Carbon Black.

PSC センサー インストール ガイド

Cb Predictive Security Cloud

2018 年 10 月 1 日

内容

PSC センサーは、Windows エンドポイントおよび macOS エンドポイントに展開され、Carbon Black 分析およびクラウドと通信します。PSC センサーは次の方法でエンドポイントにインストールできます。

- エンド ユーザー直接インストール
  - 招待されたユーザーが、インストール コードが記載された E メールを受け取り、招待された各ユーザーが、PSC センサーをエンドポイントに直接インストールします。
  - 少数のエンドポイントにセンサーを展開するときに役立ちます。
- 無人インストール
  - ソフトウェア配布ツールを使用して、PSC センサーをスクリプト化または自動化された方法でインストールします。
  - 多くのエンドポイントにセンサーをインストールするときに役立ちます。

運用環境の要件については、『Cb Defense 運用環境の要件』を参照してください。センサーの管理、更新、およびアンインストールについては、『Cb Defense ユーザー ガイド』を参照してください。さらにサポートが必要な場合は、Cb Defense ナレッジベースの記事を参照してください。

注意

このリリースでは、Linux センサーはベータ版でのみサポートされています。 Linux センサーをインストールする手順については、Linux センサーのインストール （ベータ）を参照してください。

センサーをインストールする前に

ポリシーをセンサーに割り当てる

Cb Defense の各センサーは、センサーに適用するポリシー ルールを決定する 1 つの「ポリシー」に割り当てられます （『Cb Defense ユーザー ガイド』の「定義済みのポリシーによる攻撃からの防御」を参照）。デフォルトでは、次のどの条件にも該当しない場合、新しい各センサーは 「標準」ポリシーに属します。

- 以前 「センサー グループ」を作成し、展開したセンサーが 「センサー グループ」の条件に一致する。また、ターゲット ポリシーが標準ポリシーではない。

  センサー グループ内のすべてのセンサーは、センサーに関連付けられているメタデータと定義した条件に基づいて、ポリシーに自動で割り当てられます。この機能には、 Windows センサー v3.1 または macOS センサー v3.2 以降が必要です。『Cb Defense ユーザー ガイド』の「ポリシー自動割り当て用のセンサー グループの管理」を参照してください。
- 無人インストール時に別のポリシーを定義する。

エンド ユーザー直接インストール時にポリシーを定義することはできません。ただし、センサーの展開後にセンサーが割り当てられたポリシーは変更できます。

ローカル スキャンの影響を考慮する

シグネチャ ファイルの更新は、デフォルトではポリシーによってオンになります。そのため、センサー展開時に初期シグネチャ ファイルをダウンロードするために帯域幅の使用率が上昇する場合があります。ネットワークが飽和状態になるのを避けるため、次のいずれかを行うことをお勧めします。

- センサーを小さいバッチで展開する。
- ポリシー設定を切り替えて自動シグネチャ更新を無効にする スタンドアロン インストーラーを使用して初期シグネチャ パックを展開してから、自動シグネチャ更新を再度有効にする。
- シグネチャ更新用のローカル ミラー サーバーをセットアップし、センサーがローカル サーバーから更新をダウンロードするようにポリシーを構成する。『Cb Defense ユーザー ガイド』の 「シグネチャ ミラーの手順」を参照してください。

High Sierra の macOS v3.1 センサー

macOS v3.1 センサーを macOS 10.13、High Sierra にインストールするには、管理ポリシーまたはエンド ユーザーによる製品カーネル機能拡張の初期 KEXT 承認が必要です。これは Apple によって求められる要件で、ドライバー コンポーネントがあるすべてのサードパーティ製品に適用されます。センサーには、以前の KEXT 承認ステータスに関係なく KEXT 承認が必要です。

Carbon Black では、 MDM ポリシー、 NetBoot、または事前構成済みイメージを使用して、事前承認済みドライバーで High Sierra エンドポイントを事前構成することをお勧めします。この方法により、特に無人モードでのセンサー展開が簡素化されます。無人インストール中に発生する CLI メッセージでは、–kext フラグでインストールをスキップして、終了する必要がありあます。

センサーのインストール前にドライバーが事前承認されていない場合の動作は次のとおりです。

- 無人インストール：インストールにより成功が確定し、返されますが、インストール ログに警告が記録されます。ドライバーをロードできないため、センサーはバイパス状態になり、この状態はクラウドに報告されます。 KEXT の承認後、センサーは 1 時間以内に復元し、完全保護状態になります。
- 直接インストールは無人インストールと同様に処理されますが、次の 2 つの点が異なります。(1) センサー インストールでは、システム設定を使って KEXT を承認するよう求めるダイアログ メッセージがエンド ユーザーに表示されます。また、(2) インストーラーはユーザーが KEXT を承認する時間を確保するために、最大 10 分間停止します。

オペレーティング システムに対応していないセンサーを含むデバイス、または承認されていないセンサー KEXT を含むデバイスを特定するには

1. PSC にログインし、［**Endpoints** （エンドポイント）］をクリックします。
2. ［**Status** （ステータス）］フィルターを ［**All** （すべて）］に変更し、次の検索クエリを入力します。

   ```
   sensorStates:UNSUPPORTED_OS
   ```

3. 次の検索クエリを使用すると、使用されているセンサーがオペレーティング システムに対応しているが、センサー KEXT が承認されていないデバイスを特定できます。

