AMP for Endpoints の導入戦略

最終更新日: 2018 年 6 月 21 日

目次

第 1 章: 計画 5

システム要件とサポートされているオペレーティング システム 6
AMP for Endpoints Windows コネクタ 6
AMP for Endpoints Mac コネクタ 8
AMP for Endpoints Linux コネクタ 8
Cisco Security Connector 10

エンドポイント セキュリティに関する情報収集 10

他のセキュリティ製品での AMP for Endpoints に対する除外項目の作成 11
McAfee 製品で除外項目を作成する 11
Symantec 製品で除外項目を作成する 12
Microsoft Security Essentials で除外項目を作成する 13

カスタム アプリケーションに関する情報収集 13

プロキシ サーバに関する情報収集 14

ファイアウォール ルールの確認 14
AMP for Endpoints Windows ファイアウォールの除外 14
AMP for Endpoints Mac ファイアウォールの除外 16
AMP for Endpoints Linux ファイアウォールの除外 18
Cisco Security Connector ファイアウォールの除外 19

評価用導入に使用するコンピュータの選択 20

第 2 章: ポータルの設定 21

除外項目の作成 21

アウトブレイク コントロール リストの作成 24

ポリシーの作成 24

グループの作成 26

ゴールド マスターからホワイトリストを作成 27

インストーラのダウンロード 28

第 3 章: AMP for Endpoints Connector の導入 29

コマンド ライン スイッチ 29
インストーラ終了コード 31

導入 32
Microsoft System Center Configuration Manager 32

第 4 章: トラブルシューティング 39
初期設定の失敗 39
パフォーマンス 39
Outlook パフォーマンス 40
クラウドに接続できない 40
[デバイス トラジェクトリ(Device Trajectory)] にコピー、移動、または実行イベントが記録されない 41
[デバイス トラジェクトリ(Device Trajectory)] にネットワーク イベントが記録されない 42
ポリシーが更新されない 42
プロキシ 43
コネクタの重複 44
原因 44
重複コネクタの削除 45
シンプル カスタム検出 45
カスタム ホワイトリスト 46
アプリケーション ブロッキング 46
サポートへの問い合わせ 47

付録 A: 脅威の説明 49
侵害の兆候 49
DFC 検出 51

付録 B: 関連資料 52
シスコ AMP for Endpoints ユーザ ガイド 52
シスコ AMP for Endpoints クイックスタートガイド 52
シスコ AMP for Endpoints 導入戦略ガイド 52
Cisco Endpoint IOC の属性 52
Cisco AMP for Endpoints API ドキュメンテーション 53
シスコ AMP for Endpoints リリース ノート 53
シスコ AMP for Endpointsデモ データのシナリオ 53
シングル サインオンの設定 53
シスコ ユニバーサル クラウド契約 54

第 1 章
計画

このマニュアルでは、初めて AMP for Endpoints を導入する際のベスト プラクティスについて説明します。この戦略に従うことで、AMP for Endpoints の導入および評価が成功する可能性が高くなります。

インストール後のトラブルシューティング作業を軽減するため、導入を開始する前に、環境に関してできる限り多くの情報を収集してください。Windows 用 AMP for Endpoints コネクタを効果的に導入するには、まず、使用する環境を特定しなければなりません。それには、次の質問に答える必要があります。

- 何台のコンピュータに Windows 用 AMP for Endpoints コネクタをインストールするか。
- それらのコンピュータが実行しているオペレーティング システムは何か。
- コンピュータのハードウェア仕様はどうなっているか。
- オペレーティング システムと仕様は、Windows 用 AMP for Endpoints コネクタの最小要件を満たしているか。
- コンピュータにはどのようなアプリケーションがインストールされているか。
- コンピュータに、カスタム アプリケーションや普及していないアプリケーションがインストールされているか。
- コンピュータはプロキシを介してインターネットに接続するか。
- AMP for Endpoints コネクタを Windows サーバに導入することを予定しているか。
- どのようなツールを使用してソフトウェアをエンドポイントにプッシュしているか。
- コンピュータにインストールされているセキュリティ製品は何か（AV、HIDS など）。
- ユーザに AMP for Endpoints コネクタ ユーザ インターフェイス、デスクトップ アイコン、プログラム グループ、および右クリック メニューを表示するか。

作業する環境を特定した後、アルファ リリースの候補を特定する際の最初のベスト プラクティスを適用できます。アルファの候補を選ぶベスト プラクティスは、オペレーティング システムごとに 3 台のコンピュータ、カスタム アプリケーションごとに 3 台のコン

ピュータ、プロキシ サーバごとに 3 台のコンピュータ、セキュリティ製品ごとに 1 台のコンピュータ、そして部門ごとに 1 台のコンピュータを選択することです。アルファ リリースには、おそらく約 100 台のコンピュータの代表例が含まれます。

システム要件とサポートされているオペレーティング システム

オペレーティング システムに応じた AMP for Endpoints コネクタの最小システム要件は以下のとおりです。ここに記載されていないオペレーティング システムは、現在サポートされていません。

AMP for Endpoints Windows コネクタ

AMP for Endpoints Windows コネクタは、次のオペレーティング システムの 32 ビット バージョンと 64 ビット バージョンをサポートします。

現時点でのサポート対象のバージョン

Microsoft Windows 7

- 1 GHz 以上のプロセッサ
- メモリ 1 GB
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

Microsoft Windows 8 および 8.1（AMP for Endpoints コネクタ 3.1.4 以降が必要）

- 1 GHz 以上のプロセッサ
- メモリ 512 MB
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

Microsoft Windows 10（AMP for Endpoints コネクタ 4.3.0 以降が必要）

- 1 GHz 以上のプロセッサ
- 1 GB の RAM（32 ビット）または 2 GB の RAM（64 ビット）
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

Microsoft Windows Server 2008 R2

- 2 GHz 以上のプロセッサ
- メモリ 2 GB
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

Microsoft Windows Server 2012（AMP for Endpoints コネクタ 3.1.9 以降が必要）

- 2 GHz 以上のプロセッサ
- メモリ 2 GB
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

以前サポート対象だったバージョン

Microsoft Windows XP with Service Pack 3 以降（AMP for Endpoints Windows コネクタ バージョン 5.x.x 以前が必要）

- 500 MHz 以上のプロセッサ
- メモリ 256 MB
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

Microsoft Windows Vista with Service Pack 2 以降（AMP for Endpoints Windows コネクタ バージョン 5.x.x 以前が必要）

- 1 GHz 以上のプロセッサ
- メモリ 512 MB
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

Microsoft Windows Server 2003（AMP for Endpoints Windows コネクタ バージョン 5.x.x 以前が必要）

- 1 GHz 以上のプロセッサ
- メモリ 512 MB
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

Microsoft Windows Server 2008（AMP for Endpoints Windows コネクタ バージョン 5.x.x 以前が必要）

- 2 GHz 以上のプロセッサ
- メモリ 2 GB
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB の使用可能なハード ディスク領域：TETRA

互換性のないソフトウェアと構成

AMP for Endpoints Windows コネクタは現在、以下のソフトウェアとの互換性がありません。

- ZoneAlarm by Check Point
- Carbon Black
- Res Software AppGuard

AMP for Endpoints コネクタは現在、次のプロキシ構成をサポートしていません。

- Websense NTLM クレデンシャル キャッシュ。AMP for Endpoints で現在サポートされている回避策は、Websense で NTLM クレデンシャル キャッシュを無効にするか、AMP for Endpoints コネクタに認証除外を使用したプロキシ認証の省略を許可することです。
- HTTPS コンテンツ インスペクション。現在サポートされている回避策は、HTTPS コンテンツ インスペクションを無効にするか、AMP for Endpoints コネクタの除外を設定することです。
- Kerberos/GSSAPI 認証。現在サポートされている回避策は、基本認証と NTLM 認証のどちらかを使用することです。

AMP for Endpoints Mac コネクタ

オペレーティング システムに応じた AMP for Endpoints Mac コネクタの最小システム要件は以下のとおりです。AMP for Endpoints Mac コネクタがサポートするのは 64 ビットの macOS のみです。

macOS X 10.8

- メモリ 2 GB
- 65 MB の使用可能なハードディスク領域

macOS X 10.9

- メモリ 2 GB
- 65 MB の使用可能なハードディスク領域

macOS X 10.10（AMP for Endpoints Mac コネクタ 1.0.6 以降が必要）

- メモリ 2 GB
- 65 MB の使用可能なハードディスク領域

macOS X 10.11（AMP for Endpoints Mac コネクタ 1.0.7 以降が必要）

- メモリ 2 GB
- 65 MB の使用可能なハードディスク領域

Apple OS X 10.12（AMP for Endpoints Mac コネクタ 1.2.4 以降が必要）

- メモリ 2 GB
- 65 MB の使用可能なハードディスク領域

macOS X 10.13（AMP for Endpoints Mac コネクタ 1.5.0 以降が必要）

- メモリ 2 GB
- 65 MB の使用可能なハードディスク領域

互換性のないソフトウェアと構成

AMP for Endpoints Mac コネクタは現在、次のプロキシ構成をサポートしていません。

- Websense NTLM クレデンシャルキャッシュ：AMP for Endpointsで現在サポートされている回避策は、Websense で NTLM クレデンシャル キャッシュを無効にするか、AMP for Endpoints コネクタに認証除外を使用したプロキシ認証の省略を許可することです。
- HTTPS コンテンツインスペクション：現在サポートされている回避策は、HTTPS コンテンツインスペクションを無効にするか、AMP for Endpoints コネクタ用の除外をセットアップすることです。
- Kerberos/GSSAPI 認証：現在サポートされている回避策は、基本認証と NTLM 認証のどちらかを使用することです。

AMP for Endpoints Linux コネクタ

オペレーティング システムに応じた AMP for Endpoints Linux コネクタの最小システム要件は以下のとおりです。AMP for Endpoints Linux コネクタがサポートするのは x64 アーキテクチャのみです。

CentOS 6.4/6.5/6.6/6.7/6.8/7.2/7.3

- メモリ 1 GB
- 400 MB の使用可能なハードディスク領域

CentOS 6.9（AMP for Endpoints Linux コネクタ 1.5.0 以降が必要）

- メモリ 1 GB
- 400 MB の使用可能なハードディスク領域

Red Hat Enterprise Linux 6.5/6.6/6.7/6.8/7.2/7.3

- メモリ 1 GB
- 400 MB の使用可能なハードディスク領域

Red Hat Enterprise Linux 6.9（AMP for Endpoints Linux コネクタ 1.5.0 以降が必要）

- メモリ 1 GB
- 400 MB の使用可能なハードディスク領域

重要! AMP for Endpoints Linux コネクタはカスタム カーネルに正しくインストールされない場合があります。カスタム カーネルを使用している場合は、インストールする前にサポートまで連絡してください。

