求できます。この機能を macOS の CylanceOPTICS エージェントで使用するには、CylancePROTECT Desktop バージョン 3.1 以降も必要です。

1. 管理コンソールのメニューバーで、［設定］ > ［アプリケーション］をクリックします。
2. ［エージェントをアンインストールするにはパスワードが必要です］チェックボックスをオンにします。
3. パスワードを指定します。
4. ［保存］をクリックします。

CylancePROTECT Mobile のセットアップ

手順	アクション
1	CylancePROTECT Mobile アプリのソフトウェア要件とネットワーク要件を確認します。
2	会社のディレクトリから CylancePROTECT Mobile ユーザーを Cylance Endpoint Security に追加する場合は、会社のディレクトリにリンクします。
3	CylancePROTECT Mobile アプリユーザーを追加します。 オプションで、ユーザーを管理するグループを追加します。
4	CylancePROTECT Mobile ポリシーの作成。
5	登録ポリシーの作成。
6	デバイスユーザーは CylancePROTECT Mobile アプリをインストールしてアクティブ化します。手順については、「Cylance Endpoint Security ユーザーガイド」を参照してください。
7	必要に応じて、アラートをデバイスのリスクレベルにマッピングするリスク評価ポリシーを作成します。カスタムリスク評価ポリシーを割り当てない場合は、デフォルトのリスク評価ポリシーがテナントのユーザーに適用されます。
8	必要に応じて、Cylance Endpoint Security と Microsoft Intune を統合し、デバイスのリスクレベルを Intune にレポートして、Intune がデバイスで必要な緩和アクションを実行できるようにします。

Cylance Endpoint Security では、Microsoft Intune アプリ保護ポリシーを使用して、CylancePROTECT Mobile が報告したデバイス脅威レベルに基づいて特定の Microsoft アプリへのアクセスを許可または制限することもサポートされています。この機能を有効にするには、さまざまな一連の展開手順が必要です。この機能を設定するには、「Intune アプリの保護ポリシーと CylancePROTECT Mobile の併用」を参照してください。

CylancePROTECT Mobile ポリシーの作成

CylancePROTECT Mobile ポリシーを作成してユーザーとグループに割り当て、サービスを有効にして、使用する機能を制御します。

作業を始める前に： CylancePROTECT Mobile アプリと CylanceGATEWAY ユーザーの追加。

1. 管理コンソールのメニューバーで、［ポリシー］ > ［ユーザーポリシー］をクリックします。
2. ［**Protect Mobile**］タブで［ポリシーを追加］をクリックします。
3. ポリシーの名前と説明を入力します。

4. ［通知］セクションで、CylancePROTECT Mobile アプリが脅威を検出したときにユーザーに提示される通知の数と間隔を指定できます。［デバイス設定］セクション（手順 6）で、通知のタイプ（デバイス、メール、または通知なし）を指定します。
5. CylancePROTECT Mobile アプリが脅威を報告したときに特定の情報を難読化して、情報をプレーンテキストで管理コンソールに保存および表示できないようにするには、［データプライバシー］セクションで、［データプライバシー］をオンにして、難読化するフィールドを選択します。
6. ［デバイス設定］セクションで、［**Android**］または［**iOS**］をクリックし、使用する機能をオンにします。CylancePROTECT Mobile 機能の詳細については、「CylancePROTECT Mobile の主な機能」を参照してください。
   a) 有効にする機能ごとに、該当するチェックボックスを選択して、デバイス通知とメール通知を有効または無効にします。デバイス通知とメール通知を無効にした場合、ユーザーは CylancePROTECT Mobile アプリを開いてアラートを表示する必要があります。
   b) 次のいずれかの機能を有効にする場合は、次の追加手順を実行します。

機能	プラットフォーム	追加の手順
悪意のあるアプリ	Android	**a.** マルウェアスキャンからセーフリストのアプリを除外するには、［安全なアプリのリストのアプリを常に許可する］をオンにします。 **b.** 安全でないリストにあるアプリを自動的にブロックするには、［制限対象アプリリストのアプリを常にブロックする］をオンにします。 **c.** デバイスのシステムパーティションにプリインストールされているシステムアプリをスキャンする場合は、［システムアプリをスキャン］をオンにします。 **d.** Wi-Fi 接続経由で CylancePROTECT Mobile サービスにアプリをアップロードする場合は、［安全性チェックのために **Wi-Fi** 接続経由でアプリパッケージをアップロードする］をオンにします。Wi-Fi 経由でアップロードできるアプリの最大サイズ（MB 単位）と、1 か月（30 日）にアップロードできるすべてのアプリの最大サイズを指定します。いずれかの最大値を超えると、アップロードは行われず、デバイスログにエラーが追加されます。 **e.** モバイルネットワーク経由で CylancePROTECT Mobile サービスへのアプリのアップロードを有効にするには、［安全性チェックのためにモバイルネットワーク接続経由でアプリパッケージをアップロードする］をオンにします。モバイルネットワーク経由でアップロードできるアプリの最大サイズ（MB 単位）と、1 か月（30 日）にアップロードできるすべてのアプリの最大サイズを指定します。いずれかの最大値を超えると、アップロードは行われず、デバイスログにエラーが追加されます。
サポート対象外のデバイスモデル	Android iOS	［編集］をクリックして、制限するデバイスモデルを選択します。

機能	プラットフォーム	追加の手順
サポート対象外のOS	Android iOS	使用可能な OS バージョンを、組織のセキュリティ標準に基づいて、サポート対象およびサポート対象外のリストに追加します。
SafetyNet または Play Integrity 認証失敗	Android	CylancePROTECT Mobile アプリで、互換性テストスイートの一致を有効にする場合は、［**CTS** プロファイル照合を有効にする］をオンにします。
ハードウェア認証の失敗	Android	**a.** ［要求する最低限のセキュリティレベル］ドロップダウンリストで、適切なレベルをクリックします。詳細については、Android 開発者サイトの「SecurityLevel」を参照してください。 **b.** デバイスに最低限のセキュリティパッチレベルを適用する場合は、［セキュリティパッチレベル］をオンにします。適切なデバイスモデルを追加し、セキュリティパッチの日付を指定します。
安全でない Wi-Fi	Android	組織のセキュリティ基準に基づいて、使用可能な Wi-Fi アクセスアルゴリズムをセーフリストと危険リストに追加します。
安全ではないメッセージ	Android iOS	**a.** ［スキャニングオプション］ドロップダウンリストで、次のいずれかのオプションを選択します。 • CylancePROTECT Mobile サービスにメッセージを送信して安全かどうかを確認する場合は、［クラウドスキャニング］をオンにします。 • CylancePROTECT Mobile アプリのローカルでの機械学習モデルのみを使用して危険な URL を識別する場合には、［オンデバイススキャニング］をクリックします。 • URL スキャンを無効にする場合は、［スキャンしない］をクリックします。 **b.** Android デバイスの場合、［スキャニングオフセットを開始］フィールドで、スキャン対象のテキストメッセージの経過時間を時間単位で指定します。「0」を指定すると、新しいメッセージのみがスキャン対象になります。

7. ［追加］をクリックします。

終了したら：

- ポリシーをユーザーおよびグループに割り当てます。
- 必要に応じて、ポリシーをランク付けします。
- 登録ポリシーを作成し、ユーザーに割り当てます。ユーザーに登録ポリシーが割り当てられると、CylancePROTECT Mobile アプリをダウンロードしてアクティブ化する手順を記載したメールがユーザーに送信されます。詳細については、『Cylance Endpoint Security ユーザーガイド』を参照してください。
  - デフォルトのモバイルブラウザーで JavaScript を有効にするようにユーザーに指示します（CylancePROTECT Mobile アプリは Google Chrome、Samsung、Safari をサポートしています）。これは CylancePROTECT Mobile アプリをアクティブ化するために必要です。

    - アプリをインストールした後で CylancePROTECT Mobile のバックグラウンドアクティビティを許可するよう Android ユーザーに指示します。
- 必要に応じて、リスク評価ポリシーを作成します。カスタムリスク評価ポリシーの作成と割り当てを行わない場合は、デフォルトのリスク評価ポリシーがテナントのユーザーに適用されます。

リスク評価ポリシーの作成

リスク評価ポリシーは、CylancePROTECT Mobile アプリが検出したアラートをマッピングします（たとえば、侵害されたデバイスを高リスクとして扱うように指定できます）。アラートのリスクレベルは、モバイルデバイスの全体的なリスクレベルを決定するために使用されます。デバイスのリスクレベルは、管理コンソール（［アセット］ > ［モバイルデバイス］でデバイスの詳細）で表示できます。

リスク評価ポリシーを作成しない場合は、デフォルトポリシーがテナントのユーザーに適用されます。デフォルトのポリシーは編集できますが、削除はできません。

リスク評価ポリシーは、次の Cylance Endpoint Security 機能に使用できます。

- Cylance Endpoint Security を Microsoft Intune と統合している場合、Cylance Endpoint Security は、モバイルデバイスの全体的なリスクレベルを Intune に定期的に送信します。Intune を使用して、デバイスリスクレベルの軽減アクションを設定できます。
- モバイルデバイスのリスクレベルは CylanceGATEWAY ネットワークアクセスルールに組み込むことができます。

作業を始める前に： CylancePROTECT Mobile をセットアップします。

1. 管理コンソールのメニューバーで、［ポリシー］ > ［ユーザーポリシー］をクリックします。
2. ［リスク評価］タブをクリックします。
3. ［ポリシーを追加］をクリックします。
4. ポリシーの名前と説明を入力します。
5. ［リスク評価］セクションで、［検出を追加］ > ［検出］をクリックします。
6. 適用するリスクレベルに検出をドラッグアンドドロップします。
   検出の詳細については、「CylancePROTECT Mobile の主な機能」を参照してください。
7. ［追加］をクリックします。

終了したら：

- ポリシーをユーザーおよびグループに割り当てます。
- 必要に応じて、ポリシーをランク付けします。
- オプションで、Cylance Endpoint Security と Intune を統合し、モバイルの脅威に対応します。

Cylance Endpoint Security と Microsoft Intune の統合によるモバイルの脅威への対応

Cylance Endpoint Security を Microsoft Intune に接続して、Cylance Endpoint Security から Intune にデバイスのリスクレベルを報告できるようにすることができます。デバイスのリスクレベルは、Intune 管理対象デバイス上の CylancePROTECT Mobile アプリによるモバイル脅威の検出に基づき、計算されます。Intune は、デバイスのリスクレベルに基づいて軽減アクションを実行できます。

Cylance Endpoint Security を Intune に接続すると、統合が適用されるデバイスタイプと Intune グループを定義するアプリ設定ポリシーが作成されます。CylancePROTECT Mobile アプリによって検出されたイベントを、選択したリスクレベル（高、中、低）にマッピングするリスク評価ポリシーを作成して割り当てます。Intune 管理対象デバイス上の CylancePROTECT Mobile アプリが脅威（悪意のあるアプリやサイドロードされたアプリなど）を検出すると、その脅威にマッピングされているリスクレベルが、そのデバイスに対して Cylance Endpoint Security で算出される全体的なリスクレベルに織り込まれます。Cylance Endpoint Security はデバイスのリスクレベルを Intune に報告し、Intune はそのリスクレベルに設定されている軽減アクションを実行します。

この機能を使用するすべての Intune 管理対象デバイスを Cylance コンソールでアプリ設定ポリシーに含める必要があります。この機能では CylancePROTECT Mobile アプリバージョン 2.0.1.1099 以降が必要です。

Cylance Endpoint Security では、Microsoft Intune アプリ保護ポリシーを使用して、CylancePROTECT Mobile が報告したデバイス脅威レベルに基づいて特定の Microsoft アプリへのアクセスを許可または制限することもサポートされています。この機能を有効にするには、「Intune アプリの保護ポリシーと CylancePROTECT Mobile の併用」を参照してください。

Cylance Endpoint Security の Intune への接続

作業を始める前に： Intune との接続に使用する Cylance Endpoint Security 管理者アカウントには、Intune ライセンスが必要です。

1. 管理コンソールのメニューバーで、［設定］ > ［コネクタ］をクリックします。
2. ［接続を追加］ > ［**Microsoft Intune**］をクリックします。
3. Entra テナント ID を指定します。［次へ］をクリックします。
4. Entra の管理者資格情報を指定します。

   管理者の同意を求めるプロンプトに従います。必要に応じて、組織の Intune 管理者と協力して、Microsoft Intune 管理センターの CylancePROTECT Mobile MTD コネクタに関する同意を得ます。
5. ［アプリ設定ポリシー］画面で、Intune 統合を適用する OS プラットフォームをオンにし、各プラットフォームで次の手順を実行します。この機能を使用するすべての Intune 管理対象デバイスをアプリ設定ポリシーに含める必要があります。後でアプリ設定ポリシーを作成する場合は、［キャンセル］をクリックします。
   a) 必要に応じて、ポリシーの名前を変更します。ターゲットアプリを変更しないでください。
   b) Intune インスタンスのすべてのグループにポリシーを適用する場合は、［すべてのグループ］をオンにします。
   c) Intune インスタンスの特定のグループにポリシーを適用する場合は、⊕ をクリックします。グループを検索して選択し、［追加］をクリックします。
6. ［保存］をクリックします。Android 用のアプリ設定ポリシーを追加した場合は、表示される管理者の同意プロンプトに従ってください。

作成したアプリ設定ポリシーは、Intune 管理センターに表示されます。

終了したら：

- リスク評価ポリシーをまだ作成していない場合は作成して、CylancePROTECT Mobile アプリで検出された脅威を目的のリスクレベルにマッピングします。
- Intune 管理センターで CylancePROTECT Mobile MTD コネクタを編集し、コンプライアンスポリシーのオプションをオンにして、Android と iOS デバイスを CylancePROTECT に接続します。

Intune アプリの保護ポリシーと CylancePROTECT Mobile の併用

Microsoft Intune アプリの保護ポリシーを CylancePROTECT Mobile と併用して、CylancePROTECT Mobile が報告したデバイス脅威レベルに基づいて特定の Microsoft アプリへのアクセスを許可または制限できます。

1. CylancePROTECT Mobile アプリのソフトウェア要件とネットワーク要件を確認します。
2. 会社のディレクトリに Cylance Endpoint Security をリンクします。
3. Intune ユーザーを CylancePROTECT Mobile ユーザーとして Cylance Endpoint Security に追加します。
4. CylancePROTECT Mobile のポリシーを作成し、ユーザーに割り当てます。
5. 登録ポリシーを作成し、ユーザーに割り当てます。

   CylancePROTECT Mobile アプリをダウンロードして有効にする手順が記載されたメールがユーザーに送信されます。ユーザーに、今はメールを無視するように指示します。アプリのダウンロードと有効化は手順 10 で行います。CylancePROTECT Mobile アプリの有効化のために QR コードが必要になるため、ユーザーにメールを保存するよう指示します。
6. アラートをデバイスのリスクレベルにマッピングするリスク評価ポリシーを作成します。カスタムリスク評価ポリシーを割り当てない場合は、デフォルトのリスク評価ポリシーがテナントのユーザーに適用されます。
7. Cylance Endpoint Security の Intune への接続。
8. Intune 管理センターで次のように操作します。
   a) CylancePROTECT Mobile MTD コネクタを編集し、アプリ保護ポリシーのオプションをオンにして、Android と iOS デバイスを CylancePROTECT に接続します。
   b) Android および iOS デバイスのアプリ保護ポリシーを作成および設定し、報告されたリスクレベルに基づいて特定のアプリへのアクセスを CylancePROTECT Mobile で許可または制限する方法を指定します。
   c) アプリ保護ポリシーをユーザーグループに割り当てます。
9. Intune アプリ保護ポリシーを使用して保護する Microsoft アプリを展開します。保護された Microsoft アプリのインストール後、ユーザーは Microsoft Authenticator アプリ（iOS）または Intune Company Portal アプリ（Android）をインストールしてデバイスを登録するように求められます。
10. 保護された Microsoft アプリを起動し、「アクセス取得」プロンプトに従って CylancePROTECT Mobile アプリをインストールして有効にするようユーザーに指示します。手順 5 で受け取った QR コードを使用するようユーザーに指示します。

    Android ユーザーに CylancePROTECT Mobile アプリのインストールを求めるプロンプトが表示されない場合は、保護された Microsoft アプリを閉じて再度開くよう指示します。

ユーザーは、保護された Microsoft アプリを開くと、デバイスの現在のリスクレベルによってアプリへのアクセスが制限された場合に通知を受信します。

CylanceOPTICS のセットアップ

手順	アクション
1	ソフトウェアの要件を確認します。
2	CylanceOPTICS エージェントのデバイスへのインストール。
3	CylanceOPTICS の有効化と設定。
4	CylancePROTECT Desktop および CylanceOPTICS エージェントの更新の管理。

CylanceOPTICS エージェントのデバイスへのインストール

CylanceOPTICS を有効にするには、デバイスに CylanceOPTICS エージェントをインストールする必要があります。管理コンソールから CylanceOPTICS エージェントのインストーラをダウンロードし、組織で適切な方法によってデバイス上で実行します。たとえば、IT 管理者がデバイスにエージェントを事前インストールしてからユーザーに提供したり、信頼できるソフトウェア配布プロセスを使用してインストールをプッシュしたりできます。

作業を始める前に：

- CylanceOPTICS ソフトウェアの要件を確認します。
- CylanceOPTICS エージェントをインストールする前に、デバイスに CylancePROTECT Desktop エージェントをインストールする必要があります。
- CylanceOPTICS エージェントを macOS Big Sur（11.x）以降のデバイスにインストールする場合は、「macOS 11.x 以降の構成要件」を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［展開］をクリックします。
2. ［製品］ドロップダウンリストで［**CylanceOPTICS**］をクリックします。
3. OS、バージョン、および形式を選択します。

   メモ：

   - macOS デバイスの場合は、.pkg ファイルを使用することをお勧めします。.dmg ファイルは、インストールのためにディスクイメージをマウントする必要がある場合に使用できる、.pkg ファイルのディスクイメージです。
   - エージェントを macOS デバイスに展開する前に、KB article 66578: Allowing Cylance kernel extensions to address "Driver Failed To Connect"（KB 記事 66578：「ドライバの接続に失敗しました」の解決に Cylance カーネル拡張を許可する）を参照してください。
   - Oracle Linux Server UEK 8 および Oracle Linux Server 8 デバイスの場合は、Oracle 8 インストールファイルを使用します（CylanceOPTICS エージェント 3.2 以降が必要）。
4. ［ダウンロード］をクリックします。

5. 組織で適切なソフトウェア配布方法を使用して、インストールファイルをデバイスに展開して実行します。
   OS コマンドを使用して、CylanceOPTICS エージェントを Windows または macOS デバイスにインストールする場合、または Linux, にインストールする場合は、「CylanceOPTICS エージェントの OS コマンド」を参照してください。

終了したら：

- デバイスポリシーで、CylanceOPTICS の有効化と設定を行い、ポリシーを 1 つ以上のゾーンに割り当てます。
- CylanceOPTICS エージェントの更新管理の詳細については、「CylancePROTECT Desktop および CylanceOPTICS エージェントの更新の管理」を参照してください。

macOS 11.x 以降の構成要件

CylanceOPTICS エージェントのバージョン 3.0 以降を macOS Big Sur（11.x）以降を搭載するデバイスにインストールするには、次の構成要件に注意してください。要件は、デバイスが MDM ソリューション（Jamf Pro など）で管理されているかどうかによって異なります。

MDM で管理されているデバイス

以下の情報は、MDM ソリューションとして Jamf Pro を使用していますが、他の MDM ソリューションにも適用されます。

要件	手順
CylanceOPTICS のフルディスクアクセスを有効にします。	設定プロファイルを作成し、次のプライバシー設定を行います。 • 識別子：com.cylance.Optics • 識別子のタイプ：バンドル ID • コード要件： `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 サービス：許可
CylanceOPTICS システム拡張機能を有効にします。	設定プロファイルを作成し、次のプライバシー設定を行います。 • 表示名：Cylance Endpoint Security Optics システム拡張機能 • システム拡張機能のタイプ：使用可能なシステム拡張機能 • チーム識別子：6ENJ69K633 • 使用可能なシステム拡張機能：com.cylance.CyOpticsESF.extension

要件	手順
CylanceOPTICS システム拡張機能のフルディスクアクセスを有効にします。	設定プロファイルを作成し、次のプライバシー設定を行います。 • 識別子：com.cylance.CyOpticsESF.extension • 識別子のタイプ：バンドル ID • コード要件： `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 サービス：許可
CylanceOPTICS ネットワーク拡張機能を有効にします。	構成プロファイルを作成し、次のコンテンツフィルター設定を構成します。 • フィルター名：com.cylance.CyOpticsESF.extension • 識別子：com.cylance.CyOpticsESF.extension • ソケットフィルターバンドル識別子：com.cylance.CyOpticsESF.extension • ソケットフィルター指定要件： `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")` • ネットワークフィルターバンドル識別子：com.cylance.CyOpticsESF.extension • ネットワークフィルター指定要件： `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")`
インストール後に再起動します。	上記の設定手順を完了したら、CylanceOPTICS エージェントをインストールし、デバイスを再起動します。

MDM で管理されていないデバイス

CylanceOPTICS エージェントをインストールした後、以下を行います。

1. デバイスを再起動します。

2. ［セキュリティとプライバシー］設定に移動し、CyOpticsESFLoader を承認します。
3. メッセージが表示されたら、CylanceOPTICS ネットワークフィルターを許可します。
4. デバイスでシステム整合性保護（SIP）が有効になっている場合は、［プライバシー］タブで、［フルディスクアクセス］をクリックし、［CyOpticsESFLoader］が選択されていることを確認します。［CyOpticsESFLoader］がリストにない場合は、［+］をクリックし、［/Library/Application Support/Cylance/Optics］に移動して、［CyOptics］を選択します。
5. デバイスを再起動します。

システム拡張機能が読み込まれていることを確認するには、次の手順に従います。

1. `$ systemextensionsctl list` を実行し、出力に `com.cylance.CyOpticsESF.extension` が含まれていることを確認します。
2. `$ ps aux | grep -i extension | grep -i Cylance` を実行し、出力に `com.cylance.CyOpticsESF.extension.systemextension` が含まれていることを確認します。

CylanceOPTICS エージェントの OS コマンド

CylanceOPTICS エージェントインストーラは、次の OS コマンドをサポートしています。

Windows

操作	コマンド
インストールディレクトリを指定します。	`INSTALLFOLDER=<path>`
ローカル CylanceOPTICS データストアのディレクトリを指定します。	`OPTICSROOTDATAFOLDER=<path>`
ユーザーの操作を必要としないサイレントインストールを実行します。	.exe パッケージの場合、次のいずれかを使用します。 • `-q` • `-quiet` • `-s` • `-silent` .msi パッケージの場合、次のいずれかを使用します。 • `/q` • `/quiet`
インストールログファイルを作成します。	.exe パッケージ場合、次のいずれかを使用します。 • `-l <path_for_log>` • `-log <path_for_log>` .msi パッケージの場合、次のいずれかを使用します。 • `/l <path_for_log>` • `/log <path_for_log>`

操作	コマンド
CylanceOPTICS エージェントのプロキシバイパスを無効にします（.msi パッケージのみ）。	CylanceOPTICS エージェントが、常に指定のプロキシで CylanceOPTICS クラウドサービスに接続するようにするには、このオプションを使用します。ほとんどの環境では任意ですが、CylanceHYBRID を使用している場合、このオプションは必須になります。 以下のコマンドでインストーラを実行する前に、デバイス上に ProxyServer レジストリキーを作成します。「CylancePROTECT Desktop および Cylance Optics エージェントのプロキシ設定」を参照してください。CylanceHYBRID を使用している場合は、「CylanceHYBRID 管理ガイド」の Windows セットアップ手順を参照のうえ、CylanceHYBRID の必要値を使用して ProxyServer レジストリキーを作成します。 デバイスに ProxyServer レジストリキーを作成したら、次のコマンドを使用してエージェントをインストールします： `HYBRID=True` インストーラは、「True」の設定値を使用して、デバイスに DisableProxyBypass レジストリキーを作成します。詳細については、「CylanceOPTICS エージェントのプロキシオプション」を参照してください。コマンドの設定が `False` の場合、インストーラはレジストリキーを作成しません。
CylanceOPTICS エージェントをアンインストールします。	`"<CylanceOPTICS_program_directory>\CyOpticsUninstaller.exe"` 例: `"C:\Program Files\Cylance\Optics\CyOpticsUninstaller.exe"` ユーザーの操作を必要としないサイレントアンインストールを実行するには、次のコマンドを追加します： `--use_cli -t v20` CylanceOPTICS エージェントでアンインストールパスワードが要求されるように設定した場合は、次のコマンドを追加します： `--password <password>` 例: `"C:\Program Files\Cylance\Optics\CyOpticsUninstaller.exe" --use_cli -t v20 --password samplepass`

macOS

アクション	コマンド
CylanceOPTICS エージェントをインストールします。	`sudo installer -pkg CylanceOPTICS.pkg -target /`
CylanceOPTICS エージェントをインストールし、インストールログファイルを作成します。	`sudo installer -verboseR -dumplog -pkg CylanceOPTICS.pkg -target /`

アクション	コマンド
CylanceOPTICS エージェントのプロキシバイパスを無効にします。	CylanceOPTICS エージェントが、常に指定のプロキシで CylanceOPTICS クラウドサービスに接続するようにするには、このオプションを使用します。ほとんどの環境では任意ですが、CylanceHYBRID を使用している場合、このオプションは必須になります。 CylanceOPTICS エージェントのインストール前に、Cylance Endpoint Security のプロキシ要件 の手順に従って macOS デバイスのプロキシバイパスを設定します。
CylanceOPTICS サービスを開始します。	`sudo launchctl load /Library/LaunchDaemons/com.cylance.cyoptics_service.plist`
CylanceOPTICS サービスを停止します。	`sudo launchctl unload /Library/LaunchDaemons/com.cylance.cyoptics_service.plist`
CylanceOPTICS エージェントをアンインストールします。	`sudo /Applications/Cylance/Optics/Uninstall\ CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS`
UI を使用せずに CylanceOPTICS エージェントをアンインストールします。	`sudo /Applications/Cylance/Optics/Uninstall\ CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS --noui` このコマンドを使用する場合は、macOS 11.x デバイスで追加の操作が必要です。詳細については、Cylance Endpoint Security の管理に関するコンテンツのトラブルシューティングのセクションを参照してください。

Linux

アクション	コマンド
RHEL/CentOS、SUSE、または Amazon Linux 2 に CylanceOPTICS エージェントをインストールします。	`yum install CylanceOPTICS-<version>.rpm`、ここで、<version> は .rpm ファイルのバージョンです。
CylanceOPTICS エージェントを Ubuntu にインストールします。	`dpkg -i cylance-optics_<version>_amd64.deb`、ここで、<version> は .deb ファイルのバージョンです。
CylanceOPTICS サービスを開始します。	`systemctl start cyoptics.service`
CylanceOPTICS サービスを停止します。	`systemctl stop cyoptics.service`

アクション	コマンド
RHEL/CentOS、SUSE、または Amazon Linux 2 の CylanceOPTICS エージェントをアンインストールします。	`rpm -e CylanceOPTICS`
Ubuntu の CylanceOPTICS エージェントをアンインストールします。	`dpkg -P cylance-optics`

CylanceOPTICS の有効化と設定

デバイスポリシーで CylanceOPTICS を有効にし、そのポリシーをデバイスおよびゾーンに割り当てると、各デバイスの CylanceOPTICS エージェントはイベントを収集し、データを CylanceOPTICS データベースに格納します。エージェントは、CylanceOPTICS を有効にするまでデータを収集しません。

作業を始める前に： CylancePROTECT Desktop アプリケーション制御機能が有効になっていないことを確認します。アプリケーション制御は、セットアップ後に変更されない固定機能デバイス（POS マシンなど）用に設計されています。アプリケーション制御が有効になっている場合、CylanceOPTICS エージェントは期待どおりに機能しません。

1. 管理コンソールのメニューバーで、［ポリシー］ > ［デバイスポリシー］をクリックします。
2. 新しいポリシーを作成するか、既存のポリシーをクリックします。
3. ［**CylanceOPTICS** の設定］タブで、［**CylanceOPTICS**］チェックボックスをオンにします。
4. CylanceOPTICS データベースからコンソールへの脅威関連のフォーカスデータの自動アップロードを有効にする場合は、［脅威］セクションで［自動アップロード］チェックボックスをオンにします。

   このオプションを選択しない場合は、コンソールを使用してデバイスのフォーカスデータを要求する必要があります。
5. CylanceOPTICS データベースからコンソールへのメモリ関連のフォーカスデータの自動アップロードを有効にする場合は、［メモリ保護］セクションで［自動アップロード］チェックボックスをオンにします。

   このオプションを選択しない場合は、コンソールを使用してデバイスのフォーカスデータを要求する必要があります。
6. ［設定可能なセンサ］セクションで、有効にするオプションの CylanceOPTICS センサを選択します。オプションセンサは、64 ビットオペレーティングシステムでのみサポートされています。
7. ［最大デバイスストレージの設定］フィールドで、CylanceOPTICS エージェントが各デバイスでアクセスできるストレージの最大容量（MB 単位）を指定します。デフォルト値は 1000MB です。
8. CylanceOPTICS エージェントが Windows または macOS デバイス上のユーザーに OS 通知を提供できるようにするには、［**CylanceOPTICS** デスクトップ通知を有効にする］チェックボックスをオンにします。
9. 検出ルールセットをデバイスポリシーに関連付ける場合は、［検出セットを選択］ドロップダウンリストでルールセットをクリックします。
10. ［作成］または［保存］をクリックします。

既存のポリシーを変更し、現在の設定を新しいデバイスポリシーとして保存する場合は、［名前を付けて保存］をクリックします。

終了したら：

- ポリシーをデバイスまたはゾーンに割り当てます。
- ユーザーによるサービス停止を Windows 用の CylanceOPTICS エージェント（CylanceOPTICS 3.1 以降と CylancePROTECT Desktop 3.0 以降）および macOS（CylanceOPTICS 3.3 以降と CylancePROTECT Desktop 3.1 以降）で行えないようにするには、デバイスポリシーの［保護設定］で、［デバイスからのサービスシャットダウンを防止］をオンにします。この設定を有効にすると、macOS ユーザーは、デバイスプロパティの自己保護レベルが［ローカル管理者］に設定されている場合にのみ、サービスを停止できるようになります（［アセット］ > ［デバイス］ > デバイスをクリック）。この設定が有効になっている限り、Windows ユーザーはエージェントサービスを停止できません。
- ユーザーによる CylancePROTECT Desktop エージェント、Windows 用 CylanceOPTICS エージェントバージョン 3.1 以降、macOS 用 CylanceOPTICS エージェントバージョン 3.3 以降のアンインストール時にパスワード入力を必要としたい場合は、［設定］ > ［アプリケーション］で、［エージェントのアンインストール時にパスワードを必要とする］をオンにします。この機能を macOS の CylanceOPTICS エージェントで使用するには、CylancePROTECT Desktop バージョン 3.1 以降も必要です。

CylanceOPTICS センサ

デバイスポリシーで CylanceOPTICS をオンにすると、CylanceOPTICS エージェントで次のセンサがデフォルトで有効になります。これらのセンサを無効にすることはできません。有効にできるオプションのセンサの詳細については、「CylanceOPTICS のオプションのセンサ」を参照してください。

デフォルトのセンサとオプションのセンサの両方に関連付けられているイベント、アーチファクト、およびイベントタイプの詳細については、「脅威を識別するために CylanceOPTICS が使用するデータ構造」を参照してください。

センサ	プラットフォーム	説明	イベントタイプ
デバイス	macOS Linux	関連するデバイス情報を収集します	マウント
ファイル	Windows macOS Linux	ファイル操作に関する情報を収集します	• 作成 • 削除 • 上書き • 名前変更 • 書き込み
メモリ	macOS Linux	メモリ操作に関する情報を収集します	• Mmap • MProtect
ネットワーク	Windows macOS Linux	ネットワーク接続に関する情報を収集します	接続