   ```
   sensorStates:DRIVER_INIT_ERROR
   ```

詳細については、「インストール / アップグレード用に Mac Sensor 3.0 KEXT を承認する方法」および Apple Technical Note TN2459 を参照してください。

エンド ユーザー直接インストール

エンド ユーザー直接インストールは、展開するセンサーの数が少ない場合や、無人インストール方法を使用できない場合に便利です。

重要

センサーをインストールするには、エンドポイントの管理者権限がエンド ユーザーに必要です。

エンド ユーザー直接インストールを実行するようにユーザーを招待するには

1. PSC にログインし、［**Endpoints** （エンドポイント）］をクリックします。
2. ［**Sensor Options** （センサー オプション）］をクリックし、［**Add user(s)** （ユーザーの追加）］をクリックします。
3. 1 人または複数のユーザーを追加します。複数のユーザーを追加するには、E メール アドレスをコンマで区切って入力し、［**Add** （追加）］をクリックします。

   ユーザーはインストーラーのダウンロード リンクとユニークなシングル ユース インストール コードが記載された E メールの招待を受け取ります。インストール コードの有効期間は 1 週間です。

ヒント：E メールの招待を送信することをユーザーに事前に知らせることをお勧めします。事前に送信する E メールでは、どちらのバージョンをダウンロードするかをユーザーに伝えてください （32 ビットまたは 64 ビット）。 32 ビット バージョンのセンサーは、 64 ビット版の Windows では動作しません。

この事前の E メールでは、展開中にインストール コードを手動で入力する必要があることも説明してください。インストール コードのコピー / 貼り付けがいつも適切に機能するとは限りません。

新しいインストール コードを送信するには

1. PSC にログインし、［**Endpoints** （エンドポイント）］をクリックします。
2. インストール コードが期限切れになっているセンサーを検索して選択します。
3. ［**Take Action**（アクション実行）］をクリックしてから、［**Send new installation code** （新しいインストール コードの送信）］をクリックします。

無人インストール

無人インストールは、センサーのインストールを、グループ ポリシー、システム管理ツールなど、さまざまな方法を使用してエンドポイント上でローカルに実行する、スクリプト化または自動化された方法です。

この方法は、多くのエンドポイントにセンサーをインストールするときに役立ちます。

無人インストール作業は、次の手順に分けられます。

ステップ 1：会社登録コードを取得する。

ステップ 2：センサー キットをダウンロードする。

ステップ 3：ソフトウェア配布ツールを使用してセンサーを展開する。

注意

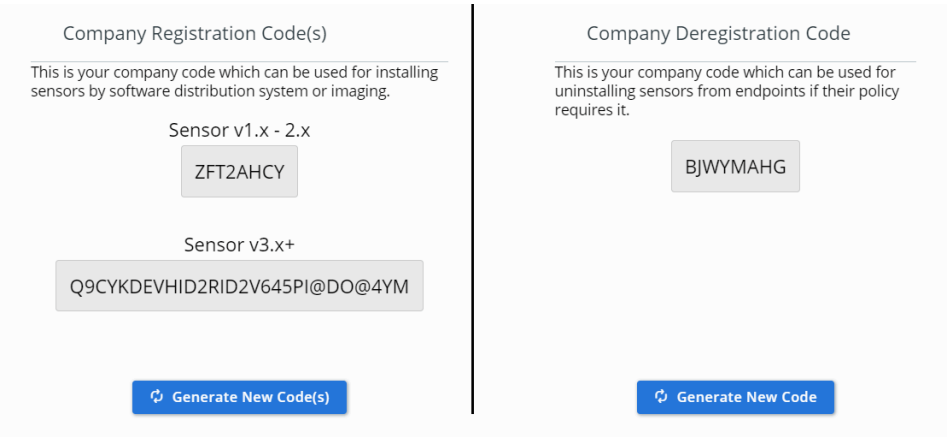
センサーは、初回のインストール時にプロキシ設定の自動検出を試みます。これにはテストが必要です。自動検出が成功しない場合は、無人インストール時の MSI コマンド ラインにプロキシ IP とポートが含まれるようにパラメーターを定義する必要があります。組織でプロキシが使用されている場合は、『Cb Defense ユーザー ガイド』の 「プロキシの構成」を参照してください。

ステップ 1：会社登録コードを取得する

新しいセンサーを組織に登録するには、会社登録コードが必要です。

会社登録コードを取得するには

1. PSC にログインし、［**Endpoints** （エンドポイント）］をクリックします。
1. ［**Sensor Options** （センサー オプション）］をクリックし、［**Company codes** （会社コード）］をクリックします。
2. ［**Company Registration Code(s)** （会社登録コード） ］の下にある ［**Generate New Code(s)** （新しいコードの生成）］ボタンをクリックします。



3. 生成されたコードを、展開中に入力できるようにメモします。

備考

3.0 バージョン以降のセンサーについては、会社登録コードが長くなりました。3.0 以降のセンサーのインストールには、3.0 と指定されているコードを使用してください。また、バージョン 3.0 より前のセンサーの更新には、1.x ～ 2.x のコードを使用してください。センサー インストール時のコード入力プロセスは同じです。ソフトウェア展開ツールや既存のインストール スクリプトは、長くなった新しいコードを使用するように更新する必要があります。