互換性のないソフトウェアと構成

AMP for Endpoints Linux コネクタは現在、以下のソフトウェアとの互換性がありません。

- F-Secure Linux Security
- Kaspersky Endpoint Security
- McAfee VSE for Linux
- McAfee Endpoint Security for Linux
- Sophos Server Security 9
- Symantec Endpoint Protection

AMP for Endpoints Linux コネクタでは、Centos および Red Hat Enterprise Linux バージョン 6.x で、リムーバブル メディアまたは一時ファイル システムが標準以外のロケーションにマウントされていると、マウント解除に失敗する可能性があります。ファイルシステム階層の標準に従って、USB ストレージ、DVD、および CD-ROM などのリムーバブルメディアは/media/にマウントし、NFS ファイルシステムマウントのような一時的にマウントされるファイルシステムは/mnt/にマウントする必要があります。リムーバブルメディアや一時ファイルシステムを他のディレクトリにマウントすると、競合が発生し、デバイスがビジーになることが原因でアンマウントが失敗する可能性があります。アンマウントの障害が発生した場合、ユーザは Cisco AMP サービスを停止し、アンマウント操作を再試行して、Cisco AMP を再始動する必要があります。

```
sudo initctl stop cisco-amp
sudo umount {dir\device}
sudo initctl start cisco-amp
```

AMP for Endpoints Linux Connector は UEFI セキュアブートをサポートしていません。

AMP for Endpoints Linux Connector がカーネルモジュールを、Red Hat Enterprise Linux 7.x または CentOS 7.x へのロード時に使用すると、そのカーネルは汚染されます。AMP

がカーネル侵害に影響を与えることを一時的に回避するために、AMP サービスを無効化できます。これにより、システムの再始動後にカーネルモジュールがロードされないようにできます。AMP サービスを無効化すると、システムに対する AMP の保護が実質的に無効になるため、この手順に従う場合は注意が必要です。AMP サービスを無効化するには、以下のコマンドを実行します。

```
sudo systemctl disable cisco-amp
sudo systemctl stop cisco-amp
```

カーネルをリロードし、カーネルの汚染値をリセットするには、システムを再始動する必要があります。AMP サービスを再始動するには、以下のコマンドを実行します。

```
sudo systemctl enable cisco-amp
sudo systemctl start cisco-amp
```

Cisco Security Connector

以下は、Cisco Security Connectorの最小システム要件です。

- iOS バージョン（11.3 以降）を実行している iOS デバイス。
- デバイスは監視モードで実行されていて、Mobile Device Manager（MDM）およびデバイス登録プログラム（DEP）と Volume Purchase Program（VPP）を使用して管理されている必要があります。
- 5 MB の空き容量。

また、AMP コンソールと次のいずれかの Mobile Device Manager との間で MDM Integration を設定する必要があります。

- API アクセスが有効になっている Meraki システム マネージャ（SM）。
  - システム マネージャと統合ネットワーク型のみサポートされます。
- MobileIron エンタープライズ モビリティ管理（EMM）On-Prem 9.4 以降。
- AirWatch Mobility Management Cloud 9.2 以降。

エンドポイント セキュリティに関する情報収集

1 台のコンピュータで複数のセキュリティ アプリケーションを実行すると、競合が発生する可能性があります。アプリケーション間の競合を防ぐには、他のセキュリティ アプリケーションに AMP for Endpoints に対する除外項目を作成するとともに、それらのセキュリティ アプリケーションを AMP for Endpoints から除外する必要があります。

まず、インストールされているセキュリティ アプリケーションの数を調べてください。組織内の複数のグループで異なる製品を使用していますか。インストールされている各セキュリティ製品のインストール、更新、データ、および検疫パスを調べて、その情報をメモします。

次に、AMP for Endpoints コネクタのインストール パス（5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP）を決定します。ウイルス対策製品をはじめ、他のセキュリティアプリケーションから、AMP for Endpoints コネクタ ディレクトリを除外する必要があります。

他のセキュリティ製品での AMP for Endpoints に対する除外項目の作成

McAfee 製品で除外項目を作成する

ePolicy Orchestrator 4.6

1. ePolicy Orchestrator にログインします。
2. メニューから [ポリシー(Policy)] > [ポリシー カタログ(Policy Catalog)] を選択します。
3. [製品(Product)] プルダウンから VirusScan Enterprise の適切なバージョンを選択します。
4. オンアクセス高リスク プロセス ポリシーを編集します。
5. [除外(Exclusions)] タブを選択して、[追加(Add)] ボタンをクリックします。
6. [パターンを使用(By Pattern)] フィールドで、AMP for Endpoints コネクタのインストール環境へのパス(5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP)を入力し、[サブフォルダも除外(Also exclude subfolders)] ボックスをオンにします。
7. [OK] をクリックします。
8. [保存(Save)] をクリックします。
9. オンアクセス低リスク プロセス ポリシーを編集します。
10. このポリシーにステップ 5 ～ 8 を繰り返します。

VirusScan Enterprise 8.8

1. VirusScan コンソールを開きます。
2. [タスク(Task)] メニューで、[オンアクセススキャナのプロパティ(On-Access Scanner Properties)] を選択します。
3. 左ペインで、[すべてのプロセス(All Processes)] を選択します。
4. [除外(Exclusions)] タブを選択します。
5. [除外(Exclusions)] ボタンをクリックします。
6. [除外の設定(Set Exclusions)] ダイアログで、[追加(Add)] ボタンをクリックします。
7. [参照(Browse)] ボタンをクリックして、AMP for Endpoints コネクタのインストールディレクトリ(5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP)を選択し、[サブフォルダも除外(Also exclude subfolders)] ボックスをオンにします。
8. [OK] をクリックします。
9. [除外の設定(Set Exclusions)] ダイアログで、[OK] をクリックします。
10. [オンアクセススキャナのプロパティ(On-Access Scanner Properties)] ダイアログで、[OK] をクリックします。

Symantec 製品で除外項目を作成する

管理対象の Symantec Enterprise Protection 12.1

1. Symantec Endpoint Protection Manager にログインします。
2. 左ペインで、[ポリシー(Policies)] をクリックします。
3. [ポリシー(Policies)] リストの下にある [除外(Exceptions)] エントリを選択します。
4. 新しい除外ポリシーを追加するか、既存のポリシーを編集できます。
5. ポリシーを開いたら、[除外(Exceptions)] をクリックします。
6. [追加(Add)] ボタンをクリックし、リストから [Windows の除外(Windows Exceptions)] を選択し、サブメニューから [フォルダ(Folder)] を選択します。
7. [セキュリティリスクフォルダの除外の追加(Add Security Risk Folder Exception)] ダイアログで、[プレフィクス変数(Prefix variable)] ドロップダウン メニューから [PROGRAM_FILES] を選択し、[フォルダ(Folder)] フィールドに「シスコ」と入力します。[サブフォルダを含める(Include subfolders)] がオンになっていることを確認します。
8. [このフォルダを除外するスキャンのタイプを指定(Specify the type of scan that excludes this folder)] メニューで、[すべて(All)] を選択します。
9. [OK] をクリックします。
10. 組織内の AMP for Endpoints コネクタがインストールされたすべてのコンピュータでこの除外が使用されていることを確認します。

非管理対象の Symantec Enterprise Protection 12.1

1. SEP を開いて、左ペインで [設定の変更(Change Settings)] をクリックします。
2. [除外(Exceptions)] エントリの横にある [設定の構成(Configure Settings)] をクリックします。
3. [除外(Exceptions)] ダイアログで [追加(Add)] ボタンをクリックします。
4. [セキュリティリスクの除外(Security Risk Exception)] サブメニューで、[フォルダ(Folders)] を選択します。
5. ダイアログでAMP for Endpoints コネクタのインストールフォルダ(5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP)を選択し、[OK] をクリックします。
6. [除外(Exceptions)] ダイアログで [追加(Add)] ボタンをクリックします。
7. [SONARの除外(SONAR Exception)] サブメニューで、[フォルダ(Folder)] を選択します。
8. ダイアログでAMP for Endpoints コネクタのインストールフォルダ(5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP)を選択し、[OK] をクリックします。
9. [閉じる(Close)] ボタンをクリックします。

Microsoft Security Essentials で除外項目を作成する

1. Microsoft Security Essentials を開いて、[設定(Settings)] タブをクリックします。
2. 左ペインで、[除外されたファイルと場所(Excluded files and locations)] を選択します。
3. [参照(Browse)] ボタンをクリックして、AMP for Endpoints コネクタのインストール フォルダ(5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP)に移動して、[OK] をクリックします。
4. [追加(Add)] ボタンをクリックして、変更の [保存(Save)] をクリックします。
5. 左ペインで、[除外されたプロセス(Excluded processes)] を選択します。
6. [参照(Browse)] ボタンをクリックし、sfc.exe ファイルまたは agent.exe ファイル(5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire\FireAMP\x.x.x\sfc.exe、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP\x.x.x\sfc.exe、ここで x.x.x は AMP for Endpoints コネクタのバージョン番号)に移動して、[OK] をクリックします。
7. [追加(Add)] ボタンをクリックして、変更の [保存(Save)] をクリックします。

重要! Microsoft Security Essentials でのプロセスの除外には sfc.exe ファイルへの特定のパスが必要なため、AMP for Endpoints コネクタを新しいバージョンにアップグレードする場合は、この除外を更新する必要があります。

カスタム アプリケーションに関する情報収集

カスタム アプリケーションが、初期導入で問題になる可能性があります。普及しているアプリケーションは、AMP for Endpoints クラウドですでにクリーン ファイルとしてマークされ、AMP for Endpoints コネクタでテスト済みとなっています。カスタム アプリケーションには、このメリットが適用される可能性は小さいため、特に注意が必要です。実行されているカスタム アプリケーションまたはレガシー アプリケーションの有無を確認し、存在する場合は、それぞれのインストール パスを調べてメモします。該当するアプリケーションをインストールしているのが特定のユーザ グループだけである場合、どのユーザであるかに留意します。カスタム アプリケーションが別個の情報ストアを使用している場合、その情報ストアのファイル パスをメモします。

可能な場合は、md5deep などのプログラムを使用して、カスタム アプリケーションの実行可能ファイルの SHA-256 値を計算します。

プロキシ サーバに関する情報収集

組織内のコンピュータがプロキシ サーバを使用してインターネットに接続している場合、プロキシ サーバに関する次の情報を収集する必要があります。

- プロキシ ホスト名
- プロキシ ポート
- プロキシ タイプ
- 認証用のユーザ名とパスワード（必要な場合）
- PAC ファイルの URL（使用されている場合）
- プロキシ サーバが、DNS 名前解決に使用されているかどうか
- プロキシ サーバが TCP ポート 32137 経由の通信を許可するかどうか

ファイアウォール ルールの確認

シスコ システムとの通信を AMP for Endpoints コネクタに許可するには、クライアントが特定のポートを介して特定のサーバに接続することをファイアウォールで許可する必要があります。ユーザの所在地（欧州、アジア太平洋/中華圏、およびその他の地域）に応じて、3 セットのサーバが存在します。