センサ	プラットフォーム	説明	イベントタイプ
プロセス	Windows macOS Linux	プロセス操作に関する情報を収集します	サポートされるイベントタイプは、プラットフォームによって異なります。「脅威を識別するために CylanceOPTICS が使用するデータ構造」の「プロセス」セクションを参照してください。 • 異常終了 • 終了 • 強制終了 • PTrace • 開始 • 一時停止 • 不明なLinuxプロセスイベント
レジストリ	Windows	レジストリ操作に関する情報を収集します	• KeyCreated • KeyDeleting • ValueChanging • ValueDeleting

CylanceOPTICS のオプションのセンサ

次の CylanceOPTICS センサのいずれかを有効にすることにより、標準のプロセス、ファイル、ネットワーク、レジストリの各イベント以外の追加データを収集できます。オプションのセンサを有効にすると、デバイスのパフォーマンスとリソース使用率、および CylanceOPTICS データベースに保存されるデータ量に影響が及ぶ可能性があります。BlackBerry では、最初に少数のデバイスでオプションのセンサを有効にして影響を評価することをお勧めします。

オプションのセンサは、特に記載のない限り、64 ビットオペレーティングシステムでのみサポートされています。

センサ	説明	ベストプラクティス	注
高度なスクリプトの可視性	この CylanceOPTICS エージェントは、JScript、PowerShell（コンソールおよび統合スクリプト環境）、VBScript、および VBA マクロスクリプト実行からのコマンド、引数、スクリプト、およびコンテンツを記録します。 信号対雑音比：高 データの保持とパフォーマンスへの影響の可能性：低から中程度	推奨環境： • デスクトップ • ノートパソコン • サーバー Microsoft Exchange およびメールサーバーには推奨されません。	• Microsoft またはその他のサードパーティ製ソリューションが提供するツールの操作実行は、PowerShell に大きく依存している場合があります。 • データの保持期間を長くするため、BlackBerry では、PowerShell を頻繁に使用する信頼済みツールに対し、検出例外を設定することをお勧めします。
高度な WMI の可視性	この CylanceOPTICS エージェントは、追加の WMI 属性とパラメーターを記録します。 信号対雑音比：高 データの保持とパフォーマンスへの影響の可能性：低	推奨環境： • デスクトップ • ノートパソコン • サーバー	• 一部の Windows のバックグラウンドやメンテナンスのプロセスは、タスクのスケジューリングやコマンドの実行に WMI を使用します。その結果、WMI のアクティビティが短時間急増することがあります。 • BlackBerry は、このセンサを有効にする前に、お使いの環境での WMI 使用状況を分析することをお勧めします。
API センサ	CylanceOPTICS エージェントは、指定された一連の Windows API 呼び出しを監視します。 信号対雑音比：中程度 データ保持とパフォーマンスに影響する可能性：このセンサを有効にすると、デバイスの CPU パフォーマンスに影響を与える可能性があります	推奨環境： • デスクトップ • ノートパソコン • サーバー	• x86 または x64 Windows オペレーティングシステムでサポートされています。 • CylancePROTECT Desktop エージェントのバージョン 3.0.1003 以降が必要です。 • CylanceOPTICS エージェントのバージョン 3.2 以降が必要です。

センサ	説明	ベストプラクティス	注
COM オブジェクトの可視性	CylanceOPTICS エージェントは、COM インターフェイスと API コールを監視して、スケジュールされたタスクの作成などの悪意のある動作を検出します。 信号対雑音比：高 データ保持とパフォーマンスに影響する可能性：このセンサを有効にすると CPU パフォーマンスに影響を与える可能性があります	推奨環境： • デスクトップ • ノートパソコン サーバーには推奨されません。	• Windows のみ。 • CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。 • CylanceOPTICS エージェントのバージョン 3.3 以降が必要です。
クリプトジャッキング検出	この CylanceOPTICS エージェントは、Intel CPU のアクティビティをハードウェアレジスタの使用により処理し、クリプトマイニングやクリプトハッキングのアクティビティの可能性を検出します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	サポート対象： • Windows 10 x64 • Intel 第 6 世代から第 10 世代	メモ：BlackBerry では、このセンサの無効化を推奨しています。現在、デバイス OS でこのセンサに起因する安定性の問題を調査しているためです。 • 仮想マシンではサポートされていません。 • Intel 第 11 世代以降のプロセッサではサポートされていません。BlackBerry では、第 11 世代以降でこのセンサを有効にすることをお勧めしません。
DNS の可視性	この CylanceOPTICS エージェントは、DNS 要求と応答、およびドメイン名、解決済みアドレス、レコードタイプなどの関連データフィールドを記録します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：中程度	推奨環境： • デスクトップ • ノートパソコン DNS サーバーには推奨されません。	• このセンサは大量のデータを収集することもありますが、他のツールでは記録が困難なデータを可視化することもできます。 • データの保持期間を長くするため、BlackBerry では、クラウドベースのサービスを大量に利用する信頼済みツールに対し、検出例外を設定することをお勧めします。

センサ	説明	ベストプラクティス	注
強化されたファイル読み取りの可視性	CylanceOPTICS エージェントは、指定されたディレクトリセット内のファイル読み取りを監視します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	推奨環境： • デスクトップ • ノートパソコン • サーバー	• サードパーティ製のセキュリティツールの中には、このセンサがデータを収集する Windows API を使用するものがあります。場合によっては、この CylanceOPTICS が、無関係なデータや既に信頼済みのデータを記録することがあります。 • データの保持期間を長くし、信号対雑音比を向上させるため、BlackBerry では、信頼できるセキュリティツールに対し、検出例外を設定することをお勧めします。
ポータブル実行可能ファイル解析強化	この CylanceOPTICS エージェントは、ファイルバージョン、インポート機能、パッカータイプなど、移植可能な実行可能ファイルに関連付けられたデータフィールドを記録します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	推奨環境： • デスクトップ • ノートパソコン • サーバー	• このセンサによって収集されたデータは、拡張実行可能ファイル分析を支援するためにコンテキスト分析エンジンに渡され、CylanceOPTICS データベースには保存されません。 • このセンサを有効にしても、CylanceOPTICS のデータ保持にはほとんど影響しません。 • 文字列リソースを分析する検出ルールを追加して有効にすると、CylanceOPTICS エージェントが CPU とメモリのリソースを大量に消費する可能性があります。

センサ	説明	ベストプラクティス	注
強化されたプロセスとフッキングの可視性	この CylanceOPTICS エージェントは、Win32 API およびカーネル監査メッセージからのプロセス情報を記録して、プロセスフックと注入の形式を検出します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	推奨環境： • デスクトップ • ノートパソコン • サーバー	• サードパーティ製のセキュリティツールの中には、このセンサがデータを収集する Windows API を使用するものがあります。場合によっては、この CylanceOPTICS が、無関係なデータや既に信頼済みのデータを記録することがあります。 • データの保持期間を長くし、信号対雑音比を向上させるため、BlackBerry では、信頼できるセキュリティツールに対し、検出例外を設定することをお勧めします。
HTTP の可視性	CylanceOPTICS エージェントは、Windows のイベントトレース、WinINet API、WinHTTP API などの Windows HTTP トランザクションを追跡します。 信号対雑音比：高 データ保持とパフォーマンスに影響する可能性：このセンサを有効にすると CPU パフォーマンスに影響を与える可能性があります	推奨環境： • デスクトップ • ノートパソコン サーバーには推奨されません。	• Windows のみ。 • CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。 • CylanceOPTICS エージェントのバージョン 3.3 以降が必要です。
モジュールロードの可視性	CylanceOPTICS エージェントはモジュールのロードを監視します。 信号対雑音比：高 データ保持とパフォーマンスに影響する可能性：このセンサを有効にすると CPU パフォーマンスに影響を与える可能性があります	推奨環境： • デスクトップ • ノートパソコン • サーバー	• Windows のみ。 • CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。 • CylanceOPTICS エージェントのバージョン 3.3 以降が必要です。

センサ	説明	ベストプラクティス	注
プライベートネットワークアドレスの可視性	この CylanceOPTICS エージェントは、RFC 1918 および RFC 4193 アドレス空間内でのネットワーク接続を記録します。 信号対雑音比：低 データの保持とパフォーマンスへの影響の可能性：低	デスクトップに推奨。 非推奨環境： • DNSサーバー • リソースが不足しているシステム • RDP またはその他のリモートアクセスソフトウェアを使用するシステム	• このセンサは大量のデータを収集するため、データが CylanceOPTICS データベースに保存される時間に影響が及ぶ可能性があります。 • BlackBerry では、プライベートネットワークアドレス通信を完全に可視化する必要がある環境でのみ、このセンサを有効にすることをお勧めします。
Windows の高度な監査の可視性	この CylanceOPTICS エージェントは、Windows の追加のイベントタイプとカテゴリを監視します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	—	このセンサは、次のイベント ID の監視を有効にします。 • 4769 Kerberos チケットの要求 • 4662 Active Directory オブジェクトの操作 • 4624 ログオンに成功 • 4702 スケジュールされたタスクの作成
Windows イベントログの可視性	この CylanceOPTICS エージェントは、Windows のセキュリティイベントとその関連属性を記録します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：中程度	推奨環境： • デスクトップ • ノートパソコン • サーバー 非推奨環境： • ドメインコントローラ • Microsoft Exchange とメールサーバー	• このセンサが収集したデータ元の Windows イベントログは、通常のシステム使用中に頻繁に生成されます。 • 重複するデータを減らし、データの保持期間を長くするため、Windows イベントログからデータを収集するツールが組織に既に存在しているかどうかを確認してください。

脅威を識別するために **CylanceOPTICS** が使用するデータ構造

イベント、アーチファクト、ファセットは、デバイスで発生するアクティビティを分析、記録、調査するために CylanceOPTICS が使用する 3 つの主要なデータ構造です。InstaQuery、フォーカスデータ、Context Analysis Engine（CAE）などの CylanceOPTICS の機能が、これらのデータ構造を利用します。

このセクションでは、CylanceOPTICS がデバイス上のアクティビティを解釈して関与する仕組みについて詳しく説明します。これにより、検出データ、クエリデータ、フォーカスデータをさらに深く理解して活用できるようになります。

OS 別のデータソース

CylanceOPTICS エージェントは、次のデータソースを使用します。

OS	データソース
Windows	• CyOpticsDrv カーネルドライバ • イベントトラッキング • セキュリティ監査ログ
macOS	CyOpticsDrvOSX カーネルドライバ
Linux	ZeroMQ

CylanceOPTICS によってデフォルトで除外されるネットワークトラフィックのタイプについては、「KB65604」を参照してください。

イベント

イベントとは、デバイスに対して観察可能な変更またはアクションをもたらす構成要素のことです。イベントは、2 つの主要なアーチファクト（アクションを開始するインスティゲーティングアーチファクトと、操作を実行するターゲットアーチファクト）から構成されます。

次の表では、CylanceOPTICS による検出および操作が可能なイベントタイプの詳細を示します。

イベント：任意

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：プロセス、ユーザー
- プラットフォーム：Windows、macOS、Linux

イベントタイプ	説明
任意	すべてのイベントは、それらを生成したプロセスと、アクションに関連付けられたユーザーを記録します。

イベント：アプリケーション

- 有効にするデバイスポリシーオプション：高度な WMI の可視性
- アーチファクトタイプ：WMI トレース
- プラットフォーム：Windows

イベントタイプ	説明
フィルターを作成 - コンシューマバインディング	プロセスによって WMI の永続性が使用されました。
一時コンシューマを作成	プロセスによって WMI イベントがサブスクライブされました。
操作を実行	プロセスによって WMI 操作が実行されました。

- 有効にするデバイスポリシーオプション：強化されたプロセスとフッキングの可視性
- アーチファクトタイプ：ファイル
- プラットフォーム：Windows

イベントタイプ	説明
CBT	SetWindowsHookEx API によって、CBT アプリケーションに役立つ通知を受信するためのフックがインストールされました。
DebugProc	SetWindowsHookEx API によって、他のフックプロシージャをデバッグするためのフックがインストールされました。
非同期キー状態を取得	プロセスによって Win32 GetAsyncKeyState API が呼び出されました。
JournalPlayback	SetWindowsHookEx API によって、WH_JOURNALRECORD フックプロシージャが前に記録したメッセージを監視するフックがインストールされました。
JournalRecord	SetWindowsHookEx API によって、システムメッセージキューに入れられた入力メッセージを監視するフックがインストールされました。
キーボード	SetWindowsHookEx API によって、キーストロークメッセージを監視するフックがインストールされました。
低レベルキーボード	SetWindowsHookEx API によって、低レベルのキーボード入力イベントを監視するフックがインストールされました。
低レベルマウス	SetWindowsHookEx API によって、低レベルのマウス入力イベントを監視するフックがインストールされました。
メッセージ	SetWindowsHookEx API によって、メッセージキューに入れられたメッセージを監視するフックがインストールされました。
マウス	SetWindowsHookEx API によって、マウスメッセージを監視するフックがインストールされました。
Raw Inputデバイスを登録	プロセスによって、Win32 RegisterRawInputDevices API が呼び出されました。

イベントタイプ	説明
Windows イベントフックを設定	プロセスによって、Win32 SetWinEventHook API が呼び出されました。
Windows フックを設定	SetWindowsHookEx API によって、リストにないフックタイプ値がインストールされました。
ShellProc	SetWindowsHookEx API によって、シェルアプリケーションに役立つ通知を受信するためのフックがインストールされました。
SysMsg	SetWindowsHookEx API によって、ダイアログボックス、メッセージボックス、またはスクロールバーでの入力イベントの結果として生成されるメッセージを監視するフックがインストールされました。
WindowProc	SetWindowsHookEx API によって、Windows プロシージャメッセージを監視するフックがインストールされました。

- 有効にするデバイスポリシーオプション：API センサ
- アーチファクトタイプ：API 呼び出し
- プラットフォーム：Windows

イベントタイプ	説明
関数	重要な関数呼び出しが実行されました。

- 有効にするデバイスポリシーオプション：モジュールロードの可視性
- アーチファクトタイプ：ファイル
- プラットフォーム：Windows

イベントタイプ	説明
ロード	アプリケーションがモジュールをロードしました。

- 有効にするデバイスポリシーオプション：COM オブジェクトの可視性
- プラットフォーム：Windows

イベントタイプ	説明
作成済み	COM オブジェクトが作成されました。

イベント：デバイス

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：ファイル
- プラットフォーム：macOS、Linux

イベントタイプ	説明
マウント	デバイスがマシンに接続されているか、フォルダが特定のネットワークロケーションにマウントされています。

イベント：ファイル

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：ファイル
- プラットフォーム：Windows、macOS、Linux

イベントタイプ	説明
作成	ファイルが作成されました。
削除	ファイルが削除されました。
上書き	ファイルが上書きされました。
名前変更	ファイルの名前が変更されました。
書き込み	ファイルが変更されました。

- 有効にするデバイスポリシーオプション：強化されたファイル読み取りの可視性
- アーチファクトタイプ：ファイル
- プラットフォーム：Windows

イベントタイプ	説明
オープン	ファイルが開かれました。

イベント：メモリ

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：プロセス
- プラットフォーム：macOS、Linux

イベントタイプ	説明
Mmap	一定のメモリ領域が、特定の目的（通常はプロセスに割り当てられます）に対応付けられました。
MProtect	メモリ領域のメタデータが変更されました。通常はステータスが変更（実行可能になるなど）されます。

イベント：ネットワーク

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：ネットワーク

- プラットフォーム：Windows、macOS、Linux

イベントタイプ	説明
接続	ネットワーク接続が確立されました。デフォルトでは、ローカルトラフィックは収集されません。

- 有効にするデバイスポリシーオプション：プライベートネットワークアドレスの可視性
- アーチファクトタイプ：ネットワーク
- プラットフォーム：Windows

イベントタイプ	説明
接続	接続イベントにはローカルトラフィックが含まれます。

- 有効にするデバイスポリシーオプション：DNS の可視性
- アーチファクトタイプ：DNS 要求
- プラットフォーム：Windows、Linux

イベントタイプ	説明
要求	プロセスによって、キャッシュ保存されなかったネットワーク DNS 要求が作成されました。
応答	プロセスによって、DNS 応答が受信されました。

- 有効にするデバイスポリシーオプション：HTTP の可視性
- アーチファクトタイプ：HTTP
- プラットフォーム：Windows

イベントタイプ	説明
ゲット	Windows が WinINet または WinHTTP を使用して HTTP 要求を行いました。
投稿	Windows が WinINet または WinHTTP を使用してデータを送信しました。

イベント：プロセス

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：プロセス

イベントタイプ	プラットフォーム	説明
異常終了	macOS Linux	事前選択センサによって、プロセスが完了せずに終了した（例外によるプロセスの終了など）ことが検知されました。

イベントタイプ	プラットフォーム	説明
終了	Windows macOS Linux	プロセスが終了しました。
強制終了	macOS Linux	事前選択センサによって、プロセスが別のプロセスによって強制終了されたことが検知されました。
PTrace	macOS Linux	あるプロセスが別のプロセスを監視および制御できるようにする Unix のシステムツールです。
開始	Windows macOS Linux	プロセスが開始されました。
一時停止	Linux	事前選択センサによって、プロセスが中断されたことが検知されました。
不明な Linux プロセスイベント	macOS Linux	事前選択センサによって、対象としてプロセスで不明なイベントが発生したことが検知されました。これは、悪意のあるソフトウェアがその活動を隠している兆候である可能性があります。

- 有効にするデバイスポリシーオプション：強化されたプロセスとフッキングの可視性
- アーチファクトタイプ：プロセス
- プラットフォーム：Windows

イベントタイプ	説明
SetThreadContext	プロセスによって、SetThreadContext API が呼び出されました。
停止	扇動プロセスによって、別の対象プロセスが終了させられました。

イベント：レジストリ

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：レジストリ、ファイル（レジストリキーが特定のファイルを参照している場合）
- プラットフォーム：Windows

イベントタイプ	説明
KeyCreated	レジストリキーが作成されました。
KeyDeleting	レジストリキーが削除されました。
ValueChanging	レジストリキーの値が変更されました。

イベントタイプ	説明
ValueDeleting	レジストリキー値が削除されました。

イベント：スクリプティング

- 有効にするデバイスポリシーオプション：高度なスクリプトの可視性
- アーチファクトタイプ：Powershell トレース
- プラットフォーム：Windows

イベントタイプ	説明
コマンドを実行	Windows PowerShell がコマンドを実行しました。パラメーターは不明です。
スクリプトを実行	Windows PowerShell がスクリプトを実行しました。
ScriptBlock を実行	Windows PowerShell によってスクリプトブロックが実行されました。
コマンドを呼び出す	Windows PowerShell によって、バインドされたパラメーターを持つコマンドが呼び出されました。
スクリプトを禁止	AMSI ScanBuffer の結果は、スクリプトが管理者によって検出またはブロックされたことを示しています。

イベント：ユーザー

- 有効にするデバイスポリシーオプション：高度なスクリプトの可視性
- アーチファクトタイプ：Windows イベント
- プラットフォーム：Windows

イベントタイプ	説明
バッチログオフ	次の Windows イベント ID が発生しました：4634（タイプ 4）
バッチログオン	次の Windows イベント ID が発生しました：4624（タイプ 4）
キャッシュされた対話型ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 11）
キャッシュされた対話型ログオン	次の Windows イベント ID が発生しました：4624（タイプ 11）
対話型ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 2）
対話型ログオン	次の Windows イベント ID が発生しました：4624（タイプ 2）
ネットワークログオフ	次の Windows イベント ID が発生しました：4634（タイプ 3）

イベントタイプ	説明
ネットワークログオン	次の Windows イベント ID が発生しました：4624（タイプ 3）
NetworkClearText ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 8）
NetworkClearText ログオン	次の Windows イベント ID が発生しました：4624（タイプ 8）
NewCredentials ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 9）
NewCredentials ログオン	次の Windows イベント ID が発生しました：4624（タイプ 9）
リモート対話型ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 10）
リモート対話型ログオン	次の Windows イベント ID が発生しました：4624（タイプ 10）
サービスログオフ	次の Windows イベント ID が発生しました：4634（タイプ 5）
サービスログオン	次の Windows イベント ID が発生しました：4624（タイプ 5）
ロック解除ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 7）
ロック解除ログオン	次の Windows イベント ID が発生しました：4624（タイプ 7）
ユーザーログオフ	次の Windows イベント ID が発生しました：4634（リストにないタイプ値）
ユーザーログオン	次の Windows イベント ID が発生しました：4624（リストにないタイプ値）

アーチファクトとファセット

アーチファクトは、CylanceOPTICS が使用できる複合的な情報です。コンテキスト分析エンジン（CAE）は、デバイス上のアーチファクトを識別し、それらを使用してインシデントへの自動応答と修正アクションをトリガーできます。InstaQuery では、クエリの基礎としてアーチファクトが使用されます。

ファセットは、イベントに関連付けられたアーチファクトの特徴を識別するために使用できるアーチファクトの属性です。ファセットは、潜在的に悪意のあるアクティビティを特定するために、分析時に関連付けて組み合わせられます。たとえば、「explorer.exe」という名前のファイルは、本来疑わしいものではないかもしれませんが、ファイルが Microsoft によって署名されておらず、一時ディレクトリにある場合、環境によっては疑わしいものに区別されることがあります。

CylanceOPTICS では、次のアーチファクトとファセットが使用されます。

アーチファクト	ファセット
API呼び出し	• 関数 • DLL • パラメーター
DNS	• 接続 • IsRecursionDesired • IsUnsolicitedResponse • Opcode • RequestId • レゾリューション • ResponseOriginatedFromThisDevice • クエスチョン
イベント	• 発生時間 • 登録時間
ファイル	• 実行可能ファイルレコード（バイナリのみ） • ファイル作成時間（OS による報告） • ファイルパス • ファイルの署名（バイナリのみ） • ファイルサイズ • 最終変更時間（OS による報告） • MD5 ハッシュ（バイナリのみ） • 最近の書き込み位置 • SHA256 ハッシュ（バイナリのみ） • 疑わしいファイルタイプ • ユーザー
ネットワーク	• ローカルアドレス • ローカルポート • プロトコル • リモートアドレス • リモートポート
PowerShell トレース	• EventId • ペイロード • PayloadAnalysis • ScriptBlockText • ScriptBlockTextAnalysis

アーチファクト	ファセット
プロセス	• コマンドライン • 実行可能ファイルの実行元 • 親プロセス • プロセスID • 開始時刻 • ユーザー
レジストリ	• 値がシステム上のファイルを参照しているかどうか • レジストリパス • 値
ユーザー	• ドメイン • OS 固有の ID（SID など） • ユーザー名 ユーザーアーチファクトには、以下のいずれかの値を含めることができますが、ほとんどのデバイスではデータを使用できません。 • AccountType • BadPasswordCount • Comment • CountryCode • FullName • HasPasswordExpired • HomeDirectory • IsAccountDisabled • IsLocalAccount • IsLockedOut • IsPasswordRequired • LanguageCodePage • LogonServer • PasswordAge • PasswordDoesNotExpire • ProfilePath • ScriptPath • UserPrivilege • Workstations

アーチファクト	ファセット
Windows イベント	• クラス • イベントID • ObjectServer • PrivilegeList • プロセスID • プロセス名 • プロバイダ名 • サービス • SubjectDomainName • SubjectLogonId • SubjectUserName • SubjectUserSid
WMI トレース	• ConsumerText • ConsumerTextAnalysis • EventId • Namespace • Operation • OperationAnalysis • OriginatingMachineName

レジストリキーと値

CylanceOPTICS は、一般的な永続性、プロセスの起動、権限の昇格キーと値、および「KB 66266」に示されている値を監視します。

CylanceOPTICS がレジストリ内の永続化ポイントを監視する方法の詳細については、「KB 66357」を参照してください。

CylanceGATEWAY のセットアップ

メモ：CylanceGATEWAY がテナントで有効になっていない場合、それを設定するメニューオプションは管理コンソールに表示されません。十分な権限を持たないユーザーが管理コンソールにログインした場合、メニューオプションを選択したときに権限がないことを示すエラーメッセージが表示されます。エラーメッセージの詳細については、support.blackberry.com/community にアクセスして、記事 98223 を参照してください。

IPv6 アドレスの DNS 解決はサポートされていません。IPv6 アドレスは CylanceGATEWAY エージェントに返されません。

手順	アクション
1	BlackBerry Connectivity Node と、少なくとも 1 つの CylanceGATEWAY Connector をインストールしセットアップします。
2	プライベートネットワークの一部であるアドレスを指定します。
3	プライベート DNS の設定とサフィックスを指定します。
4	既存の CylanceGATEWAY ネットワークサービスをレビューしたり、独自でサービスを定義したりして、テナントにアクセス制御リスト（ACL）ルールを作成しやすくします（オプション）。
5	テナントで ACL ルールを設定して、CylanceGATEWAY がアクセスを許可およびブロックするインターネットやプライベートネットワークの宛先を管理します。
6	ネットワーク保護の構成 CylanceGATEWAY が検出する脅威と応答方法を指定する方法。
7	CylanceGATEWAY のユーザーを追加します。
8	Gateway サービスオプションの設定 OS 固有のオプションを指定する方法。
9	登録ポリシーを設定して、ユーザーがデバイス上で CylancePROTECT Mobile アプリや CylanceGATEWAY エージェントをアクティブ化できるようにします。
10	管理者、ユーザー、およびグループへのポリシーの割り当て。ユーザーが CylanceGATEWAY エージェントをアクティベートする前に、登録ポリシーと Gateway サービスポリシーを割り当てる必要があります。

手順	アクション
11	デバイスユーザーは、CylancePROTECT Mobile アプリを iOS、Android、Chromebook デバイスに、さらに CylanceGATEWAY エージェントを Windows および macOS デバイスにインストールしてアクティベートします。必要に応じて、CylanceGATEWAY エージェントのサイレントインストールまたはアップグレードを実行できます。 エージェントは、BlackBerry Web サイトからダウンロードできます。CylancePROTECT Mobile アプリと CylanceGATEWAY エージェントの詳細については、『Cylance Endpoint Security ユーザーガイド』を参照してください。 必要に応じて、Cylance Endpoint Security を BlackBerry UEM または Microsoft Intune と統合して、iOS および Android デバイスが UEM または Intune で管理されているかどうかを、CylanceGATEWAY を使用する前に確認することができます。詳細については、「Cylance Endpoint Security を MDM ソリューションに接続して、デバイスが管理されているかどうかを確認」を参照してください。
12	自分の IP アドレスを使用する（BYOIP） を使用して、ソース IP ピンに組織独自の IP アドレスを使用したり、複数の非連続 IP アドレスではなく、単一の IP アドレス範囲や CIDR アドレスを許可したりするなど、大規模な専用 IP アドレスでトラフィックを制御します。（オプション）

プライベートネットワークの定義

CylanceGATEWAY を使用してプライベートネットワークへのアクセスを制御するには、プライベートネットワークを定義する必要があります。プライベートネットワークを定義する場合、ユーザーによるネットワークリソースへのアクセス時に最も制限的な権限とマイクロセグメンテーションを適用するように CylanceGATEWAY を構成できます。CylanceGATEWAY オンプレミス環境とクラウド環境の両方で、複数のプライベートネットワーク（セグメント、データセンター、VPC など）へのアクセスをサポートします。接続を許可するアクセス制御リスト（ACL）ルールがユーザーに割り当てられていない限り、CylanceGATEWAY はプライベートネットワーク内の任意のロケーションへのユーザーの接続をブロックします。

プライベートネットワークごとにコネクタグループを追加して、プライベートネットワークを定義し、ユーザーがリソースにアクセスできるようにします。2023年7月以前に CylanceGATEWAY サービスを有効にして、CylanceGATEWAY Connectors が 1 つ以上含まれている場合、既存のすべてのコネクタは「デフォルトコネクタグループ」に移動しています。このデフォルトコネクタグループの名前を変更することも、必要に応じてグループを追加しコネクタを割り当てることもできます。

各テナントは、最大 8 つのコネクタグループをサポートします。

コネクタグループは、次の要素で構成されます。

- IP アドレス、IP アドレス範囲、および CIDR 表記。グループごとに指定します。CylanceGATEWAY Connectors は、これらのアドレスをプライベートネットワークの 1 つの一部として認識します。
- ヘルスチェック URL。これはグループに固有であり、グループ内の各 CylanceGATEWAY Connector がプライベートネットワークへの接続を確認するために使用します。
- IP 制限。Gateway が、指定した IP アドレスのコネクタからのみ接続を受け入れるように指定できます。

ユーザーのデバイスとプライベートネットワークの間で安全なトンネルを確立するには、1 つまたは複数の CylanceGATEWAY Connectors をインストールし、グループに割り当てる必要があります。

各コネクタグループは、最大 8 つの CylanceGATEWAY Connectors をサポートします。

プライベート DNS サーバーのアドレスと、検索に使用するプライベート DNS サフィックスを指定することもできます。DNS 設定は、環境内のすべてのグループのコネクタに適用されます。これは、1 つのグループに追加する必要があります。

類似した宛先 IP アドレスまたはアドレス範囲を持つ複数のグループが含まれる環境では、データフローは、IP アドレスがコネクタグループに一致するまで、リストされているコネクタグループに順番に送られます。その後、一致する IP アドレスを含むコネクタグループを使用して、リソースにアクセスする宛先に接続をルーティングします。

CylanceGATEWAY Connector のセットアップ

CylanceGATEWAY Connector は、CylanceGATEWAY を使用してユーザーのデバイスとプライベートネットワーク間のセキュリティ保護されたトンネルを確立する場合にインストールする必要がある仮想アプライアンスです。CylanceGATEWAY Connector の展開と登録は、プライベートネットワークの指定時に定義したアドレスへのフルアクセスが可能なネットワーク部に対して行う必要があります。CylanceGATEWAY Connector をインストールしない場合は、CylanceGATEWAY を使用して、パブリックインターネットの宛先へのアクセスをブロックし、ソース IP ピン設定を使用してクラウドアプリケーションへの安全なアクセスを確保することだけが可能です。

複数の CylanceGATEWAY Connector をインストールすることをお勧めします。複数のインスタンスをインストールすると、ロードバランシングを行ったり、プライベートネットワークの定義内の個別のセグメントやプライベートクラウドにアクセスしたりできます。ネットワークに CylanceGATEWAY Connector の複数のインスタンスをインストールして構成している場合、同じコネクタグループに割り当てられているすべての正常な CylanceGATEWAY Connector 間でクライアント接続が均等に分散され、1 つのインスタンスが使用不可能になった場合や問題のトラブルシューティングを行う場合の冗長性が確保されます。

各テナントは、最大 8 つのコネクタグループをサポートします。

各コネクタグループは、最大 8 つの CylanceGATEWAY Connectors をサポートします。

BlackBerry では、それぞれのコネクタグループでヘルスチェック URL を指定し、各 CylanceGATEWAY Connector のステータスを定期的に監視することをお勧めします。ヘルスチェック URL を指定しなかった場合、CylanceGATEWAY は、プライベートネットワークへの接続があるかどうかを確認できず、コネクタのヘルスチェックステータス列（［プライベートネットワーク］ > ［Gateway Connector］）には DNS および HTTP 情報が表示されなくなります。詳細については、「CylanceGATEWAY コネクタの管理」を参照してください。

CylanceGATEWAY を別のパッケージを必要とする環境にインストールする場合は、BlackBerry の営業担当者までお問い合わせください。

CylanceGATEWAY Connector をセットアップするには、次の操作を実行します。

手順	アクション
1	「要件：CylanceGATEWAY コネクタ」を確認します。

手順	アクション
2	CylanceGATEWAY Connector を自分の環境にインストールします。CylanceGATEWAY Connector は、次の環境でサポートされています。個々の環境への CylanceGATEWAY Connector のインストール方法のチュートリアルについては、「環境に応じた CylanceGATEWAY Connector ワークフローのインストール」を参照してください。 • vSphere 環境 • ESXi 環境 • Microsoft Entra ID 環境 • Hyper-V 環境 • AWS 環境
3	VM 環境での CylanceGATEWAY Connector の設定 （オプション）。
4	OpenSSH を使用して CylanceGATEWAY Connector にアクセスする （オプション）。
5	CylanceGATEWAY Connector 用ファイアウォールの設定。
6	BlackBerry Infrastructure への CylanceGATEWAY Connector の登録。
7	CylanceGATEWAY Connector の設定 （オプション）。
8	CylanceGATEWAY Connectors の管理 を行い、オプションの設定とコネクタステータスの確認をします。