会社登録コードは変更できます。特定の会社登録コードを使用してセンサーを展開した後に、コードを変更し、新しいコードを使用してセンサーを展開しても、古いセンサーは引き続き動作します。インストール済みのセンサーには影響はありません。新しいコードを使用する必要があるのは、新しいインストール パッケージのみです。

ステップ 2：センサー キットをダウンロードする

1. PSC にログインし、［**Endpoints**（エンドポイント）］をクリックします。
2. ［**Sensor Options**（センサー オプション）］をクリックし、［**Download sensor kits**（センサー キットのダウンロード）］をクリックします。
3. 適切なセンサーキットの**バージョン**を選択し、リンクをクリックしてダウンロードします。

ステップ 3：ソフトウェア配布ツールを使用してセンサーを展開する

このセクションでは、次の展開を実行する方法について説明します。

- Windows センサーの無人インストール
- グループ ポリシーを使用した Windows センサーの無人インストール
- macOS センサーの無人インストール
- VDI 環境へのセンサーの無人インストール
- Linux センサーのインストール （ベータ）

Windows センサーの無人インストール

無人Windowsインストール時には、次のコマンド ライン パラメーターが使用されます。

パラメーター	必須または任意	説明
/q	必須	このパラメーターを指定せずにインストールを実行すると、有人インストーラーが有効になり、 6 桁のインストール コードを入力するように求められます。
/i	必須	このパラメーターは、 MSI にインストールを実行するよう指示します。
/L*	任意	MSI インストール ログ ファイルを作成します。
/L*vx	任意	詳細なMSIインストール ログ ファイルを作成します。これは、/L* パラメーターよりも推奨されます。インストール時の問題のトラブルシューティングに役立つより詳細な情報が提供されるためです。

Windows インストールの例

次のコマンドは、 1 行で入力する必要があります。ここでは、ドキュメントの書式上の都合のため、複数行にわたって記載されています。

会社登録コードを使用する基本的な無人インストールの例

```
msiexec /q /i C:\Users\UserFolderName\Desktop\installer_vista_win7_win8-32-2.0.4.9.msi /L* log.txt COMPANY_CODE=3TRY2U2QHP5@3P5@KH08FPL5NL0XU
```

この基本インストールの例では、ポリシーが指定されていません。したがって、センサーは、標準ポリシー、またはセンサー グループによって指定されたポリシーに割り当てられます（センサー グループが定義済みで、センサーがセンサー グループの条件と一致する場合）。

特定のポリシーに対する基本的な無人インストールの例

```
msiexec /q /i C:\Users\UserFolderName\Desktop\installer_vista_win7_win8-32-2.0.4.9.msi /L* log.txt COMPANY_CODE=3TRY2U2QHP5@3P5@KH08FPL5NL0XU GROUP_NAME=Phase1
```

インストール スクリプトで GROUP_NAME（ポリシー割り当てオプション）を使用すると、センサーは手動で特定のポリシーに割り当てられます。センサー グループを使用してポリシーの割り当てを決定するには、このオプションを省略します。

エンドポイントをバイパス状態にする基本的な無人インストールの例

```
msiexec /q /i "C:\UsersUserFolderName\Desktop\installer_vista_
win7_win8-64-1.0.6.193.msi" /L* log.txt
COMPANY_CODE=3TRY2U2QHP5@3P5@KH08FPL5NL0XU BYPASS=1
```

バイパス モードでは、センサーからクラウドにデータが送信されません。センサーは受動的に機能しており、エンドポイントのアプリケーションに干渉することも、アプリケーション監視を行うこともありません。

センサーをバイパス モードでインストールすると、詳細なテストが可能になります。センサーとエンドポイント上の別のアプリケーションとの間で相互運用性に関する問題が発生しても、その問題は、アクティブに切り替えられたセンサーに限定されます。Carbon Black User eXchange に記載されている情報を参照してもその問題を解決できない場合は、 Carbon Black テクニカル サポートにお問い合わせください。

Windows でサポートされるコマンド

次の表に記載されていないコマンドを使用すると、インストールに失敗する場合があります。

PSC は、プロキシ設定の自動検出をサポートしていますが、プロキシ認証（有効な場合）で使用されるマシンの認証情報の入力を求めたり、認証情報の受け渡しを行ったりすることはありません。環境でプロキシ認証が必要な場合は、コマンド ライン オプションを使用して、PROXY_SERVER= 値、PROXY_USER= 値、および PROXY_PASSWD= 値を指定してください。

Windows でサポートされるコマンド

コマンド オプション（大文字小文字を区別）	値	備考
AUTO_UPDATE= 値	1/0 または true/false	デフォルトは true（自動更新が有効）です。これをオフにすると、更新がバックエンドからプッシュされなくなります。
BACKGROUND_SCAN= 値	1/0 または true/false	デフォルトは true です。
BASE_IMAGE= 値	1/0 または true/false	デフォルトは false です。インストールされたイメージは、子イメージにクローンされる基本のイメージです。このオプションは、 VDI ではサポートされません。