重要! ファイアウォールでの IP アドレスの除外設定が必要な場合は、このシスコ TechNote を参照してください。

AMP for Endpoints Windows ファイアウォールの除外

北米

北米内にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.amp.cisco.com
- **管理サーバ**：mgmt.amp.cisco.com
- **ポリシー サーバ**：policy.amp.cisco.com
- **エラー レポート**：crash.amp.cisco.com
- **エンドポイント IOC ダウンロード**：ioc.amp.cisco.com
- **高度なカスタム シグニチャ**：custom-signatures.amp.cisco.com
- **コネクタアップグレード**：upgrades.amp.cisco.com（TCP 80 および 443）
- **リモートファイル取得**：rff.amp.cisco.com

ファイルとネットワークの分類の検索のためにシスコ クラウド サーバとの通信をコネクタに許可するには、ファイアウォールが次のサーバへの TCP 443 接続を許可する必要があります。

- **クラウド ホスト**：cloud-ec.amp.cisco.com

AMP for Endpoints Windows バージョン 5.0 以降の場合は、代わりに次のクラウド ホスト アドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウド ホスト**：cloud-ec-asn.amp.cisco.com
- **登録サーバ**：cloud-ec-est.amp.cisco.com

AMP for Endpoints コネクタのいずれかで TETRA を有効にした場合は、シグニチャ更新用として TCP 80 および 443 経由での次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：tetra-defs.amp.cisco.com

欧州連合

EU 内にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.eu.amp.cisco.com
- **管理サーバ**：mgmt.eu.amp.cisco.com
- **ポリシー サーバ**：policy.eu.amp.cisco.com
- **エラー レポート**：crash.eu.amp.cisco.com
- **エンドポイント IOC ダウンロード**：ioc.eu.amp.cisco.com
- **高度なカスタム シグニチャ**：custom-signatures.eu.amp.cisco.com
- **コネクタアップグレード**：upgrades.eu.amp.cisco.com（TCP 80 および 443）
- **リモートファイル取得**：rff.eu.amp.cisco.com

ファイルとネットワークの分類の検索のためにシスコ クラウド サーバとの通信をコネクタに許可するには、ファイアウォールがクライアントに次のサーバへの TCP 443（デフォルト）または TCP 32137 経由の接続を許可する必要があります。

- **クラウド ホスト**：cloud-ec.eu.amp.cisco.com

AMP for Endpoints Windows バージョン 5.0 以降の場合は、代わりに次のクラウド ホスト アドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウド ホスト**：cloud-ec-asn.eu.amp.cisco.com
- **登録サーバ**：cloud-ec-est.eu.amp.cisco.com

AMP for Endpoints コネクタのいずれかで TETRA を有効にした場合は、シグニチャ更新用として TCP 80 および 443 経由での次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：tetra-defs.eu.amp.cisco.com

アジア太平洋地域、日本、中華圏

アジア太平洋地域、日本、および中華圏にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.apjc.amp.cisco.com
- **管理サーバ**：mgmt.apjc.amp.cisco.com
- **ポリシー サーバ**：policy.apjc.amp.cisco.com
- **エラー レポート**：crash.apjc.amp.cisco.com
- **エンドポイント IOC ダウンロード**：ioc.apjc.amp.cisco.com
- **高度なカスタム シグニチャ**：custom-signatures.apjc.amp.cisco.com

- **コネクタアップグレード**：upgrades.apjc.amp.cisco.com（TCP 80 および 443）
- **リモートファイル取得**：rff.apjc.amp.cisco.com

ファイルとネットワークの分類の検索のためにシスコ クラウド サーバとの通信をコネクタに許可するには、ファイアウォールがクライアントに次のサーバへの TCP 443（デフォルト）または TCP 32137 経由の接続を許可する必要があります。

- **クラウド ホスト**：cloud-ec.apjc.amp.cisco.com

AMP for Endpoints Windows バージョン 5.0 以降の場合は、代わりに次のクラウド ホスト アドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウド ホスト**：cloud-ec-asn.apjc.amp.cisco.com
- **登録サーバ**：cloud-ec-est.apjc.amp.cisco.com

AMP for Endpoints コネクタのいずれかで TETRA を有効にした場合は、シグニチャ更新用として TCP 80 および 443 経由での次のサーバへのアクセスを許可する必要があります。

更新サーバ：tetra-defs.apjc.amp.cisco.com

AMP for Endpoints Mac ファイアウォールの除外

北米

北米内にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.amp.cisco.com
- **管理サーバ**：mgmt.amp.cisco.com
- **ポリシー サーバ**：policy.amp.cisco.com
- **エラー レポート**：crash.amp.cisco.com
- **コネクタアップグレード**：upgrades.amp.cisco.com（TCP 80 および 443）
- **リモートファイル取得**：rff.amp.cisco.com

ファイルとネットワークの分類の検索のためにシスコ クラウド サーバとの通信をコネクタに許可するには、ファイアウォールがクライアントに次のサーバへの TCP 443（デフォルト）または TCP 32137 経由の接続を許可する必要があります。

- **クラウド ホスト**：cloud-ec.amp.cisco.com

AMP for Endpoints Mac バージョン 1.2 以降の場合は、代わりに次のクラウド ホスト アドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウド ホスト**：cloud-ec-asn.amp.cisco.com
- **登録サーバ**：cloud-ec-est.amp.cisco.com

AMP for Endpoints Mac コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新のために次のサーバに対して TCP 80 経由のアクセスを許可する必要があります。

- **更新サーバ**：clam-defs.amp.cisco.com

欧州連合

EU 内にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.eu.amp.cisco.com
- **管理サーバ**：mgmt.eu.amp.cisco.com
- **ポリシー サーバ**：policy.eu.amp.cisco.com
- **エラー レポート**：crash.eu.amp.cisco.com
- **コネクタアップグレード**：upgrades.eu.amp.cisco.com（TCP 80 および 443）
- **リモートファイル取得**：rff.eu.amp.cisco.com

ファイルとネットワークの分類の検索のために シスコクラウド サーバとの通信をコネクタに許可するには、ファイアウォールがクライアントに次のサーバへの TCP 443（デフォルト）または TCP 32137 経由の接続を許可する必要があります。

- **クラウド ホスト**：cloud-ec.eu.amp.cisco.com

AMP for Endpoints Mac バージョン 1.2 以降の場合は、代わりに次のクラウド ホスト アドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウド ホスト**：cloud-ec-asn.eu.amp.cisco.com
- **登録サーバ**：cloud-ec-est.eu.amp.cisco.com

AMP for Endpoints Mac コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新のために TCP 80 経由で次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：clam-defs.eu.amp.cisco.com

アジア太平洋地域、日本、中華圏

アジア太平洋地域、日本、および中華圏にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.apjc.amp.cisco.com
- **管理サーバ**：mgmt.apjc.amp.cisco.com
- **ポリシー サーバ**：policy.apjc.amp.cisco.com
- **エラー レポート**：crash.apjc.amp.cisco.com
- **コネクタアップグレード**：upgrades.apjc.amp.cisco.com（TCP 80 および 443）
- **リモートファイル取得**：rff.apjc.amp.cisco.com

ファイルとネットワークの分類の検索のためにシスコ クラウド サーバとの通信をコネクタに許可するには、ファイアウォールがクライアントに次のサーバへの TCP 443（デフォルト）または TCP 32137 経由の接続を許可する必要があります。

- **クラウド ホスト**：cloud-ec.apjc.amp.cisco.com

AMP for Endpoints Mac バージョン 1.2 以降の場合は、代わりに次のクラウド ホスト アドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウド ホスト**：cloud-ec-asn.apjc.amp.cisco.com
- **登録サーバ**：cloud-ec-est.apjc.amp.cisco.com

AMP for Endpoints Mac コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新のために TCP 80 経由で次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：clam-defs.apjc.amp.cisco.com

AMP for Endpoints Linux ファイアウォールの除外

北米

北米内にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.amp.cisco.com
- **管理サーバ**：mgmt.amp.cisco.com
- **ポリシー サーバ**：policy.amp.cisco.com
- **エラー レポート**：crash.amp.cisco.com
- **コネクタアップグレード**：upgrades.amp.cisco.com（TCP 80 および 443）

コネクタにファイルとネットワークの分類・検索目的でシスコ クラウド サーバとの通信を許可するには、ファイアウォール上で、クライアントから次のサーバへの TCP 443 接続を許可する必要があります。

- **クラウド ホスト**：cloud-ec-asn.amp.cisco.com
- **登録サーバ**：cloud-ec-est.amp.cisco.com

AMP for Endpoints Linux コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新のために TCP 80 経由で次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：clam-defs.amp.cisco.com

欧州連合

EU 内にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.eu.amp.cisco.com
- **管理サーバ**：mgmt.eu.amp.cisco.com
- **ポリシー サーバ**：policy.eu.amp.cisco.com
- **エラー レポート**：crash.eu.amp.cisco.com
- **コネクタアップグレード**：upgrades.eu.amp.cisco.com（TCP 80 および 443）

コネクタにファイルとネットワークの分類・検索目的でシスコ クラウド サーバとの通信を許可するには、ファイアウォール上で、クライアントから次のサーバへの TCP 443 接続を許可する必要があります。

- **クラウド ホスト**：cloud-ec-asn.eu.amp.cisco.com
- **登録サーバ**：cloud-ec-est.eu.amp.cisco.com

AMP for Endpoints Linux コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新のために TCP 80 経由で次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：clam-defs.eu.amp.cisco.com

アジア太平洋地域、日本、中華圏

アジア太平洋地域、日本、および中華圏にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベント サーバ**：intake.apjc.amp.cisco.com
- **管理サーバ**：mgmt.apjc.amp.cisco.com

- **ポリシー サーバ**:policy.apjc.amp.cisco.com
- **エラー レポート**:crash.apjc.amp.cisco.com
- **コネクタアップグレード**:upgrades.apjc.amp.cisco.com(TCP 80 および 443)

ファイルとネットワークの分類・検索目的でシスコ クラウド サーバとの通信をコネクタに許可するには、ファイアウォール上で、クライアントから次のサーバへの TCP 443 接続を許可する必要があります。

- **クラウド ホスト**:cloud-ec-asn.apjc.amp.cisco.com
- **登録サーバ**:cloud-ec-est.apjc.amp.cisco.com

AMP for Endpoints Linux コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新のために次のサーバに対して TCP 80 経由のアクセスを許可する必要があります。

更新サーバ:clam-defs.apjc.amp.cisco.com

Cisco Security Connector ファイアウォールの除外

北米

北米内にある組織は、コネクタから次のサーバまでの間で HTTPS(TCP 443)経由の接続を許可する必要があります。

- **イベント サーバ**:intake.amp.cisco.com/event/
- **管理サーバ**:mgmt.amp.cisco.com/agent/v1/
- **クラウド ホスト**:cloud-ios-asn.amp.cisco.com
- **登録サーバ**:cloud-ios-est.amp.cisco.com