CylanceGATEWAY コネクタの vSphere 環境へのインストール

静的 IP を使用して CylanceGATEWAY Connector を設定できます。インストール後に CylanceGATEWAY Connector ネットワーク設定を変更する場合は、VM の vApp オプションを編集し、CylanceGATEWAY Connector を再起動して変更を有効にすることができます。OVF の詳細を編集する方法については、VMware のマニュアルを参照して、「仮想マシンの OVF 詳細の編集」を参照してください。

作業を始める前に： 自分に OVF テンプレートを vSphere 環境に展開する権限があることを確認します。

1. CylanceGATEWAY Connector の OVA ファイル（cylance-gateway-connector-*version*.ova）を *my*Account からダウンロードします。
2. vSphere 環境にログインします。
3. CylanceGATEWAY Connector のインストール先であるクラスタを右クリックし、［**OVF** テンプレートのデプロイ］を選択します。
4. ［**OVF** テンプレートの選択］画面で、［ローカルファイル］をクリックします。
5. ［ファイルをアップロード］をクリックして、cylance-gateway-connector.ova ファイルに移動します。
6. ［次へ］をクリックします。

7. ［名前とフォルダの選択］画面で、仮想マシンの名前を入力し、［次へ］をクリックします。
   デフォルト名は cylance-gateway-connector です。
8. ［コンピューターリソースの選択］画面で、仮想マシンの場所を選択し、［次へ］をクリックします。
9. 互換性チェックが完了したら、［次へ］をクリックします。
10. ［詳細の確認］画面で、セットアップ情報を確認し、［次へ］をクリックします。
11. ［ストレージの選択］画面の［仮想ディスクフォーマット］で、［シンプロビジョニング］を選択し、［次へ］をクリックします。
12. ［ネットワークの選択］画面で、この CylanceGATEWAY Connector の［ターゲットネットワーク］を設定します。
    ［ソースネットワーク］を NAT に設定します。
13. ［次へ］をクリックします。
14. **[**テンプレートをカスタマイズ］画面で、追加の仮想マシンプロパティを指定します（オプション）。

    メモ：IP アドレスは、ドット 10 進表記の IPv4 アドレスとして入力する必要があります。

    - デフォルトでは、［**DHCP** を使用する］オプションが有効になっており、コネクタは自動的に割り当てられた IP アドレスを使用します。コネクタを静的 IP アドレスで設定する場合は、［DHCP を使用する］チェックボックスをオフにして、次の設定の IP アドレスを指定する必要があります。
    - ［**IP** アドレス/プレフィックス長］フィールドに、デバイスに割り当てることができる IP アドレスとプレフィックス（例：192.0.2.100/24）を入力します。複数の IP アドレスを追加する場合は、各 IP アドレスとプレフィックスをカンマ（,）で区切ります。
    - ［ゲートウェイ］フィールドに、ネットワークゲートウェイの IP アドレス（例：192.0.2.1）を入力します。
    - ［**DNS**］フィールドで、使用する DNS サーバーの IP アドレス（例：192.0.2.120）を指定します。複数の DNS サーバーを追加する場合は、アドレスをカンマ（,）で区切ります。
15. ［最終確認］画面で、設定を確認して［完了］をクリックします。

終了したら： コネクタをインストールしたら、OVA ファイルが仮想環境に正しくインストールされていることを確認できます。手順については、「VM 環境での CylanceGATEWAY Connector の設定」を参照してください。

ESXi 環境への CylanceGATEWAY Connector のインストール

CylanceGATEWAY Connector のネットワークインターフェイスは、DHCP を使用するように設定、または CylanceGATEWAY Connector をインストールした場合にのみ静的 IP を設定できます。設定を変更する場合は、CylanceGATEWAY Connector をアンインストールしてから、新しいネットワークインターフェイス設定でインストールする必要があります。

作業を始める前に： OVF テンプレートを ESXi 環境に展開する権限があることを確認します。

1. CylanceGATEWAY Connector の OVA ファイル（cylance-gateway-connector-*version*.ova）を *my*Account からダウンロードします。
2. ESXi 環境にログインします。
3. ［ナビゲーター］パネルで、［仮想マシン］を選択します。
4. ［仮想マシンの作成/登録］ボタンをクリックします。
5. ［新規仮想マシン］画面で、［**OVF** ファイルまたは **OVA** ファイルから仮想マシンをデプロイ］を選択し、［次へ］をクリックします。
6. 仮想マシンの名前を入力します。

7. cylance-gateway-connector-*version*.ova ファイルに移動します。ダイアログボックスにファイルをドラッグアンドドロップします。
8. ［次へ］をクリックします。
9. ［ストレージの選択］画面で、［標準］とデータストアを選択し［次へ］をクリックします。
10. ［デプロイのオプション］画面の［ディスクプロビジョニング］で、［シン］を選択します。
11. ［追加設定］画面で、［オプション］を展開して、追加の VMware プロパティを指定します（オプション）。

    メモ：IP アドレスは、ドット 10 進表記の IPv4 アドレスとして入力する必要があります。

    - デフォルトでは、［**DHCP** を使用する］が有効になっており、コネクタは自動的に割り当てられた IP アドレスを使用します。コネクタを静的 IP アドレスで設定する場合は、［DHCP を使用する］チェックボックスをオフにして、次の設定の IP アドレスを指定する必要があります。
    - ［**IP** アドレス/プレフィックス長］フィールドで、デバイスに割り当てることができる IP アドレスとプレフィックス（例：192.0.2.100/24）を指定します。複数の IP アドレスを使用するには、IP アドレスをカンマ（,）で区切ります。
    - ［ゲートウェイ］フィールドに、ネットワークゲートウェイのアドレス（例：192.0.2.1）を入力します。
    - ［**DNS**］フィールドで、使用する DNS サーバーの IP アドレス（例：192.0.2.120）を指定します。複数の DNS サーバーを使用するには、アドレスをカンマ（,）で区切ります。
12. ［次へ］をクリックします。
13. ［最終確認］画面で、設定を確認して［完了］をクリックします。

終了したら： コネクタをインストールしたら、OVA ファイルが仮想環境に正しくインストールされていることを確認できます。手順については、「VM 環境での CylanceGATEWAY Connector の設定」を参照してください。

CylanceGATEWAY Connector を Microsoft Entra ID 環境にインストールするための前提条件

- Entra プライベートネットワークで DNS が有効になっていて、コネクタ VM からアクセスできることを確認します。
- オプションで、プライベートネットワーク環境に HTTP および HTTPS の送信トラフィック用のプロキシサーバーがあることを確認します。
- CylanceGATEWAY で使用できるようにするサービスが、プライベートネットワークの CylanceGATEWAY Connector からアクセスできることを確認します。
- VHD テンプレートを Entra 環境に展開できることを確認します。

CylanceGATEWAY Connector を Microsoft Entra ID 環境にインストールする

コネクタをインストールすると、VHD ファイルが BLOB として Microsoft Entra ID ポータルにアップロードされます。BLOB を使用して、コネクタ VM で使用されるイメージを作成します。Entra 環境の設定については、Azure ポータルのドキュメント - Azure ポータル | Microsoft ドキュメントを参照してください。

作業を始める前に：「CylanceGATEWAY Connector を Microsoft Entra ID 環境にインストールするための前提条件」を確認します。

1. *my*Account から CylanceGATEWAY Connector の VHD ファイル（cylance-gateway-connector-fixed-<*version*>.vhd）をダウンロードします。
2. Microsoft Entra ID 管理ポータル（https://portal.azure.com）にログインします。
3. VHD ファイルを BLOB としてアップロードします。

a) ［**Azure** サービス］セクションで［ストレージアカウント］をクリックします。ストレージアカウントがない場合は、アカウントを作成します。
b) ストレージアカウントをクリックします。
c) 左側の列の［データストレージ］セクションで、［コンテナー］をクリックします。コンテナがない場合は、コンテナを作成します。
d) コンテナをクリックします。
e) ［アップロード］をクリックします。
f) ［**BLOB** のアップロード］画面で、ダウンロードした cylance-gateway-connector-fixed-<*version*>.vhd ファイルに移動します。
g) ［詳細設定］を展開し、［**BLOB** の種類］ドロップダウンリストを［ページ **BLOB**］に設定します。
h) ［アップロード］をクリックします。

4. アップロードされた BLOB からイメージを作成します。
a) 管理ポータルの左側の列で、ポータルメニューの［すべてのサービス］をクリックします。
b) ［サービスフィルター］フィールドに、「images」と入力します。
c) ［イメージ］をクリックし、リソースの種類として［**Microsoft.Compute/images**］が使用されていることを確認します。
d) ［作成］をクリックします。
e) ご利用の環境に必要なフィールドについて入力します。［**OS** ディスク］セクションで、次の設定を指定します。

- OS の種類：Linux
- VM の世代：第 1 世代
- ストレージ BLOB：手順 3 で作成した BLOB に移動します。

f) ［タグ］タブをクリックし、必要なタグを追加します（オプション）。
g) ［レビューと作成］をクリックします。
h) ［作成］をクリックします。
i) ［リソースに移動］をクリックします。［仮想マシンの作成］画面が開かれます。

5. コネクタ VM を作成します。
a) ［基本］タブで、ご利用の環境に必要なフィールドについて入力します。次の設定を指定します。

- イメージ：手順 4 で作成したイメージを選択します。
- サイズ：2 つの vCPU と少なくとも 4.5GB のメモリを含むサイズを選択します。
- 認証の種類：［パスワード］を選択します。
- ユーザー名：任意の値を入力します。コネクタ VM イメージではこのフィールドは無視されます。
- パスワードとパスワードの確認：任意の値を入力します。コネクタ VM イメージではこれらのフィールドは無視されます。

b) ［ディスク］タブをクリックします。
c) ［ディスク］ページの［**OS** ディスクの種類］ドロップダウンリストで、［**Standard HDD**］を選択します。コネクタ VM には、低遅延のディスクアクセスは必要ありません。
d) ［ネットワーク］タブをクリックします。ご利用の環境に必要なフィールドについて入力します。コネクタイメージがプライベートネットワークを使用していることを確認します。コネクタは、Entra の高速ネットワーク機能をサポートしていません。この設定を有効にすると、コネクタ VM が想定どおりに機能しない場合があります。
e) ［管理］タブをクリックします。このイメージは「Azure AD でのログイン」をサポートしていません。この設定を有効にすると、コネクタ VM が想定どおりに機能しない場合があります。

f) ［詳細設定］タブをクリックします。ご利用の環境に応じて設定します。コネクタは、「カスタムデータ」または「ユーザーデータ」の設定をサポートしていません。「カスタムデータ」または「ユーザーデータ」の設定は、環境で必要な場合は設定できますが、コネクタ VM では無視されます。BlackBerry では、コネクタ VM を実行している VM に追加の VM アプリケーションをインストールすることはお勧めしません。
g) ［タグ］タブをクリックします。ご利用の環境に応じてタグを設定します。
h) ［レビューと作成］タブをクリックします。設定を確認します。
i) ［作成］をクリックします。

メモ：VM リソースが作成される際に、タイムアウトエラーメッセージが表示されることがあります。必要な場合は画面を更新します。

CylanceGATEWAY Connector を Hyper-V 環境にインストールする

作業を始める前に： VHD ファイルを展開し、コネクタイメージを作成する権限があることを確認します。

1. CylanceGATEWAY Connector の VHD ファイル（cylance-gateway-connector-dynamic<バージョン>.vhd）を *my*Account からダウンロードします。
2. Hyper-V マネージャーを管理者として実行します。
3. Hyper-V マネージャーのメニューで、［アクション］ > ［新規］ > ［仮想マシン］の順にクリックします。［次へ］をクリックします。
4. ［名前と場所の指定］画面で、VM の名前を指定します。［次へ］をクリックします。
5. ［世代の指定］画面で、［第 **1** 世代］を選択します。［次へ］をクリックします。
6. ［メモリの割り当て］画面で、［次へ］をクリックします。
7. ［ネットワークの構成］画面で、適切な接続を選択します。［次へ］をクリックします。
8. ［仮想ハードディスクの接続］画面で、［既存の仮想ハードディスクを使用する］を選択します。
9. 手順 1 でダウンロードした cylance-gateway-connector-dynamics-<バージョン>.vhd ファイルに移動します。
10. ［メモリの割り当て］画面で、コネクタに 5 GB 以上のメモリがあることを確認します。［次へ］をクリックします。
11. ［仮想マシンの新規作成ウィザードの完了］画面で設定を確認し、［完了］をクリックします。
12. コネクタを開始します。

終了したら： コネクタをインストールした後で、VHD ファイルが仮想環境に正しくインストールされていることを確認できます。手順については、「VM 環境での CylanceGATEWAY Connector の設定」を参照してください。

AWS 環境への CylanceGATEWAY Connector のインストール

CylanceGATEWAY Connector をインストールするには、AWS マーケットプレイスで AMI を使用します。

1. https://aws.amazon.com/console から AWS 管理コンソールにサインインします。
2. CylanceGATEWAY Connector インスタンスを作成するには、次の操作を実行します。
   a. **EC2** サービスを開きます。
   b. 左側の列のインスタンスにある［インスタンス］をクリックします。
   c. ［インスタンスの起動］をクリックします。
   d. ［インスタンスの起動］画面で、CylanceGATEWAY Connector インスタンスの名前を入力します。
   e. ［**Amazon Machine Image**（**AMI**）］セクションで［その他の **AMI** を参照］をクリックします。

f. ［**Amazon Machine Image**（**AMI**）を選択］画面で、［**AWS** マーケットプレイス **AMI**］タブをクリックします。
g. ［選択した **AMI**］検索フィールドに「CylanceGATEWAY」と入力します。**Enter** キーを押します。
h. 組織の要件に応じてインスタンスタイプを選択します。

メモ：BlackBerry では、実稼働環境で c6in または c5n のインスタンスタイプの選択をお勧めします。

i. OpenSSH を介してコネクタインスタンスに安全に接続するキーペアを選択します。
j. ［ネットワーク設定］セクションで［編集］をクリックして、次の設定を指定します。
   1. ［**VPC**］のドロップダウンをクリックして、プライベートネットワークを選択します。
   2. 必要に応じて、［自動割り当てパブリック **IP**］をクリックして、［有効］を選択します。インストールされているプライベートネットワークを使用してコネクタのウェブインタフェースにアクセスできない場合、パブリック IP アドレスを CylanceGATEWAY Connectorのみに割り当てる必要があります。
   3. 組織の要件に応じてセキュリティグループを選択または作成します。セキュリティグループには、登録が行われたネットワークから CylanceGATEWAY Connector への SSH（ポート 22）、HTTP（ポート 80）および HTTPS（ポート 443）アクセス権が必要です。
k. ［インスタンスを起動］をクリックします。

終了したら： BlackBerry Infrastructure への CylanceGATEWAY Connector の登録

VM 環境での **CylanceGATEWAY Connector** の設定

メモ： AWS CylanceGATEWAY Connector AMI は EC2 シリアルコンソールへのアクセスをサポートしていません。AWS 環境にコネクタをインストールしている場合は、このタスクを実行しないでください。CylanceGATEWAY Connector セットアップを続行するには、「CylanceGATEWAY Connector 用ファイアウォールの設定」を参照してください。

CylanceGATEWAY Connector は、ユーザーがログインしなくても動作する Ubuntu オペレーティングシステムの最小インストールです。デフォルト設定を更新する場合や、OVA または VHD が正しく展開されていることを確認する場合にのみ、ログインする必要があります。

1. 以下のいずれかの方法で、環境のコンソールを開きます。

環境	手順
vSphere	a. ご利用の環境にログインします。 b. CylanceGATEWAY Connector のホスト名をクリックします。 c. ［リモートの起動］または［**Web** コンソールの起動］をクリックします。
ESXi	a. ご利用の環境にログインします。 b. CylanceGATEWAY Connector のホスト名をクリックします。 c. ［コンソール］をクリックします。
Microsoft Entra ID	a. Microsoft Entra ID 管理ポータル（https:// portal.azure.com）にサインインします。 b. ［仮想マシン］をクリックします。 c. 左側の列の［サポート + トラブルシューティング］セクションで、［シリアルコンソール］をクリックします。

環境	手順
Hyper-V	**a.** Hyper-V マネージャーを開きます。 **b.** アクセスするコネクタを右クリックし、［接続］をクリックします。

2. UNIX プロンプトで、管理者のユーザー名を入力してから **Enter** キーを押します。
   デフォルトのユーザー名は、**admin** です。
3. 管理者のパスワードを入力します。
   デフォルトのパスワードは **admin** です。
4. 次のいずれかの操作を実行します。

タスク	環境	手順
ネットワークインターフェイスの設定を確認する。	vSphere ESXi	「`sudo /var/lib/cylance-gateway/scripts/configure-network --ovfenv --check`」を入力します。**Enter** キーを押します。プロンプトが表示されたら、管理者パスワードを入力します。
コネクタのキーボードレイアウトを変更する。	すべて	デフォルトでは、Ubuntu は、US キーボードレイアウトのみをサポートします。 **a.** 新しいキーボードレイアウトを選択するには、`sudo dpkg-reconfigure keyboard-configuration` と入力します。**Enter** キーを押します。 **b.** プロンプトが表示されたら、管理者パスワードを入力します。 **c.** 画面の指示に従います。

OpenSSH を使用して **CylanceGATEWAY Connector** にアクセスする

メモ：OpenSSH は、デフォルトで AWS CylanceGATEWAY Connector AMI で有効です。AWS 環境にコネクタをインストールしている場合は、このタスクを実行しないでください。CylanceGATEWAY Connector セットアップを続行するには、「CylanceGATEWAY Connector 用ファイアウォールの設定」を参照してください。

OpenSSH はコネクタイメージにプリインストールされており、CylanceGATEWAY Connector にアクセスしたり、SSH プロトコルを使用してシステムの操作とメンテナンスを実行できるようにしたりします。デフォルトでは、OpenSSH サービスは無効です。OpenSSH を使用して CylanceGATEWAY Connector インスタンスにアクセスするには、毎回 OpenSSH サービスを有効にしてホストキーを生成する必要があります。Microsoft Entra ID 環境では、受信 TCP トラフィックを許可する必要があります。

作業を始める前に： ポート 22（SSH）、ポート 80（HTTP）、ポート 443（HTTPS）が開いていること、および セキュリティグループが登録の接続元ネットワークから CylanceGATEWAY Connector にアクセスできることを確認します。

1. 以下のいずれかの方法で、環境のコンソールを開きます。

環境	説明
vSphere	**a.** ご利用の環境にログインします。 **b.** CylanceGATEWAY Connector のホスト名をクリックします。 **c.** ［リモートコンソールの起動］または［**Web** コンソールの起動］をクリックします。
ESXi	**a.** ご利用の環境にログインします。 **b.** CylanceGATEWAY Connector のホスト名をクリックします。 **c.** ［コンソール］をクリックします。
Microsoft Entra ID	**a.** Microsoft Entra ID 管理ポータル（https://portal.azure.com）にサインインします。 **b.** ［仮想マシン］をクリックします。 **c.** 「CylanceGATEWAY Connector を Microsoft Entra ID 環境にインストールする」の手順 5 で作成したコネクタをクリックします。 **d.** 左側のメニューの［サポート **+** トラブルシューティング］セクションで、［シリアルコンソール］をクリックします。 **e.** 左の列の［ブート診断］をクリックします。 **f.** ［設定］タブをクリックします。 **g.** ［カスタムストレージアカウントで有効にする］を選択します。 **h.** ［診断ストレージアカウント］ドロップダウンリストで、「CylanceGATEWAY Connector を Microsoft Entra ID 環境にインストールする」の手順 3 で作成したストレージアカウントを選択します。 **i.** ［保存］をクリックします。 **j.** コネクタ画面の左側のメニューにある［サポート **+** トラブルシューティング］セクションで、［シリアルコンソール］をクリックします。
Hyper-V	**a.** Hyper-V マネージャーを開きます。 **b.** アクセスするコネクタを右クリックし、［接続］をクリックします。

2. UNIX プロンプトで、管理者のユーザー名を入力してから **Enter** キーを押します。デフォルトのユーザー名は、admin です。
3. 管理者のパスワードを入力します。デフォルトのパスワードは admin です。
4. OpenSSH サービスのホストキーを生成します。「`sudo dpkg-reconfigure openssh-server`」を入力します。**Enter** キーを押します。
5. プロンプトが表示されたら、管理者パスワードを入力します。
6. OpenSSH サービスを有効にします。「`sudo systemctl --system enable ssh`」を入力します。**Enter** キーを押します。

   メモ：このコマンドはサービスを開始しません。
7. OpenSSH サービスを開始します。「`sudo systemctl --system start ssh`」を入力します。**Enter** キーを押します。
8. 次のいずれかの操作を実行できます（オプション）。

タスク	手順
システム起動時に OpenSSH サービスが開始されないようにする。	「sudo systemctl --system disable ssh」を入力します。このコマンドはサービスを停止しません。
OpenSSH サービスを停止する。	「sudo systemctl --system stop ssh」を入力します。**Enter** キーを押します。
OpenSSH サービスが有効になっているかどうかを確認する。	「sudo systemctl --system is-enabled ssh」を入力します。
OpenSSH サービスが実行中かどうかを確認する。	「sudo systemctl --system is-active ssh」を入力します。
OpenSSL サービスのステータスを取得します。	「sudo systemctl --system status ssh」を入力します。

9. コンソールを終了します。
10. オプションで、Microsoft Entra ID 環境では、手順 1 で設定したコネクタ VM のブート診断設定を無効にすることもできます。

CylanceGATEWAY Connector 用ファイアウォールの設定

CylanceGATEWAY Connector は、ファイアウォールの内側にあるプライベートネットワーク内で動作し、プライベート IP アドレスを使用します。HTTPS と UDP を使用して CylanceGATEWAY クラウドサービスに接続します。CylanceGATEWAY Connector は、ファイアウォール経由（NAT 経由）で CylanceGATEWAY に接続できる必要があります。

CylanceGATEWAY Connector は、DNS を使用してパブリック CylanceGATEWAY FQDN をインターネット IP アドレスに解決できる必要があります。CylanceGATEWAY Connector は、プライベート DNS サーバーを使用してこれを行います。

CylanceGATEWAY エージェントは、セキュア Web ソケット（WSS）経由で通信するため、この接続を直接確立できる必要があります。CylanceGATEWAY エージェントがアクティブ化され、定期的に認証されるようにするには、適切なドメイン（idp.blackberry.com およびお住まいの地域のドメインなど）へのアクセスを許可する必要があります。ご使用の環境で認証プロキシを使用している場合は、プロキシサーバー上のトラフィックを許可する必要があります。

FQDN、ポート、IP アドレス範囲、およびその他のファイアウォール要件の詳細については、support.blackberry.com/community の記事 79017 を参照してください。Cylance Endpoint Security のネットワーク要件の詳細については、Cylance Endpoint Security ネットワーク要件 を参照してください。

BlackBerry Infrastructure への CylanceGATEWAY Connector の登録

CylanceGATEWAY Connector をインストールし、そのファイアウォールを設定したら、BlackBerry Infrastructure に接続する必要があります。

1. Web ブラウザーで、CylanceGATEWAY Connector の IP アドレスに移動します。
2. 自己署名証明書を受け入れて、HTTPS サービスに進むには、［**HTTPS** サービスに進む］をクリックします。
3. プロンプトで、デフォルトの管理者ユーザー名とパスワードを入力し、［サインイン］をクリックします。
   デフォルトのユーザー名は、admin です。デフォルトのパスワードは「blackberry」です。
4. CylanceGATEWAY Connector Web インターフェイスに初めてログインする場合は、CylanceGATEWAY Connector のデフォルトの管理者パスワードを変更する必要があります。これにより、ESXi、vSphere、Microsoft Entra ID ポータル、AWS コンソール、Hyper-V 管理コンソールで、CylanceGATEWAY Connector のパスワードが変更されることはありません。
5. 新しいパスワードを使用して、CylanceGATEWAY Connector Web インターフェイスに再度ログインします。
6. ［**BlackBerry** ソリューション使用許諾契約書］画面で使用許諾契約書を確認して、［同意する］をクリックします。
7. CylanceGATEWAY Connector を組織の BlackBerry Infrastructure に対して承認するには、コネクタを登録する必要があります。
   a) プライバシー通知を確認し、同意します。［**BlackBerry** プライバシー通知に同意します］チェックボックスをオンにします。
   b) ［**URL**］フィールドに、管理コンソールにアクセスするコネクタの URL を入力します。
      URL を取得するには、管理コンソールで［設定］**>**［ネットワーク］**>**［プライベートネットワーク］をクリックし、［**Gateway Connector**］タブで［コネクタを追加］をクリックします。
   c) ［プロキシ **URL**］フィールドに、プロキシサーバーの URL を入力します。この画面でプロキシ URL を入力すると、［設定］ページの［プロキシ **URL**］フィールドに同じ URL が入力されます（逆の手順でも同じ動作になります）。
8. ［このコネクタを登録］をクリックします。管理コンソールが開きます。
9. 管理コンソールに管理者としてログインします。
10. ［コネクタ名］フィールドに、コネクタの名前を入力します。
11. ［コネクタグループ］ドロップダウンリストで、割り当てるコネクタグループを選択します。
12. ［承認］をクリックします。

CylanceGATEWAY コネクタのリストに、割り当てられたコネクタ、そのバージョン、およびコネクタグループが表示されます。［ステータス］列に、プライベートネットワークとその DNS、およびヘルスチェックが正常に機能しているかどうかが表示されます。表示のステータスについては、次を参照してください。 CylanceGATEWAY Connectors の管理

終了したら： CylanceGATEWAY Connector を登録していても、そのトンネルが BlackBerry Infrastructure に接続されていない場合は、接続テストを開始して、プライベートネットワークから送信された UDP パケットが BlackBerry Infrastructure によって受信されたかどうか、および BlackBerry Infrastructure から送信された UDP パケットがプライベートネットワークによって受信されたかどうかを確認することができます。ご利用の環境（vSphere など）のログインプロンプトで「`/var/lib/cylance-gateway/bin/udp-connectivity-test`」を入力します。**Enter** キーを押します。このコマンドは、任意のシェル（csh、bash など）で実行できます。接続結果の詳細については、「UDP 接続テストの応答」を参照してください。

登録されている **CylanceGATEWAY Connector** の詳細の表示

CylanceGATEWAY Connector の詳細は、登録後に CylanceGATEWAY Connector の Web インターフェイスで確認できます。ネットワークに CylanceGATEWAY Connector のインスタンスが複数ある場合は、各インスタンスの Web インターフェイスにアクセスする必要があります。管理コンソールで、環境内のすべてのコネクタのステータスを表示できます。

- コネクタを BlackBerry Infrastructure に登録すると、次の情報が表示されます。［このコネクタの管理］ をクリックすると、Cylance Endpoint Security 管理コンソールが開き、CylanceGATEWAY Connector を管理できます。
  - インスタンスの識別で BlackBerry Infrastructure が使用する CylanceGATEWAY Connector 識別子
  - インスタンスの現在のステータスと登録情報
  - CylanceGATEWAY Connector により BlackBerry Infrastructure に接続されるトンネルの数
- ログファイルをダウンロードできます。ログファイルは、ダウンロードフォルダーに zip ファイルでダウンロードされ、複数の CylanceGATEWAY Connector ログファイルを含めることができます。［ログをダウンロード］をクリックします。ログを抽出して確認するか、zip ファイルを BlackBerry サポートに送信して、潜在的な問題のトラブルシューティングに役立てます。各インスタンスのログファイルは、CylanceGATEWAY Connector のページのコネクタ情報ペインにて、管理コンソールからダウンロードすることもできます。
- CylanceGATEWAY Connector を設定できます。

CylanceGATEWAY Connector の設定

CylanceGATEWAY Connector Web インターフェイスでは、さまざまなタスクを実行できます。ネットワークに CylanceGATEWAY Connector の複数のインスタンスがインストールおよび設定されている場合、必要に応じて各自の環境内の各 CylanceGATEWAY Connector インスタンスでタスクを完了する必要があります。管理コンソールの［Gateway Connector］ページで、環境内のすべてのコネクタのステータスを表示できます。各 CylanceGATEWAY Connector のステータスは、Web ブラウザで確認できます。詳細については、次を参照してください。 登録されている CylanceGATEWAY Connector の詳細の表示

作業を始める前に： 1 つ以上の CylanceGATEWAY Connector インスタンスが展開されていることを確認します。

1. Web ブラウザーで、CylanceGATEWAY Connector の IP アドレスに移動します。
2. 資格情報を入力し、［サインイン］をクリックします。
3. 次のタスクのいずれかを実行します。

タスク	手順
設定を編集する。	次の設定を 1 つ以上指定できます（オプション）。 **a.** ［設定］をクリックします。 **b.** 次の設定を 1 つ以上指定します。 • 新しい自己署名 TLS 証明書を生成します。TLS 証明書はいつでも再生成できます。デフォルトでは、証明書の有効期間は 1 年間です。Web インターフェイスには、証明書の有効期限日時、シリアル番号、証明書と紐づけられているホストが表示されます。新しい TLS 証明書を生成するたびに、新しい証明書を受け入れるように求められます。 • HTTP/S プロキシ設定：インターネット向けの HTTP/HTTPS 要求に使用される認証されていないプロキシサーバーが各自の環境で設定されている場合は、プロキシの URL を入力できます。プロキシの URL が追加されると、CylanceGATEWAY Connector によって実行された BlackBerry Infrastructure への HTTPS 要求はプロキシを使用します。トンネルトラフィックはプロキシを使用しません。 • 最大転送単位（MTU、Maximum Transfer Unit）の設定：デフォルトでは、CylanceGATEWAY Connector ネットワークの MTU を自動的に検出します。場合によっては、CylanceGATEWAY Connector で使用できる MTU 値を指定する必要があります。BlackBerry は、自動検出を使用することをお勧めします。 メモ：MTU を指定し、自動検出を使用する場合は、vSphere、Hyper-V、Microsoft Entra ID、AWS、ESXi の環境内から CylanceGATEWAY Connector を再起動する必要があります。 • ネットワークタイムプロトコル（NTP）設定：デフォルトでは、CylanceGATEWAY Connector は、時刻同期に Ubuntu の ntp.ubuntu.com サーバーを使用します。カスタム NTP サーバーを指定できます。 • APT（Advanced Package Tool）の設定：デフォルトでは、CylanceGATEWAY Connector は Ubuntu のリポジトリホスト archive.ubuntu.com および security.ubuntu.com を使用します。詳細については、support.blackberry.com/community にアクセスし、記事 79017 を参照してください。CylanceGATEWAY Connector が使用するカスタムパッケージリポジトリを指定できます。セキュリティ更新は自動的に適用されます。更新を有効にするには、管理コンソールで、CylanceGATEWAY Connector を再起動する必要があります。 **c.** 次の操作のいずれかを実行します。 • ［設定を更新］をクリックして、［設定］画面で変更を保存します。 • ［デフォルトの設定を復元］をクリックすると、すべてのデフォルト設定が復元されます。変更を有効にするには、資格情報を入力する必要があります。ネットワーク接続が中断される場合があります（たとえば MTU を指定した場合は、CylanceGATEWAY Connector を再起動する必要があります）。 • ［工場出荷時設定にリセット］をクリックすると、自己署名 TLS 証明書を含む CylanceGATEWAY Connector のすべての設定が消去されます。CylanceGATEWAY Connector を再起動する必要があり、ネットワーク接続が中断されます。

タスク	手順
管理者のパスワードを変更する。	CylanceGATEWAY Connector パスワードの管理者パスワードはいつでも変更できます。これによって、vSphere、Hyper-V、Microsoft Entra ID、AWS、ESXi の環境で、CylanceGATEWAY Connector のアクセスに使用される管理者パスワードが変更されることはありません。パスワードを変更するたびに、新しいパスワードを使用して再度ログインするように求められます。 **a.** ［管理者パスワードを変更］をクリックします。 **b.** 現在の管理者パスワードを入力します。 **c.** 新しいパスワードを入力して確認します。 **d.** ［パスワードを変更］をクリックします。 **e.** プロンプトが表示されたら、**[**今すぐログイン］をクリックします。しばらくすると、自動的にログインプロンプトにリダイレクトされます。 **f.** 管理者のユーザー名と新しいパスワードを入力し、［サインイン］をクリックします。