Windows でサポートされるコマンド

コマンド オプション（大文字小文字を区別）	値	備考
BYPASS= 値	1/0 または true/false	デフォルトは false です。これを true に設定すると、センサーのバイパス モードが有効になります。
CLI_USERS=sid	認証されたユーザー グループの SID 値	このフィールドを使用して、RepCLI ツールを有効にします。指定されたユーザー グループの任意のメンバーが認証済み RepCLI コマンドを使用できます。『Cb Defense ユーザー ガイド』を参照してください。
COMPANY_CODE= 値	会社登録コード	無人インストールでは必須です。エンド ユーザー直接インストールでは有効ではありません。
CONNECT_LIMIT= 値	毎時の接続数	オプション。デフォルトでは、無制限になっています。
DELAY_SIG_DOWNLOAD= 値	1/0	デフォルトでは、シグネチャ / 定義のダウンロードは遅延されます。デフォルト値を変更しないことをお勧めします。
DISABLE_LIVE_RESPONSE= 値	1/0	値を 1 にすると、センサーの Live Response 機能が無効になります。デフォルト値は 0 です。 Live Response の詳細については、『Cb Defense ユーザー ガイド』の「Live Response の使用」を参照してください。
FILE_UPLOAD_LIMIT= 値	メガバイト数を表す 4 バイトの整数	例:値として 3 を指定すると、3*1024*1024バイトに制限されます。デフォルトは5です。
GROUP_NAME= 値	文字列値	オプションのポリシー名の割り当て。ポリシー名にスペースが含まれている場合、この値は二重引用符で囲む必要があります。
LAST_ATTEMPT_PROXY_SERVER	値の例： 10.101.100.99:8080	オプション。他のすべての方法が失敗した場合 （動的プロキシ検出を含む） 、センサーはこの設定を使用してクラウドへのアクセスを試みます。

Windows でサポートされるコマンド

コマンド オプション（大文字小文字を区別）	値	備考
LEARNING_MODE= 値	値には、イベント タイプを制限する、センサーのインストール後の時間数を指定します。 これは、初期インストール後に一部のレポート タイプをドロップして、バックエンドの負荷を軽減するためのメカニズムです。 通常、センサーのインストール直後はバックエンドに送信されるレポートが多くなります。これは、ハッシュ動作の通常負荷に加えて、新しく検出されたハッシュに関してセンサーがレポートするためです。 学習モードでは、センサーがハッシュを検出している間、ファイルおよびプロセス動作のみレポートされます。学習モードの期間中、API、レジストリ、およびネットワーク動作はドロップされます。	オプション。デフォルトでは、無効になっています。
PROXY_PASSWD= 値	プロキシのパスワード	オプション。
PROXY_SERVER= 値	サーバー：ポート	オプション。
PROXY_USER= 値	プロキシ ユーザー名	オプション。
QUEUE_SIZE= 値	イベント バックログ（MB 単位）	オプション。デフォルトは 100MB です。この値には SSL オーバーヘッドが含まれません。
RATE_LIMIT= 値	KB/ 時	オプション。デフォルトでは、無制限になっています。
VDI= 値	1/0 または true/false	デフォルトは false です。
USER_EMAIL= 値	Email address（E メール アドレス） 使用例： user@example.com	オプション。

Windows ログ ファイル

Windows インストール プロセスを示す MSI ログを取得するには、`/L* log.txt` コマンド ライン オプションを使用します。`C:\Users\Username\AppData\Local\Temp` にクラウドへのセンサー登録の試行を示す `confer-temp.log` ファイルも生成されます。これらの 2 つのログ ファイルは、インストールおよびアップグレードの問題をトラブルシューティングするために必要です。

Windows でインストールされるサービス

- メインのセンサー サービス：RepMgr64.exe、RepMgr32.exe、Scanhost.exe（ローカル スキャンが有効の場合）
- ユーティリティ：RepUtils32.exe、 RepWmiUtils32.exe
- UI：RepUx.exe

グループ ポリシーを使用した Windows センサーの無人インストール

グループ ポリシーを使用して、センサーの無人 Windows インストールを実行できます。これを行うには、編集した MSI にパラメーターを渡すバッチ ファイルを作成する必要があります。

グループ ポリシーを使用すると、デフォルトでは起動時にソフトウェアがインストールされます。そのため、センサーをインストールするには、エンドポイントを再起動する必要があります。

.MST ファイルを作成するには

1. PSC にログインし、［**Endpoints** （エンドポイント）］をクリックします。
2. ［**Sensor Options** （センサー オプション） ］をクリックし、［**Download sensor kits** （センサー キットのダウンロード） ］をクリックします。展開するセンサーの `.msi` ファイルをダウンロードします。
3. Orca インストーラーが含まれている Windows SDK を https://developer.microsoft.com/en-us/windows/downloads/sdk-archive からダウンロードします。
4. Windows SDK をインストールし、`Orca.msi` をインストールします。
5. `C:\Program Files (x86)\Orca` に移動し、`Orca.exe` を実行します。
6. ステップ 2 でダウンロードした `.msi` ファイルを右クリックし、［**Edit with Orca** （Orca で編集）］をクリックします。
7. ［**Transform** （トランスフォーム） ］＞ ［**New Transform** （新規トランスフォーム）］の順にクリックします。
8. ［**Tables** （テーブル）］＞ ［**Property** （プロパティ）］の何もない場所で右クリックして、［**Add row** （行の追加）］をクリックします。
9. ［**Property** （プロパティ）］をクリックし、「COMPANY_CODE」と入力します。
10. ［**Value** （値）］をクリックし、会社登録コードを入力します （「ステップ 1：会社登録コードを取得する」（6 ページ）を参照）。