欧州連合のファイアウォールの除外

EU 内にある組織は、コネクタから次のサーバまでの間で HTTPS(TCP 443)経由の接続を許可する必要があります。

- **イベント サーバ**:intake.amp.cisco.com/event/
- **管理サーバ**:mgmt.amp.cisco.com/agent/v1/
- **クラウド ホスト**:cloud-ios-asn.eu.amp.cisco.com
- **登録サーバ**:cloud-ios-est.eu.amp.cisco.com

アジア太平洋地域、日本、および中華圏のファイアウォールの除外

アジア太平洋地域、日本、および中華圏にある組織は、コネクタから次のサーバまでの間で HTTPS(TCP 443)経由の接続を許可する必要があります。

- **イベント サーバ**:intake.amp.cisco.com/event/
- **管理サーバ**:mgmt.amp.cisco.com/agent/v1/
- **クラウド ホスト**:cloud-ios-asn.apjc.amp.cisco.com
- **登録サーバ**:cloud-ios-est.apjc.amp.cisco.com

評価用導入に使用するコンピュータの選択

1 台のコンピュータに AMP for Endpoints コネクタをインストールする代わりに、さまざまなユーザの代表的コンピュータを選択します。異なる複数のオペレーティング システムおよびアプリケーションが使用されている場合は、各イメージ タイプの少なくとも 1 つに導入するようにしてください。

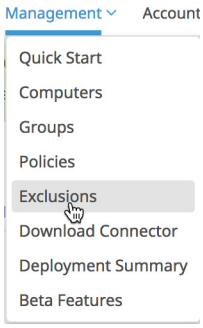
第 2 章
ポータルの設定

AMP for Endpoints Connector を導入する前に、収集した情報に基づいて AMP for Endpoints ポータルで実行すべきタスクがあります。

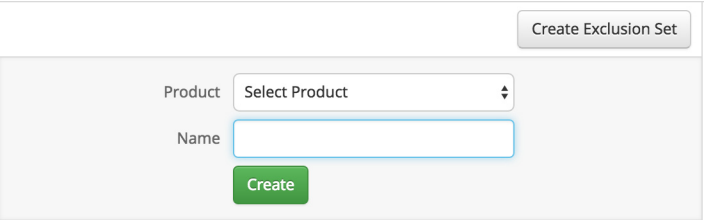
除外項目の作成

AMP for Endpoints Connector とウイルス対策製品（または他のセキュリティ ソフトウェア）との間で競合を避けるには、コネクタがウイルス対策ソフトウェアのディレクトリをスキャンせず、ウイルス対策ソフトウェアがコネクタのディレクトリをスキャンしないように除外設定を作成する必要があります。ウイルス対策シグニチャに含まれている文字列について、悪意（または検疫済みのファイルに伴う問題）が含まれるとコネクタにより判断された場合は、問題になる可能性があります。

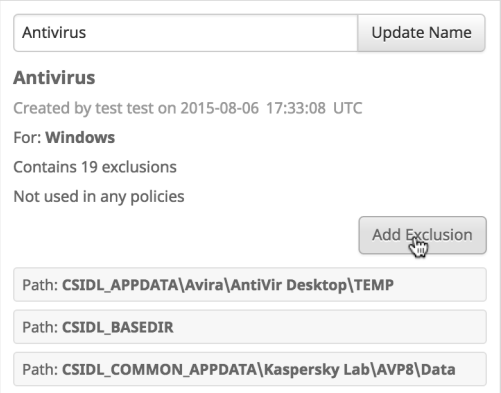
最初のステップは、AMP for Endpoints コンソールで [管理（Management）] > [除外（Exclusions）] に移動して、除外設定を作成することです。



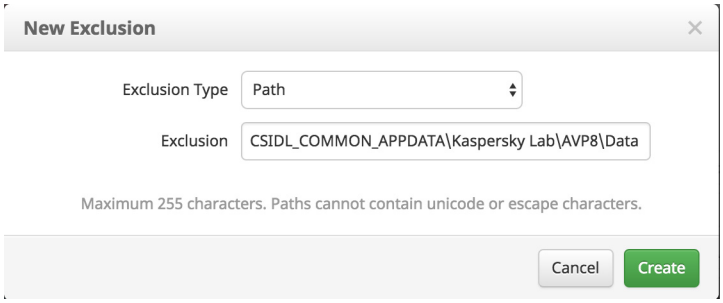
[除外設定の作成(Create Exclusion Set)] をクリックして、除外の新しいリストを作成します。リストの名前(たとえば、「Desktop Exclusions」)を入力してから、[作成(Create)] をクリックします。



次に、[除外の追加(Add Exclusion)] をクリックして、リストに除外項目を追加します。



その後、除外タイプを選択するように要求されます。パス、脅威名、ファイル拡張子、プロセスを追加するか、ファイル名、拡張子、またはパスの代わりにワイルドカードを使用します。パスを選択し、エンドポイント上にインストールしたセキュリティ製品の CSIDL を入力して、[作成(Create)] をクリックします。



重要! パス内の「スペース」文字をエスケープする必要はありません。英語以外の一部言語では、パスの区切り記号に異なる文字が使用されている場合があります。コネクタの除外設定で使用できる有効なパス区切り記号は「\」に限られます。

セキュリティ アプリケーションに関連付けられたパスごとに手順を繰り返します。CSIDL の詳細については、こちらを参照してください。共通の CSIDL には以下が含まれます。

Symantec Endpoint Protection:

- CSIDL_COMMON_APPDATA\Symantec
- CSIDL_PROGRAM_FILES\Symantec\Symantec End Point Protection
- CSIDL_PROGRAM_FILESx86\Symantec\Symantec Endpoint Protection
- CSIDL_COMMON_APPDATA\Symantec

McAfee VirusScan Enterprise:

- CSIDL_COMMON_APPDATA\VSE
- CSIDL_PROGRAM_FILES\VSE

Trend Micro

- CSIDL_PROGRAM_FILES\Trend Micro
- CSIDL_PROGRAM_FILESX86\Trend Micro

Microsoft ForeFront

- CSIDL_PROGRAM_FILES\Microsoft Forefront
- CSIDL_PROGRAM_FILESX86\Microsoft Forefont

Microsoft Security Client

- CSIDL_PROGRAM_FILES\Microsoft Security Client
- CSIDL_PROGRAM_FILESX86\Microsoft Security Client

Sophos

- CSIDL_PROGRAM_FILES\Sophos
- CSIDL_PROGRAM_FILESX86\Sophos

Splunk:

- CSIDL_PROGRAM_FILES\Splunk

重要! CSIDL では大文字と小文字が区別されます。

次に、サーバ用の除外設定と、Active Directory ドメイン コントローラ用の除外設定を作成します。上記のデスクトップ除外設定に含めたセキュリティ製品をすべて除外してください。また、サーバの役割（Active Directory、ファイル サーバ、DHCP など）とインストール済みソフトウェア（Exchange、SQL、IIS など）に基づく除外も作成する必要があります。Microsoft サーバ製品に関する除外事項のリンクは、http://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx にリストされています。

アウトブレイク コントロール リストの作成

導入の初期段階では、これまで見つかっていなかったマルウェアが検出されたり、カスタム アプリケーションが誤検出されたりする場合があります。AMP for Endpoints Connector がこれらの事態に適切に対処できるよう、ポリシーに関連付けるシンプル カスタム検出リストとカスタム ホワイトリストを作成することをお勧めします。

シンプル カスタム検出リストを作成するには、[アウトブレイクコントロール(Outbreak Control)] > [シンプル(Simple)] に移動します。[作成(Create)] をクリックして新しいシンプル カスタム検出を作成し、任意の名前(「Quick SCD」など)を付けた後、[保存(Save)] をクリックします。

カスタム ホワイトリストを作成するには、[アウトブレイクコントロール(Outbreak Control)] > [ホワイトリスト(Whitelisting)] に移動します。[作成(Create)] をクリックして新しいカスタム ホワイトリストを作成し、任意の名前(「Quick WL」など)を付けた後、[保存(Save)] をクリックします。

ポリシーの作成

初期導入時に、[管理(Management)] > [グループ(Groups)] に移動して、次のポリシーを固有設定で作成することをお勧めします。

監査のみ

AMP for Endpoints Connector で悪意のあるファイルの検出のみを行い、検疫は行いません。悪意のあるトラフィックも検出はされますが、ブロックされません。

- すべてデフォルトのポリシー設定を使用しますが、[モードとエンジン(Mode and Engine)] > [ファイル(Files)] は [監査(Audit)] に設定します。
- 事前に収集されたプロキシ サーバ情報は [プロキシ(Proxy)] の下に入力されている必要があります。
- 以前に作成した除外設定をこのポリシーに関連付けます。
- 作成した Quick SCD リストをこのポリシーに関連付けます。
- 作成した Quick WL リストをこのポリシーに関連付けます。

保護

AMP for Endpoints Connector の標準ポリシーです。悪意のあるファイルを検疫し、悪意があるネットワーク接続をブロックします。AMP for Endpoints Connector の動作を十分に理解したら、固有要件に応じてこのポリシーを微調整できます。

- すべてデフォルトのポリシー設定を使用しますが、[モードとエンジン(Modes and Engines)] > [TETRA] はオフにします。
- 事前に収集されたプロキシ サーバ情報は [プロキシ(Proxy)] の下に入力されている必要があります。
- 以前に作成した除外設定をこのポリシーに関連付けます。
- 作成した Quick SCD リストをこのポリシーに関連付けます。
- 作成した Quick WL リストをこのポリシーに関連付けます。

トリアージ

マルウェア感染の疑いがあるコンピュータや、感染が判明しているコンピュータを、オフライン エンジンで積極的にスキャンします。

- すべてデフォルトのポリシー設定を使用しますが、[モードとエンジン(Modes and Engines)] > [TETRA] をオンにし、[モードとエンジン(Modes and Engines)] > [ネットワーク(Network)] は [ブロック(Block)] に設定します。

  重要: TETRA を有効にした場合、別のウイルス対策製品がすでにインストールされているエンドポイントでこのポリシーを使用しないでください。

- 事前に収集されたプロキシ サーバ情報は [プロキシ(Proxy)] の下に入力されている必要があります。
- 以前に作成した除外設定をこのポリシーに関連付けます。
- 作成した Quick SCD リストをこのポリシーに関連付けます。
- 作成した Quick WL リストをこのポリシーに関連付けます。

サーバ

最大限のパフォーマンスと稼働時間を必要とする高可用性コンピュータ/サーバ向けの、低負荷で強制力の弱いポリシーです。

- すべてデフォルトのポリシー設定を使用しますが、[モードとエンジン(Mode and Engine)] > [ファイル(Files)] は [監査(Audit)] に設定します。
- サーバ ポリシーで [モードとエンジン(Modes and Engines)] > [TETRA] を有効にできますが、ポリシーを実稼働サーバに展開する前にテスト サーバに展開することを強くお勧めします。また、TETRA 定義の更新にはローカル AMP 更新サーバを使用することをお勧めします。