CylanceGATEWAY Connectors の管理

CylanceGATEWAY Connectors を登録した後、ヘルスチェック URL を指定し、コネクタの IP アドレスを制限することができます。ヘルスチェック URL が指定されていない場合、コネクタのヘルスチェックステータスに DNS と HTTP の情報は表示されません。CylanceGATEWAY Connectors で実行できる操作は以下のとおりです。

画面	操作
Gateway Connector リスト画面	• アクティブな接続の数を表示します。 • CylanceGATEWAY Connector が属しているコネクタグループを表示します。 • 各コネクタインスタンスの追加のヘルスチェックメタデータを表示します。 • 各コネクタインスタンスのバージョンを表示します。 • コネクタのステータスを表示します。 • CylanceGATEWAY Connectors 情報を再読み込みします。 • 各コネクタインスタンスのログファイルをダウンロードします。 • コネクタを無効にして、新しい接続がそのコネクタ経由でルーティングされないようにします。アクティブなネットワーク接続は中断されません。
［コネクタ情報］ページ	• CylanceGATEWAY Connector が属しているコネクタグループを表示します。 • コネクタの［プライベート URL］フィールドを編集し、別のページで URL を開きます。 • コネクタを別のコネクタグループに割り当てます。 • コネクタを無効にして、新しい接続がそのコネクタ経由でルーティングされないようにします。アクティブなネットワーク接続は中断されません。 • コネクタのバージョンを表示します。 • コネクタの接続ステータスを表示します。 • コネクタのログファイルをダウンロードします。 • 公開鍵を表示します。 • コネクタの接続履歴を表示します。接続履歴の時刻は UTC です。

ソース IP アドレスを制限すると、指定した IP アドレスを持つ CylanceGATEWAY Connectors 以外はプライベートネットワークに接続できなくなるので、セキュリティが強化されます。ソース IP アドレスを制限する場合、vSphere 環境 または ESXi 環境で展開するときは、CylanceGATEWAY Connector に静的 IP アドレスを設定するか、ネットワーク上に DHCP IP 予約を作成することによって、各自の CylanceGATEWAY Connectors の IP アドレスを固定する必要があります。

環境内のアクティブな CylanceGATEWAY ユーザー数によっては、コネクタからの着信トンネルの管理を担当する BlackBerry Infrastructure のコンポーネントが、組織に割り当てられたリソースを拡張する可能性があります。各 CylanceGATEWAY Connector は、このコンポーネントへのトンネルを確立し、ヘルスチェックを実行します。［ヘルスチェックのステータス］列および［ステータス］列には、管理責任のあるコンポーネントとコネクタをつなぐトンネルの状態が表示されます。たとえば［ヘルスチェック］列に $X/2$ と表示されている場合、その時点で組織には 2 つのコンポーネントが割り当てられていることを意味します。列に 2/2 と表示されている場合、コネクタはコンポーネントに対して 2 つのトンネルを正常に確立しています。0/2 または 1/2 と表示されている場合、コネクタはトンネルを確立していないか、必要な 2 つのトンネルのうち 1 つを確立していることを意味します。ステータスが ⚠ の場合、すべてのユーザーではなく一部のユーザーのみがプライベートネットワーク上のリソースにアクセスできます。

ヘルスチェック URL には、CylanceGATEWAY ユーザーが接続できるプライベートネットワーク内の任意の URL を指定できます。CylanceGATEWAY は、定期的に HTTP または HTTPS GET 要求を送信します。これには、この URL への各 CylanceGATEWAY Connector トンネルを経由する DNS ルックアップが含まれます。ヘルスチェックのステータスが展開され、各コネクタのトンネル、DNS、および HTTP 接続ステータスが表示されます。2/2 のステータスは、すべてが正常に動作していることを示します。0/0 のステータスは、新しい接続のステータスチェックがまだ保留中であることを示します。

ステータスの列には、CylanceGATEWAY Connector への BlackBerry Infrastructure の登録ステータスが表示されます。✅ は、CylanceGATEWAY Connector が登録プロセスを正常に完了しており、BlackBerry Infrastructure への接続が確立済みであることを示します。ステータスの列に表示されるのは接続状態ですが、セキュリティメッセージが含まれている場合もあります（たとえば、更新を適用するためコネクタの再起動が必要など）。

列	説明
ヘルスチェックのステータス	これは、CylanceGATEWAY Connector の全体的なステータスであり、次の情報が含まれます。 • トンネル：これは CylanceGATEWAY Connector の BlackBerry Infrastructure への接続ステータスです。ステータスに接続の問題が示されている場合は、BlackBerry のサポート担当者にお問い合わせください。 • **DNS**：これは、CylanceGATEWAY Connector から指定された DNS サーバーの DNS クエリのステータスです。ステータスが問題のあることを示している場合は、プライベート DNS サーバーを正しく指定していることを確認します。 • **HTTP**：これは、ヘルスチェック URL 用に CylanceGATEWAY Connector に対して作成された HTTP クエリのステータスです。ステータスが問題のあることを示している場合は、CylanceGATEWAY Connector からヘルスチェック URL に到達できることと、DNS 前方ルックアップゾーンが指定済みであることを確認します。

列	説明
ステータス	これは、BlackBerry Infrastructure への CylanceGATEWAY Connector 接続の全体的なステータスであり、ヘルスチェックのステータスを含みます。 • : コネクタは登録プロセスを完了していません。このステータスは、最初のコネクタ登録時にのみ表示されます。 • : コネクタは登録プロセスを完了し、BlackBerry Infrastructure への接続を確立しています。 • : コネクタは登録プロセスを完了しましたが、BlackBerry Infrastructure へのすべての接続が確立されているわけではありません。この状態が表示された場合は、関連するセキュリティメッセージに目を通して、ヘルスチェック URL がコネクタグループで指定されていることを確認します。 • : コネクタ登録プロセスが完了していないか、BlackBerry Infrastructure へのすべての接続の確立中にエラーが発生しています。次のエラーメッセージが表示される場合があります。 • ストレージエラーのため登録できませんでした：CylanceGATEWAY Connector の登録に十分なディスク容量があることを確認してください。 • 失敗：トンネル、DNS、HTTP 情報など、コネクタのすべてのヘルスチェックステータスを確認してください。たとえば、DNS に「失敗」と表示されている場合は、DNS 設定が正確であることを確認します。

CylanceGATEWAY コネクタの管理

各コネクタグループについて、このタスクを実行します。

1. 管理コンソールのメニューバーで、［設定］ > ［ネットワーク］をクリックします。
2. ［プライベートネットワーク］タブをクリックします。
3. ［コネクタグループ］をクリックします。コネクタグループをクリックします。
4. ［ヘルスチェック］をクリックします。
5. プライベートネットワーク内の、CylanceGATEWAY Connector からアクセスできる URL を指定して、CylanceGATEWAY がその URL に接続できることを確認します。

   ヘルスチェック URL には、プライベート DNS サーバーが解決できる完全修飾ドメイン名（FQDN）が含まれている必要があります。FQDN は、プライベートネットワークに定義された IP スペース内の IP アドレスに解決される必要があります。
6. CylanceGATEWAY Connectors に許可する IP アドレスを指定するには、［ソース **IP** 制限］をクリックします。
7. ［追加］をクリックします。
8. ［保存］をクリックします。
9. CylanceGATEWAY Connector に関する追加情報の表示、コネクタログファイルのダウンロード、プライベート URL へのカスタム FQDN または IP アドレスの入力を行うには、CylanceGATEWAY Connector の名前をクリックします。

   メモ：カスタムの FQDN または IP アドレスを入力した場合、FQDN や IP アドレスの検証はされません。
10. CylanceGATEWAY Connectors 情報をリロードするには、 をクリックします。

CylanceGATEWAY Connector の更新

CylanceGATEWAY Connector の更新または仮想マシン OS の更新が利用可能かどうかを確認できます。

作業を始める前に： Cylance Endpoint Security 管理コンソールの［設定］ > ［ネットワーク］ > ［プライベートネットワーク］ > ［Gateway Connector］で、インストールされている CylanceGATEWAY Connector のバージョンを確認します。

1. *my*Account または Cylance Endpoint Security リリースノートをチェックして、CylanceGATEWAY Connector ソフトウェアの新しいバージョンが使用可能かどうかを確認し、次のいずれかの操作を実行します。
   - 新しい CylanceGATEWAY Connector ソフトウェアが利用可能である場合は、ご利用の環境に応じて手順 2 を実行します。
   - 新しい CylanceGATEWAY Connector ソフトウェアの更新が利用可能でない場合は、Linux OS のアップデートを確認します。
2. 次のタスクのいずれかを実行します。

環境	手順
CylanceGATEWAY Connector バージョン 2.9 以降を更新します。	DEB ファイルを使用してコネクタインスタンスを更新し、設定を保持します。 **a.** *my*Account でコネクタの DEB バージョンをダウンロードします。 **b.** アップグレードするコネクタに DEB パッケージをコピーします。SSH が有効である場合、SCP を使用して、SSH でアクセスできるホストからコネクタに DEB パッケージをコピーできます。手順については、「OpenSSH を使用して CylanceGATEWAY Connector にアクセスする」を参照してください。それ以外の場合は、コネクタ上の SCP を使用して、コネクタで到達できる SSH 対応ホストから DEB パッケージをコピーできます。 **c.** Unix コンソールで、「`sudo apt install <path>/cylance-gateway-connector-<version>.deb`」と入力します。 例： `sudo apt install /home/admin/cylance-gateway-connector-2.10.0.938.deb` **d.** **Enter** キーを押します。
CylanceGATEWAY Connector バージョン 2.8 以前を更新するか、完全な再インストールを実行します。	使用環境用にコネクタの新しいインスタンスを作成します。手順については、「CylanceGATEWAY Connector のセットアップ」を参照してください。

3. ［ステータス］列の［**OS** のアップデートとセキュリティ修正を適用するには、再起動が必要です］と表示されている CylanceGATEWAY Connector については、仮想マシンを再起動して OS アップデートのインストールを完了してください。

終了したら： CylanceGATEWAY Connector を登録していても、そのトンネルが BlackBerry Infrastructure に接続されていない場合は、接続テストを開始して、プライベートネットワークから送信された UDP パケットが BlackBerry Infrastructure によって受信されたかどうか、および BlackBerry Infrastructure から送信された UDP パケットがプライベートネットワークによって受信されたかどうかを確認することができます。ご利用の環境（vSphere など）のログインプロンプトで「`/var/lib/cylance-gateway/bin/udp-connectivity-test`」と入力します。**Enter** キーを押します。このコマンドは、任意のシェル（csh、bash など）で実行できます。接続結果の詳細については、「UDP 接続テストの応答」を参照してください。

UDP 接続テストの応答

ここでは、CylanceGATEWAY Connector と BlackBerry Infrastructure の間の UDP パスを確認するときに表示される出力の例を示します。

これらの例では次の条件を使用しています。

- 「Endpoint」は、テストする udp-connectivity-test の IP アドレスおよびポートです。
- 「Client Address:Port」は、BlackBerry Infrastructure から見た CylanceGATEWAY Connector の外部 IP アドレスおよびポートです。
- 「Server」は BlackBerry Infrastructure です。

例：**UDP** トラフィックが正常に送受信されています。

この例では、プライベートネットワークのコネクタと BlackBerry Infrastructure の間で UDP トラフィックが正常に送受信されています。

```
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
```

例：アウトバウンド **UDP** トラフィックはブロックされています。

この例では、UDP 接続テストクライアントはクライアント hello を送信できましたが、BlackBerry Infrastructure はタイムアウト期間内に応答を受信しませんでした。

```
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
```

例：インバウンド **UDP** トラフィックがブロックされています。

この例では、UDP 接続テストクライアントは UDP 接続テストクライアント hello を送信し、BlackBerry Infrastructure はそれを受信して応答しましたが、テストクライアントはタイムアウト期間内に応答を受信しませんでした。

```
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
```

プライベートネットワークの指定

作業を始める前に：

- プライベートネットワークの一部として定義するすべての宛先の IP アドレスまたは IP アドレス範囲のリストがあることを確認します。この情報は、ネットワーク管理者から入手できます。
- プライベートネットワークアクセスを設定するには、CylanceGATEWAY Connector をインストールする必要があります。ここで指定したアドレスへのフルアクセス権を持つネットワークの一部に、1 つ以上の CylanceGATEWAY Connector がインストールされていることを確認します。CylanceGATEWAY Connector のインストール手順については、「CylanceGATEWAY Connector のセットアップ」を参照してください。
- コネクタグループは最大 8 個まで作成できます。各コネクタグループには、最大 8 個の CylanceGATEWAY Connector を追加できます。

1. メニューバーで、［設定］ > ［ネットワーク］をクリックします。
2. ［プライベートネットワーク］タブをクリックします。
3. ［コネクタグループ］をクリックします。
4. ［コネクタグループを追加］をクリックします。
5. 名前と説明を入力します。コネクタ名は 3～250 文字です。説明は 3～500 文字です。
6. ［ネットワークルーティング］タブで、［アドレスを追加］をクリックします。
7. 1 つまたは複数の IP アドレス、IP 範囲、または CIDR を入力し、［追加］をクリックします。

   すべてのネットワークトラフィックをオンプレミスのインフラストラクチャにリダイレクトする必要がある場合は、`0.0.0.0/0` と入力します。BlackBerry では、プライベートネットワーク上のリソース宛てのトラフィックのみをリダイレクトし、インターネットの宛先へのトラフィックには CylanceGATEWAY クラウドサービスを使用するように環境を設定することが推奨されています。

   メモ：ネットワークルーティングに 0.0.0.0 を指定すると、すべての非 DNS トラフィック（HTTP トラフィックなど）が CylanceGATEWAY Connector を経由してルーティングされます。プライベートネットワークに含まれないリソースへのトラフィックの場合は、接続が確立されトラフィックが CylanceGATEWAY Connector

を経由してルーティングされる前に、DNS クエリをプライベート DNS サーバーではなくパブリック DNS サーバーに送信する必要があります。

8. 住所を編集するには、住所の横にある をクリックします。
9. アドレスを削除するには、アドレスの横にある をクリックします。
10. リストの順序を変更するには、コネクタグループの をリスト内の適切な場所にドラッグします。
11. コネクタグループを削除するには、割り当てられているすべての CylanceGATEWAY Connector をコネクタグループから削除するか、または再割り当てします。 をクリックします。

プライベート DNS の指定

プライベート DNS での設定により、CylanceGATEWAY でプライベートネットワーク内のトラフィックをルーティングできるようになります。DNS サーバーの IP アドレス、前方ルックアップのために DNS サーバーに委任されるドメイン名、逆引きルックアップのために DNS サーバーに委任される CIDR を指定できます。DNS サーバーの IP アドレスは、すべてのコネクタグループで共有されます。これらは、1 つのコネクタグループに含める必要があります。この情報は、ネットワーク管理者から入手できます。

1. メニューバーで、［設定］ > ［ネットワーク］をクリックします。
2. ［プライベートネットワーク］タブをクリックします。
3. ［**DNS**］をクリックします。
4. DNS サーバーを指定するには、次のアクションを実行します。
   a) ［**DNS** サーバー］をクリックします。
   b) ［**DNS** サーバーを追加］をクリックします。
   c) DNS サーバーの IP アドレスを入力し、［追加］をクリックします。
5. 前方ルックアップのドメインを指定するには、次のアクションを実行します。最大 100 件の前方ルックアップゾーンを指定できます。
   a) ［前方ルックアップゾーン］をクリックします。
   b) ［前方ゾーンを追加］をクリックします。
   c) ドメイン名を入力して、［追加］をクリックします。

   前方ルックアップゾーンを指定しないと、CylanceGATEWAY Connector ヘルスチェックが失敗します。分割トンネルを有効にし、前方ルックアップゾーンを指定しなかった場合は、すべての DNS クエリがトンネルを通過します。
6. 逆引きルックアップ用の CIDR を指定するには、次のアクションを実行します。
   a) ［逆引きルックアップゾーン］をクリックします。
   b) ［逆引きゾーンを追加］をクリックします。
   c) CIDR を入力し、［追加］をクリックします。
7. アドレスやドメイン名を編集するには、 をクリックします。
8. アドレスやドメイン名を削除するには、 をクリックします。

DNS サフィックスの指定

非修飾名の検索にプライベート DNS が追加するサフィックスは、最大 32 個指定できます。この情報は、ネットワーク管理者から入手できます。複数のサフィックスを指定する場合は、それらをランク付けできます。

1. メニューバーで、［設定］ > ［ネットワーク］をクリックします。
2. ［クライアント **DNS**］タブをクリックします。
3. ［**DNS** 検索ドメイン（またはサフィックス）］をオンにします。

4. ［**DNS** サフィックスを追加］をクリックします。
5. DNS サフィックス名を入力し、［追加］をクリックします。
6. 追加するサフィックスごとに手順 4 と 5 を繰り返します。
7. サフィックスを編集するには、 をクリックします。
8. サフィックスを削除するには、 をクリックします。
9. リストの順序を変更するには、サフィックスの をリスト内の適切な場所にドラッグします。
10. ［保存］をクリックします。

プライベート **CylanceGATEWAY** エージェントの **IP** 範囲の指定

CylanceGATEWAY は、プライベート IP 範囲からトンネルのプライベート IP アドレスを CylanceGATEWAY エージェントに割り当てます。この IP 範囲は、システム全体で構成されているもので、各テナント共通になります。テナントのプライベートネットワーク範囲と CylanceGATEWAY エージェントが重複しないエンドポイントトンネルのプライベート IP 範囲を指定することもできます。たとえば、エージェントがアクセスしようとするプライベートネットワークサービスが、エージェントと同じ IP アドレスを有していることがあります。プライベート IP 範囲を指定すると、このような衝突の可能性を防ぐことができます。エージェントの IP 範囲は IPv4 CIDR 形式であり、プライベートネットワーク内の他のエンドポイントへのルーティングの問題を防ぐために、ネットワーク内で一意である必要があります。デフォルトの範囲は 10.10.0.0/16 です。サフィックスは 17 未満である必要があります。

警告：エージェント IP 範囲を変更した場合、関連付けられているエージェントおよび CylanceGATEWAY Connector が切断され、再接続される場合があります。切断および再接続中に［Gateway Connector］画面（［設定］ > ［ネットワーク］ > ［プライベートネットワーク］）にアクセスすると、次のいずれかのメッセージが表示されます。 をクリックします。

- 登録を完了できませんでした：500
- 失敗しました。OS のアップデートとセキュリティ修正を適用するには、再起動が必要です

1. メニューバーで、［設定］ **>** ［ネットワーク］をクリックします。
2. ［プライベートネットワーク］タブをクリックします。
3. **[**エージェント **IP** 範囲］をクリックします。
4. CIDR を入力します。
5. ［保存］をクリックします。

自分の **IP** アドレスを使用する（**BYOIP**）

ネットワークの送信トラフィック管理に使用する CylanceGATEWAY に、IPv4 CIDR /24 範囲内の専用 IP アドレスを追加することができます。

専用 IP アドレスは、次のような場合に使用します。

- ソース IP ピンに組織独自の IP アドレスを使用します。
- 一部の Web サイトが AWS IP 範囲をブロックするという問題を回避します。
- アドレスの GeoIP 情報を反映します。
- 不連続な複数の IP ではなく、単一の CIDR を許可します。

CylanceGATEWAY に専用 IP アドレスを追加するには、BlackBerry Technical Support Services に要求を送信してください。手順については、https://support.blackberry.com/community にアクセスして記事 100189 を参照してください。

CylanceGATEWAY を使用したネットワークアドレス変換

デフォルトの場合、CylanceGATEWAY では、プライベートネットワークへのトラフィックフローにネットワークアドレス変換（NAT）が適用されます。NAT は、ユーザーがインターネットや SaaS アプリにアクセスするとき、エンドポイント（デバイスなど）にも適用されます。NAT の適用後、実際の IP アドレスは隠され、特定のエンドポイントへのすべての着信接続は防止されます。CylanceGATEWAY トンネルを使用しないフロー（セーフモードなど）には、NAT は適用されません。

メモ：エンドポイントへの着信接続は CylanceGATEWAY によって防止されます（たとえば、リモートデスクトップ接続などのリモート IT ツールを使用してエンドポイントへの接続を確立することはできません）。

NAT は、CylanceGATEWAY Connector を経由してプライベートネットワークに流れるトラフィックに適用されます。コネクタは、ネットワークイベント画面（CylanceGATEWAY > ［イベント］）に表示される UDP および TCP フローに関する追加情報を提供します。ブロックされたか潜在的に悪意のあるものとして識別されたイベントのプライベート送信元 IP およびプライベート送信元ポートを特定できます。詳細については、以下を参照してください。

- イベント詳細ページの表示
- データフロー：プライベートネットワークのアプリケーションサーバーまたはコンテンツサーバーへのアクセス

NAT は、トンネルを通過してインターネットの宛先やクラウドベースの SaaS アプリケーションにアクセスするトラフィックに、CylanceGATEWAY によって適用されます。ユーザーが外部宛先へのアクセスに使用したゲートウェイトンネル IP アドレスに基づいて、イベントをフィルタリングできます。詳細については、以下を参照してください。

- イベント詳細ページの表示
- データフロー：クラウドベースのアプリケーションまたはインターネット上の宛先へのアクセス

ネットワークサービスの定義

ネットワークサービスは、アクセス制御リスト（ACL）ルールの設定を簡素化するために使用できるアドレスのグループ（FQDN または IP アドレス）です。ACL ルールを作成するときは、各アドレスを個別に指定する代わりに、ネットワークサービスを指定できます。BlackBerry ではプロセスを簡素化するために、多くの一般的な SaaS アプリケーションのネットワークサービスを保守し、定期的に更新しています。パブリックアプリケーションとプライベートアプリケーションの両方に追加のネットワークサービスを定義できます。既存のネットワークサービスはネストすることができます。ネットワークサービスをネストすると、追加した各ネットワークサービス中の宛先が参照されるようになり、そこに含まれているすべての宛先にアクセスできます。結合されたネットワークサービス中の 1 つが変更された場合、そうした変更は即座に自動的に反映されます。追加したネットワークサービスについては、検索することができます。検索の詳細については、「ACL ルールとネットワークサービスの検索」を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［ネットワーク］をクリックします。
2. ［ネットワークサービス］タブをクリックします。
3. ［追加］をクリックします。
4. ネットワークサービスの名前と説明を入力します。
5. 必要に応じて、［ネットワークサービス］をクリックし、1 つまたは複数のネットワークサービスを選択します。

6. 必要に応じて、［アドレス］をクリックします。宛先の IP アドレス、FQDN、またはワイルドカードドメインを入力します。他のアドレスを追加する場合は、＋をクリックします。次のアドレス形式がサポートされています。
   - IP アドレス範囲：172.16.10.0〜172.16.10.255
   - 単一のアドレス：172.16.10.2
   - IP アドレス範囲：172.16.10.0〜172.16.10.255
   - CIDR：172.16.10.0/24
   - FQDN：domain.example.com
   - ワイルドカードを含むドメイン：*.example.com
7. ［プロトコル］をクリックし、接続の試行に使用するプロトコルを選択し、使用する単一のポートまたはポート範囲を指定します。他のプロトコルとポートを追加する場合は、＋をクリックします。
8. 手順 6 と 7 を繰り返して、他のアドレスとポートを追加します。
9. ［追加］をクリックします。
10. ネットワークサービスを編集するには、編集するフィールドをクリックして変更を加えます。BlackBerry によって定義されたサービスは編集できません。
11. ネットワークサービスを削除するには、サービス、アドレス、またはポートの横にある✕をクリックします。アドレスとポートの行を削除するには、適切な宛先アドレスとポートの行の横にある✕をクリックします。BlackBerry によって定義されたサービスは削除できません。

終了したら： ネットワークサービスリストを検索して、情報を表示することができます。🔍をクリックして、1 つまたは複数の事前定義された有効範囲および条件を選択し、基準を指定します。設定を表示したいネットワークサービスをクリックします。✕をクリックすると検索がリセットされます。

ネットワークアクセスの制御

CylanceGATEWAY に登録されたデバイスが接続できるネットワークリソースは、アクセス制御リスト（ACL）を使用して定義します。ACLは、プライベートネットワークおよびパブリックネットワーク上の許可およびブロックされる対象を定義します。ACL は、Gateway サービスポリシーが割り当てられているユーザーにのみ適用されます。

ACL は、テナント内のすべての CylanceGATEWAY ユーザーに適用されます。デバイスによる各ネットワークアクセス試行は、接続フェーズ（DNS ルックアップ、接続確立、TLS ハンドシェイク）ごとに、試行に一致するルールが見つかるまでルールに対して評価されます。ルールは、対象または対象のカテゴリ、指定されたユーザーまたはグループ、および対象に対して決定されたリスクレベルを含む、指定されたすべてのプロパティで一致する必要があります。最初の一致ルールは、アクセス試行がブロックされるか、次の段階への続行が許可されるかを決定します。すべての段階で許可されたアクセス試行は、完全に確立されます。ネットワークアクセス試行が ACL 内のどのルールとも一致しない場合、アクセスはブロックされます。ACL は、最大 1000 個のルールをサポートしています。

ACL ルールの適用

ACL ルールは、テナント内のすべての CylanceGATEWAY ユーザーに適用されます。ACL ルールは、管理コンソールに表示される順に、各ネットワークアクセス試行を上から順番に評価します。デフォルトルールは常に最後に評価され、以前のルールがいずれも一致しない場合は、すべてのリソースへのアクセスがブロックされます。デフォルトルールを無効にしたり、変更したりすることはできません。

ACL ルールを作成する場合は、ACL ルールを作成し、次の順序で表示されていることを確認するようお勧めします。

1. CylanceGATEWAY で指定されたカテゴリを含むインターネットコンテンツへのアクセスをブロック
2. 組織の要件に基づき、分類されていないサービスへのアクセスをブロック
3. プライベートネットワーク内の組織全体のサービスへのアクセスを許可
4. すべてのパブリックインターネットの宛先へのアクセスを許可
5. デフォルト

次の表に、ルールとその必要な設定の例を示します。

ルール	説明
ユーザーがパブリックインターネットの宛先にアクセスできるようにする	このルールを使用すると、組織がパブリックインターネットと見なすすべての宛先にユーザーがアクセスできるようになります。ユーザーは指定された RFC1918 アドレスにはアクセスできません。 このルールを作成するには、次の設定を指定できます。 ・ ［アクション］セクションで、 ・ ［アクション］ドロップダウンリストに［許可］と表示されます。 ・ ［ネットワーク保護に対するアクセス試行を確認］チェックボックスをオンにします。この設定により、ルールが ACL を通過できるようになり、また Gateway によるさらなる検査も通過可能になります。 ・ ［宛先］セクションで、 ・ ［ターゲット］ドロップダウンリストに［一致しません］と表示されます。 ・ ［アドレスとポート］、［アドレス］フィールドに RFC1918 ネットワークの範囲を入力します。

ルール	説明

ユーザーがプライベートネットワークにアクセスできるようにする	このルールにより、ユーザーはプライベートネットワーク内のネットワークサービスにアクセスできるようになります。
	ユーザーがプライベートネットワークにアクセスするには、次の前提条件を満たす必要があります。
	• トラフィックがプライベートネットワークに到達できるよう、CylanceGATEWAY Connector がネットワークにインストールされていることを確認します。お使いの環境で CylanceGATEWAY Connector をインストールする方法については、「CylanceGATEWAY Connector のセットアップ」を参照してください。
	• ユーザーにアクセスさせるプライベートネットワークリソースを含むネットワークサービスが定義されていることを確認します。ネットワークサービスを定義する方法については、「ネットワークサービスの定義」を参照してください。
	次の設定を指定できます。
	• ［アクション］セクション：
	  • ［アクション］ドロップダウンリストに［許可］と表示されます。
	  • 必要に応じて、［ネットワーク保護に対するアクセス試行を確認］チェックボックスをオフにします。これ以上の検査は Gateway では行われません。
	• ［宛先］セクション：
	  • ［ターゲット］ドロップダウンリストに［いずれかに一致］と表示されます。
	  • ［ネットワークサービス］フィールドで、ユーザーにアクセスさせるネットワークサービスを選択します。

ACL パラメーター

ACL はルールの順序付きリストで、CylanceGATEWAY ユーザーがインターネットまたはプライベートネットワーク上の宛先にアクセスしようとしたときの動作を定義します。各ルールには、宛先、ユーザー、およびルールが一致する可能性があるその他の要素、およびルールが一致するときに実行するアクションを指定できる複数のパラメーターが含まれています。ネットワークアクセス試行がどの ACL ルールとも一致しない場合、アクセスはブロックされます。

ACL ルールを追加または編集すると、更新はコミットされるまでドラフトルールのリストに追加されます。管理者ごとに各自のドラフトルールのリストがあります。管理者がルールの更新をコミットすると、ドラフトルールリストを持つ他のすべての管理者に、続行する前にドラフトルールリストを削除または更新するよう通知されます。

各ルールには、次のパラメーターを含めることができます。

項目	説明
一般的な情報	

項目	説明
名前	これはルールの名前です。
説明	これは、ルールの目的の簡単な説明です。
有効	この設定は、ルールが ACL の一部であるかどうかを指定します。このオプションをオフにすると、ルールを削除せずに無効にできます。
アクション	
アクション	この設定は、試行がルールに一致する場合にアクセスを許可するかブロックするかを指定します。アクセス試行を続行できる場合は、試行の次の段階で再評価される可能性があります。
ネットワーク保護に対してアドレスを確認	ルールのアクションでアクセスが許可されている場合でも、潜在的なネットワークの脅威が検出されたときには、CylanceGATEWAY は接続をブロックするかどうかをこの設定で指定します。特定のユーザーが潜在的に悪意のある宛先に接続する必要がない限り、このオプションは選択したままにしてください。
ブロックされた通知メッセージをデバイスに表示します	ルールのアクションがアクセスをブロックする場合、この設定は、アクセス試行がブロックされたときにデバイスに表示される通知メッセージを指定します。
トラフィックプライバシー	この設定は、ネットワークアクセス試行を［ネットワークイベント］画面（CylanceGATEWAY > ［イベント］）に表示するかどうかを指定します。法的責任やプライバシー上の事情がある場合は、［トラフィックプライバシー］を有効にすることをおすすめします。この設定を有効にすると、ネットワークアクセス試行は［ネットワークイベント］画面に表示されません。イベントを SIEM ソリューションまたは syslog サーバーに送信する際に、接続試行がトラフィックプライバシーのルールと一致する場合、そのイベントは SIEM ソリューションにも syslog サーバーにも送信されません。
コンテンツログの記録	この設定では、［ネットワークイベント］>［イベントの詳細］ページに、プレーンテキストで暗号化されていない元の HTTP 接続データを含めるかどうかを指定します。HTTP フローは復号化されません。この設定を有効にすると、イベントの要求と応答の詳細のサマリーが［イベントの詳細］ページに表示されます。イベント内のすべての HTTP トランザクションを表示できます。［イベントの詳細］ページには、イベントの総数のうち最初の 3 つの HTTP イベントが含まれます。すべてのイベントと、それぞれに関連する詳細を表示できます。［トラフィックプライバシー］と［コンテンツログの記録］の両方を含むルールを作成した場合は、トラフィックプライバシーが優先されます。
ポートを無視	この設定は、アクセス制御の試行の宛先ポートをこのルールの一部として評価するか、それとも無視するかを指定します。
移行先	