11. VDI 環境に展開する場合は、「VDI」と 「GROUP_NAME」のプロパティを追加します。VDI 環境への展開の詳細については、「VDI 環境へのセンサーの無人インストール」（18 ページ）を参照してください。
12. ［**Transform** （トランスフォーム）］＞ ［**Generate Transform** （トランスフォームの生成）］の順にクリックし、 `.mst` ファイル形式でファイルを保存します。

> **注意**
>
> PSC の `.msi` および `.mst` ファイルのパスは、ネットワーク内のどの場所からでもアクセスでき、全ユーザーが少なくとも読み取り権限を持つネットワーク共有に配置してください。

グループ ポリシーを使用してセンサーを展開するには

1. ［**スタート**］＞［**管理ツール**］＞［**グループ ポリシー管理**］の順にクリックします。
2. ［**フォレスト：YOURDOMAIN**］＞ ［**ドメイン**］＞ **YOURDOMAIN** ＞ ［**グループ ポリシー オブジェクト**］に移動します。
3. `Group Policy Objects` フォルダーを右クリックし、［**New** （新規）］をクリックします。
4. 新しいグループ ポリシー オブジェクト (GPO) の名前を入力します。
5. ［**グループ ポリシー オブジェクト**］フォルダーで新しい GPO をクリックします。
6. 右下のパネルの ［**セキュリティ フィルター処理**］フォルダーから ［**認証済みユーザー**］のエントリを削除します。
7. 特定のエンドポイントにのみセンサーを展開するには、センサーを展開する特定の特定のコンピューターの名前をすべて追加します。ドメイン内のすべてのエンドポイントにセンサーを展開するには、「Domain Computers」グループを追加します。［**ナビゲーション**］パネルで `YOURDOMAIN` フォルダーを右クリックします。［**Link an existing GPO** （既存の GPO のリンク）］をクリックします。新しい GPO をクリックし、［**OK**］をクリックします。
8. `Group Policy Objects` フォルダーで GPO を右クリックし、［**Edit** （編集）］をクリックします。
9. 新しいウィンドウで、［**コンピューターの構成**］＞ ［**ポリシー**］＞ ［**ソフトウェアの設定**］＞ ［**ソフトウェア インストール**］に移動します。右側にある空のパネル内を右クリックし、［**新規**］＞ ［**ソフトウェア パッケージ**］に移動します。表示される新しいウィンドウで、以前作成した共有 （`\\YOURSERVERNAME\FOLDERNAME`) に移動します。
10. ［**展開方法**］で ［**詳細設定**］をクリックします。識別しやすいパッケージ名を追加します （*PSCSensor32* など）。
11. 32 ビットの .msi ファイルの場合のみ、［**展開**］タブで ［**詳細設定**］をクリックし、［**Win64 のコンピューターで、この 32 ビット X86 アプリケーションを利用できるようにする**］の選択を解除します。［**OK**］をクリックします。

12. ［**変更**］タブをクリックし、［**追加**］をクリックします。
13. 前の手順で作成した `.mst` ファイルを選択し、変更を保存します。
14. スクリプトを使用して強制的に再起動してポリシー オブジェクトを更新する場合は、スクリプトを実行します。
15. センサーが正しく展開されていることを確認するには、コンソールを定期的に見て、センサー情報が設定されていること、およびセンサーが定期的にチェックインしていることを確認します。

macOS センサーの無人インストール

`Cb Defense install.pkg` および `cbdefense_install_unattended.sh` スクリプトは、macOS センサーのリリースの一部であり、Cb Defense DMG に組み込まれています。無人インストールには、両方のファイルが必要です。

macOS センサーの無人インストールを実行するには

1. センサーのリリースの DMG ファイルから抽出します。
2. 必要に応じて、選択したソフトウェア開発ツールに対応したカスタムのラッパー パッケージ バンドルを作成します。カスタム パッケージにより、オプションをセットアップしてセンサー PKG のインストールを起動するユーティリティとともに、`Cb Defense Install.pkg` ファイルを埋め込みます。
3. サポートされているオプションを使用し、エンドポイントにセンサー インストーラーを展開します。

ソフトウェア展開ツール用のカスタム パッケージの作成手順については、本ガイドでは説明していません。Carbon Black では、`cbdefense_install_unattended.sh` ユーティリティ スクリプトを利用してコマンド ラインで `Cb Defense Install.pkg` ペイロードをインストールする方法について、一般的な手順を説明しています。この手順はソフトウェア展開ツールに適用することができます。

ユーティリティ スクリプトは次の方法で使用することができます。

- そのまま使用する （インストール プロセスをカスタマイズするために渡されるコマンドライン オプション）。
- インストール オプションをハードコードして展開を簡素化するために、変更して使用する。
- カスタム スクリプトを作成する方法の例またはガイドとして使用する。