  警告! テストと適切な除外設定を行わずにサーバ上で TETRA を実行すると、パフォーマンスに重大な影響を与える可能性があります。

- パフォーマンス上の問題が発生するためにサーバ上で TETRA を実行したくない場合は、[モードとエンジン(Modes and Engines)] > [TETRA] がオフになっていることを確認してください。

  警告! TETRA が実行されていないサーバに AMP for Endpoints Connector をインストールする際は、このポリシー設定と併せて /skiptetra コマンド ライン スイッチを使用する必要もあります。

- 多数のネットワーク接続を必要とするサービス/アプリケーション(SMB、SQL、Exchange など)をサーバでホストしている場合は、[モードとエンジン(Modes and Engines)] > [ネットワーク(Network)] を [無効(Disabled)] に設定することをお勧めします。

  警告! サーバに AMP for Endpoints Connector をインストールする際に、このポリシー設定と併せて /skipdfc コマンド ライン スイッチを使用する必要もあります。

- 事前に収集されたプロキシ サーバ情報は [プロキシ(Proxy)] の下に入力されている必要があります。
- 以前に作成したサーバの除外設定をこのポリシーに関連付けます。
- 作成した Quick SCD リストをこのポリシーに関連付けます。
- 作成した Quick WL リストをこのポリシーに関連付けます。

Domain Controller

Active Directory ドメイン コントローラで使用する強制力の弱いポリシーです。

- すべてデフォルトのポリシー設定を使用しますが、[モードとエンジン(Mode and Engine)] > [ファイル(Files)] は [監査(Audit)] に設定します。
- ネットワークからの認証トラフィックのため、[モードとエンジン(Modes and Engines)] > [ネットワーク(Network)] は [無効(Disabled)] に設定することをお勧めします。

  警告! ドメイン コントローラに AMP for Endpoints Connector をインストールする際に、このポリシー設定と併せて /skipdfc コマンド ライン スイッチを使用する必要もあります。

- Windows 2008 サーバでは、[モードとエンジン(Modes and Engines)] > [TETRA] がオフになっている必要もあります。

  警告! ドメイン コントローラに AMP for Endpoints Connector をインストールする際に、このポリシー設定と併せて /skiptetra コマンド ライン スイッチを使用する必要もあります。

- 事前に収集されたプロキシ サーバ情報は [プロキシ(Proxy)] の下に入力されている必要があります。
- 以前に作成したドメイン コントローラの除外設定をこのポリシーに関連付けます。
- 作成した Quick SCD リストをこのポリシーに関連付けます。
- 作成した Quick WL リストをこのポリシーに関連付けます。

重要! 複数のコンピュータが複数拠点に分散しており、それぞれに異なるプロキシ サーバを使用している場合、拠点ごとに上記のポリシーを作成する必要があります。つまり、東京の監査専用ポリシー、大阪の監査専用ポリシー、などを作成します。

グループの作成

導入用に初期ポリシーを作成したため、それらのポリシーを関連付けるグループを作成する必要があります。[管理(Management)] > [(Groups)] に移動して、次のグループを作成します。

監査のみ

- 監査専用ポリシーを関連付けます。
- このグループは、導入環境内のワークステーションが属する最初のグループにしてください。これにより、誤検出によるファイル検疫を防止できます。
- また監査専用グループは、高可用性を必要とするコンピュータや、グラフィックのレンダリングといった負荷の大きいタスクを実行するコンピュータのパフォーマンス優先グループとして使用することもできます。

保護

- このグループには保護ポリシーを関連付けます。
- 監査専用グループにおけるコンピュータのパフォーマンス要件を満たしていれば、これらのコンピュータを保護グループに移して AMP for Endpoints Connector の通常動作を適用し、悪意のあるファイルを検疫してネットワークの脅威をブロックできます。

トリアージ

- トリアージ ポリシーを関連付けます。
- このグループではマルウェア スキャンが積極的に実行されるため、すでに感染しているコンピュータや、深刻な感染が疑われるコンピュータは、トリアージ グループに移す必要があります。

サーバ

- このグループにはサーバ ポリシーを関連付けます。
- Active Directory ドメイン コントローラ以外のサーバは、すべてこのグループに属している必要があります。

Domain Controller

- このグループにはドメイン コントローラ ポリシーを関連付けます。
- すべての Active Directory ドメイン コントローラは、このグループに属している必要があります。

重要! 前の項で拠点ごとにポリシーを作成した場合は、グループも拠点ごとに作成する必要があります。つまり、東京の保護グループと大阪の保護グループなどを作成します。

ゴールド マスターからホワイトリストを作成

ゴールド マスター イメージを使用できる場合は、それを基にアプリケーションをホワイトリスト登録することをお勧めします。md5deep などのツールを使用すれば、すべてのアプリケーションの SHA-256 値を生成して Quick WL ホワイトリストに追加できます。

インストーラのダウンロード

ポリシーを作成してグループに関連付けた後は、情報収集の段階で特定したコンピュータに対して AMP for Endpoints Connector の導入を開始できます。[管理(Management)] > [コネクタのダウンロード(Download Connector)] に移動し、監査専用、トリアージ、サーバ、およびドメイン コントローラの各グループ用に、再配布可能なインストーラをダウンロードします。

一般的なコンピュータでは、最初に監査専用インストーラを使用する必要があります。これにより、必要なアプリケーションがすべてホワイトリストに追加され、除外設定が適切なことを確認できます。検出によって AMP for Endpoints コンソールでアラートがトリガーされたとしても、検疫やブロックされることはありません。したがって、誤検出が発生した場合でも通常の動作には影響しません。誤検出であることを確認した場合は、該当するアプリケーションをホワイトリストに追加します。AMP for Endpoints Connectorのパフォーマンス要件を満たしたら、コンピュータを監査専用グループから保護グループに移動できます。保護グループのポリシー設定は監査専用グループと同じですが、悪意のあるファイルは検疫され、悪意のある Web サイトへの接続はブロックされます。

ドメイン コントローラ インストーラを使用するのは、Active Directory ドメイン コントローラ サーバのみです。このグループ向けのポリシーには、ツリーのディレクトリ サービスを実行するサーバに固有の除外設定が含まれています。

他のすべてのサーバ(ファイル サーバ、SQL Server、Exchange Server など)では、サーバ インストーラを使用します。

第 3 章
AMP for Endpoints Connector の導入

評価用コンピュータへ AMP for Endpoints Connector を導入する準備ができました。

コマンド ライン スイッチ

独自の導入ソフトウェアを使用している場合は、コマンド ライン スイッチを使用して導入を自動化できます。使用可能なスイッチのリストを次に示します。

- /R：5.1.13 以降の全バージョンのコネクタでは、最初にこのスイッチを使用する必要があります。
- /S：インストーラをサイレント モードに切り替える場合に使用します。

  重要： これは、最初のパラメータ（または /R の直後のパラメータ）として指定する必要があります。

- /desktopicon 0：コネクタ用のデスクトップ アイコンが作成されません。
- /desktopicon 1：コネクタ用のデスクトップ アイコンが作成されます。
- /startmenu 0：スタート メニューのショートカットは作成されません。
- /startmenu 1：スタート メニューのショートカットが作成されます。
- /contextmenu 0：右クリック コンテキスト メニューの [今すぐスキャン（Scan Now）] が無効になります。
- /contextmenu 1：右クリック コンテキスト メニューの [今すぐスキャン（Scan Now）] が有効になります。
- /remove 0：コネクタはアンインストールされますが、後で再インストールできるようにファイルは残されます。
- /remove 1：コネクタがアンインストールされ、すべての関連ファイルが削除されます。

- /uninstallpassword [Connector Protection Password]：ポリシーで [コネクタ保護（Connector Protection）] を有効にした場合にコネクタをアンインストールできます。このスイッチを使用して、**コネクタ保護**のパスワードを指定する必要があります。
- /skipdfc 1：DFC ドライバのインストールをスキップします。

  重要： このフラグを使用してインストールされたコネクタは、[モードとエンジン（Modes and Engines）] > [ネットワーク（Network）] が [無効（Disabled）] に設定されているポリシーを使用するグループに含める必要があります。

- /skiptetra 1：TETRA ドライバのインストールをスキップします。

  重要： このフラグを使用してインストールされたコネクタは、[モードとエンジン（Modes and Engines）] > [TETRA] がオフに設定されているポリシーを使用するグループに含める必要があります。

- /D=[PATH]：インストールを実行するディレクトリの指定に使用します。たとえば、/D=C:\tmp は C:\tmp にインストールします。

  重要： これは、最後のパラメータとして指定する必要があります。

- /overridepolicy 1：以前のコネクタのインストール環境上にインストールする場合に、既存の policy.xml ファイルを置き換えます。
- /overridepolicy 0：以前のコネクタのインストール環境上にインストールする場合に、既存の policy.xml ファイルを置き換えません。
- /temppath：コネクタのインストール時に作成される一時ファイルのパスを指定します。たとえば、/temppath C:\somepath\temporaryfolder のように指定します。このスイッチは AMP for Endpoints Windows コネクタ 5.0 以降でのみ使用可能です。

どのスイッチも指定せずにコマンド ライン インストーラを実行すると、/desktopicon 0 /startmenu 1 /contextmenu 1 /skipdfc 0 /skiptetra 0 として実行されます。

AMP for Endpoints Windows コネクタ 5.1.3 以降では、5.1.1 より前のバージョンから 5.1.3 以降にアップグレードする場合に、インストール ディレクトリを「Sourcefire」から「シスコ」に移行することをユーザがオプトイン（またはオプトアウト）できるコマンド ライン スイッチを使用できます。これらは次のとおりです。

- /renameinstalldir 1 は、ディレクトリを Sourcefire からシスコに変更します。
- /renameinstalldir 0 はインストール ディレクトリを変更しません。

  重要： デフォルトでは、/renameinstalldir 1 が使用されます。

AMP for Endpoints Windows コネクタ 6.0.5 以降には、Microsoft Security Advisory 3033929 の確認をスキップするためのコマンド ライン スイッチがあります。

- /skipexprevprereqcheck 1：Microsoft Windows KB3033929 の確認をスキップします。
- /skipexprevprereqcheck 0：Microsoft Windows KB3033929 を確認します（デフォルト）。

重要! このスイッチを使用しても、KB（あるいは他の Windows 7/Windows Server 2008 R2 の SHA-2 コード署名サポートを有効にする Windows 更新プログラム）がインストールされていない場合は、シスコ クラウドへの接続時に問題が発生します。

インストーラ終了コード

コマンド ライン スイッチを使用して AMP for Endpoints Connector をインストールする場合は、終了コードを把握しておく必要があります。このコードは %TEMP% フォルダ内の immpro_install.log にあります。