項目	説明
ターゲット	ターゲットの定義としては、ネットワークサービス、アドレスのセット、定義されたプロトコルとポートを持つアドレスのセット、または定義されたプロトコルとポートのみがあります。次のいずれかのオプションを選択できます。 • 該当なし：ルールには宛先は含まれません。たとえば、カテゴリだけを指定するルールや、ネットワーク保護によって接続がブロックされていない限り、特定のユーザーのすべてのアクセス試行を許可するルールを作成することができます。 • いずれかに一致：ルールは、宛先がルールで指定された任意のターゲットと一致する場合に適用されます。 • 一致しません：宛先がルールで指定されたターゲットと一致しない場合にルールが適用されます。
ネットワークサービス	1 つまたは複数のネットワークサービスを選択できます。
アドレス	この設定では、宛先アドレスの IP アドレス、FQDN、またはワイルドカードドメインを指定します。IP アドレスは IPv4 または IPv6 形式で、単一の IP アドレス、IP 範囲、または CIDR 表記で表すことができます。たとえば、次のアドレス形式がサポートされています。 • 単一の IP アドレス：172.16.10.2 • IP アドレス範囲：172.16.10.0 - 172.16.10.255 • CIDR：172.16.10.0/24 • FQDN：domain.example.com • ワイルドカードを使用したドメイン：*.example.com
プロトコル	この設定では、ルールが TCP、UDP、またはその両方を使用した接続試行と一致するかどうかを指定します。オプションを選択しない場合、デフォルトはすべてのポートで TCP と UDP の両方です。
ポート	この設定では、宛先が使用するポートを指定します。単一のポートまたはポートの範囲を指定できます。
カテゴリ	カテゴリは、サイトで利用可能なコンテンツのタイプを定義します。CylanceGATEWAY は、利用可能な情報に基づいて、ベストフォートにより、宛先サイトのカテゴリを決定します。次のいずれかのオプションを選択できます。 • 該当なし：ルールにはカテゴリは含まれません。 • いずれかに一致：ルールは、宛先がルールで指定された任意のカテゴリと一致する場合に適用されます。このオプションを選択すると、選択できるカテゴリのリストが表示されます。 • 一致しません：宛先がルールで指定されたカテゴリと一致しない場合にルールが適用されます。このオプションを選択すると、選択できるカテゴリのリストが表示されます。 指定できる有効なカテゴリの詳細情報については、次を参照してください。 宛先コンテンツのカテゴリ

項目	説明
条件	
ユーザープロパティ	この設定では、ルールに含めるユーザー、ユーザーグループ、またはオペレーティングシステムを指定します。任意の数のユーザー、ユーザーグループ、およびオペレーティングシステム、またはそれらの組み合わせを指定できます。［ユーザープロパティ］ドロップダウンをクリックし、条件を指定するユーザープロパティを選択します。次のいずれかのオプションを選択できます。 • 該当なし：ルールは、すべてのユーザー、グループ、およびオペレーティングシステムに適用されます。 • いずれかに一致：ルールは、ルールに追加したユーザー、グループ、またはオペレーションシステムにのみ適用されます。このオプションを選択すると、ユーザープロパティを追加するフィールドが表示されます。 • 一致しません：ルールは、ルールのリストに含まれていないユーザー、グループ、またはオペレーションシステムにのみ適用されます。このオプションを選択すると、ユーザープロパティを追加するフィールドが表示されます。 名前またはユーザーグループの入力を開始すると、一致するユーザー名のリストがリストに表示されます。オペレーティングシステムを指定する場合は、リストから選択する必要があります。次の OS オプションから選択できます。 • Android • iOS • macOS • Windows 行を追加して、任意の数のユーザー、グループ、およびオペレーションシステムを指定できます。
リスク	この設定では、リスク評価ポリシーで設定されているとおりにデバイスの許容リスクレベルを指定します。リスク評価ポリシーの作成についての詳細は、リスク評価ポリシーの作成 を参照してください。 • 該当なし：リスクレベルはアクセスの条件ではありません。 • いずれかに一致：接続を許可するには、デバイスが許容可能なリスクレベルの範囲内である必要があります。このオプションを選択すると、許容可能なリスクレベルを選択できます。デフォルトのリスクレベルは「安全」（リスクなし）です。

宛先コンテンツのカテゴリ

これらのカテゴリは、ユーザーが利用可能なサイトでアクセスできるコンテンツのタイプを制御します。カテゴリ全体またはサブカテゴリを選択してコンテンツを指定できます。

アダルト

成人向けのコンテンツ。次のオプションを使用できます。

- アダルト
- 酒とタバコ
- デート
- ギャンブル
- ヌード
- わいせつな言葉
- ヌード
- わいせつな言葉
- パーソナルとデート
- ポルノ
- 大人のおもちゃ
- 水着と下着
- 武器

帯域幅

ネットワークのデータ転送速度に影響を与える可能性のあるサイト。次のオプションを使用できます。

- アプリケーションソフトウェアのダウンロード
- ダウンロードサイト
- インターネット通信とテレフォニー
- メディア共有
- オンラインストレージとバックアップ
- パークドメイン
- パークドメイン
- ピアツーピア
- パーソナルネットワークストレージとバックアップ
- フォトギャラリー
- シェアウェアとフリーウェア
- スパム
- ストリーミングメディア
- サーベイランス
- ビデオホスティング
- VVOIP

コンピュータおよび情報技術

コンピュータと IT をテーマにしたコンテンツ。次のオプションを使用できます。

- コンピュータとインターネットの情報
- コンテンツ配信ネットワーク
- 発信ダイヤルサイト
- DoH
- メール
- 情報技術
- インターネット
- インターネットポータル
- オンラインサービス
- リモートアクセス
- リモート制御
- 検索エンジン
- テクノロジとコンピューティング
- 更新サイト
- URL リダイレクタ
- URL 短縮サービス
- VPN サイト
- Web アプリケーション
- Web コラボレーション
- Web ホスティング
- Web インフラストラクチャ
- Web ベース電子メール

一般的な関心事 - ビジネス

ビジネスをテーマにしたコンテンツ。次のオプションを使用できます。

- バンキング
- ビットコイン
- ビジネス
- ビジネスと経済
- ビジネスアプリケーション
- 金融サービス
- 非営利団体
- オンライン支払い
- 専門機関
- 株価情報とツール

一般的な関心事 - パーソナル

個人的な関心事をテーマにしたコンテンツ。次のオプションを使用できます。

- 宿泊施設
- アドバイス
- 弁護
- アートとカルチャ
- 星占い
- オークションのブログとフォーラム
- ブログと Wiki
- 漫画
- セレブリティ
- 料理
- カルト
- 教育とリファレンス
- 教育機関
- エンターテイメント
- エンターテイメントとアート
- ファッションと美容
- 飲食
- ゲーム
- 一般組織
- 健康と医学
- ホーム&ガーデン
- ユーモアと風刺
- ハンティングとフィッシング
- 施設
- インターネットオークション
- インターネットショッピング
- 求人検索
- キッズ
- ライフスタイル
- モバイル通信
- 携帯電話
- 自動車
- ミュージック
- ニュース
- オカルト
- オピニオン
- ペイツーサーフ
- 個人
- 個人サイトとブログ
- 薬局
- 哲学と政治的主張
- 政治
- プレス
- 職能団体
- プロフェッショナルネットワーキング
- 公開情報
- 不動産
- レクリエーションと趣味
- 資料と調査
- 宗教と哲学
- レストランと食べ物
- 宗派
- ショッピング
- ソーシャルネットワーキング
- 社会
- スポーツ
- 推奨
- タブロイド
- トレーニングとツール
- 変換
- トラベル

行政

行政をテーマにしたコンテンツ。次のオプションを使用できます。

- 行政
- 行政事業
- 法的事項
- ミリタリ

潜在的責任

潜在的責任を問われるテーマのコンテンツ。次のオプションを使用できます。

- 試験のカンニング
- 著作権侵害
- 犯罪
- クリプトジャッキング
- 危険物
- 薬物
- 過激主義
- 不正
- ヘイトと差別
- 違法
- マリファナ
- 麻薬
- プロキシ回避とアノニマイザ
- 疑惑
- 自殺
- 暴力

生産性

生産性に影響する可能性のあるコンテンツをテーマにしたサイト。次のオプションを使用できます。

- 広告と分析
- チャットと IM
- 不十分なコンテンツ
- マーケティングと広告
- 生産性アプリケーション
- Web 広告
- Web と電子メールマーケティング

セキュリティリスク

悪意のあるサイトではないが、セキュリティ上のリスクがある可能性のある情報（スパイウェアについて説明するコンテンツなど）を共有しているサイト。次のオプションを使用できます。

- ボットネットワーク
- コマンドと制御
- Web サイト侵入
- DDoS
- DNS トンネリング
- 動的 DNS
- グレーサイト
- ハッキング
- マルウェア
- 混合コンテンツ
- フィッシング攻撃
- 潜在的に有害
- 望ましくない可能性のあるソフトウェア
- スパイウェア
- 疑わしい Web サイト
- 無許可マーケットプレイス
- ウェアーズ

不明

悪意ある可能性が不確実なサイトのコンテンツ。次のオプションを使用できます。

- その他
- 新規ドメイン
- 未解決
- 不明

ネットワークの宛先のリスクレベルの評価

管理コンソールを使用して、CylanceGATEWAY クラウドサービスによって分析および判定されたネットワーク宛先のリスクレベルを評価し、そのカテゴリとサブカテゴリを特定できます。この機能を使用すると、CylanceGATEWAY エージェントが宛先にアクセスしようとするときに、宛先をどのように分類するかを把握できます。これは、アクセス制御リスト（ACL）ルールを作成および更新して、宛先を許可またはブロックするのに役立ちます。悪意があると評価されていない宛先は、カテゴリとサブカテゴリのみを返します。

作業を始める前に： コンソールでこの機能にアクセスするには、管理者ロールが必要です。

1. 管理コンソールのメニューバーで、［保護］ > ［ネットワークの脅威］をクリックします。
2. テキストフィールドに、宛先の IP アドレス、FQDN、または URL を入力します。
3. ［分析］をクリックします。

アクセス制御リストの設定

CylanceGATEWAY では、5 分ごとに既存の宛先への接続を評価します。評価の際、CylanceGATEWAY では、ACL ルールが再適用されます。場合によっては、確立されている接続が切断されることがあります。これは、ユーザーのリスクレベルが変更された場合や、接続の確立後に宛先のレピュテーションが更新された場合などに発生します。

作業を始める前に： 組織のニーズに合わせてプライベートネットワークが定義されていることを確認してください。手順については、「プライベートネットワークの定義」を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［ネットワーク］の順にクリックします。
2. ［アクセス制御リスト］タブをクリックします。

3. ルールのドラフトセットが処理中であるという通知が確認された場合は、［ドラフトルール］タブをクリックします。

   処理中のルールのドラフトセットがない場合、更新を行うとルールのドラフトセットが作成されます。
4. 次の操作のいずれかを実行します。

   - ルールまたはドラフトルールを検索するには、🔍 をクリックして、事前定義された範囲と条件を 1 つ以上選択して、基準を指定します。設定を表示するルールをクリックします。✕ をクリックすると検索がリセットされます。検索の詳細については、「ACL ルールとネットワークサービスの検索」を参照してください。
   - リストの最後に新しいルールを追加するには、［ルールを追加］をクリックします。
   - 既存ルールの上または下に新しいルールを追加するには、既存のルールの行にある ··· をクリックし、［上のルールを追加］または［下のルールを追加］を選択します。
   - ルールをコピーして既存ルールの上または下に追加するには、既存ルールの行にある ··· をクリックして、［上のルールをコピー］または［下のルールをコピー］を選択します。
   - 既存ルールを編集するには、ルールの名前をクリックします。
   - ルールを無効にするには、そのルールの行にある 🟢 をクリックします。
   - ルールを有効にするには、そのルールの行にある ⚫ をクリックします。
   - ルールを削除するには、そのルールの行にある ··· をクリックし、［ルールの削除］を選択します。
   - ルールの順序を変更するには、［順序］をクリックし、リスト内で矢印を使用してルールを上下に移動します。
   - ブロックされている悪意のある宛先にユーザーがアクセスする必要がある場合（脅威調査の実施など）に、ルールを追加してそのトラフィックを許可するには、次の設定で［ルールを追加］をクリックします。このルールは、宛先へのアクセス許可に関するルールの中で、順序が最初になっている必要があります。

     - アクション：許可
     - ［ネットワーク保護に対するアクセス試行を確認］チェックボックス：オフ
     - ターゲット：いずれかに一致。宛先アドレスを追加します。
     - ユーザーまたはグループ：いずれかに一致。宛先へのアクセスを必要とするユーザーまたはグループを追加します。
5. ルールの追加または編集を選択した場合は、ACL ルールのパラメーターを指定して［保存］をクリックします。
6. ［ルールをコミット］をクリックして変更を ACL に適用します。

   また、後でページを離れてドラフトルールに戻ることもできます。ドラフト ACL をコミットすると、ドラフトルールリストを持つ他のすべての管理者は、古いドラフトを破棄するように求められます。

ネットワーク保護の構成

CylanceGATEWAY が脅威を検出して対応するさまざまな方法を設定できます。宛先へのアクセスを許可するようにアクセス制御リスト（ACL）ルールを構成しても、引き続き CylanceGATEWAY は、潜在的な脅威が特定された場合に宛先へのユーザーアクセスをブロックできます。［ネットワークイベント］画面と［アラート］表示に表示できる情報や、SIEM ソリューションまたは syslog サーバーに送信される情報（設定されている場合）を制御することもできます。追加のネットワーク保護を有効にする場合は、個々の ACL ルールで［ネットワーク保護に対してアドレスを確認］パラメーターが選択されていることを確認します。この設定はデフォルトで有効になっています。

- 署名検出：署名検出を使用することで、ネットワーク接続の署名を使ってディープネットワーク脅威検出を有効にできます。署名検出を有効にしておくと、ACL ルールと宛先が一致した場合、CylanceGATEWAY は脅威の検出された接続を自動的にブロックし、ネットワーク保護のチェックをします。署名検出を無効にすると、脅威はログに記録されますが、接続はブロックされません。検出のリストとそのアクションの詳細については、「ネットワークアクティビティの表示」を参照してください。署名検出はデフォルトで有効になっています。
- 宛先防御：宛先評価を使用して、指定したリスクレベル（低、中、高）に一致する、潜在的に悪意のある IP アドレスおよび FQDN をブロックできます。有効にした場合、デフォルトのリスクレベルは高にされます。ACL ルールと宛先が一致した場合、CylanceGATEWAY はログに記録して、リスクレベル設定に一致した宛先への接続を自動的にブロックし、ネットワーク保護を確認します。宛先防御を無効にすると、脅威はログに記録されますが、接続はブロックされません。検出のリストとそのアクションの詳細については、「ネットワークアクティビティの表示」を参照してください。宛先評価はデフォルトで有効になっています。

  リスクレベルの特定では、機械学習（ML）モデルと静的 IP レピュテーションデータベースの組み合わせを用いて、宛先に潜在的な脅威が含まれているかを判断しています。

  - ML モデル：ML モデルでは、ユーザーがアクセスする可能性のある宛先に対して信頼レベルを割り当てます。ML モデルは、宛先に潜在的な脅威が含まれている可能性の有無を継続的に学習します。
  - IP レピュテーションデータベース：IP レピュテーションデータベースは、オープンおよび商用の IP レピュテーションフィードに基づき、IP アドレスに信頼レベルを割り当てます。CylanceGATEWAY はレピュテーションフィードを参照して、IP アドレスのリスクレベルを判断します。CylanceGATEWAY は、特定の宛先を危険と判定したベンダーの数とソースの信頼性を考慮してリスクレベルを割り当てます（たとえば、大部分のソースと IP レピュテーションエンジンによって潜在的な脅威を含む宛先だと確認された場合、CylanceGATEWAY はその宛先に高いリスクレベルを割り当てます）。リスクレベルの詳細については、「宛先評価リスクのしきい値」を参照してください。

  CylanceGATEWAY は、ML モデルと IP レピュテーションデータベースを組み合わせて使用し、悪意のある脅威を含む可能性があると特定された IP レピュテーション検出に、動的リスクカテゴリとサブカテゴリを自動的に適用します。データベースは継続的に変更され、宛先エントリが追加または削除されます。動的リスクとして分類されたネットワークイベントに関する追加のメタデータと詳細は、［ネットワークイベント］画面で表示できます。動的リスクカテゴリには、次のサブカテゴリがあります。

• ビーコン • コマンドと制御 • DNSトンネリング	• マルウェア • フィッシング攻撃 • 潜在的に有害	• 疑わしい Web サイト • ドメイン生成アルゴリズム（DGA）

宛先評価リスクのしきい値

設定した最小しきい値に基づいて、悪意のある可能性のある宛先へのネットワークアクセスを CylanceGATEWAY がブロックする必要があるかを指定できます。

項目	説明
高	このリスクカテゴリは、80% を超える信頼度にて、宛先が有害または悪意あるものであることを示しています。
中	このリスクカテゴリは、60〜80% の信頼度にて、宛先がサイバー脅威である可能性を示しています。

項目	説明
低	このリスクカテゴリは、50〜60% の信頼度にて、疑わしい脅威、または潜在的な脅威が宛先に含まれていることを示しています。

ネットワーク保護設定の構成

［ネットワークイベント］画面で有効にし、表示する検出を指定できます。また、SIEM ソリューションまたは syslog サーバーに送信される情報も指定できます。CylanceGATEWAY が悪意のある可能性のある宛先への接続をブロックするたびに、ユーザーにメッセージを表示するように CylanceGATEWAY を構成することもできます。利用可能なリスクレベルについては、宛先評価リスクのしきい値を参照してください。ネットワーク保護設定を構成すると、CylanceGATEWAY により、［アラート］表示に表示されるアラートが生成されます。詳細については、「Cylance Endpoint Security サービスにわたるアラートの管理」を参照してください。

作業を始める前に： 各 ACL ルールで［ネットワーク保護に対するアクセス試行の確認］が選択されていることを確認してください。ACL の詳細については、ネットワークアクセスの制御 を参照してください。

1. メニューバーで、［設定］ > ［ネットワーク］をクリックします。
2. ［ネットワーク保護］タブをクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
有効にする検出を指定し、検出によってブロックされたときにユーザーに通知するかどうかを指定します。	**a.** ［保護］タブをクリックします。 **b.** CylanceGATEWAY が接続をブロックしたときにユーザーにメッセージを表示したい場合は、［ブロックされた通知メッセージをデバイスに表示します］を選択します。 **c.** ［メッセージ］フィールドに、ユーザーに表示するメッセージを入力します。 **d.** 署名検出をオンにするには、［署名検出を有効にする］を選択します。 有効にすると、アラートは、ブロックされた署名検出について生成され、［アラート］表示に表示されます。無効にすると、アラートは生成されません。詳細については、「Cylance Endpoint Security サービスにわたるアラートの管理」を参照してください。 **e.** 宛先のレピュテーションをオンにするには、［宛先のレピュテーションを有効にする］を選択し、ブロックする潜在的に悪意のある IP アドレスおよび FQDN の最小リスクレベルを選択します。 有効にすると、設定したリスクレベルに基づいてアラートが生成され、［アラート］表示に表示されます。たとえば、リスクレベル［中以上］を選択した場合、中または高リスクであるアラートが［アラート］表示に表示されます。無効にすると、デフォルトでは、CylanceGATEWAY が高リスクと見なしたアラートが生成され、［アラート］表示に表示されます。

タスク	手順
［ネットワークイベント］画面に表示する検出を指定および制御します。 メモ：トラフィックプライバシーを有効にし、ネットワークアクセス試行が ACL ルールと一致した場合、ネットワークアクセス試行は［ネットワークイベント］画面に表示されません。	**a.** ［レポート］タブをクリックします。 **b.** 許可されているネットワークイベントの署名検出を表示するには、［許可された署名検出イベントを表示］を有効にします。デフォルトでは、自動的にブロックされた署名検出は、［ネットワークイベント］画面に表示されます。 **c.** 許可されたネットワークイベントの宛先のレピュテーションの検出を表示するには、［許可された宛先のレピュテーションイベントを表示］を有効にし、表示する潜在的に悪意のある IP アドレスの最小リスクレベルを選択します。このオプションが無効になっている場合、署名イベントは通常の許可されたトラフィックとして記録されます。 **d.** DNS トンネリング検出を表示するには、［**DNS** トンネリング検出を表示］を有効にし、クライアントから DNS サーバーへの DNS トラフィックの分析に基づいて潜在的な脅威の最小リスクレベルを選択します。デフォルトでは、このリスクレベルは［中］です。 **e.** ゼロデイ検出を表示するには、［ゼロデイ検出を表示］を有効にし、以前に特定されていない新たに特定された悪意のある宛先の最小リスクレベルを選択します。デフォルトでは、このリスクレベルは［中］です。

タスク	手順
［アラート］表示に表示し、SIEM ソリューションまたは syslog サーバーに送信する検出を指定および制御します。 メモ：トラフィックプライバシーを有効にし、ネットワークアクセス試行が ACL ルールと一致した場合、ネットワークアクセス試行は SIEM ソリューションまたは syslog サーバー（設定されている場合）に送信されません。	**a.** ［共有］タブをクリックします。 **b.** 署名検出がある、許可またはブロックされたネットワークイベントとアラートを送信するには、［署名検出イベントを共有］を有効にします。有効にすると、デフォルトでは、ブロックされた署名検出は、［アラート］表示に表示され、SIEM ソリューションまたは syslog サーバーに送信されます。必要に応じて、［許可されたイベント］を選択して、許可されたイベントを送信します。 **c.** 設定した最小限のリスクレベルに基づいて、許可またはブロックされた宛先のレピュテーション検出があるネットワークイベントとアラートを送信するには、［宛先のレピュテーションイベントを共有］を有効にします。有効にすると、デフォルトでは、ブロックされた宛先のレピュテーションイベントは、［アラート］表示に表示され、SIEM ソリューションまたは syslog サーバーに送信されます。必要に応じて、［許可されたイベント］を選択して、許可されたイベントを送信します。 **d.** 設定した最小限のリスクレベルに基づいて、DNS トンネリング検出があるネットワークイベントとアラートを送信するには、［**DNS** トンネリング検出を共有］を選択します。デフォルトでは、このリスクレベルは［中］です。 **e.** 設定した最小限のリスクレベルに基づいて、ゼロデイ検出があるネットワークイベントとアラートを送信するには、［ゼロデイ検出を共有］を選択します。デフォルトでは、このリスクレベルは［中］です。 **f.** ACL ルールによってブロックされたネットワークイベントを送信するには、［ブロックされた **ACL** イベントを共有］を有効にします。ブロックされた ACL イベントと許可された ACL イベントは、［アラート］表示に表示されません。

4. ［保存］をクリックします。

ACL ルールとネットワークサービスの検索

CylanceGATEWAY に追加した ACL ルールとネットワークサービスは、検索することができます。CylanceGATEWAY には、検索条件として定義済みの範囲と条件が用意されています。

検索では、範囲と条件で検索フィールドに指定された条件に応じて検索結果が返されます。たとえば、名前に「IT」が含まれるルールの ACL ルールを検索すると（たとえば、範囲 = Name、条件 = Contains、検索条件 = IT）、指定された「IT」がルール名に含まれるすべてのルールが返されます。

メモ：コミットされた ACL ルールを検索するか、またはドラフト ACL ルールを検索できます。コミットされた ACL ルールとドラフト ACL ルールにまたがる検索は行えません。

複数の範囲と検索条件が指定されるような高度な検索では、検索エンジンは検索条件の間に AND 演算子を使用します。すべての検索結果に、指定されたすべての条件が含まれます。たとえば、サービスの名前が「example」で FQDN が example.com であるネットワークサービスを検索する場合（例：範囲 = Name、条件 = Contains、検索条件 = Example かつ範囲 = FQDN、条件 = Contains、検索条件 = example.com）、両方の条件を含むすべてのルールが返されます。

検索では大文字と小文字は区別されません。たとえば、Example を検索しても example を検索しても、同じ結果が得られます。

ソース IP ピン設定の使用

CylanceGATEWAY により、ソース IP ピン設定に使用できる専用 IP アドレスを取得できます。多くの SaaS アプリケーションでは、特定の範囲の信頼できる IP アドレスからの接続のみにアクセスを制限する方法として、ソース IP のピン設定を許可しています。組織では、既にこの方法を使用して、SaaS アプリケーションテナントへのアクセスを、組織のネットワークに接続されているデバイスが使用する IP アドレスに制限している場合があります。リモートユーザーの場合は、ソース IP ピン設定を使用して、組織の VPN を使用せずに、ユーザーとクラウドベースのアプリケーション間のアクセスをセキュリティで保護することができます。これにより、ネットワーク上のトラフィックを軽減し、ユーザーの接続を向上させることができます。

CylanceGATEWAY に対してソース IP ピン設定を有効にしている場合、ソース IP ピン設定ネットワーク設定には、BlackBerry が組織専用に割り当てた IP アドレスが表示されます。

専用の IP アドレスを取得するには、support.blackberry.com/community にアクセスして、記事 96499 を参照してください。

割り当てられた IP アドレスを表示するには、メニューバーで、［設定］ > ［ネットワーク］の順にクリックしてから ［ソース **IP** をピン設定］タブを選択します。

Gateway サービスのオプション設定

Gateway サービスポリシーを設定して、アプリでトンネルを使用できるようにするかどうかを制御する OS 固有のオプションを指定したり、評価の低い宛先にユーザーがアクセスできるようにするかどうかを指定したり、ユーザーがトンネルを確立する前に本人確認をするようにしたりします。

Gateway サービスポリシーのパラメーター

CylanceGATEWAY などの EMM ソリューションによってアクティブ化されているデバイス上で BlackBerry UEM を設定する場合は、EMM ソリューションでオプションを指定して、デバイス上での CylanceGATEWAY の動作を制御することもできます。

項目	説明
一般的な情報	
名前	これはルールの名前です。
説明	これは、ルールの目的の簡単な説明です。
エージェントの設定	

項目	説明
デバイスが BlackBerry UEM または Microsoft Intune で管理されている場合のみ Gateway の実行を許可	この設定では、ユーザーが CylanceGATEWAY を使用する前に、iOS、Android、または Chromebook デバイスを BlackBerry UEM または Microsoft Intune で管理する必要があることを指定します。 この機能の使用条件は次のいずれかのとおりです。 • BlackBerry UEM：BlackBerry UEM コネクタが Cylance Endpoint Security テナントに追加され、BlackBerry UEM からアプリが送信されていること。 • Intune：Microsoft Intune コネクタが Cylance Endpoint Security テナントに追加されていて、統合が適用されるデバイスタイプと Intune ユーザーグループを定義するアプリ設定ポリシーが作成されていること。 詳細については、次を参照してください。 Cylance Endpoint Security を MDM ソリューションに接続して、デバイスが管理されているかどうかを確認
Gateway が管理対象 VPN として構成されている MDM 管理対象デバイスでのみ Gateway のトンネル確立を許可	CylanceGATEWAY の仕事モードでそのデバイスにトンネルを作成する前に、CylanceGATEWAY が VPN プロバイダーとして設定されている組織のモバイルデバイス管理（MDM）に、デバイスを登録させるようにすることができます。 この機能は、次のデバイスでサポートされています。 • macOS 2.7 以降向けの CylanceGATEWAY エージェント • iOS 2.14 以降向けの CylancePROTECT Mobile アプリ
デバイスで CylancePROTECT Desktop もアクティブ化されている場合のみ、Gateway の実行を許可	この設定を行うには、ユーザーにより CylancePROTECT Desktop はインストール済みで、同じテナントからアクティブ化されている必要があります。この機能は、次のデバイスでサポートされています。 • Windows for CylanceGATEWAY を実行している Windows デバイスのみ。 • macOS 3.0 以降および CylancePROTECT Desktop for CylanceGATEWAY 2.0.17 以降を実行している macOS デバイス。CylancePROTECT Desktop のバージョン 3.0 以前を実行しているデバイスでこの機能を有効にすると、トンネルは期待どおりに機能にしない場合があります。

項目	説明
セーフモード	ユーザーに対してセーフモードを有効にできます。セーフモードの場合、CylanceGATEWAY は、アプリおよびユーザーが潜在的に悪意のある宛先にアクセスできないようにブロックし、DNS 要求をインターセプトすることで、許容可能な使用ポリシー（AUP）を強制します。CylanceGATEWAY クラウドサービスは、設定されている ACL ルールとネットワーク保護設定（DGA、フィッシング、マルウェアなどの DNS トンネリングおよびゼロデイ検出など）に照らして各 DNS クエリを評価し、リアルタイムで要求を許可またはブロックするようエージェントに指示します。許可された場合、DNS 要求が、正常にベアラーネットワーク経由で完了します。それ以外の場合、CylanceGATEWAY エージェントが、通常の応答を上書きしてアクセスを防止します。 有効にすると、仕事モードが無効になっているときにセーフモードが自動的に有効になります。Windows デバイスで有効にすると、エージェントは起動時にシステムトレイ内で最小化されます。セーフモードを有効にしても、ユーザーはエージェントを開いたり、仕事モードを有効または無効にしたりすることができます（ユーザーのポリシーでこのような操作が許可されている場合）。 セーフモードイベントは、［CylanceGATEWAY イベント］画面と［アラート］表示に表示され、SIEM ソリューションまたは syslog サーバーに送信されます（設定されている場合）。 メモ：セーフモードを有効にすると、CylanceGATEWAY トンネルを使用しないすべての DNS トラフィックが保護されます（たとえば、Gateway が管理対象 VPN、アプリごとのトンネル、分割トンネルとして設定されている MDM 管理対象デバイスでのみトンネルを確立できるようにします）。 この機能は、次のデバイスでサポートされています。 • Windows 2.8 以降向けの CylanceGATEWAY エージェント。 • macOS 2.7 以降向けの CylanceGATEWAY エージェント。 メモ：この機能は、DoT（DNS-over-TLS）および DoH（DNS-over-HTTPS）プロトコルでセキュアな DNS を使用する環境ではサポートされていません。DoT または DoH を使用して送信された DNS クエリは、CylanceGATEWAY では表示できません。 セーフモードと **macOS** 用の **CylanceGATEWAY** エージェント：macOS では、CylanceGATEWAY エージェントはシステム拡張機能を使用してセーフモードを実装します。「P7E3XMAM8G:com.blackba.big3.gatewayfilter」システム拡張機能を許可リストに追加すると、ユーザーが操作しなくても、CylanceGATEWAY エージェントがアクティブ化されたときに自動的にこれをロードできます。それ以外の場合は、アクティベーション中にプロンプトが表示されたときに、CylanceGATEWAY システム拡張機能を許可するようにユーザーに指示します。システム拡張機能を許可リストに追加する方法については、macOS のドキュメントを参照してください。CylanceGATEWAY エージェントをアクティブ化してセーフモードを使用する方法の詳細については、ユーザーガイドの「CylanceGATEWAY エージェントでのセーフモードのアクティブ化」を参照してください。 セーフモードとサードパーティ **VPN**：ご利用の環境がセーフモードとサードパーティ VPN を使用するように設定されている場合は、VPN DNS 設定を確認し、必要に応じてこの設定を調整して、VPN トンネルを使用するように定義されたトラフィックの DNS クエリのみをルーティングするようにします。セーフモードを有効にしても、VPN DNS 設定を確認しなかった場合、VPN が想定どおりに動作しない可能性があります。デフォルトでは、多くの VPN の設定で、VPN トンネルがアクティブの場合にすべての DNS トラフィックが VPN 経由でルーティングされます。

項目	説明
［サインインしたら CylanceGATEWAY を起動］設定を適用する	この設定では、macOS または Windows デバイスで、ユーザーがログインしたときに、CylanceGATEWAY エージェントを自動的に起動するかどうかを指定します。このポリシー設定は、エージェントの［サインインしたら CylanceGATEWAY を起動］設定よりも優先されます。 BlackBerry では、Gateway サービスポリシーでこのオプションを有効にすることが推奨されています。 この機能は、次のデバイスでサポートされています。 • macOS 2.7 以降向けの CylanceGATEWAY エージェント • Windows 2.7 以降向けの CylanceGATEWAY エージェント
ユーザーのサインイン時に CylanceGATEWAY を自動的に起動する	この設定では、ユーザーがデバイスにサインインしたときに CylanceGATEWAY エージェントが自動的に開始されますが、ユーザーが手動でエージェントを停止することもできます。Windows デバイスに対してこの設定と［仕事モードを自動的に有効化］の両方を有効にすると、エージェントは起動時にシステムトレイ内で最小化されます。 この設定は、［［サインインしたら CylanceGATEWAY を起動］設定を適用する］が有効な場合にのみ有効です。
［仕事モードを自動的に有効にする］設定を適用する	この設定では、macOS または Windows デバイスで、CylanceGATEWAY エージェントが起動したときに、エージェントで仕事モードを有効にするかどうかを指定します。このポリシー設定は、エージェントの［仕事モードを自動的に有効化］設定よりも優先されます。 この機能は、次のデバイスでサポートされています。 • macOS 2.7 以降向けの CylanceGATEWAY エージェント。 • Windows 2.7 以降向けの CylanceGATEWAY エージェント
仕事モードを自動的に有効化	この設定では、CylanceGATEWAY エージェントの起動時に仕事モードが自動的に有効になりますが、エージェント起動後にユーザーが手動で仕事モードを有効または無効にすることもできます。Windows デバイスに対してこの設定と［ユーザーのサインイン時に CylanceGATEWAY を自動的に起動する］の両方を有効にすると、エージェントは起動時にシステムトレイ内で最小化されます。 この設定は、［仕事モードを自動的に有効化］が有効になっている場合にのみ有効です。
トンネル使用	