最も一般的な展開方法の 1 つは、ユーティリティ スクリプトをそのまま使用して、スクリプトと PKG ペイロード （どちらのファイルもカスタム パッケージにバンドルすることが可能）をターゲット デバイスにプッシュしてから、ユーティリティ スクリプトを実行する方法です。

macOS インストール ファイルを抽出して準備するには

1. ［**Cb Defense DMG**］をクリックするか、システム ツールを使用してマウントします。 DMG が `/Volumes/CbDefense-X.X.X.X` ディレクトリにマウントされます（X.X.X.X はセンサーのバージョンです）。

または、hdiutil コマンドを使用して、ダウンロードしたセンサーのリリースのディスク イメージをマウントします。たとえば、次のコマンドを実行します。

```
hdiutil attach /path/to/confer_installer_mac-X.X.X.X.dmg.
```

2. マウントしたボリュームの /Volumes/CbDefense-X.X.X.X/ ディレクトリから CbDefense Install.pkg ファイルを抽出します。 .pkg ファイルはセンサー インストーラー ペイロードです。
3. cbdefense_install_unattended.sh ユーティリティ スクリプトを /Volumes/CbDefense-X.X.X.X/docs/ ディレクトリから抽出します。
4. マウントしたボリュームは、残りの手順には不要なため、マウント解除することができます。**Finder** を使用するか、次のコマンドを実行してマウント解除できます。

   ```
   hdiutil eject /Volumes/CbDefense-X.X.X.X
   ```

5. 抽出した CbDefense Install.pkg および cbdefense_install_unattended.sh ファイルを使用して、お使いのソフトウェア開発ツールに対応したカスタム パッケージを作成します。または、2 つのファイルをターゲットの macOS デバイスに直接展開します。

注意

cbdefense_install_unattended.sh および CbDefense Install.pkg ペイロードは、ユーティリティとインストーラー ペイロード間の互換性を確保するために、同じメジャー バージョンとマイナー バージョンの DMG リリース ファイルから抽出する必要があります。2 つのファイルが同じリリースから抽出されたものでない場合、インストールが失敗する場合があります。

通常、抽出した cbdefense_install_unattended.sh ファイルと CbDefense Install.pkg ファイルは、ターゲットのエンドポイントにプッシュします。これらのファイルを使用して、特定のソフトウェア開発ツールに対応したカスタムのインストール バンドルを作成することもできます。

macOS コマンド ライン パラメーター

cbdefense_install_unattended.sh ユーティリティ スクリプトでは、次の共通コマンド ライン パラメーターがサポートされています。パラメーターはインストーラーに渡されます。-c と -i パラメーターは、無人インストールの場合にのみ必要なオプションです。

すべてのコマンド ライン パラメーターを表示するには、 -h パラメーターとともにコマンドを実行します。

macOS コマンド ライン パラメーター

パラメーター	必須または任意	説明
-c COMPANY CODE	必須	会社登録コード。 登録コードは必ず一重引用符で囲みます。そうしないと、インストールが失敗することがあります。
-i PKG_FILE	必須	PKG インストーラー ペイロードの絶対パス。 ファイル パスを引用符で囲むことをお勧めします。
-d	任意	インストール直後にバイパス モード （保護が無効）に入ります。後で保護を有効にすることができます。
-g POLICY_NAME	任意	センサーを追加するポリシーを指定します。ポリシーの詳細については、『Cb Defense ユーザー ガイド』を参照してください。 特に、名前に空白文字や特殊文字が含まれている場合は、ポリシー名を引用符で囲むことをお勧めします。
-p PROXY_SERVER:PORT	任意	優先するプロキシ サーバーとポート。例： -p ‘10.5.6.7:54443’ セミコロンで区切ると、複数のプロキシ サーバーを指定することができます。例：-p ‘10.5.6.8:54443;10.5.6.7:54443’ 指定されていなくても、プロキシ サーバーやポートが必要な場合、センサーはプロキシの自動検出を試みます。
-x PROXY_USER:PASSWORD	任意	プロキシ サーバーを使用するためのプロキシ認証情報 （必要な場合） 。プロキシ サーバーが自動検出されたか、指定されている場合、この認証情報が適用されます。 使用例：-x ‘proxy_user:proxy_password’ プロキシ認証情報が指定されていなくても、プロキシ サーバーによって要求された場合、macOS センサーは、検出または指定されたプロキシ サーバーに対応する、キーチェーンに格納されたプロキシ認証情報を検出して使用しようとします。
-h		この表では説明していない高度な追加オプションを含め、すべてのコマンド ライン オプションを表示します。 サポートされているすべてのインストール オプションの最新のリストについては、cbdefense_install_unattended.sh ユーティリティ スクリプトの組み込みヘルプを常に参照してください。

macOS センサーの無人インストールを実行するには、`cbdefense_install_unattended.sh` ユーティリティ スクリプトと `CbDefense Install.pkg` ペイロードをターゲット デバイスに展開し、必須オプションを使用してユーティリティ スクリプトを実行します。

macOS インストールの例

次のコマンドは、 1 行で入力する必要があります。ここでは、ドキュメントの書式上の都合のため、複数行にわたって記載されています。

次の例は、必要なファイルがターゲット デバイスの `/tmp/` ディレクトリに展開されていることを前提としています。

- 必須パラメーターを使用して無人インストールを実行するコマンド：

```
sudo /tmp/cbdefense_install_unattended.sh -i '/tmp/CbDefense
Install.pkg' -c '3TRY2U2QHP5@3P5@KH08FPL5NL0XU'
```