- 0：成功。
- 1500：インストーラはすでに実行中です。
- 1618：別のインストールがすでに進行中です。
- 1633：サポートされていないプラットフォーム（例：64 ビットへの 32 ビット版のインストールまたはその逆）
- 1638：このバージョンと同じか、さらに新しいバージョンの製品がすでに存在します。
- 1801：インストール パスが無効です。
- 3010：成功（リブートが必要です。このコードが使用されるのはアップグレード時のみです）。
- 16001：試用版の期限が切れています。
- 16002：インストールする前に完了しているべきリブートが保留になっています。
- 16003：サポートされていないOS（例：XP SP2、Win2000）です。
- 16004：ユーザ アクセス許可が無効です（管理者として実行していません）。
- 16005：既存の AMP for Endpoints Connector がすでに停止されているか、あるいはコネクタ保護が使用されていますが、パスワードが指定されていません。
- 16006：Windows Connector と干渉する PoS OS の特定の機能（Enhanced Write Filter（EWF）または File-Based Write Filter（FBWF））が現在、有効になっています。この機能を無効にしてからやり直してください。PoS OS は公式にはサポートされていません。
- 16007：コネクタのアップグレードを完了するにはリブートが必要ですが、リブートのブロック オプションがポリシーに設定されています。
- 16008：コンピュータ上ですでに必要とされていたリブートが保留されているため、コネクタのアップグレードがブロックされました。
- 16009：Windows 7 および Windows Server 2008 R2 の SHA-2 コード署名サポート用のパッチがありません（KB3033929）。

導入

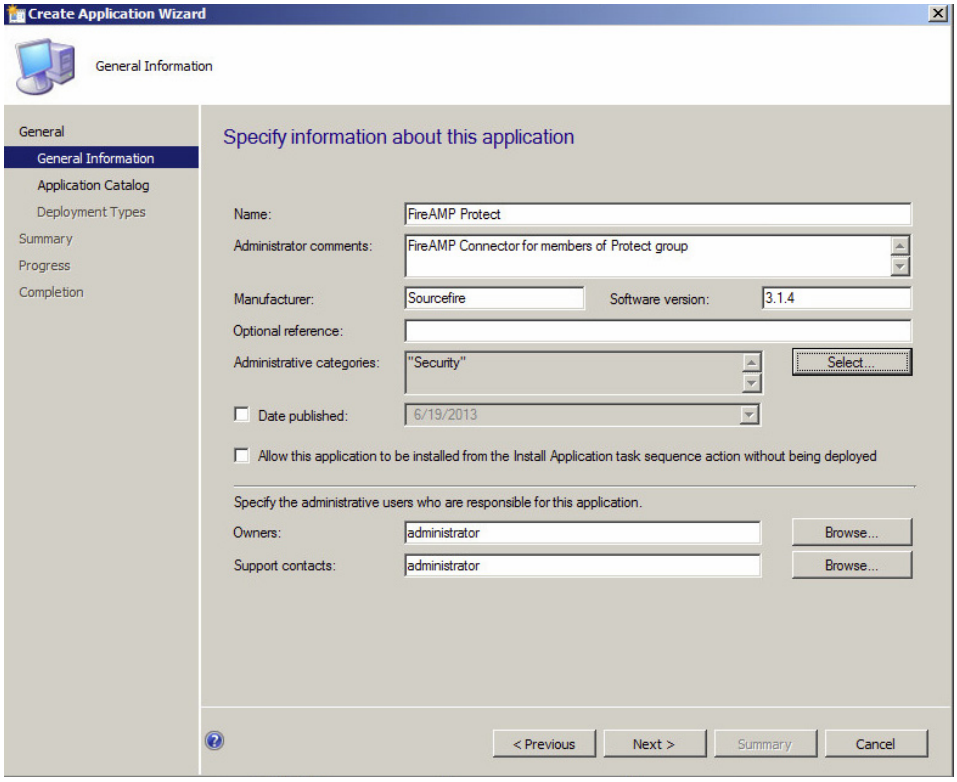
[管理(Management)] > [コネクタのダウンロード(Download Connector)] からインストーラをダウンロードしてファイル共有先に保存すれば、インストーラをログイン スクリプトでインストールしたり、企業のソフトウェア展開ツールで配布したりできます。

Microsoft System Center Configuration Manager

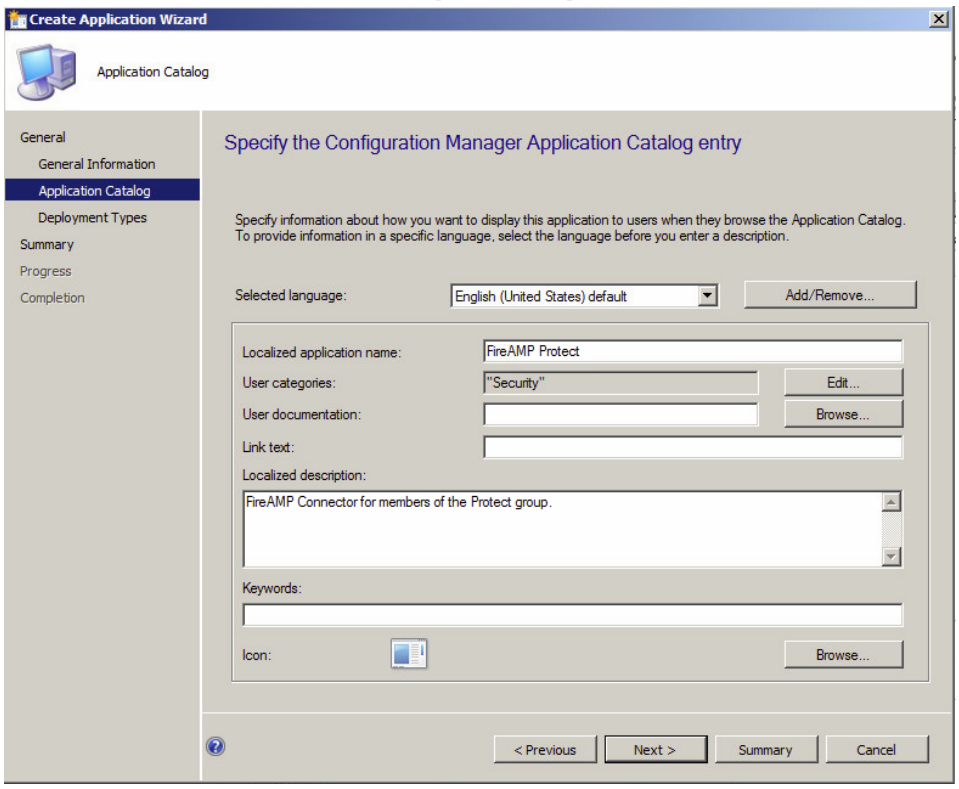
Microsoft System Center Configuration Manager(SCCM)を使用して AMP for Endpoints Connector をインストールするには、最初に各グループの再配布可能インストーラをダウンロードする必要があります。

1. [管理(Management)] > [コネクタのダウンロード(Download Connector)] に移動し、グループのうちの 1 つを選択して [再配布可能インストーラの作成(Create Redistributable Installer)] ボックスをオンにしてから、[ダウンロード(Download)] をクリックします。ダウンロードされるファイルには、識別に役立つグループ名も含まれます(「Protect-FireAMPSetup.exe」など)。
2. SCCM サーバ上の共有ソース ファイル ディレクトリに AMP for Endpoints によりブロック フォルダを作成し、そのフォルダにインストーラ ファイルをコピーします。
3. 次に、Configuration Manager コンソールを開き、[ソフトウェア ライブラリ(Software Library)] > [概要(Overview)] > [アプリケーション管理(Application Management)] > [アプリケーション(Application)] に移動して、[アプリケーションの作成(Create Application)] をクリックします。
4. [アプリケーションの作成(Create Application)] ウィザードの最初の画面で、[アプリケーションの情報を手動で指定する(Manually specify the application information)] を選択してから [次へ(Next)] をクリックします。

5. アプリケーション パッケージの識別情報を入力します。AMP for Endpoints Connector の複数のグループ バージョンの導入を予定している場合は、ソフトウェア ライブラリ内でも各グループを容易に区別できるようなグループ名の使用をお勧めします。必要な情報を入力した後、[次へ(Next)] をクリックします。



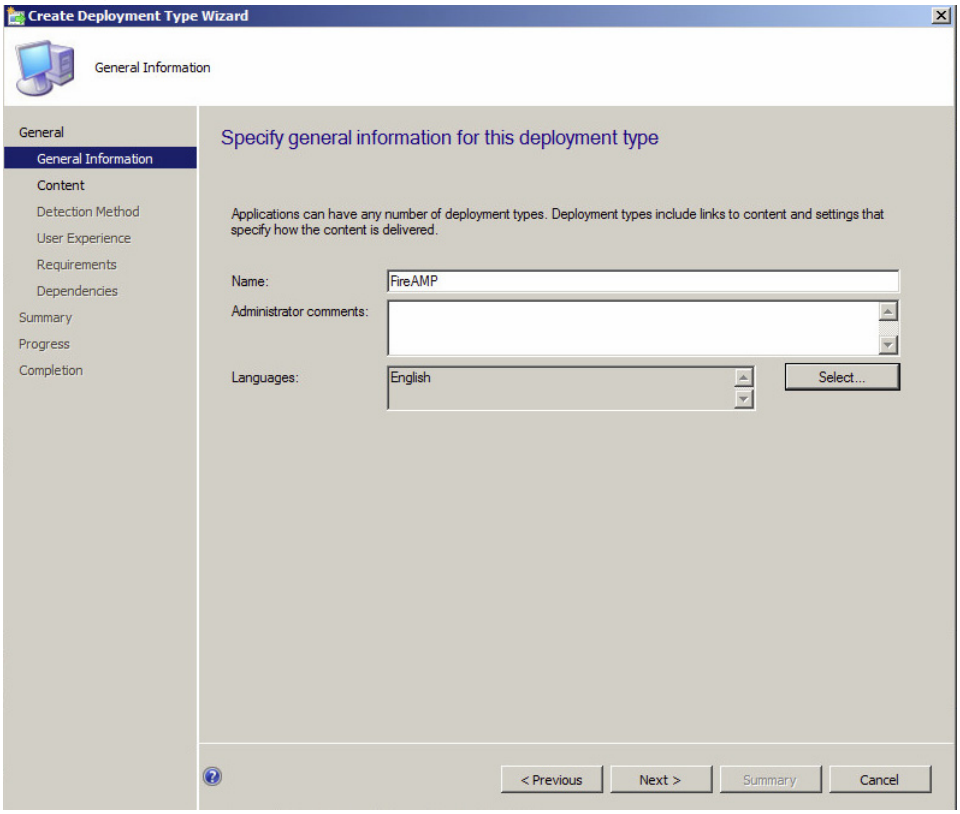
6. [アプリケーション カタログ(Application Catalog)] に、ユーザが表示できる情報を入力します。必要な情報を入力した後、[次へ(Next)] をクリックします。