項目	説明
アプリごとのトンネル	この設定では、CylanceGATEWAY クラウドサービスにトンネル経由でデータを送信できるアプリを指定します。許可されたアプリまたは制限されたアプリリストのいずれかを使用して、アプリごとのトンネルを設定できます。たとえば、［許可されたアプリ］オプションを選択してトンネルを使用できるアプリを指定してから、オプションを［制限対象アプリ］に変更すると、リストされたアプリではトンネルを使用できなくなります。 次のオプションを使用できます。 • トンネルを使用するアプリを指定するには、［許可されたアプリ］を選択します。他のアプリはトンネルを使用できません。システムアプリと Windows DNS は常にトンネルを使用します。このオプションを選択すると、設定された ACL ルールまたはネットワークアクセス制御ポリシーが適用されます。ACL ルールおよびネットワークアクセス制御ポリシーの詳細については、「ネットワークアクセスの制御」を参照してください。 • トンネルを使用できないアプリを指定するには、［制限対象アプリ］を選択します。他のすべてのアプリはトンネルを使用できます。 • ⊕ をクリックして、デスクトップアプリのフルパスを入力、パスにワイルドカードを含める、またはストアアプリの Windows パッケージファミリー名（PFN）を追加します。最大 200 のアプリケーションパスまたは PFN を組み合わせて指定できます。 パスにワイルドカードを含める場合は、次の点を考慮してください。 • パスごとに含めることができるワイルドカードは 1 つだけです。サポートされている形式は *\ です（例：%ProgramFiles%*Folder_Name**\Application_Name*.exe） • 次の場合、ワイルドカードはサポートされません。 • 環境変数の代わりに使用する場合 • パス内のルートディレクトリの代わりに使用する場合 • ディレクトリ名の一部に使用する場合（例：「C:\Win*\notepad.exe」）。 • 実行可能ファイル名で使用する場合（例：「C:\Windows*.exe」）。 ワイルドカードは、Windows 2.7 以降向けの CylanceGATEWAY エージェントを実行している Windows デバイスでサポートされています。 この機能は、次のデバイスでサポートされています。 • Windows 2.0.0.13 以降向けの CylanceGATEWAY • Android アプリを実行している Chromebook または CylancePROTECT Mobile デバイスユーザー。

項目	説明
アプリにトンネルの使用を強制	この設定では、すべての非ループバック接続がトンネルを使用する必要があります。このオプションを選択し、分割トンネルを有効にした場合、すべてのトラフィックがトンネルを使用します。Windows デバイスでは、このオプションを選択して分割トンネルを有効にしている場合、トンネルを使用しない接続は予期したとおりに機能しない可能性があります。この機能は、次のデバイスでサポートされています。 • macOS 10.15 以降および macOS for CylanceGATEWAY 2.0.17 以降を実行している管理対象外の macOS デバイス。 • iOS 14.0 以降および iOS アプリ 2.4.0.1731 以降を実行している管理対象外の CylancePROTECT Mobile デバイス。 • Windows for CylanceGATEWAY を実行している Windows デバイスのみ。
アプリがローカルネットワークを使用することを許可	これを設定すると、トンネル使用を強制されているアプリがローカルネットワークの宛先に到達可能になります。この機能は、次のデバイスでサポートされています。 • macOS 10.15 以降および macOS for CylanceGATEWAY 2.0.17 以降を実行している管理対象外の macOS デバイス。 • iOS 14.2 以降および iOS アプリ 2.4.0.1731 以降を実行している管理対象外の CylancePROTECT Mobile デバイス。 • Windows for CylanceGATEWAY 2.5 以降を実行している Windows デバイスのみ。 この設定は、［アプリにトンネルの使用を強制］が有効になっている場合にのみ有効です。
制限されたアプリからのネットワークトラフィックをブロック	この設定では、トンネルを使用できないアプリからの非ループバックネットワーク接続をすべて禁止します。この設定を選択しない場合、制限されたアプリはデフォルトのネットワーク接続を使用できます。この機能は、CylanceGATEWAY for Windows エージェントを実行しているデバイスでサポートされています。
他のWindowsユーザーにトンネルの使用を許可	この設定では、同じ Windows デバイスを使用するすべてのユーザーがトンネルを使用できるように指定します。このオプションを選択すると、アプリごとのトンネル基準が適用されます。このオプションを選択しない場合、他の Windows ユーザーが実行するアプリは制限対象アプリとして扱われます。
受信接続を許可	この設定では、非トンネル、非ループバックインターフェイスからの受信 TCP 接続および UDP フローを許可するよう指定します。CylanceGATEWAY では、トンネルを介して着信接続をルーティングしません。この機能は、CylanceGATEWAY for Windows エージェントを実行しているデバイスでサポートされています。
トンネルの再認証	

項目	説明
トンネルの再認証	この設定では、トンネル確立前に必要なユーザーの認証頻度を指定します。 この機能を有効にした場合、BlackBerry では、［認証の再利用を許可］オプションを設定して、ユーザーの再認証が必要になるまでの期間を指定することが推奨されています。 この機能は、次のデバイスでサポートされています。 • CylanceGATEWAY 2.5 以降向けの macOS • CylanceGATEWAY 2.5 以降向けの Windows
認証の再利用を許可	この設定を有効にすると、認証されてトンネルを確立したユーザーが再度の認証を必要とするまでの再利用期間を指定できます。再利用期間として設定可能な値は、最後の認証から 5 分から 365 日までの間です。たとえば、リセット期間を 10 日に設定した場合、トンネル確立前に必要なユーザーの再認証は、最初の認証から 10 日後になります。この設定はデフォルトで無効になっています。 メモ：［認証の再利用を許可］を有効にせずに、再利用期間を指定した場合、ユーザーはトンネルを確立するごとに認証を行う必要があります。 この設定は［トンネルの再認証］が有効になっている場合にのみ有効です。
猶予期間	この設定では、トンネル接続の確立が接続の切断から 2 分以内に行われた場合、ユーザーは認証なしでトンネルを再接続できます。デフォルトでは、トンネルの再認証をオンにした場合、このオプションは有効になります。 この設定は［トンネルの再認証］が有効になっている場合にのみ有効です。
分割トンネル	

項目	説明
分割トンネル	この設定では、パブリックの宛先へのトラフィックが CylanceGATEWAY をバイパスできるようにします。トンネルを経由する必要のある宛先の CIDR アドレスまたは FQDN を入力できます。ユーザー体験の向上を図るため、管理コンソールは FQDN の IP アドレス解決を定期的に更新しています。 メモ：FQDN アドレスはワイルドカードをサポートしていません。 分割トンネルを有効にすると、宛先への接続でトンネルを使用するように指定しない限り、許可されたパブリックの宛先への接続はトンネルおよび CylanceGATEWAY クラウドサービスをバイパスします。分割トンネルを有効にし、分割 DNS を有効にしなかった場合、トラフィックがパブリックの宛先にルーティングされる前に、設定されている ACL ルールに照らしてすべての DNS クエリが評価され、ネットワークアクセス制御が適用されます。トンネルを経由する必要のある宛先の CIDR アドレスまたは FQDN を入力できます。ソース IP のピン設定を使用している場合、ソース IP ピン設定用に設定されたすべての宛先でトンネルを使用する必要があります。 トンネリング設定または着信接続に変更を加えた場合、その変更を適用するには、CylanceGATEWAY および Windows デバイスにインストールされている macOS エージェント、または CylancePROTECT Mobile、iOS、および 64 ビット Android デバイスにインストールされている Chromebook アプリの仕事モードを無効にしてから有効にする必要があります。
分割 DNS	この設定を有効にすると、［プライベートネットワーク］>［DNS］>［前方ルックアップゾーン］設定にリストされているドメインの DNS ルックアップを、ネットワークアクセスコントロールが適用されているトンネルを介して実行できます。その他の DNS ルックアップはすべて、ローカル DNS を使用して実行されます。セーフモードを有効にした場合、Gateway トンネルを使用しない DNS トラフィックはセーフモードで保護されます。分割 DNS はデフォルトで無効になっています。 Android および 64 ビットの Chromebook デバイスでは、分割 DNS トンネルがサポートされていないため、アクセス制御が適用されているトンネルが使用されます。 この設定は［分割トンネル］が有効になっている場合にのみ有効です。

Gateway サービスオプションの設定

1. メニューバーで、［ポリシー］>［ユーザーポリシー］をクリックします。
2. ［**Gateway** サービス］タブをクリックします。
3. ［ポリシーを追加］をクリックします。
4. Gateway サービスポリシーのパラメーターを指定します。
5. ［追加］をクリックします。
6. トンネリング設定または着信接続に変更を加えた場合、その変更を適用するには、Windows および macOS デバイスにインストールされている CylanceGATEWAY エージェント、または iOS、Android、Chromebook デバイスにインストールされている CylancePROTECT Mobile アプリの仕事モードを無効にしてから有効にする必要があります。

終了したら：

- ポリシーをユーザーおよびグループに割り当てます。
- 必要に応じて、ポリシーをランク付けします。

EMM ソリューションでアクティブ化されたデバイスが CylanceGATEWAY トンネルを使用する方法の指定

CylanceGATEWAY は、クラウドネイティブの人工知能（AI）支援ゼロトラストネットワークアクセス（ZTNA）ソリューションです。デバイスで CylanceGATEWAY が有効になっている場合、そのデバイスは、CylanceGATEWAY をゼロトラストネットワークアクセスプロファイルを確立する VPN プロバイダーとして認識します。BlackBerry UEM または別の EMM ソリューションを使用してデバイスをアクティブ化した場合、EMM ソリューションで設定した VPN オプションは、デバイス上での CylanceGATEWAY の動作に影響を与える可能性があります。

iOS デバイスの場合、BlackBerry UEM または別の EMM ソリューションを使用してアプリ単位で VPN を設定し、CylanceGATEWAY トンネル経由でデータを送信するアプリを指定できます。VPN 管理とアプリ管理を許可するには、デバイスをアクティブ化する必要があります。詳細については、以下を参照してください。

- iOS デバイスで CylanceGATEWAY を使用するアプリの指定
- Microsoft Intune 環境の iOS デバイスで CylanceGATEWAY を使用するアプリの指定

Android デバイスの場合、BlackBerry UEM または別の EMM ソリューションを使用して、CylanceGATEWAY を常に有効にし、ユーザーが作業プロファイルの VPN 設定を変更するのを禁止することができます。詳細については、以下を参照してください。

- Android Enterprise デバイスでの CylanceGATEWAY オプションの指定
- Microsoft Intune 環境の Android Enterprise デバイスでの CylanceGATEWAY オプションの指定

iOS デバイスで CylanceGATEWAY を使用するアプリの指定

iOS デバイスで、組織でアプリ単位の VPN 設定をサポートする EMM ソリューションを使用してデバイスを管理している場合、デバイスを設定して、CylanceGATEWAY を VPN プロバイダーとして認識させ、アプリ単位の VPN を設定して、CylanceGATEWAY トンネルを通してどのアプリがデータを送信するかを指定させることができます。

アプリベーストンネルオプションを設定するには、EMM ソリューションを使用してアクティブ化された iOS デバイスでの VPN 管理とアプリ管理の権限が必要です。BlackBerry UEM で CylanceGATEWAY トンネルを使用するアプリを指定するには、次の手順を実行します。

1. UEM 管理コンソールで、CylanceGATEWAY を通して UEM にデータを送信するアプリを追加し、それらをユーザーに割り当てます。

   CylanceGATEWAY トンネルを使用するのは、ユーザーに割り当てられたアプリだけです。デフォルトのブラウザーまたは CylancePROTECT Mobile アプリをユーザーに割り当てないでください。割り当てた場合、デバイスは CylanceGATEWAY とトンネルを確立することができなくなります。

   「ユーザーのプライバシー 」および「ユーザーのプライバシー - ユーザー登録 」アクティベーションタイプのデバイスでは、割り当てられた内部アプリと、Apple ボリューム購入プログラムを通してライセンスされたアプリだけが、トンネルを使用できます。
2. 次のアクティベーションタイプのいずれかを割り当てるアクティベーションプロファイルを作成します。
   - MDM 制御
   - ユーザーのプライバシー - ユーザー登録

- VPN 管理とアプリ管理が有効になっている ユーザーのプライバシー

3. VPN プロファイルを作成し、次の設定を含めます。

設定	説明
接続タイプ	カスタム
VPN バンドル ID	com.blackberry.protect
サーバー	この設定では、VPN サーバーの FQDN または IP アドレスを指定します。値は 127.0.0.1 にする必要があります。
認証の種類	パスワード
パスワード	このフィールドは空白のままにします
per-app VPN を有効にする	選択済み
ドメイン設定	CylanceGATEWAY トンネルを介して接続を確立できるドメインを指定します。ドメインを指定すると、割り当てられたアプリは、指定されたドメインへの接続にのみトンネルを使用します。Safari、カレンダー、連絡先、メールのドメイン、および apple-app-site-association ファイルに含まれているドメインを指定できます。トンネルを使用しないドメインを指定することもできます。 「ユーザーのプライバシー 」および「ユーザーのプライバシー - ユーザー登録 」アクティベーションタイプを持つデバイスの場合、［サーバー］フィールドで指定されたルートドメインの子ではないドメインを指定すると、デバイスは無効なドメインだけでなく、VPN プロファイル全体を無視します。
アプリの自動接続を許可する	アプリが自動的に接続を開始できるように指定するには、このオプションを選択します。 メモ： CylanceGATEWAY トンネルを介した接続は、CylanceGATEWAY がデバイスの CylancePROTECT Mobile アプリで有効になっている場合にのみ開始できます。
トラフィックトンネル	IP レイヤー

4. プロファイルをユーザーに割り当て、デバイスをアクティブにするように指示します。

Microsoft Intune 環境の iOS デバイスで CylanceGATEWAY を使用するアプリの指定

CylanceGATEWAY が VPN プロバイダーとして認識されるように iOS デバイスを設定し、CylanceGATEWAY トンネルを経由してデータを送信するアプリを per-app VPN の設定で指定できます。Microsoft Intune では、CylanceGATEWAY に影響する設定を構成できます。

アプリベーストンネルオプションを設定するには、Intune を使用してアクティブ化された iOS デバイスでの VPN 管理とアプリ管理の権限が必要です。Intune で CylanceGATEWAY トンネルを使用するアプリを指定するには、次の手順を実行します。

1. Microsoft Intune 管理センターで、CylanceGATEWAY を通して Intune にデータを送信するアプリを追加し、それらをユーザーに割り当てます。

   CylanceGATEWAY トンネルを使用するのは、ユーザーに割り当てられたアプリだけです。デフォルトのブラウザーまたは CylancePROTECT Mobile アプリをユーザーに割り当てないでください。割り当てた場合、デバイスは CylanceGATEWAY とトンネルを確立することができなくなります。
2. VPN プロファイルを作成し、次の設定を含めます。iOS および iPadOS の設定の詳細については、「iOS デバイスおよび iPadOS デバイスに VPN 設定を追加する」を参照してください。

設定	説明
接続タイプ	カスタム VPN
VPN サーバーアドレス	値は 127.0.0.1 にする必要があります。この値は CylanceGATEWAY では使用されません。
認証方法	ユーザー名とパスワード
分割トンネル	無効化
VPN 識別子	iOS デバイスの場合は、com.blackberry.protect と入力します macOS デバイスの場合は、com.blackberry.big と入力します
	• キー：*key* • 値：*value* Microsoft Intune では、1 つのカスタム属性が必要とされます。CylanceGATEWAY では、この設定は使用されません。任意の属性を入力できます。
自動 VPN	Per-app VPN
プロバイダータイプ	パケットトンネル
Safari の URL	CylanceGATEWAY トンネルを介して接続を確立できるドメインを指定します。Intune では、ドメイン内のワイルドカードはサポートされていません。これらは暗黙的に使用されます。たとえば、「org」と入力した場合は、「*.org」を意味します。 メモ：CylanceGATEWAY トンネルを介した接続は、CylanceGATEWAY がデバイスの CylancePROTECT Mobile アプリで有効になっている場合にのみ開始できます。 blackberry.com を管理対象の Safari VPN として指定すると、新たにアクティブ化する CylancePROTECT Mobile アプリはアクティブ化されなくなります。

3. 必要に応じて、ユーザーに CylancePROTECT Mobile アプリをアクティブ化してもらいます。

Android Enterprise デバイスでの CylanceGATEWAY オプションの指定

Android デバイスの場合、CylanceGATEWAY サービスポリシーを使用して、CylanceGATEWAY トンネルを介してデータを送信するアプリを指定できます。組織が BlackBerry UEM などの EMM ソリューションを使用して Android Enterprise デバイスを管理している場合は、CylanceGATEWAY に影響する EMM プロバイダーの設定を構成できます。

BlackBerry UEM で IT ポリシーを使用して、CylanceGATEWAY がデバイスで常に有効になっているかどうか、およびユーザーがデバイスの仕事用プロファイルで VPN 設定を変更できるかどうかを指定できます。UEM IT ポリシールールの詳細については、UEM IT のポリシーリファレンスをダウンロードしてください。

1. UEM 管理コンソールで、IT ポリシーを作成または編集します。
2. 次の操作のいずれかを実行します。
   a) CylanceGATEWAY を常に有効にするには、Android 仕事用プロファイルに次の IT ポリシールールを設定します。

IT ポリシールール	説明
VPN を強制的に常時オンにする	選択済み
VPN 接続に BlackBerry Secure Connect Plus を使用する	未選択
VPN アプリパッケージ ID	com.blackberry.protect
仕事用アプリで VPN のみを使用するように強制する	未選択。このオプションが選択されている場合、デバイスで CylancePROTECT Mobile アプリをアクティブ化することはできません。
VPN から除外される仕事用アプリ	［仕事用アプリで VPN のみを使用するように強制する］ルールが選択されている場合、 • 「com.android.chrome」と入力して、Chrome ブラウザがネットワークにアクセスし、VPN が接続される前に、デバイスで CylancePROTECT Mobile アプリをアクティブ化できるようにする必要があります。このルールは、Android OS 10.0.0 以降を実行しているデバイスに適用されます。 • 「com.android.protect」と入力した場合、CylancePROTECT Mobile アプリは、VPN が接続されていないときにのみ、VPN を使用せずにネットワークにアクセスできます。

   b) ［**VPN** を強制的に常時オンにする］が選択されていない場合にデバイスが CylanceGATEWAY トンネル経由でデータを送信できるようにするには、［仕事用領域でユーザー設定 **VPN** を許可する］を選択します。

［**VPN** を強制的に常時オンにする］も［仕事用領域でユーザー設定 **VPN** を許可する］も選択されていない場合、デバイスは仕事用アプリがトンネルを介してデータを送信することを許可しません。

3. ユーザーに IT ポリシーを割り当てます。

Chromebook デバイスでの **CylanceGATEWAY** オプションの指定

64 ビット Chromebook デバイスの場合、CylanceGATEWAY サービスポリシーを使用して、CylanceGATEWAY トンネルを介してデータを送信するアプリを指定できます。組織で Google ドメインを使用して Chrome OS Enterprise デバイスを管理している場合は、CylanceGATEWAY を常に有効にし、ユーザーが CylancePROTECT Mobile アプリで VPN 設定を変更できないようにすることができます。手順については、https://support.google.com/ にアクセスし、「バーチャルプライベートネットワークを設定する（Android VPN アプリ）」を参照してください。Chromebook Enterprise デバイスの管理を、BlackBerry UEM などの EMM プロバイダーに拡張することもできます。詳細については、「Chrome OS デバイスの管理を BlackBerry UEM に拡張する」を参照してください。

Microsoft Intune 環境の **Android Enterprise** デバイスでの **CylanceGATEWAY** オプションの指定

Android デバイスの場合、Gateway ポリシーを使用して、CylanceGATEWAY トンネルを介してデータを送信するアプリを指定できます。Microsoft Intune では、CylanceGATEWAY に影響する設定を構成できます。

設定プロファイルを使用して、CylanceGATEWAY がデバイスで常に有効になっているかどうか、およびユーザーがデバイスのプロファイルで VPN 設定を変更できるかどうかを指定できます。構成プロファイル設定の詳細については、「VPN を設定するための Android Enterprise デバイス設定」を参照してください。

1. Microsoft Intune 管理センターで、構成プロファイルを作成します。次の設定を設定します。
   - プラットフォーム：Android Enterprise
   - プロファイルタイプ：デバイスの制限
2. 構成プロファイルに次のルールを設定します。

設定	説明
常時オン VPN	有効化
VPN クライアント	カスタム
パッケージ ID	com.blackberry.protect
LockDown モード	設定されていません。このオプションが選択されている場合、CylancePROTECT Mobile アプリがアクティブ化されないことがあります。

3. 設定プロファイルをユーザーに割り当てます。
4. CylancePROTECT Mobile アプリをユーザーに割り当てます。

Cylance Endpoint Security を MDM ソリューションに接続して、デバイスが管理されているかどうかを確認

Cylance Endpoint Security を BlackBerry UEM または Microsoft Intune に接続して、Cylance Endpoint Security から iOS および Android デバイスが管理されているかどうかを確認できます。

UEM への接続を確立したら、統合が適用される iOS および Android デバイス、ユーザー、およびグループを設定します。UEM については、UEM 管理コンソールで使用可能なユーザーやグループの管理機能を使

用して、サポートされているアクティベーションタイプでユーザーがアクティブ化されていることを確認し、CylancePROTECT Mobile アプリの配布を管理します。

この機能を使用するすべての BlackBerry UEM 管理対象デバイスには、BlackBerry UEM インスタンスから CylancePROTECT Mobile アプリが展開されている必要があります。

Intune の統合で Cylance Endpoint Security を Intune に接続すると、統合が適用されるデバイスタイプと Intune ユーザーグループを定義するアプリ設定ポリシーが作成されます。この機能を使用するすべての Intune 管理対象デバイスを Cylance コンソールで［アセット］>［ユーザーグループ］を通じてアプリ設定ポリシーに含める必要があります。

Cylance コンソールでは、デバイスが BlackBerry UEM または Intune によって管理されている場合にのみ Gateway を実行できるようにする Gateway サービスポリシーを作成し、割り当てます。ユーザーが MDM 管理対象デバイス上のネットワークの宛先にアクセスしようとすると、宛先が許可されている場合、ネットワークトラフィックがセキュリティ保護されたトンネルを介して送信されます。

Cylance Endpoint Security を BlackBerry UEM に接続するには、次の操作を実行します。

手順	アクション
1	前提条件を確認します。
2	会社のディレクトリにリンクします。 • Cylance Endpoint Security では、「会社のディレクトリへのリンク」を参照してください。 • BlackBerry UEM では、「会社のディレクトリに接続する」を参照してください。
3	BlackBerry Connectivity Node をインストールおよび設定します。 • Cylance Endpoint Security では、「BlackBerry Connectivity Node のインストールまたはアップグレード」を参照してください。 • BlackBerry UEM では、「BlackBerry Connectivity Node インスタンスのインストール」を参照してください。
4	BlackBerry UEM コネクタの追加。
5	BlackBerry UEM の使用によるデバイスへの CylancePROTECT Mobile アプリのインストール。

Cylance Endpoint Security を Intune に接続するには、次の操作を実行します。

手順	アクション
1	前提条件を確認します。
2	Cylance Endpoint Security の Intune への接続。

前提条件：デバイスが **MDM** で管理されていることの確認

- BlackBerry UEM
  - BlackBerry UEM Cloud または UEM オンプレミスバージョン 12.15 以降がサポートされています。
  - BlackBerry UEM Cloud および BlackBerry UEM インスタンスに、有効な BlackBerry UEM の SRP ID および認証キーがあることを確認します。UEM インスタンスの SRP ID と認証キーを、*my*Account の［組織］ > ［サービス］ > ［UEM］で表示できます。
  - 組織の Cylance Endpoint Security テナントと UEM ドメインには、同じ組織 ID が設定されている必要があります。
  - オンプレミス環境の BlackBerry UEM では、BlackBerry UEM コネクタからの接続を許可する必要があります。BlackBerry UEM コネクタからの接続を許可しないと、テナント情報を保存しようとしたときに、「UEM 接続要求が無効です」というエラーメッセージが表示され、情報を保存できません。BlackBerry UEM コネクタを有効にする方法については、support.blackberry.com/community にアクセスし、記事 97480 を参照してください。BlackBerry UEM Cloud 環境では、これはデフォルトで有効になっています。
  - ユーザーのアカウントは、Cylance コンソールでは同じ Active Directory または Entra ID アカウントを使用する必要があります。
  - Cylance Endpoint Security は、1 つの UEM ドメインへの接続をサポートします。
  - BlackBerry UEM の使用によるデバイスへの CylancePROTECT Mobile アプリのインストール する必要があります。ユーザーが App Store または Google Play からアプリをダウンロードしてインストールする場合は、必要なアプリ設定がないため、UEM からアプリを配布する必要があります。
  - iOS デバイスの前提条件については、前提条件： iOS デバイスが UEM によって管理されていることの確認 を参照してください。
  - Android デバイスの前提条件については、次を参照してください： 前提条件：Android デバイスが UEM によって管理されていることの確認
- Microsoft Intune
  - Intune との接続に使用する Cylance Endpoint Security 管理者アカウントには、Intune ライセンスが必要です。
  - Cylance Endpoint Security は、1 つの Intune インスタンスへの接続をサポートします。
  - この機能を使用するすべての Intune 管理対象デバイスを Cylance コンソールでアプリ設定ポリシーに含める必要があります。詳細については、「Cylance Endpoint Security の Intune への接続」を参照してください。

前提条件： **iOS** デバイスが **UEM** によって管理されていることの確認

iOS デバイスは、次のいずれかのアクティベーションタイプ*を使用してアクティブ化する必要があります。

- MDM 制御
- ユーザーのプライバシー
- ユーザーのプライバシー - ユーザー登録

ユーザーがユーザープライバシーアクティベーションタイプでアクティブ化されている場合は、次のいずれかのタスクを実行します。

タスク	手順
Cylance Endpoint Security の使用による per-app VPN の管理	1. ユーザープライバシーアクティベーションタイプで、［**VPN** 管理を許可する］チェックボックスをオフにし、［アプリの管理を許可する］チェックボックスをオンにします。 2. Cylance Endpoint Security コンソールで、Gateway サービスのオプション設定を行います。
UEM の使用による per-app VPN の管理	1. ユーザープライバシーアクティベーションプロファイルで、［**VPN** 管理を許可する］および［アプリの管理を許可する］チェックボックスをオンにします。 2. カスタム VPN プロファイルを作成します。［**VPN** バンドル **ID**］フィールドに、CylancePROTECT Mobile バンドル ID「`com.blackberry.protect`」を入力します。 3. Cylance Endpoint Security コンソールで、Gateway サービスのオプション設定を行います。

* UEM インスタンスからデバイスを無効化する場合は、［仕事用データのみを削除］コマンドを使用して、デバイス上の仕事用データ（IT ポリシー、プロファイル、アプリ、証明書など）を削除します。［デバイスを削除］コマンドを選択した場合、デバイスが UEM インスタンスから削除されますが、データおよびプロファイルは削除されず、デバイスがメールおよび他の仕事用データの受信を継続することがあります。BlackBerry では、デバイスが回復不能なほど失われた、または損傷して、サーバーに再度接続することが想定されていない場合にのみ、［デバイスを削除］コマンドを使用することをお勧めします。デバイスに送信できるコマンドに関する詳細については、BlackBerry UEM コンテンツの「iOS デバイスのコマンド」を参照してください。

前提条件：**Android** デバイスが **UEM** によって管理されていることの確認

Android デバイスは、次のいずれかのアクティベーションタイプを使用してアクティブ化する必要があります。

- 仕事用と個人用 - ユーザープライバシー（仕事用プロファイルがある Android Enterprise）
- 仕事用領域のみ（Android Enterprise 完全管理のデバイス）
- 仕事用と個人用 - フルコントロール（仕事用プロファイルがある Android Enterprise 完全管理のデバイス）
- 仕事用領域専用（Samsung Knox）
- 仕事用と個人用 - フルコントロール（Samsung Knox）
- 仕事用と個人用 - ユーザープライバシー（Samsung Knox）

BlackBerry UEM コネクタの追加

デフォルトでは、［コネクタ］ページには、現在の環境で使用されている BlackBerry UEM コネクタの名前、接続タイプ、および接続ステータスが表示されます。Cylance Endpoint Security テナントが接続をサポートする UEM ドメインは 1 つです。

作業を始める前に： BlackBerry UEM Connector の前提条件を確認します。

1. 管理コンソールのメニューバーで、［設定］ > ［コネクタ］をクリックします。
2. ［コネクタを追加］をクリックし、ドロップダウンリストから［**BlackBerry UEM**］を選択します。
3. ［テナント情報］画面で、BlackBerry UEM テナントの SRP ID と認証キーを入力します。
4. ［保存］をクリックします。

BlackBerry UEM の使用によるデバイスへの CylancePROTECT Mobile アプリのインストール

UEM を使用して、デバイスに CylancePROTECT Mobile アプリをインストールできます。ユーザーが BlackBerry Web サイト、App Store、または Google Play からアプリをダウンロードしてインストールする場合は、必要なアプリ設定がないため、UEM からアプリを配布する必要があります。

メモ：

UEM を使用してデバイスに CylancePROTECT Mobile アプリをインストールする場合は、次の機能の制限事項を考慮してください。

- Android Enterprise アクティベーションタイプがユーザープライバシーまたはフルコントロールになっているデバイスでは、SMS メッセージスキャンはサポートされません。
- Android Enterprise アクティベーションタイプのデバイスでは、画面ロックの検出はサポートされていません。

作業を始める前に：「前提条件：デバイスが MDM で管理されていることの確認」を確認します。

1. UEM 管理コンテンツの指示に従って、CylancePROTECT Mobile アプリをアプリリストに追加します。
   - iOS アプリをアプリリストに追加
   - Android アプリをアプリリストに追加

   次のアプリの設定を指定します。

OS	アプリの設定
iOS	• アプリ設定名： *name* • キー：uemperimeterid • 値：%perimeterid%
Android	名前： *name* 次の設定が事前に入力されています。 • ユーザー ID：userid • UEM ペリメータ ID：%perimeterid%

2. CylancePROTECT Mobile アプリをユーザーまたはグループに割り当てます。
3. CylancePROTECT Mobile アプリの処理を［必須］に設定します。

終了したら：

- CylancePROTECT Mobile のアクティベーションメールで受け取った情報を使用してアプリをアクティブ化するようユーザーに指示します。Cylance Endpoint Security は 登録ポリシーを割り当てた後、アクティベーションメールを送信します。
- Cylance Endpoint Security を MDM ソリューションに接続して、デバイスが管理されているかどうかを確認 の指示に従います。

Cylance Endpoint Security の Intune への接続

作業を始める前に：

Intune との接続に使用する Cylance Endpoint Security 管理者アカウントには、Intune ライセンスが必要です。

1. 管理コンソールのメニューバーで、［設定］ > ［コネクタ］をクリックします。

2. ［コネクタを追加］をクリックし、ドロップダウンリストから［**Microsoft Intune**］を選択します。
3. Entra テナント ID を指定します。［次へ］をクリックします。
4. Entra の管理者資格情報を指定します。
5. ［アプリ設定ポリシー］画面で、Intune 統合を適用する OS プラットフォームをオンにし、各プラットフォームで次の手順を実行します。この機能を使用するすべての Intune 管理対象デバイスをアプリ設定ポリシーに含める必要があります。後でアプリ設定ポリシーを作成する場合は、［キャンセル］をクリックします。
   a) 必要に応じて、ポリシーの名前を変更します。ターゲットアプリを変更しないでください。
   b) Intune インスタンスのすべてのグループにポリシーを適用する場合は、［すべてのグループ］をオンにします。
   c) Intune インスタンスの特定のグループにポリシーを適用する場合は、⊕ をクリックします。グループを検索して選択し、［追加］をクリックします。
6. ［保存］をクリックします。Android 用のアプリ設定ポリシーを追加した場合は、表示される管理者の同意プロンプトに従ってください。