- エンドポイントのポリシーを指定するコマンド：

```
sudo /tmp/cbdefense_install_unattended.sh -i '/tmp/Confer
Sensor Install.pkg' -c '3TRY2U2QHP5@3P5@KH08FPL5NL0XU' -g
"Monitored"
```

- バイパス モードのエンドポイントをインストールするコマンド：

```
sudo /tmp/cbdefense_install_unattended.sh -i '/tmp/Confer
Sensor Install.pkg' -c '3TRY2U2QHP5@3P5@KH08FPL5NL0XU' -d
```

macOS のインストールされるサービス

- センサー ドライバー バンドル：`/System/Library/Extensions/CbDefenseSensor.kext`
- センサー サービス：`/Applications/Confer.app/Contents/MacOS/repmgr`
- センサー UI：`/Applications/Confer.app/Contents/MacOS/CbDefense`

macOS のインストールされるユーティリティ

- アップグレード ヘルパー：`/Applications/Confer.app/Contents/MacOS/UpgradeHelper`
- アンインストーラー ヘルパー：`/Applications/Confer.app/Contents/MacOS/UnInstaller`

macOS のアンインストーラー

- 3.X：`/Applications/Confer.app/uninstall`
- 1.X センサー：`/Applications/Confer.app/uninstall.sh`

VDI 環境へのセンサーの無人インストール

Cb Defenseでは、次のVMware Desktop Infrastructure (VDI)がサポートされています。

- VMware Horizon View
- Citrix XenDesktop 7.7 および 7.6

VDI 環境に展開する前に、「Virtual Desktops （仮想デスクトップ）」という名前のポリシーを作成することをお勧めします。Cb Defense は、このポリシーにすべての VDI センサー展開を自動的に配置します。このポリシーが存在しない場合、Cb Defense はデフォルトの標準ポリシーに VDI 展開を配置します （展開したセンサーのポリシーは、いつでも変更できます。『Cb Defense ユーザー ガイド』の 「センサーのポリシー割り当ての管理」を参照してください）。

非永続 VDI の場合は、クローンされた VDI センサー展開を、指定した任意のポリシーにインストールしたり変更したりすることができます。ただし、 VDI をシャットダウンしてから再起動すると、 VDI センサー展開は Virtual Desktops ポリシーに配置されます。このポリシーが存在しない場合、 Cb Defense はクローンされた VDI 展開を標準ポリシーに配置します。

永続 VDI の場合は、 VDI デバイスをシャットダウンしてから再起動した後も、クローンされたすべてのデバイスがインストール先のポリシーまたは変更後のポリシー内に維持されます。

無人インストール時に **VDI** パラメーターを **1** に設定します。そうしないと、 1 つの仮想デスクトップが重複して登録される場合があり、さまざまな問題が発生するおそれがあります。

VDI スイッチは、センサーに再登録トリガーを検出するよう通知します。このスイッチを指定しないと、クローンがすべて同じデバイス （つまりマスター イメージ）として表示されます。

コマンド ラインの例を次に示します。

```
msiexec.exe /i
C:\Users\UserFolderName\Desktop\installer_vista_win7_win8-32-2.0.4.9.msi
/q /L* log.txt COMPANY_CODE=3TRY2U2QHP5@3P5@KH08FPL5NL0XU VDI=1
AUTO_UPDATE=0.
```

非永続 VDI の場合は、**AUTO_UPDATE** を **0** に設定する必要があります （センサーをマスターで更新する必要があります）。永続 VDI の場合は、センサーを VDI に直接インストールでき、**AUTO_UPDATE** を **1** に設定できます。マスター イメージは、定期的に更新して、最新の AV シグネチャを取得する必要があります。更新後、リンクされているクローン VM がある場合は、それらを再構成する必要があります。

VDI=1 を使用してセンサーをマスターの非永続基本 VDI イメージにインストールした場合、ユーザーがデバイスにログインしたときに、センサーが新しいデバイス ID を Cb Defense に自動で登録します。

インストール オプション **BASE_IMAGE=1** を VDI インストール オプションの代わりに、または VDI インストール オプションとともに使用することはできません。これを行うと、センサーで予期しない動作が発生する場合があります。**BASE_IMAGE=1** オプションは、物理デバイスまたは永続 VDI の基本イメージにセンサーをインストールするときにのみ使用してください。

コマンド ライン オプションの詳細については、「Windows でサポートされるコマンド」（9 ページ）を参照してください。

Cb Defense を VDI に展開するには、次の手順を実行します。

1. センサーをマスター イメージにインストールします。
2. マスターから VM をクローンします。
3. VM が起動してドメインに参加します。
4. VM がクローンであることをセンサーが判別します。
5. センサーは、クローンされたデバイスの情報に基づく新しいデバイス ID を作成します。
6. センサーは、自身を新しいデバイスとして登録します。
7. センサーは、ユーザーがログオンするまで、未割り当ての状態になります。