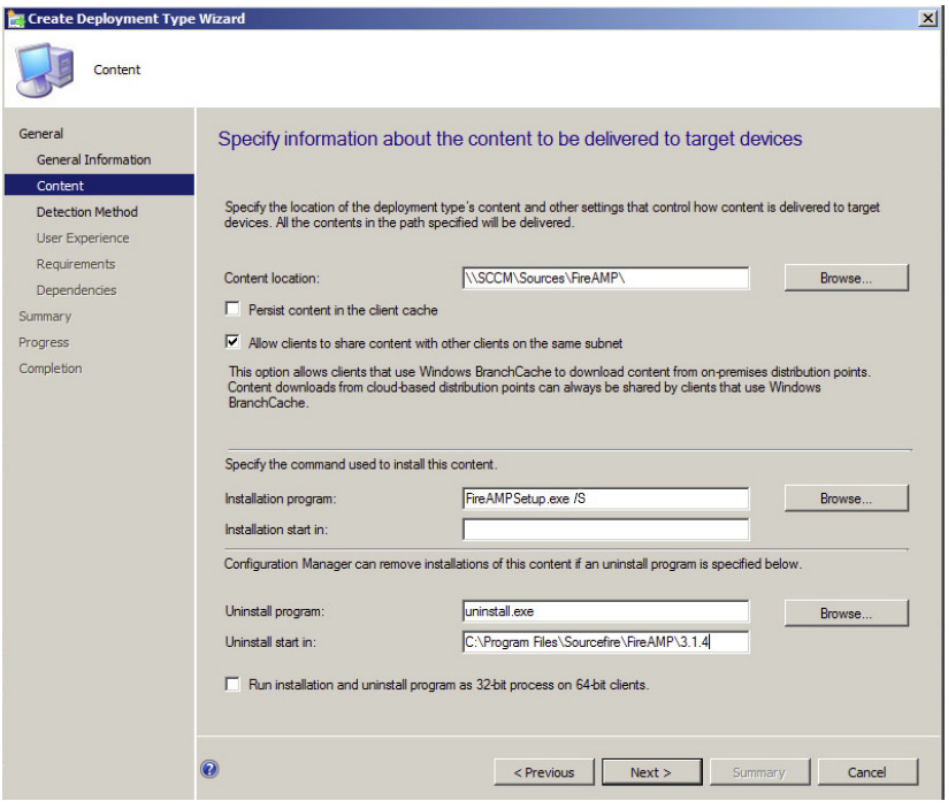
7. [展開の種類(Deployment Types)] 画面で、[追加(Add)] ボタンをクリックして [展開の種類の作成(Create Deployment Type)] ウィザードを開始します。

8. [展開の種類の情報を手動で指定する(Manually specify the deployment type information)] を選択し、[次へ(Next)] をクリックします。

9. アプリケーション名を入力し、言語を選択してから、[次へ(Next)] をクリックします。

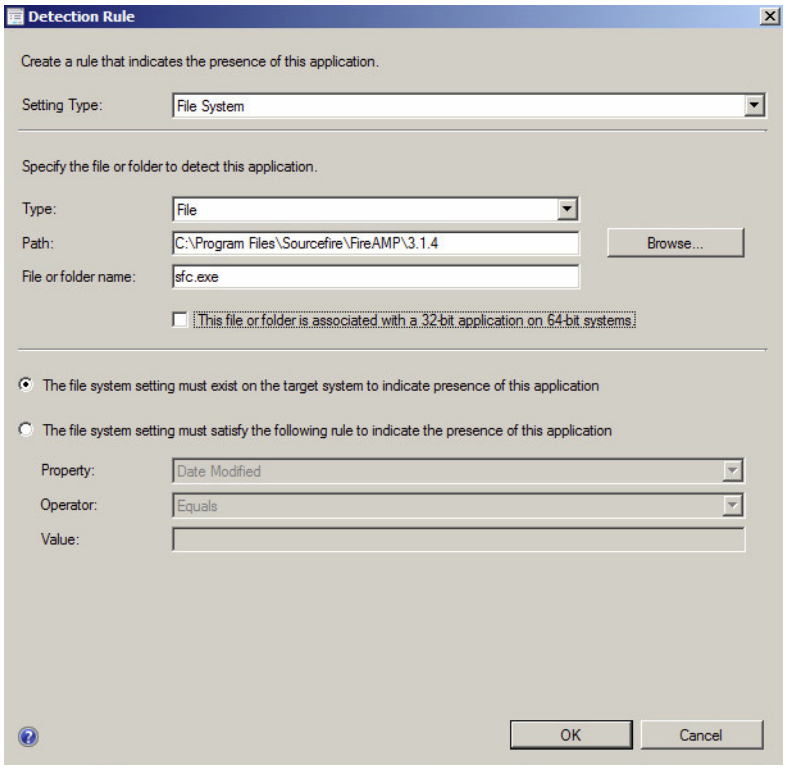


10. [コンテンツの場所(Content location)] フィールドには、ダウンロードしたインストーラ ファイルのパスをグループごとに入力します。[インストール プログラム(Installation program)] フィールドに、使用するコマンド ライン スイッチと併せて実行可能インストーラ ファイルの名前を入力します。アンインストール プログラムとパス(5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire\FireAMP\[version]\uninstall.exe、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP\[version]\uninstall.exe、ここで [version] はインストールする Connector のバージョン(5.1.1 など))を指定することもできます。[次へ] をクリックして、次に進みます。

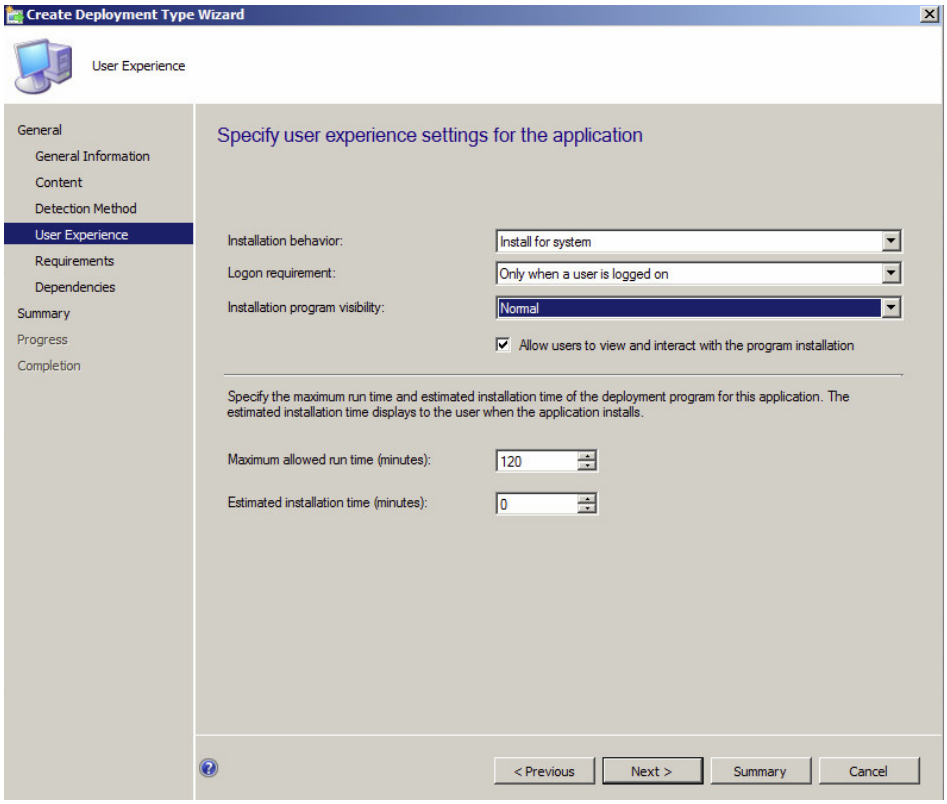


11. [検出方法(Detection Method)] 画面で [句の追加(Add Clause)] をクリックします。

12. [設定の種類(Setting Type)] として [ファイル システム(File System)] を選択し、[種類(Type)] として [ファイル(File)] を選択します。[ファイルまたはフォルダ名(File or folder name)] フィールドに、エンドポイント上の AMP for Endpoints Connector をインストールする予定の場所のパス(5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire\FireAMP\[version]、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP\[version]、ここで [version] はインストールする Connector のバージョン(5.1.1 など))を入力してから、「sfc.exe」と入力します。[OK] をクリックし、[検出方法(Detection Method)] ページでは [次へ(Next)] をクリックします。



13. [インストールの動作(Installation behavior)] として [システム用にインストールする(Install for system)] を選択し、[必要なログオン状態(Logon requirement)] には [ユーザがログオンしているときのみ(Only when a user is logged on)] を選択します。必要な [インストール プログラムの表示(Installation program visibility)] 設定を選択してから、[プログラムのインストールの表示および対話をユーザに許可する(Allow users to view and interact with the program installation)] をオンにします。[次へ] をクリックします。



14. [要件(Requirements)] 画面では、インストール要件を指定することも、そのまま [次へ(Next)] をクリックすることもできます。
15. [依存関係(Dependencies)] 画面で、[次へ(Next)] をクリックします。
16. [概要(Summary)] 画面で設定を確認し、変更する必要がなければ [次へ(Next)] をクリックします。
17. ウィザードが正常に完了したら、[閉じる(Close)] をクリックして [アプリケーションの作成(Create Application)] ウィザードに戻ります。[次へ] をクリックします。
18. [概要(Summary)] 画面で設定を確認し、変更する必要がなければ [次へ(Next)] をクリックします。
19. ウィザードが正常に完了したら、[閉じる(Close)] をクリックします。

アプリケーションが [ソフトウェア ライブラリ(Software Library)] に一覧表示されます。コンテンツを導入ポイントに導入し、ユーザとグループに導入するか、またはデバイスに導入するかを選択します。

第 4 章
トラブルシューティング

このセクションでは、AMP for Endpoints コネクタのインストール後に発生する可能性のある問題と、問題の修復手順について説明します。

初期設定の失敗

まれに、AMP for Endpoints によりブロック プライベート クラウド デバイスの初期設定が失敗する場合があります。その場合には、プライベート クラウド デバイスを仮想マシンコンソールから削除して、OVA を再度インポートする必要があります。それでも初期設定が失敗する場合は、サポートまで連絡してください。

パフォーマンス

AMP for Endpoints によりブロック は、フィルタ ドライバを使用してファイルのコピー、移動、および実行操作を識別しますその際、データベースなどの I/O 負荷が高いアプリケーションでは、ファイル操作に余分な遅延が発生することがあります。遅延を短縮するには、以下の手順に従って AMP for Endpoints によりブロック から除外する必要があるものを判別します。

1. アプリケーション ファイルの場所を特定します。
2. データ ファイルが使用されている場所を判別します。
3. 両方の場所を除外します。
4. それでも特定のアプリケーションで問題が解決しない場合は、AMP for Endpoints コネクタのポリシーのデバッグ ロギングをオンにします。
5. それらのログを使用して、使用されているすべての一時ファイルを判別します。