作成したアプリ設定ポリシーは、Intune 管理センターに表示されます。

終了したら：

- 組織の Intune 管理者に、Intune 管理センターで CylancePROTECT Mobile MTD コネクタを編集して、次のオプションをオンにするよう指示します。コネクタを有効にするには、次の手順を実行します。
  1. Intune 管理センターにログインします。
  2. ［テナント管理］**>**［コネクタとトークン］をクリックします。
  3. ［クロスプラットフォーム］セクションで、［**Mobile Threat Defense**］をクリックします。
  4. ［追加］をクリックします。
  5. ［セットアップする **Mobile Threat Defense** コネクタの選択］ドロップダウンで、［**CylancePROTECT Mobile**］を選択します。
  6. ［作成］をクリックします。
- 後でアプリ設定ポリシーを追加する場合、または別のポリシーを追加する場合は、［設定］**>**［コネクタ］で、Intune 接続の［アプリ設定を生成］をクリックします。
- Cylance Endpoint Security を Intune に接続して、デバイスのリスクレベルも管理する場合は、「Cylance Endpoint Security と Microsoft Intune の統合によるモバイルの脅威への対応」を参照してください。

CylanceGATEWAY エージェントのインストール

CylanceGATEWAY エージェントは、デバイスがネットワークに接続されていない場合でも、デバイスに到達させたくないインターネットの宛先への接続をブロックできるようにすることで、ユーザーの Windows 10、Windows 11、macOS デバイスを保護します。BlackBerry は、エンドポイントの接続をブロックするため、安全でないインターネットの宛先リストを増やし続けています。ユーザーが許容される使用基準を満たしていない特定のサイトへアクセスすることも組織でブロックする場合は、ポリシーを作成して、すべてのユーザーまたは特定のユーザーやグループがアクセスできない別の宛先を指定できます。

CylanceGATEWAY エージェントはユーザーのデバイスにインストールされ、ネットワークリソースに安全にアクセスできるようにし、不審なネットワークアクティビティや潜在的に悪意のあるネットワークアクティビティからデバイスを保護します。CylanceGATEWAY エージェントがインストールされ、仕事モードが有効になっている場合、CylanceGATEWAY は、ユーザーのデバイスと組織のネットワークやパブリックインターネットとの間で安全な接続を確立し、ネットワークアクティビティを分析し、管理しているネットワークアクセスポリシーを適用します。macOS および Windows デバイスのセーフモードを有効にすると、CylanceGATEWAY は、仕事モード

が有効になっていないときのデバイスのテナント ACL ルールとエンドポイント保護を拡張して、トンネルを使用しないネットワークトラフィックに対してデバイスが常に保護されるようにします。

CylanceGATEWAY エージェントの新規インストールを展開するとき、ユーザーのデバイスを再起動する必要があります。また、ユーザーは手動でインストールプロセスを完了し、仕事モードを有効化するか、セーフモードをアクティブ化する必要があります。CylanceGATEWAY エージェントのアップグレードを展開するとき、アップグレードを完了するには、ユーザーのデバイスを再起動する必要があります。アップグレード中、CylanceGATEWAY エージェントはすべての設定を保持します。ユーザーが他に何かする必要はありません。

CylanceGATEWAY エージェントのインストールをエンタープライズデバイス管理ツール（Microsoft System Center Configuration Manager（SCCM）やその他の展開ツールなど）によって制御する場合は、エージェントをアクティブ化するときのユーザーの操作を最小限に抑えるために customDomain パラメーターを指定することができます。カスタムドメイン名は、［設定］>［アプリケーション］の［カスタムドメイン名］フィールドから取得できます。このパラメーターは、Windows デバイスの場合はコマンドラインから指定でき、macOS デバイスの場合は管理対象アプリ設定または MCX アプリプリファレンスを使用して指定できます。CylanceGATEWAY エージェントを手動でダウンロードしてインストールし、仕事モードを有効化するか、セーフモードをアクティブ化するようにユーザーに指示することもできます。

- macOS デバイスの場合は、次の値を指定して、ユーザーが CylanceGATEWAY エージェント 2.9 以降をアクティブ化するときに使用するカスタムドメイン名を指定します。

  ```
  <dict>
    <key>customDomain</key>
    <string>Your_custom_domain_name</string>
  </dict>
  ```

- Windows デバイスの場合は、次のコマンドを使用して、ユーザーが CylanceGATEWAY エージェント 2.9 以降をアクティブ化するときに使用するカスタムドメイン名を指定します。

  ```
  CylanceGATEWAY-<version>.exe /v"CUSTOM_DOMAIN=<your_custom_domain_name>"
  ```

  サイレントインストールのカスタムドメイン名を指定するには、「CylanceGATEWAY エージェントのサイレントインストールとアップグレードの実行」を参照してください。

CylanceGATEWAY エージェントのサイレントインストールとアップグレードの実行

CylanceGATEWAY エージェントをユーザーに展開できます。新規インストール展開の場合、ユーザーはデバイスを再起動し、インストールプロセスを手動で完了し、仕事モードを有効にするか、セーフモードをアクティブにする必要があります。新しい展開の場合は、［設定］>［アプリケーション］の［カスタムドメイン名］フィールドから取得するカスタムドメイン名を指定できます。アップグレード展開の場合、ユーザーはアップグレードを完了するために、デバイスを再起動する必要があります。CylanceGATEWAY エージェントの設定は保持され、ユーザーは追加のアクションを実行する必要はありません。

作業を始める前に： BlackBerry Web サイトから Windows 用の CylanceGATEWAY エージェントのコピーをダウンロードし、コンピュータ上に保存します。

1. コマンドプロンプトを開き、管理者として実行します。
2. CylanceGATEWAY エージェントを保存した場所に移動します。次のタスクのいずれかを実行します。この例では、バージョン 2.7.0.19 の CylanceGATEWAY エージェントを使用します。
   - ユーザーのデバイスを再起動せずにサイレントインストールまたはアップグレードを実行するには、次のコマンドを入力します。

     ```
     .\CylanceGATEWAY-2.7.0.19.exe /s /v" REBOOT=Suppress /qn"
     ```

- サイレントインストールまたはアップグレードを実行し、ユーザーのデバイスを直ちに再起動するには、次のコマンドを入力します。 `.\CylanceGATEWAY-2.7.0.19.exe /s /v" /qn"`
- サイレントインストールまたはアップグレードを実行し、GWInstall というインストールログファイルを作成するには、次のコマンドを入力します。

  `.\CylanceGATEWAY-2.7.0.19.exe /s /v" REBOOT=Suppress /qn /l*v .\GWInstall.log"`
- 新規インストールを実行し、カスタムドメイン名を指定するには、次のコマンドを入力します

  `.\CylanceGATEWAY-<2.9.x.x>.exe /s /v" CUSTOM_DOMAIN=<*your_custom_domain_name*> /qn"`

  この機能には Windows 用 CylanceGATEWAY エージェント 2.9 以降が必要です。

3. 必要に応じて、デバイスを再起動して画面の指示に従うようにユーザーに指示します。

CylanceAVERT のセットアップ

項目	説明
1	ソフトウェアの要件を確認します。
2	機密コンテンツを定義します。
3	CylanceAVERT をインストールします。
4	情報保護ポリシーを作成します。
5	管理者、ユーザー、およびグループへのポリシーの割り当て

CylanceAVERT エージェントのインストール

CylanceAVERT は BlackBerry myAccount ポータルの［ダウンロード］ページからダウンロードしてインストールできます。

CylanceAVERT は SCCM または JAMF を使用してサイレントモードでユーザー向けにインストールできます。これを行うには、`IAgreetoBBSLA=true` コマンドラインパラメータを含め、エンドユーザー使用許諾契約書（EULA）に同意する必要があります。EULA はユーザーには表示されません。CylanceAVERT をサイレントモードでインストールしたら、システムを再起動する必要があります。

メモ：CylanceAVERT をサイレントモードでインストールする前に、BlackBerry プライバシー通知を含む BlackBerry ソリューション使用許諾契約書を読む必要があります。アプリケーションは、上記の方法で BlackBerry ソリューション使用許諾契約書の利用規約に同意した場合にのみインストールできます。**BlackBerry** ソリューション使用許諾契約書の利用規約に同意しない場合には、**CylanceAVERT** をインストールまたは使用しないでください。

CylanceAVERT エージェントをインストールすると、メールの送信時、USB 経由でのファイルの転送時、および Web サイトへのファイルのアップロード時に、機密性の高い会社データが不正に共有される可能性についてのセキュリティ通知を受け取ることができるようになります。

Cylance Endpoint Security に追加されていないユーザーが CylanceAVERT をインストール済みのデスクトップにログインすると、そのユーザーは自動的に Cylance Endpoint Security に追加され、すべてのポリシーが適用されます。これには、Active Directory ディレクトリ接続または BlackBerry Connectivity Node ディレクトリ接続が必要です。ユーザー管理に BlackBerry Connectivity Node ディレクトリ接続を使用している場合は、バージョン 2.12.1 以降の BlackBerry Connectivity Node を使用する必要があります。詳細については、『Cylance Endpoint Security セットアップガイド』の「BlackBerry Connectivity Node のインストール」と「会社のディレクトリへのリンク」を参照してください。

メモ：Windows アプリケーショントレイから CylanceAVERT アプリを終了すると、窃盗イベントが発生しても Windows 通知を受信できません。

CylanceAVERT のインストール

CylanceAVERT では、CylancePROTECT Desktop のバージョン 3.1 以降が必要です。

メモ：CylanceAVERT は CylancePERSONA のコンピューターにインストールできません。

1. デバイスで CylanceAVERT エージェントインストーラをダブルクリックします。
2. インストール手順に従います。

終了したら：

- CylanceAVERT エージェントがインストールされていることを確認する方法は、次のとおりです。
  - CylanceAVERT アイコンがシステムトレイに表示されます。
  - コンソールの［アセット］ページで、CylanceAVERT ユーザーが［ユーザー］リストに表示されます。
  - Windows タスクマネージャーで CylanceAVERT プロセスが実行されていることを確認します。
- エージェントをアンインストールするには、Windows の［設定］を使用します。

メモ：CylanceAVERT のインストール後、ブラウザプラグインが、保護されていない（非 SSL）Web サイトへのファイルのアップロードを禁止します。BlackBerry では、非 SSL Web サイトにファイルをアップロードしないことをお勧めします。

情報保護の設定を使用した機密コンテンツの定義

情報保護設定では、CylanceAVERT が機密ファイル中で検索するデータタイプ、収集される証拠、信頼できると見なす電子メールやブラウザのドメイン、窃盗イベントの通知を送信する電子メールアドレスを指定できます。

証拠収集の管理

CylanceAVERT でデータ窃盗イベントを収集する方法をカスタマイズできます。データ収集設定を使用すると、監査目的で、データ窃盗イベント時に収集する証拠を設定できるようになります。データ収集設定を構成することで、さまざまな決定を下せます。たとえば、データ窃盗イベントのファイルスニペットを含める、イベント関連ファイルのコピーをすべて保存する、証拠ロッカーへのアップロードを管理する、ファイルアップロードの時間を選択する、データ証拠の保管期間を指定するなどです。

1. 管理コンソールのメニューバーで、［設定］ > ［情報保護］の順にクリックします。
2. ［データ収集］タブをクリックします。
3. 情報保護設定を構成するには、次のいずれかを実行します。

項目	手順
ファイルスニペット	［ファイルスニペットを生成］トグルをクリックして、ファイルスニペットの収集をオンまたはオフにします。［ファイルスニペットを生成］をオンにすると、データ窃盗イベントのファイルスニペットがイベントの詳細に保存されます。デフォルトでは、［ファイルスニペットを生成］はオフに設定されています。

項目	手順
証拠ファイル収集	• ［証拠ファイル収集を有効化］トグルをクリックして、証拠ファイルの収集をオンまたはオフにします。デフォルトでは、［証拠ファイル収集を有効化］はオフに設定されています。［証拠ファイル収集を有効化］をオンにすると、データ窃盗イベントに関与したすべてのファイルのコピーがイベントの詳細に保存されます。詳細については、「CylanceAVERT イベントの詳細の表示」を参照してください。 • ［ディスク容量］テキストフィールドをクリックし、リモートデバイスまたは証拠ロッカー上の証拠ファイルのキャッシュに割り当てることができる最大空きディスク容量を指定する値を入力します。デフォルトでは、［ディスク容量］は 10% に設定されています。
ファイルアップロード	［ファイルアップロードの方法］ドロップダウンメニューをクリックして、方法を選択します。［直接］を選択すると、ネットワーク上のデバイスが証拠ロッカーに直接ファイルをアップロードできるようになります。証拠ロッカーへの直接アクセスがブロックされている場合（例えばファイアウォールなどによって）、［**BlackBerry Proxy Service**］を選択すると、BlackBerry がクラウド経由でそれらのファイルをアップロードします。デフォルトでは、［直接］が選択されています。
証拠ファイルの保持	［データの保持］ドロップダウンメニューをクリックして、証拠ファイルを証拠ロッカーに保存する期間を選択します。証拠ファイルを保存できる期間の値は 30 日、60 日、または 90 日です。デフォルトでは、［データの保持］は 30 日に設定されています。

許可されたドメインと信頼済みドメインの追加

ドメインを指定することで、ファイルの安全なアップロード先として信頼できるブラウザやメールアドレスをリスト化できます。ドメインの追加後、情報保護ポリシーでドメインを使用できるようにする必要があります。特定のポリシーに対して許可されたドメインを指定しておくと、追加された証明書に対してドメインが検証されて信頼済みドメインになっている場合、機密ファイルのアップロードを検出するためにスキャンされる際も、そのドメインではポリシー違反がトリガされません。情報保護の設定でどのドメインも指定していない場合や、ポリシーで使用するドメインを追加していない場合は、すべてのドメインが信頼できないドメインとして扱われます。

メモ：

- USB デバイスのドメインもすべて信頼できないものと見なされます。
- 許可されたドメインを指定しておくと、信頼済み証明書が追加されている限り、そのサブドメインもすべて許可されたと見なされます。

作業を始める前に： 信頼済み証明書がアップロードされていることを確認します。ドメインが信頼済みと見なされるようにするには、信頼済み証明書をアップロードする必要があります。信頼済み証明書をアップロードしていない場合は、許可されたドメインをポリシーで使用していても、窃盗イベントをトリガーします。詳細については、「信頼済み証明書によるドメインの確認」を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［情報保護］の順にクリックします。
2. ［許可されたドメイン］タブをクリックします。
3. 新しいブラウザドメインを追加するには、［新しいドメインを追加］ボタンをクリックします。

4. ［許可されたドメインを追加］ダイアログボックスで、テキストフィールドにドメインの名前と説明を入力します。ドメイン名フィールドでのワイルドカード文字の使用はサポートされていません。
5. 必要に応じて、ポリシーでこのドメインを使用する機能をオンにします。
6. このドメインが既存の信頼済み証明書を使用しているかどうかを確認するには、［確認］をクリックします。証明書をアップロードしていない場合は、ここで証明書を追加します。手順については、「信頼済み証明書によるドメインの確認」を参照してください。
7. ［追加］をクリックします。
8. 新しいメールドメインを追加する場合は、［許可されたメールドメイン］セクションにドメインを入力し、カンマを使用して入力済みのドメインと区切ります。

終了したら：

許可されたドメインを削除するには、［許可されたドメイン］リストで削除するドメインの横にあるチェックボックスをオンにし、［削除］をクリックします。

テンプレートを使用したデータタイプのグループ化

テンプレートを使用して、組織がポリシーで使用する機密データのタイプをグループ化できます。

1. 管理コンソールのメニューバーで、［設定］ > ［情報保護］の順にクリックします。
2. ［テンプレート］タブをクリックします。
3. 事前定義済みのテンプレートを追加するには、［事前定義済みの追加］をクリックし、リストから事前定義済みのテンプレートを選択して、［追加］をクリックします。
4. カスタムのテンプレートを作成するには、［カスタムの作成］をクリックします。
5. ［新しいテンプレートの追加］ページの［一般情報］セクションでテンプレート名を入力し、ドロップダウンリストから地域を選択します。
6. ［地域］のドロップダウンメニューで、テンプレートを使用する地域を選択します。たとえば、Canadian Health カードや Canadian Sin 番号のデータタイプを使用してテンプレートを作成する場合は、地域を［Canada］にします。
7. ［情報タイプ］のドロップダウンメニューで、テンプレートと一致する情報タイプを選択します。カスタム、財務、健全性、個人データを指定できます。
8. ［条件ビルダー］セクションで、ドロップダウンリストからデータタイプを選択し、ポリシー違反のトリガーに必要な最小オカレンス数を指定します。グループに新たなデータタイプを追加するには、［項目の追加］をクリックします。
   - グループに新たなデータタイプを追加するには、［項目の追加］をクリックします。
   - 条件グループを新たに追加するには、［グループの追加］をクリックします。
9. ［保存］をクリックします。

終了したら：

テンプレートが追加されたら、それを情報保護ポリシーに追加することができます。詳細については、「情報保護ポリシーの管理」を参照してください。

テンプレートを削除するには、削除するテンプレートの横にある［アクション］列で、次の手順を実行します。

- 事前定義済みのテンプレートを削除 するには、⊗ をクリックします。確認のダイアログで、［削除］をクリックします。
- カスタムのテンプレートを削除するには、🗑 をクリックします。確認のダイアログで、［削除］をクリックします。

テンプレートがリストから削除されると、情報保護ポリシーで使用できなくなります。

カスタムのテンプレートを編集するには、リスト内のテンプレートをクリックして、フィールドの情報を編集します。事前定義済みのテンプレートは編集できません。詳細については、手順 4〜7 を参照してください。

テンプレートをコピーするには、コピーするテンプレートのアクション列で をクリックします。

機密データのデータタイプの指定

CylanceAVERT でスキャンされる機密データは、データタイプによって規定されます。データタイプは情報保護の設定で指定でき、組織のニーズに合わせてカスタマイズ可能です。データタイプの検索には、キーワードまたは正規表現を使用できます。

1. 管理コンソールのメニューバーで、［設定］ > ［情報保護］の順にクリックします。
2. ［データタイプ］タブをクリックします。
3. ［カスタムデータタイプの追加］をクリックします。

   メモ：また、リストに事前定義済みのデータタイプを追加して、当該のデータタイプを情報保護ポリシーで使用できるようにすることもできます。追加方法は、［事前定義済みデータタイプの追加］をクリックし、リストに追加する事前定義済みのデータタイプを選択して［追加］をクリックします。
4. ［カスタムデータタイプの追加］ページで、新しいデータタイプの名前と説明を追加します。
5. ［地域］ のドロップダウンリストで、データタイプが使用される地域を選択します。たとえば、カナダの運転免許証番号を確認する場合は、地域を［カナダ］にします。
6. ［情報タイプ］のドロップダウンメニューで、データタイプと一致する情報タイプを選択します。カスタム、財務、健全性、個人データを指定できます。
7. ［検索方法］のドロップダウンリストで、使用する検索方法を選択します。値は、キーワード、式、またはキーワード辞書です。キーワード辞書は、複数のキーワードを指定するテキストファイルです。キーワード辞書を作成するには、キーワードごとに改行して記述されたテキストファイルを作成する必要があります。
8. 次の操作のいずれかを実行します。

   - 検索方法を［キーワード］にした場合は、スキャンするキーワードを［キーワード］フィールドに入力します。キーワードが複数ある場合はカンマで区切ります。
     - キーワードが完全に一致する場合に、ファイルを機密と見なす場合は、［完全一致］を選択します。これを選択すると、キーワードがより大きなテキスト文字列の一部である場合、キーワードは一致と見なされなくなります。たとえば、キーワードとして「confidential」を指定した場合、「confidentiality」は一致とは見なされません。
     - キーワードの大文字と小文字が完全に一致する場合に、ファイルを機密と見なす場合は、［大文字と小文字を区別］を選択します。これを選択すると、テキストの大文字と小文字が区別されます。たとえば、キーワードとして「confidential」を指定した場合、「CONFIDENTIAL」は一致とは見なされません。
   - 検索方法を［正規表現］（**Regex**）にした場合は、スキャンする正規表現を［**Regex**］フィールドに入力します。

     メモ：Regex を使用する場合は、次の点に注意してください。

     - Regex は .NET 言語に準拠する必要があります。
     - Regex101 や Regex Storm などの一般的なツールを使用すると、正規表現を検証できます。
   - ［キーワード辞書］を選択した場合は、次の操作を実行します。
     - キーワードが完全に一致する場合に、ファイルを機密と見なす場合は、［完全一致］を選択します。これを選択すると、キーワードがより大きなテキスト文字列の一部である場合、キーワードは一致と見な

されなくなります。たとえば、キーワード辞書のキーワードとして「confidential」を指定した場合、「confidentiality」は一致とは見なされません。

- キーワードの大文字と小文字が完全に一致する場合に、ファイルを機密と見なす場合は、［大文字と小文字を区別］を選択します。これを選択すると、テキストの大文字と小文字が区別されます。たとえば、キーワード辞書のキーワードとして「confidential」を指定した場合、「CONFIDENTIAL」は一致とは見なされません。
- ［キーワード辞書をアップロード］をクリックし、キーワード辞書を選択します。データ型ごとにアップロードできるキーワード辞書ファイルは 1 つだけです。

メモ：キーワード辞書の制限事項は次のとおりです。

- テナント上のすべてのキーワード辞書の合計サイズは、1.5 MB を超えることはできません。
- キーワード辞書内の 1 つのキーワードは、1024 文字を超えることはできません。
- テナント上のキーワード辞書データエンティティの最大数は 1000 です。

9. ［作成］をクリックします。

終了したら：

- カスタムのデータタイプは消去できます。カスタムのデータタイプを消去するには、［アクション］列の をクリックします。確認メッセージが表示されたら、［消去］をクリックします。
  メモ： データタイプがポリシーで使用されている場合、［使用中のデータタイプ］とポップアップで表示されます。その場合、これが削除されるまで、データタイプを消去できません。
- 事前定義済みのデータタイプはリストから削除しても、消去することはできません。リストから事前定義済みのデータタイプを削除するには、［アクション］列の をクリックします。確認メッセージが表示されたら、［削除］をクリックします。［事前定義済みデータタイプの追加］をクリックすると、事前定義済みのデータタイプを再度追加して、リストで選択することができます。
  メモ： データタイプがポリシーで使用されている場合、［使用中のデータタイプ］とポップアップで表示されます。その場合、これが削除されるまで、データタイプを消去できません。
- 既存のキーワード辞書ファイルをダウンロードできます。更新されたキーワード辞書がアップロードされると、エンドポイントが再スキャンされ、ポリシーが評価されます。現在、既存のイベントは以前のデータタイプから評価されたままになります。

信頼済み証明書によるドメインの確認

信頼済み証明書を使用すると、情報保護設定に追加され、許可されたブラウザのドメインを確認できます。信頼済み証明書がない場合、許可されたドメインをポリシーで使用すると、窃盗イベントがトリガーされます。許可されたドメインの詳細については、「許可されたドメインと信頼済みドメインの追加」を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［情報保護］の順にクリックします。
2. ［信頼済み証明書］タブをクリックします。
3. ［証明書を追加］をクリックします。
4. ルート証明書または中間証明書のファイル（.pem）をアップロードします。［ファイルの参照］をクリックしてデバイス上のローカル .pem ファイルを特定し、［追加］をクリックします。

指定したメールアドレスへの通知の送信

データ窃盗イベントの発生時や証拠ロッカーが保管容量に到達した際に通知を送信するメールアドレスを指定できます。イベントの詳細を確認できるのは Cylance Endpoint Security 管理者のみですが、通知の受信は任意のユーザーが行えます。

1. 管理コンソールのメニューバーで、［設定］ > ［情報保護］の順にクリックします。
2. ［通知］タブをクリックします。
3. 指定したメール受信者に CylanceAVERT イベントのメール通知を送信できるようにするには、［情報保護イベント通知を有効にする］をオンにします。
4. ［メール受信者］テキストフィールドに、CylanceAVERT イベント通知を受信するメールアドレスを入力します。複数のメールアドレスエントリを区切るには、カンマを使用できます。
5. 証拠ロッカーストレージの容量に関するメール通知を特定のメール受信者に送信できるようにするには、［証拠ロッカーストレージの通知を有効にする］をオンにします。
6. ［メール受信者］テキストフィールドに、証拠ロッカーストレージの容量に関する通知を受信するメールアドレスを入力します。複数のメールアドレスエントリを区切るには、カンマを使用できます。

情報保護ポリシーの管理

情報保護ポリシーを使用すると、指定した条件の成立時にトリガーされる組織または規制ポリシーを作成できます。条件の追加は、テンプレートまたは条件ビルダーを使用して行えます。情報保護ポリシーは累積的なものであり、他の Cylance Endpoint Security ポリシーのようなランク付けはされません。不明なユーザーの場合、またはポリシーが割り当てられていない場合、当該ユーザーにはすべてのポリシーが適用されます。

情報保護ポリシーのタイプは、規制か組織のいずれかになります。ポリシータイプに応じて、調整ロジックは異なるものが適用されます。

- 規制ポリシータイプが特定のユーザーに複数割り当てられている場合、当該ユーザーのポリシーは統合されて、最も制限の厳しいルールと修復アクションが適用されます。
- 組織ポリシータイプが特定のユーザーに複数割り当てられている場合、当該ユーザーのポリシーは統合されて、最も制限の緩いルールと修復アクションが適用されます。

メモ：少なくとも 1 つの情報保護ポリシーが必要です。情報保護ポリシーを削除しようとすると、少なくとも 1 つのポリシーが必要であるというエラーが表示されます。

ポリシー統合のベストプラクティス

CylanceAVERT には、情報保護ポリシーで使用できる 2 つのポリシーコンプライアンスタイプがあります。

規制コンプライアンスとは、業界や政府の規制に関連する機密情報の保護に使用される、有限の機密データのセットを指します。規制データとは、経時的に変化しないデータのことです。CylanceAVERT 設定の定義済みデータタイプはすべて規制データであり、製品のセットアップを迅速化および簡素化するために BlackBerry が提供するものです。独自の規制データタイプとテンプレートを作成し、組織で必要な規制データをすべてまとめたポリシーとして使用できます。たとえば、BlackBerry が提供するテンプレートを使用する代わりに、カナダの SIN 番号、PHIN、医療サービス番号、運転免許証、銀行口座番号およびパスポート番号を組み合わせて 1 つのポリシーにしたカナダの健康規制ポリシーを作成できます。CylanceAVERT は、正規表現またはキーワードとの一致を使用して、ポリシーに記載されている関連規制情報がファイルに含まれているかどうかを判別します。

組織コンプライアンスとは、組織から組織へのデータ変更にアクセスできるコンテンツとユーザーが組織の状況に応じて常に変化するような、無限のデータセットを指します。この場合、組織コンプライアンスを使用して、会社の IP や組織に関連するその他の情報を含む機密データを保護する必要があります。

同じ機密ファイルに複数のポリシーが適用される可能性があるため、機密性の高いファイルが検出されたときに実行する修正アクションでポリシーが競合する場合があります。この場合、CylanceAVERT はこれらのポリシーの修正アクションを調整します。

ポリシーの不一致が発生すると、CylanceAVERT は自動的に調整アクションを適用します。ファイルが規制ポリシーに違反しているのか、組織ポリシーに違反しているのか、またはその両方に違反しているのかによって調整アクションは変わります。ファイルが組織ポリシーにのみ違反しているとして分類された場合は、制約が最も緩い修正アクションが実行されます。ファイルが規制ポリシーまたは組織ポリシー、あるいはその両方に違反しているとして分類された場合は、最も制約が厳しいアクションが実行されます。たとえば、「機密」という単語がファイルに 2 回使用されている場合に機密性が高いと判断する組織ポリシーと、3 回使用されている場合に機密性が高いと判断する別の組織ポリシーの対象となるファイルでは、3 回使用されている場合に機密性が高いと判断されます（最も緩い制約）。ただし、これらのポリシーのいずれかまたは両方が規制ポリシーであれば、2 回使用されている場合に機密性が高いと判断されます（最も厳しい制約）。

情報保護ポリシーの作成

1. 管理コンソールのメニューバーで、［ポリシー］ > ［ユーザーポリシー］をクリックします。
2. ［情報保護］タブをクリックします。
3. ［ポリシーを追加］をクリックします。
4. ［一般的な情報］セクションで、次の項目を入力します。
   - ［ポリシー名］フィールドに、ポリシーの名前を入力します。
   - ［説明］フィールドに、ポリシーの説明を入力します。
   - ［ポリシータイプ］のドロップダウンメニューで、作成するポリシーのタイプを選択します。ポリシータイプは規制か組織を指定できます。
     - 規制のポリシータイプとは、規制で定義されている機密データの有限セットを指しますが、必ずしも経時的に変化するものではありません（PCI、HIPAA など）。
     - 組織のポリシータイプとは、会社所有のデータを指し、データにアクセスできる対象者は常に変化する可能性があります。そのため、組織データはデータ要素（ファイルタイプ、キーワード、ファイル作成者、ファイル作成者の役割など）で分類する必要があります。
5. ［条件］セクションで、次のいずれかを使用して、ポリシー違反をトリガーする条件を設定します。

条件	説明
テンプレートを使用した条件の追加	**a.** ［テンプレートから追加］をクリックします。 **b.** ポリシーに追加するテンプレートのチェックボックスをクリックします。 メモ：検索バーを使用すると、テンプレートのリストをフィルタリングできます。

条件	説明
条件ビルダーを使用した条件の追加	メモ：条件ビルダーは、**AND** や **OR** のステートメントグループで構成されています。どのようなときにポリシーをトリガーするのかを決めるには、これらのステートメントグループの組み合わせを使用する必要があります。 **a.** **AND** 条件のセクションでは、ドロップダウンリストから条件を選択して、条件をトリガーするのに必要な最小オカレンス数を数値のドロップダウンメニューから指定します。 • 現在のステートメントグループにアイテムを新たに追加する場合、［アイテムの追加］をクリックします。 • ステートメントグループを新たに追加する場合、［グループの追加］をクリックします。 • ステートメントグループを削除する場合、［グループの削除］をクリックします。 **b.** **OR** 条件のセクションでは、ドロップダウンリストから条件を選択して、条件をトリガーするのに必要な最小オカレンス数を数値のドロップダウンメニューから指定します。

6. ［許可されたドメイン］セクションで ⊕ をクリックして、ポリシーで許可するブラウザのドメインをリストから選択します。
7. ［許可されたメールドメイン］セクションで、情報保護設定で指定されたメール受信者のうち、ポリシーで許可する受信者を選択します。
8. ［アクション］セクションのドロップダウンリストから、Web ブラウザ、USB、メールの窃盗イベントに対して実行するアクションを選択します。次のアクションから選択します。
   - レポート：このオプションでは、データ窃盗またはポリシー違反が Cylance Endpoint Security コンソールにレポートされ、Avert イベント（［Avert］ > ［イベント］）ページに表示されます。アラートが［アラート］表示で作成され、イベントは SIEM ソリューションまたは syslog サーバー（設定されている場合）に送信されます。また、通知（［設定］ > ［情報保護］）画面で指定されたメール受信者にはメールが送信されます。
   - レポートと通知：このオプションでは、データ窃盗またはポリシー違反が Cylance Endpoint Security コンソールにレポートされ、ユーザーのエンドポイントのタスクバーにデータ窃盗またはポリシー違反のバッジと通知が表示されます。
   - レポート、通知、警告：このオプションでは、データ窃盗またはポリシー違反が Cylance Endpoint Security コンソールにレポートされ、バッジと通知がタスクバーに表示されて、データ窃盗やポリシー違反の発生前にエンドポイントとポップアップに Windows 通知が追加されてユーザーが警告されます。たとえば、ユーザーが Microsoft Outlook を使用している場合、CylanceAVERT エージェントはメールをインターセプトして、機密データが送信される前にメールエディタにアラートを表示し、ユーザーに警告を表示します。
9. ［追加］をクリックします。

   メモ：ユーザーにポリシーが割り当てられている場合、これらのポリシーをすべて削除すると、そのユーザーは CylanceAVERT から削除されます。

終了したら：

次の操作のいずれかを実行します。

- ユーザーやユーザーグループにポリシーを割り当てることができます。詳細については、「CylanceAVERT ユーザーの詳細の表示」を参照してください。
- 情報保護ポリシーを削除するには、リスト内のポリシーの横にあるチェックボックスをオンにして、［削除］をクリックします。
- 情報保護ポリシーを編集するには、リスト内のポリシーをクリックして、ポリシーを変更してから［保存］をクリックします。