展開が成功したかどうかを検証するには、デバイス名の一部であるセキュリティ識別子 (SID) を確認してください。

VDI に展開するときは、ローカル スキャン設定を検討してください。リソース利用率 (RAM) に影響が及ぶ場合があります。マスター VDI イメージを頻繁に更新しないと、生成されたクローンは古いシグネチャ セットを使用して初期化されます。このため、あまり長く永続しない VDI クローンに大きなシグネチャがダウンロードされる可能性があります。 VDI が数時間しか永続しない場合、シグネチャ更新プロセスを適用できない場合があります。ローカル スキャンをオフにし、非シグネチャ ベースの追加ルールで対処してシステムを保護するか、ローカル ミラー サーバーを使用して、ネットワーク帯域幅のリスクを解消してください。ミラー サーバーについては、『Cb Defense ユーザー ガイド』の 「シグネチャ ミラーの手順」を参照してください。

注意

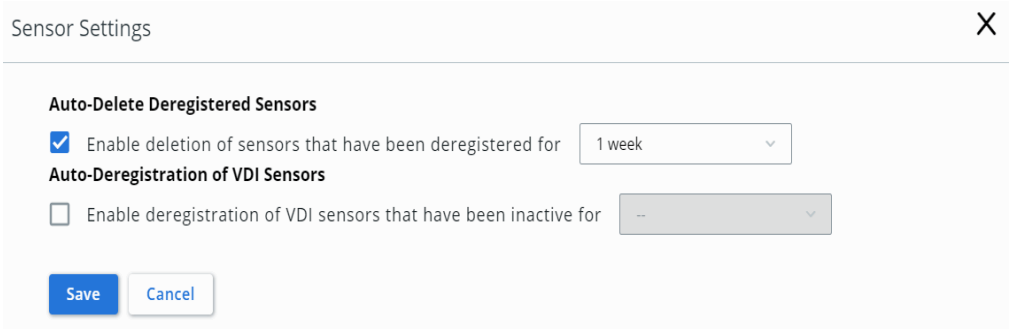
［Revert VM after user logs off（ユーザーがログオフした後に VM を復帰）］がサポートされています。復帰する VM は、再利用された VM です。［Delete VM after user logs off（ユーザーがログオフした後に VM を削除）］はサポートされていません。センサーと Cb Defense バックエンドでは、 VM が削除されたことが認識されません。

VDI 展開は、非アクティブ状態のまま 30 日間経過すると登録が取り消されます。ただし、選択した時間枠で VDI 展開の登録を自動的に取り消すよう Cb Defense を構成することもできます。

VDI 展開の登録を自動的に取り消すには

1. PSC にログインし、［**Endpoints** （エンドポイント）］をクリックします。
2. ［**Sensor Options**（センサー オプション）］をクリックし、［**Sensor Settings**（センサー設定）］をクリックします。

3. ［**Enable deregistration of VDI sensors that have been inactive for**（次の期間、非アクティブだった VDI センサーの登録取り消しを有効にする）］をオンにして、タイムアウト期間を 1 時間、 3 時間、 24 時間、または 1 週間に設定します。



4. 登録が取り消された VDI センサーを自動で削除するには、［**Enable deletion of sensors that have been degistered for**（次の期間、登録が解除されていたセンサーの削除を有効にする）］をオンにして、センサーが削除されるまでの期間をクリックして選択します。
5. ［**Save**（保存）］をクリックします。30 分以内にセンサーの登録が取り消されます。

Linux センサーのインストール （ベータ）

エンドポイントへの Linux センサーの直接インストールを実行する

1. ステップ 1：会社登録コードを取得するとステップ 2：センサー キットをダウンロードするを実行します。
2. インストーラー パッケージの内容をエンドポイントに抽出します。
   ```
   $ tar -zxf cb-psc-sensor-rhel-$BUILD-NUMBER.tgz
   ```
3. 次のコマンドを実行し、センサーをインストールして登録します。
   ```
   $ ./install.sh COMPANY_CODE
   ```

Linux センサーの無人インストールを実行する

1. 展開でスクリプト作成がサポートされている場合は、スクリプトで `cbcipher \tmp` ファイルを作成できます。サポートされていない場合は、各エンドポイントの `/tmp` フォルダーに `cbcipher` ファイルを作成し、そのファイルに会社コードを入力します。
   ```
   $ echo COMPANY_CODE > /tmp/cbcipher
   ```
2. 展開ツールを使用して RPM をプッシュします。

インストール後の手順

1. 必要に応じて、センサーのインストール ステータスを確認するには、次のコマンドを実行します（エンドポイントのオペレーティング システムによって異なります）。
   CentOS6：`$ sudo service cbagentd status`
   CentOS7：`$ sudo systemctl status cbagentd.service`
2. PSC にログインし、［**Enforce** （適用）］をクリックして ［**Policies** （ポリシー）］をクリックします。 Linux センサーに割り当てられているポリシーを選択します。
3. ポリシーに対して Live Response を有効にするには、［**Save** （保存）］をクリックします。

［**Policies** （ポリシー）］ページおよび Live Response に関してサポートが必要な場合は、『Cb Defense ユーザー ガイド』を参照してください。

Linux センサーをアンインストールする

1. インストーラー キットがアンパックされた場所で次のコマンドを実行します。
   ```
   $ sudo rpm -e cb-psc-sensor
   ```