CylancePROTECT Desktop および CylanceOPTICS エージェントの更新の管理

更新ルールを使用することで、デバイス上の CylancePROTECT Desktop エージェントおよび CylanceOPTICS エージェントの更新を管理できます。更新ルールにより Cylance Endpoint Security を設定して、更新を特定のバージョンまたは利用可能な最新バージョンに自動的にプッシュしたり、自動更新をオフにして組織の希望する方法でソフトウェア配布を管理したりすることができます。ゾーンは更新ルールに関連付けられ、ゾーンに属しているデバイスとユーザーはそのルールに従って更新を受信します（ゾーンベースの更新とも呼ばれます）。デフォルトでテスト、パイロット、および実稼働の更新ルールが用意されていますが、組織のニーズに応じてエージェントの更新を管理する新しい更新ルールを追加することもできます。

デバイスのエージェントバージョンは、必ず、更新ルールで指定されたバージョンに更新されます。デバイスが既に新しいバージョンを使用している場合でも、更新ルールを使用して以前のバージョンのエージェントをインストールできます。

デバイスの Linux ドライバが以前にデバイス上で手動で更新されたことがある場合、そのドライバはエージェントの更新の一環として自動的には更新されません。これは、自動化されたシステムが、管理者が実行したアクションを上書きしないようにするためです。

エージェントの更新をテストする際は、次の点を考慮してください。

- BlackBerry では、実稼働環境に追加した他の更新ルールを使用する前に、テスト目的で作成された更新ルール（テストおよびパイロットの更新ルールなど）とゾーンを使用してエージェント更新ルールをテストすることをお勧めします。更新をテストするときは、テストおよび評価のための専用デバイスを使用することを検討してください。
- エージェントの更新をテストするためのゾーンを作成し、テスト用の専用デバイスを追加します。作成したゾーンを、テストおよびパイロットの更新ルールに関連付けます。ゾーンの作成方法の詳細については、「CylancePROTECT Desktop および CylanceOPTICS を管理するためのゾーンの設定」を参照してください。
- テストデバイスはすべて、テストするゾーンに属していることを確認します。他の更新ルールが関連付けられたゾーンに属していないすべてのデバイスには、実稼働の更新ルールが適用されます。

メモ：デバイスポリシーで、メモリ保護、スクリプト制御、デバイス制御のいずれかまたはすべてが有効になっている場合は、エージェントのインストールまたはアップグレード後にデバイスを再起動することをお勧めしますが、厳密には必要ありません。再起動すると、新しいポリシー設定が完全に有効になります。

更新ルールとゾーンの仕組み

- デバイスは、ゾーンルールまたは手動割り当てのいずれかによってゾーンに関連付けられます。
- デバイスは、複数のゾーンに関連付けることができます。
- ゾーンは、更新ルールに割り当てられます。それらのゾーンに割り当てられたデバイスは、更新ルールに従います。
- 更新ルールはオペレーティングシステム（OS）プラットフォームに固有のものではありませんが、特定の OS プラットフォームのデバイスの更新を管理するためのゾーンを作成することもできます。更新ルールで指定されたエージェントバージョンがプラットフォームで使用できない場合、デバイスは、更新がプラットフォームで使用可能になったときに更新を受信します。
- 更新ルールはランク付けされます。デバイスが複数のゾーンに関連付けられていて、異なる更新ルールが割り当てられている場合、エージェントの更新（自動更新または特定のバージョン）を指定する最高ランクの更新ルールが有効になります。デバイスが少なくとも 1 つのゾーンにあり、更新ルールで更新が指定されている場合、デバイス上のエージェントはそれに応じて更新されます。実稼働更新ルールのランクは最低で、

更新ルールのあるゾーンに属さないデバイス、およびどのルールにもエージェントに対する更新が指定されていないゾーンに属すデバイスに適用されます。

更新ルールの例

次に、ゾーンベースの更新専用に作成されたゾーンが割り当てられた更新ルールの例を示します。

更新ルールの例	割り当てられたゾーン
Windows Server - テスト	• Windows Server - 米国テスト更新ゾーン • Windows Server - 欧州テスト更新ゾーン
Windows Server - パイロット	• Windows Server - 米国パイロット更新ゾーン • Windows Server - 欧州パイロット更新ゾーン
Windows Server - 実稼働	• Windows Server - 米国実稼働更新ゾーン • Windows Server - 欧州実稼働更新ゾーン

CylancePROTECT Desktop および CylanceOPTICS エージェントの更新の管理

作業を始める前に： エージェント更新のテスト用に予約されたデバイスを使用して、ゾーンを作成する必要があります。これらのゾーンをテストおよびパイロット更新ルールに関連付けます。テスト用またはプロダクションでの展開用に、独自の更新ルールを追加することができます。ゾーンの作成方法の詳細については、「CylancePROTECT Desktop および CylanceOPTICS を管理するためのゾーンの設定」を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［更新］をクリックします。
2. 必要に応じて、更新ルールを作成します。たとえば、エージェントの更新をテストするためのルールを作成できます。
   a) ［新しいルールを追加］をクリックします。
   b) ルールの名前を入力します。
   c) ［送信］をクリックします。
3. 更新ルールをクリックします。たとえば、［テスト］をクリックします。
4. ［ゾーン］を展開し、この更新ルールに割り当てるゾーンを選択します。
5. ［エージェント］を展開し、更新オプションを選択します。

   メモ： デバイスのエージェントバージョンを更新しない場合は、［更新しない］設定を使用します。更新ルール（実稼働ルールを含む）が異なり、そのルールがエージェントの更新（自動更新または特定バージョンへの更新）を指定する別のゾーンにデバイスが属さないことも確認する必要があります。更新ルールが更新を指定するゾーンにデバイスが属す場合、デバイスは更新されます。更新を指定する複数の更新ルールにデバイスが関連付けられている場合、最もランクの高いルールに従ってエージェントは更新されます。
6. ［**Linux** ドライバを自動更新］ チェックボックスをオンにすると、エージェントが自動的に最新のドライバに更新して、最新の Linux カーネルをサポートできるようになります。Linux ドライバの自動更新機能には、CylancePROTECT Desktop エージェントバージョン 3.1.1000 およびエージェントドライババージョン 3.1.1000 以降が必要です。

7. ［**CylanceOPTICS**］を展開し、更新オプションを選択します。

   自動更新を選択できるのは、CylancePROTECT Desktop エージェントが自動更新を使用するように設定されている場合のみです。
8. パイロット更新ルール、またはパイロットテスト用に作成したルールについては、手順 2〜7 を繰り返してください。
9. プロダクション更新ルール、またはプロダクション用に作成したルールについては、手順 2〜7 を繰り返してください。デフォルトのプロダクション更新ルールにはゾーンを割り当てないでください。このデフォルトルールは、更新ルールがあるゾーンに属さないすべてのデバイスに適用されます。

   プロダクション更新ルールで CylancePROTECT Desktop エージェントが自動更新に設定されている場合、テストルールとパイロットルールは使用できません。作成した更新ルールは、プロダクション更新ルールの構成の影響を受けません。
10. ［保存］をクリックします。

終了したら：

- 更新ルールを追加した場合は、ルールの横にある矢印をクリックして優先順位を設定します。リストの一番上にあるルールは、リストでその下にあるルールよりも優先されます。テスト、パイロット、および実稼働の各ルールは、常にリストの一番下にあり、ランキングを変更することはできません。実稼働更新ルールは、更新ルールのあるゾーンに属さないデバイス、およびどのルールにもエージェントに対する更新が指定されていないゾーンに属すデバイスに適用されます。
- 予定時間の前にデバイスの CylancePROTECT Desktop エージェントの更新をトリガーするには、デバイスでシステムトレイの CylancePROTECT Desktop アイコンを右クリックし、［更新のチェック］をクリックして、Cylance サービスを再起動するか、Cylance ディレクトリから次のコマンドを実行します。

  ```
  CylanceUI.exe-update
  ```
- デバイスポリシーで、メモリ保護、スクリプト制御、デバイス制御のいずれかまたはすべてが有効になっている場合は、エージェントのインストールまたはアップグレード後にデバイスを再起動することをお勧めしますが、厳密には必要ありません。再起動すると、新しいポリシー設定が完全に有効になります。

外部サービスへの Cylance Endpoint Security の接続

Cylance Endpoint Security では、データと機能をサードパーティのサービスや他の BlackBerry 製品と統合できるようにするさまざまなコネクタがサポートされています。1 つの Cylance Endpoint Security テナントを複数の外部サービスに接続できます。

Cylance Endpoint Security では、次のコネクタがサポートされています。

コネクタ	説明
BlackBerry UEM	BlackBerry UEM コネクタを使用すると、Android デバイスおよび iOS デバイスが UEM で管理されているかどうかを CylanceGATEWAY で確認できます。 詳細については、「Cylance Endpoint Security を MDM ソリューションに接続して、デバイスが管理されているかどうかを確認」を参照してください。
Microsoft Intune	Microsoft Intune コネクタを使用すると、Cylance Endpoint Security で組織のモバイルデバイスのリスクレベルを Intune に報告できます。デバイスのリスクレベルは、Intune 管理対象デバイス上の CylancePROTECT Mobile アプリによるモバイル脅威の検出に基づき、計算されます。Intune は、デバイスのリスクレベルに基づいて軽減アクションを実行できます。 詳細については、「Cylance Endpoint Security と Microsoft Intune の統合によるモバイルの脅威への対応」を参照してください。
Okta	Okta コネクタを使用すると、Okta サービスからログイン認証とアクセスの情報を収集し、Cylance コンソールの［アラート］表示で関連情報を表示できます。 詳細については、「Cylance Endpoint Security と Okta の統合」を参照してください。
Mimecast	Mimecast コネクタを使用すると、Mimecast サービスからメール添付ファイルのリスクスコアデータを統合し、Cylance コンソールの［アラート］表示に関連情報を表示できます。 詳細については、「Cylance Endpoint Security と Mimecast を統合」を参照してください。

Cylance Endpoint Security と Okta の統合

Cylance コンソールに Okta 接続を追加して、［アラート］表示で Okta アラートを表示できます。［アラート］表示を使用すると、管理者は 1 つの統合インターフェイスから Okta 認証を表示し、アラートにアクセスできます。Okta コネクタは、［アラート］表示でイベントテレメトリを表示するために Okta イベント API を使用します。［アラート］表示に集約された Okta ユーザー異常イベントには、疑わしいユーザーログイン試行およびブロックされたセキュリティ要求イベントが含まれます。Okta イベントをこれらのカテゴリに集約することで、サードパーティによるログイン試行、ユーザーによる誤りのあるログイン、および疑わしいソース IP アドレスからのログイン試行の可視性が向上します。

［アラート］表示では、会社のユーザーベース全体で禁止された IP アドレスからのリクエストを集約して、考えられるパターンまたはキャンペーンを把握できます。また、表示されたデータには、アクセス試行のソースデバ

イスに関する情報も含まれていることがあります。これにより、要求が人によって行われたか、機械によって行われたかを判断できます。

［アラート］表示に表示できるアラートを生成するための Okta の設定の詳細については、次のリソースを参照してください。

- Okta ヘルプセンター：パスワードポリシーを構成する
- Okta ヘルプセンター：ブロックリストネットワークゾーン

［アラート］表示の詳細については、管理関連の資料の「Cylance Endpoint Security サービスにわたるアラートの管理」を参照してください。

Okta コネクタ追加の前提条件

Cylance Endpoint Security の Okta 接続を設定するには、Okta サービスを使用していくつかのタスクを完了する必要があります。

手順	項目	説明
1	Okta ベース URL の文書化	Okta コネクタの設定中に使用する環境の Okta ベース URL を文書化する必要があります。Okta ベース URL は、Okta サーバーのプロダクション URL になります。 Okta ベース URL を見つけることに関する詳細については、Okta ドキュメントの「Okta ドメインの確認」を参照してください。
2	Okta 管理者の作成	Okta API を使用するには、Okta 管理者を作成する必要があります。BlackBerry では、手順 3 で API トークンにリンクされている専用ユーザーを作成することをお勧めします。この手順は、ワークフローの監査に役立つために推奨されています。これは他の Okta ユーザーがセキュリティ操作ワークフロー用に作成および使用されるトークンを持っていないようにするためのベストプラクティスです。 Okta 管理者の作成に関する詳細については、Okta ドキュメントの「admin を使用した管理者ロール割り当ての作成」を参照してください。
3	Okta API トークンの作成	Okta API への要求を認証するには、Okta API トークンを作成する必要があります。 Okta API トークンの作成に関する詳細については、Okta ドキュメントの「API トークンの管理」を参照してください。

これらの手順を完了したら、Okta コネクタの追加と設定 の手順に従います。

Okta コネクタの追加と設定

作業を始める前に：「Okta コネクタ追加の前提条件」を確認します。

1. 管理コンソールのメニューバーで、［設定］ > ［コネクタ］をクリックします。
2. ［コネクタを追加］ > ［**Okta**］をクリックします。
3. ［全般情報］セクションで、コネクタの名前を入力します。
4. ［**Okta** の設定］セクションで、Okta サービス API の URL、Okta API トークン、およびポーリング頻度を指定します。

   メモ：BlackBerry では、組織の特定のレート制限要件がない限り、ポーリング頻度をデフォルト値のままにすることをお勧めします。
5. ［テスト接続］をクリックします。
6. ［保存］をクリックします。

終了したら：［アラート］表示でアラートを表示および管理します。管理関連の資料の「Cylance Endpoint Security サービスにわたるアラートの管理」を参照してください。

Cylance Endpoint Security と Mimecast を統合

Mimecast 接続を Cylance コンソールに追加できます。Mimecast 添付ファイル保護は、ユーザーが受信したすべてのメール添付ファイルを分析し、設定したポリシーに基づいて添付ファイルを処理できます。

［アラート］表示を使用すると、管理者は 1 つの統合インターフェイスから Mimecast 添付ファイルリスク情報を表示できます。Mimecast は、Mimecast Attachment Protection Service によって提供される添付ファイルリスクテレメトリを表示します。Mimecast が添付ファイルに適用するアクションは、［アラート］表示の応答列に表示されます。Mimecast によって悪意のあるものとして分類されたアラートは、［アラート］表示で高優先度に分類されます。Mimecast によって危険または不明に分類されたアラートは、中優先度に分類されます。Mimecast によって低優先度と見なされたアラートは、［アラート］表示には表示されません。

［アラート］表示では、添付ファイルハッシュを使用してアラートをグループ化します。これにより、組織内の複数のユーザーが受信した類似アラートを同じ脅威のアラートとしてグループ化できます。［検出の詳細］リンクを使用して Mimecast Attachment Protection ダッシュボードにアクセスし、脅威を調査および修復できます。

［アラート］表示の詳細については、管理関連の資料の「Cylance Endpoint Security サービスにわたるアラートの管理」を参照してください。

Mimecast コネクタ追加の前提条件

Cylance Endpoint Security の Mimecast 接続を設定する前に、Mimecast サービスを使用していくつかのタスクを完了する必要があります。

手順	タスク	詳細
1	Mimecast アカウントの作成	管理者は、すべてのサービスユーザーに対して新しいアカウントを作成する必要があります。 詳細については、Mimecast のドキュメントの「Mimecast ユーザーの作成と編集」を参照してください。

手順	タスク	詳細
2	API アプリケーションの追加	API アプリケーションの詳細と設定を指定します。API アプリケーションを設定するときは、［サービスアプリケーション］が選択されていることを確認します。これは、API キーが期限切れにならないようにするために必要です。このオプションが選択されていない場合、キーの有効期限が切れると、Mimecast コネクタの接続が失われます。 Mimecast で API アプリケーションを追加する方法については、Mimecast の『API アプリケーションの管理』ガイドで「API アプリケーションの追加」を参照してください。
3	ユーザー関連付けキーの作成	Mimecast を Cylance Endpoint Security に接続するには、ユーザー関連付けキーを作成する必要があります。 ユーザー関連付けキーの作成方法については、Mimecast の『API アプリケーションの管理』ガイドで「ユーザー関連付けキーの作成」を参照してください。
4	Mimecast 設定をユーザーに通知	Mimecast 設定をユーザーに通知することをお勧めします。事前設定されたメールテンプレートを Mimecast からダウンロードできます。
5	添付ファイル保護の定義とポリシーの設定	安全でないメールが検出されたときに Mimecast が使用する添付ファイル保護の定義とポリシーを設定します。 詳細については、Mimecast のドキュメントの「添付ファイル保護の設定」を参照してください。
6	通知の有効化と設定	すべての API ユーザーに対して通知データを有効にして設定し、アラートビューで確認できるようにします。 詳細については、Mimecast のドキュメントの「添付ファイル保護の設定」を参照してください。

手順	タスク	詳細
7	ディレクトリサービスの有効化	Mimecast ディレクトリサービスを有効化していることを確認して、Mimecast ユーザー情報（メールアドレス）が、Entra または Active Directory サービスに保存されているユーザーデータに関連付けられるようにします。また、この設定では、ディレクトリサービスでユーザーに関連付けられているデバイスおよびデバイスデータとの関連付けも有効になります。 ディレクトリサービスの有効化の詳細については、Mimecast のドキュメントの「ディレクトリの同期」を参照してください。

これらの手順を完了したら、「Mimecast コネクタの追加と設定」の手順に従います。

Mimecast コネクタの追加と設定

作業を始める前に：「Mimecast コネクタ追加の前提条件」を確認します。

1. 管理コンソールのメニューバーで、［設定］ > ［コネクタ］をクリックします。
2. ［コネクタを追加］ > ［**Mimecast**］をクリックします。
3. ［全般情報］セクションで、コネクタの名前を入力します。
4. ［**Mimecast** の設定］セクションで必要な情報を指定し、ポーリング頻度を指定して、ベース URL を選択します。

   Mimecast キー生成に関する詳細については、Mimecast ドキュメントの「API アプリケーションの管理」を参照してください。
5. トグルコントロールをクリックして、ポーリングを有効にします。
6. ［テスト接続］をクリックします。
7. ［保存］をクリックします。

終了したら：［アラート］表示でアラートを表示および管理します。管理関連の資料の「Cylance Endpoint Security サービスにわたるアラートの管理」を参照してください。

付録：Windows 仮想マシンに CylancePROTECT Desktop を展開するためのベストプラクティス

CylancePROTECT Desktop を使用して、物理マシンと仮想マシンの両方を保護できます。このセクションでは、CylancePROTECT Desktop エージェントを Windows ベースの仮想デスクトップインフラストラクチャ（VDI）ワークステーションに展開するためのベストプラクティスの詳細について説明します。

CylancePROTECT Desktop は、IOPS ではなく、ゲスト単位でメモリを集中的に消費することもないため、ゲスト OS コンポーネントとして十分に機能します。仮想環境での CylancePROTECT Desktop エージェントの準備と展開は、物理コンピュータでの展開と同様です。このセクションの展開ステップとベストプラクティスにより、割り当てられたリソースが少ない仮想環境でエージェントが効率的に実行されるようになり、危険または異常なファイルがないゴールドイメージを作成できるようになります。ゴールドイメージが十分に検証されたら、そこからプロダクション VDI イメージを複製できます。

仮想マシンで CylancePROTECT Desktop を使用するための要件と考慮事項

項目	要件または考慮事項
サポートされているエンタープライズ仮想化テクノロジ	• Microsoft Hyper-V • Citrix XenDesktop • VMware Horizon/View • VMware Workstation • VMware Fusion

項目	要件または考慮事項
非永続仮想マシン	非永続 VM は、セッションが終了すると削除され、同じゴールドイメージに置き換えられます。新しい VM が作成されると、CylancePROTECT Desktop エージェントは VM を管理コンソールに登録し、同じエンドポイントであるはずのデバイスが重複して登録されます（古い方の登録は、オンラインに戻らないオフライン重複デバイスレコードとして扱われます）。 同じ VM デバイスの重複登録を防止するために、ゴールドイメージに CylancePROTECT Desktop エージェントをインストールする場合は、次のインストールパラメーターのいずれかを使用します。 • `VDI=<X>`：*<X>* の値は、エージェントがデフォルトのエージェントフィンガープリントメカニズムではなく、VDI フィンガープリントを使用して仮想マシンの識別を開始するタイミングを決定するカウンタです。エージェントが VDI フィンガープリントを使用している場合、重複デバイスは登録されません。 • たとえば、`VDI=2` パラメーターを使用して、ゴールドイメージにエージェントをインストールします。ゴールドイメージを使用して親イメージを作成します。次に、親イメージを使用してワークステーションイメージを作成します。ゴールドイメージと親イメージによってカウンタが 2 になっているため、エージェントはワークステーションイメージに対して VDI フィンガープリントの使用を開始します。 • `AD=1`：このパラメーターは `VDI=<X>` と同じように動作しますが、エージェントが VDI フィンガープリントの使用を開始するタイミングを定義するカウンタはありません。エージェントは、ゴールドイメージとゴールドイメージから作成したイメージに対して、VDI フィンガープリントを使用します。このパラメーターは、CylancePROTECT Desktop と CylanceOPTICS の統合インストーラの .exe 形式ではサポートされていません。
メモリ保護およびスクリプト制御機能	VDI 環境でメモリ保護およびスクリプト制御機能を有効にする前に、次の点を考慮してください。 • どちらの機能も、プロセスの注入を使用して、不要なコードや不正なコードを識別してブロックします。仮想化環境のプラグイン、ツール、または DLL は悪影響を及ぼすおそれがあるため、プロダクションワークステーションに展開する前に、メモリ保護およびスクリプト制御のオプションをテストする必要があります。 • メモリ保護オプションをアラートのみモードでテストし、デバイスポリシーをより厳格に変更することをお勧めします。システムが不安定になった場合は、メモリ保護をオフにできます。 • フェイルセーフオプションとしてシステムの競合や不安定性が発生した場合は、メモリ保護の互換モードを有効にできます。 • 「Known incompatibilities for Memory Protection and Script Control v2 in Protect 1580 and later（Protect 1580 以降のメモリ保護とスクリプト制御 v2 の既知の非互換性）」を参照してください。

項目	要件または考慮事項
エージェント UI を無効にするオプション	CylancePROTECT Desktop エージェント UI を無効にしてシステムリソース全体を節約するオプションがあります。詳細については、「Windows のインストールパラメーター」を参照してください。
制限事項	仮想環境で CylancePROTECT Desktop エージェントを実行したときに報告される問題を確認するには、「VDI Trending Issues（VDI トレンドの問題）」を参照してください。

仮想マシンへの CylancePROTECT Desktop の展開

作業を始める前に：「仮想マシンで CylancePROTECT Desktop を使用するための要件と考慮事項」を確認します。

1. VDI ゴールドイメージの準備に使用するデバイスポリシーを作成します。ポリシーで次のオプションを設定します。

デバイスポリシーのカテゴリ	オプション
ファイルアクション	安全ではないファイルタイプと異常ファイルタイプに対して、［自動隔離（実行制御あり）］をオンにします。
保護設定	• ［バックグラウンド脅威検出］（1 回実行）をオンにします。 • ［新しいファイルを監視］をオンにします。

2. VDI ゴールドイメージを準備します。
   a) CylancePROTECT Desktop エージェントをゴールドイメージにインストールします。たとえば、次のインストールコマンドとパラメータを使用します。

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

   b) 手順 1 で作成したデバイスポリシーをゴールドイメージに適用します。
   バックグラウンド脅威検出スキャンが完了するまで待ちます。ディスクのサイズとスキャン時のイメージ上のアクティビティによっては、完了までに数時間かかる場合があります。
   c) バックグラウンド脅威検出スキャンの結果を確認し、必要に応じて、ゴールドイメージで検出されたバイナリを CylancePROTECT Desktop の隔離リストまたはセーフリストに追加します。
3. ゴールドイメージで、レジストリからフィンガープリントの値をクリアします。
   a) CylanceSvc サービスを停止します。support.blackberry.com にアクセスして、「KB 107236」を参照してください。
   b) ローカル管理者アカウントを使用して、レジストリキーの所有権を取得し、次のレジストリにフルコントロール権限を追加します。 `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`
   c) 上記のレジストリをバックアップまたはエクスポートします。
   d) FP、FPMask、FPVersion のレジストリキーを削除します。
4. ゴールドイメージを作成します。

5. プロダクション VDI ワークステーション向けのデバイスポリシーを作成します。BlackBerry では、プロダクションワークステーションでユーザーが有効にするオプションに加えて、ポリシーで次のオプションをお勧めします。

デバイスポリシーのカテゴリ	オプション
ファイルアクション	• 安全ではないファイルタイプと異常ファイルタイプに対して、［自動隔離（実行制御あり）］をオンにします。 • ［自動アップロード］をオンにします。
保護設定	• ［新しいファイルを監視］をオンにします。 • ［バックグラウンド脅威検出］をオフにします。

6. ゴールドイメージを実稼働ワークステーションに展開して複製します。複製した各イメージの UUID または ID は、ゴールドイメージとは異なる一意のものにする必要があります。
7. 手順 5 のデバイスポリシーを実稼働ワークステーションに適用します。

終了したら： 複製されたデバイスの場合、［ゾーンベースのエージェントの更新］を［更新しない］またはエージェントの特定のバージョンに設定します。更新はゴールドイメージで管理する必要があります。「複製されたデバイスでの CylancePROTECT Desktop の更新」を参照してください。

複製されたデバイスでの CylancePROTECT Desktop の更新

作業を始める前に： 仮想マシンへの CylancePROTECT Desktop の展開。

1. ゴールドイメージで、CylancePROTECT Desktop エージェントを更新します。
2. ゴールドイメージに追加の更新またはファイルが適用された場合は、VDI 準備デバイスポリシーをゴールドイメージに適用し、バックグラウンド脅威検出スキャンを完了できるようにします。
3. バックグラウンド脅威検出スキャンの結果を確認し、必要に応じて、ゴールドイメージで検出されたバイナリを CylancePROTECT Desktop の隔離リストまたはセーフリストに追加します。
4. プロダクションデバイスポリシーをゴールドイメージに適用します。
5. ゴールドイメージを再シールします。
6. 複製されたデバイスにエージェントの更新が反映されたことを確認します。

商標などに関する情報

該当する特許は、次の場所で確認できます：www.blackberry.com/patents。

本書は、参照用として本書で取り上げるすべての文書（提供される文書または BlackBerry の Web サイトで参照可能な文書）を含めて「現状のまま」または「参照可能な形で」提供されるか、またはアクセスすることができ、BlackBerry Limited およびその関連会社（「BlackBerry」）はいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry は本書の誤記、技術的な誤りまたはその他の誤り、エラー、遺漏について何ら責任を負いません。BlackBerry の所有権、機密情報および/または企業秘密を保護するため、本書では一部の BlackBerry テクノロジの側面を一般化された用語で記述している場合があります。BlackBerry は、本書に含まれる情報を定期的に変更する権利を留保します。ただし、BlackBerry には、本書への変更、更新、拡張、または他の追加を適時ユーザーに提供する義務はないものとします。

本書は、第三者をソースとする情報、ハードウェアまたはソフトウェア、製品またはサービス（コンポーネントや、著作権保護されたコンテンツなど）、および/または第三者の Web サイト（これらをまとめて「サードパーティ製品およびサービス」という）への参照を含んでいる可能性があります。BlackBerry は、サードパーティ製品およびサービスの内容、正確性、著作権遵守、互換性、性能、信頼性、適法性、品格、リンク、他の側面などに限定することなく、サードパーティ製品およびサービスを一切管理することはなく、責任も負いません。本書においてサードパーティ製品およびサービスを参照することは、BlackBerry がサードパーティ製品およびサービスまたは第三者を保証することを意味するものではありません。

該当する司法管轄地域の適用法で明確に禁じられている場合を除き、本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスについて、耐久性、特定の目的または使用に対する適合、商品性、適性品質、権利侵害の不存在、品質満足度、権原、または制定法、慣習法、取引過程、商慣習から生じる、本書またはその使用に関する、または性能または性能の不履行に関する条件付け、承認、表明、保証などに限定することなく、明示的または黙示的に、いかなる条件付け、承認、表明、または保証も除外されます。ユーザーは、国や地域によって異なる他の権利を有する場合もあります。一部の司法管轄地域では、黙示的な保証および条件の除外事項または限定事項は禁止されています。法律で認められている範囲で、本書に関連する黙示的な保証または条件は、上記に定めるように除外できないが限定できる場合、ユーザーが本書または該当する対象物を初めて入手してから 90 日間に限定されます。

該当する司法管轄地域の適用法で認められている最大限の範囲で、本書またはその使用に関連して、または本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスの性能または性能の不履行に関連して、直接的、必然的、典型的、偶発的、間接的、特殊的、懲罰的、または加重的損害、金銭的損失による損害（利益または収益の損失、予想される貯蓄の未達成、事業の中断、ビジネス情報の消失、ビジネス機会の喪失、データの破損または消失、データの送受信の失敗、BlackBerry 製品またはサービスと併用したアプリケーションに関連する問題、ダウンタイムコスト、BlackBerry 製品またはサービスあるいはその一部の使用機会や通信サービスの使用機会の喪失、代替品コスト、保険料、設備費、保守費、資本コストなど）に限定することなく、損害を予想できたかどうかを問わず、BlackBerry が損害の可能性について勧告を受けていた場合を含め、いかなる場合においても、BlackBerry はいかなる損害の責任も負わないものとします。

該当する司法管轄地域の適用法で認められている最大限の範囲で、契約、不法行為、またはユーザーに対する過失責任または厳格責任について、BlackBerry は他のいかなる義務、責務、または責任も負わないものとします。

本書の限定事項、除外事項、および免責事項は、（A）訴訟原因、請求、またはユーザーによる行為（契約違反、過失、不法行為、厳格責任、その他の法理論など）の性質に関係なく、この契約の基本目的または本書に記載されている救済策の根本的違反または不履行を免れるため、（B）BlackBerry およびその関連会社、その後継

者、譲受人、代理業者、納入業者（通信事業者を含む）、認可された BlackBerry 販売業者（通信事業者を含む）およびその取締役、従業員、および請負業者に適用されます。

上記に定める限定事項および除外事項に加えて、いかなる場合においても、BlackBerry の取締役、従業員、代理業者、販売業者、納入業者、請負業者または BlackBerry の関連会社は、本書に起因または関連する責任を負わないものとします。

ユーザーは、サードパーティ製品およびサービスの加入、インストール、または使用前に、通信事業者がサードパーティ製品およびサービスのすべての機能をサポートすることに同意していることを確認する責任を負います。一部の通信事業者は、BlackBerry® Internet Service への加入によるインターネット閲覧機能を提供しない場合があります。サービスの利用、ローミング、サービスプラン、その他の機能については、通信事業者に問い合わせてください。BlackBerry 製品およびサービスにおけるサードパーティ製品およびサービスのインストールまたは使用には、第三者の権利を侵害または妨害しないように、特許、商標、著作権、または他のライセンスが必要になる場合があります。ユーザーは、サードパーティ製品およびサービスを使用するかどうかを決定し、使用するためにサードパーティライセンスが必要かどうかを確認する責任を負います。必要な場合、ユーザーはライセンスを取得する責任を負います。ユーザーは、必要なライセンスをすべて取得するまで、サードパーティ製品およびサービスをインストールまたは使用してはなりません。BlackBerry 製品およびサービスで提供されるサードパーティ製品およびサービスは、ユーザーの便宜のために「現状のまま」提供され、BlackBerry は明示的にも黙示的にもいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry はそれに関連するいかなる責任も負わないものとします。ユーザーによるサードパーティ製品およびサービスの使用は、ライセンスまたは BlackBerry との他の契約で明示的に対象になっている場合を除き、個別のライセンスおよび第三者との他の該当契約の条件に従うものとし、その制約を受けるものとします。

BlackBerry 製品またはサービスの使用条件は、個別のライセンスまたは BlackBerry との他の該当契約に定められています。本書の内容は、本書以外に BlackBerry 製品またはサービスの一部に対して BlackBerry が提供した文書による明示的な契約または保証を破棄するものではありません。

BlackBerry Enterprise Software には、特定のサードパーティ製ソフトウェアが組み込まれています。このソフトウェアに関連するライセンスおよび著作権情報は、http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp でご確認いただけます。

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

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

Published in Canada