参考にできるもう 1 つのヒントとして、sqlite3 の最新バージョンをダウンロードすれば（http://www.sqlite.org/download.html）、それを使用して履歴をクエリし、継続的に書き込まれているファイルを調べることができます。以下に一例を示します。

```
sqlite3.exe "C:\Program Files\Cisco\AMP\history.db"
SQLite version 3.7.16.2 2013-04-12 11:52:43
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .headers on
sqlite> select filename, count(filename) from history group by
filename order by
count(filename) desc limit 10;
filename|count(filename)
\\?\C:\WINDOWS\Tasks\User_Feed_Synchronization-{A1489466-0BD4-
42D2-A8B6-864FEA527577}.job|1706
\\?\C:\Documents and Settings\Administrator\Local
Settings\Application Data\Microsoft\Feeds\{5588ACFD-6436-411B-
A5CE-666AE6A92D3D}~\Internet Explorer Suggested Sites~.feed-
ms|341
\\?\C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-839522115-
1229272821-725345543-500UA.job|222
...
```

上記のデータにより、以下の除外項目を実装する価値があることがわかります。

FilePath: CSIDL_WINDOWS\Tasks

FileExtension: *.feed-ms

Outlook パフォーマンス

インストールしたAMP for Endpoints コネクタで Outlook のパフォーマンスが低下していることに気付いた場合、その原因としては、.pst または .ost ファイルに対する高 I/O 負荷が考えられます。このような場合には、AMP for Endpoints によりブロック コンソール内の .pst および .ost ファイルすべてを除外設定することをお勧めします。[管理（Management）] > [除外（Exclusions）] に移動し、必要な除外設定で [編集（Edit）] をクリックします。[除外の追加（Add Exclusion）] をクリックし、除外タイプのドロップダウン メニューから [ファイル拡張子（File Extension）] を選択します。フィールドに「.pst」と入力して、[作成（Create）] をクリックします。Outlook を Exchange Server とともに使用している場合は、.ost ファイル拡張子に対して上記の手順を繰り返します。

クラウドに接続できない

AMP for Endpoints コネクタがクラウドに接続できない場合、それにはいくつもの原因が考えられます。最も一般的な 2 つの原因は、ファイアウォールによってアウトバウンド接続が

妨げられていること、および、プロキシ サーバが接続に対応していないことです。いずれの場合にしても、以下の手順に従ってトラブルシューティングを開始する必要があります。

1. sfc.exe プロセス(3.1.4 より前のバージョンの場合は、agent.exe)が実行されていることを確認します。タスク マネージャを開き、[全ユーザのプロセスを表示する(Show processes from all users)] を選択して、sfc.exe プロセス(3.1.4 より前のバージョンの場合は agent.exe)がリストされていることを確認します。リストされていない場合は、管理者としてコマンド プロンプトを開き、`net start immunetprotect`(5.1.1 より古いバージョンの場合)および `net start ciscoamp_[version]`([version] はインストールされているコネクタのバージョン(5.1.1 など))を実行します。
2. タスク マネージャに iptray.exe プロセスが 1 つだけリストされていることを確認します。複数の iptray.exe プロセスがリストされている場合、すべての iptray.exe プロセスを終了してからコネクタ ユーザ インターフェイスを再起動する必要があります。
3. 正しいポートを介して cloud-ec.amp.sourcefire.com に接続できることを確認します。プロキシが設定されていない場合は、TCP 443 上での簡単な telnet テストで十分です。プロキシがある場合は、以下のプロキシに関する項を参照してください。
4. 以上の手順を実行しても接続できない場合は、AMP for Endpoints コネクタをアンインストールしてからコンピュータをリブートします。その後、使用しているポリシーに移動し、[詳細設定(Advanced Settings)] > [管理機能(Administrative Features)] > [コネクタログ レベル(Connector Log Level)] に移動して [デバッグ(Debug)] に設定します。その上で、AMP for Endpoints コネクタをダウンロードして再インストールします。これにより、問題を送信して診断するための追加情報を入手できます。

[デバイス トラジェクトリ(Device Trajectory)] にコピー、移動、または実行イベントが記録されない

コピー、移動、および実行イベントは、Immunet Protect ドライバからコネクタに送信されます。すると、コネクタはファイルに悪意があるかどうかを判別するために、この情報をクラウド サーバに渡します。クラウド サーバは、デバイス トラジェクトリが読み取り先とするデータベースにその情報をロードします。したがって、この問題のトラブルシューティングを行うには、以下の手順を実行します。

1. ドライバが正しくインストールされているかどうかを確認します。コマンド ラインから管理者として `fltmc instances` を実行すると、インストールされているドライバおよびバインドされているドライバがリストされます。ここで確認する必要があるのは、ImmunetProtectDriver がすべてのローカル ハード ドライブ(つまり、C:\、E:\ など)にバインドされていることです。
2. [詳細設定(Advanced Settings)] > [ファイルとプロセスのスキャン(File and Process Scan)] に移動し、ポリシーで [ファイルのコピーおよび移動のモニタリング(Monitor File Copies and Moves)] と [プロセス実行のモニタリング(Monitor Process Execution)] が有効になっているかどうかを確認します。これらのオプションが有効にされていなければ、これらのファイル操作はモニタされません。
3. クラウドに接続できることを確認します。

4. ポリシーで、[詳細設定(Advanced Settings)] > [管理機能(Administrative Features)] > [コネクタログレベル(Connector Log Level)] を [デバッグ(Debug)] に設定し、ログに disp=1 または disp=3 があることを確認します。disp=4 は、クラウドに対するファイルのルックアップに失敗したことを意味します。失敗の原因としては、ファイルのタイプがサポートされていないか、その他の理由が考えられます。
5. クラウドに接続されていて、クラウドから分類(disp)の 1 または 3 が返された場合は、サポート用の診断を行い、その結果を外部 IP アドレスと一緒にサポート ケースに添付してください。

[デバイス トラジェクトリ(Device Trajectory)] にネットワーク イベントが記録されない

ネットワーク情報は DFC ドライバによって取得されて、AMP for Endpoints コネクタに送信されます。コネクタは接続が悪意のあるものかどうかを調べるために、この情報をクラウド サーバに渡します。したがって、この問題のトラブルシューティングを行うには、以下の手順を実行します。

1. ポリシーで [モードとエンジン(Modes and Engines)] > [ネットワーク(Network)] が [ブロック(Block)] または [監査(Audit)] に設定されていることを確認します。
2. IP と ポートの情報をリストするイベントが確認された場合は、[詳細設定(Advanced Settings)] > [管理機能(Administrative Features)] > [コネクタログレベル(Connector Log Level)] を [デバッグ(Debug)] に設定します。

重要! AMP for Endpoints によりブロック では、プロセス実行後の最初の 100 の接続のみをモニタします。したがって、AMP for Endpoints コネクタの起動後には、必ず新しいプロセスを実行する必要があります。Internet Explorer は新しいタブのそれぞれに対してプロセスを再使用する一方、Chrome はタブの作成時に新しいプロセスを開始します。

ポリシーが更新されない

コネクタがポリシー更新の受信に失敗する最も一般的な原因は、ネットワーク接続またはプロキシ設定にあります。ネットワーク接続の問題については、プロキシおよびクラウドに接続できないを参照してください。ポリシーのプロキシ設定が誤っている場合は通常、AMP for Endpoints コネクタをアンインストールし、コンピュータをリブートしてポリシーのプロキシ設定を修正してから、AMP for Endpoints コネクタインストーラを再度ダウンロードして再インストールする必要がありです。ただし、1 台のコンピュータがグループにインストールされている場合(この目的のためだけにコンピュータをそのグループに移動できます)、次の手順を実行できます。

1. [管理(Management)] > [ポリシー(Policies)] に移動します。
2. 対象のポリシーを見つけてクリックします([編集(Edit)] をクリックしないでください)。これにより、右側にプレビューが表示されるので、[XML のダウンロード(Download XML)] ボタンをクリックします。XML ファイルのダウンロードが完了した後、以下の手順を実行します。

- AMP for Endpoints コネクタのインストール フォルダから管理者としてコマンド プロンプトに「`sfc.exe -k "password"`」と入力して、AMP for Endpoints コネクタを停止させます。コネクタ保護が有効になっている場合にのみ、引用符で囲んだパスワードを入力する必要があります。
- インストール フォルダ（5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire\FireAMP、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP）で、既存の policy.xml の名前を policy.xml.bak に変更します。
- そのフォルダに、ダウンロードした policy.xml をコピーして policy.xml に名前変更します。
- 管理者としてコマンド プロンプトから `net start immunetprotect`（5.1.1 より古いバージョンの場合）および `net start ciscoamp_[version]`（[version] はインストールされているコネクタのバージョン（5.1.1 など）を実行して、AMP for Endpoints コネクタを起動します。
- ダウンロードしたファイルの policy.xml を開き、シリアル番号をメモします。
- ポータルでポリシーに変更を加えてから、[AMP for Endpoints コネクタの設定（Connector Settings）] 画面で [同期ポリシー（Sync Policy）] をクリックします。約 2 分間待ってから、シリアル番号が変更されていることを確認します。

プロキシ

すべての組織がインターネットへの直接アウトバウンド接続を許可しているわけではありません。組織によっては、接続をプロキシにルーティングして、トラフィックのフィルタ処理とスキャンができるようにしている場合もあります。AMP for Endpoints によりブロック ではプロキシをサポートしていますが、ポリシーを正しく設定することが重要です。この場合に考えられる最善策は、ポリシーで [詳細設定（Advanced Settings）] > [管理機能（Administrative Features）] > [コネクタのログレベル（Connector Log Level）] を [デバッグ（Debug）] に設定してからAMP for Endpoints コネクタを起動することです。ログに明白なエラーが記録されていない場合は、以下の手順を実行します。

- AMP for Endpoints コネクタのインストール フォルダから管理者としてコマンド プロンプトに「`sfc.exe -k "password"`」と入力して、AMP for Endpoints コネクタを停止させます。コネクタ保護が有効になっている場合にのみ、引用符で囲んだパスワードを入力する必要があります。
- 不要なアプリケーションを閉じてから、トラブルシューティング対象のコンピュータに Wireshark をインストールして実行します。
- Wireshark を使用して、プロキシ サーバとアウトバウンド インターネット間の接続で開始されたパケット キャプチャの取得を試行します。
- コンピュータ上のブラウザでのプロキシ設定が、トラブルシューティング対象のコンピュータ上のプロキシ設定と同じであることを確認します。https://console.amp.cisco.com にアクセスできることを確認するテストを行います。
- http://curl.haxx.se/download.html から curl をインストールします。http://immunet-janus-helpdoc.s3.amazonaws.com/FireAMP_Helper/FireAMP_Helper.vbs から FireAMP_Helper.vbs をダウンロードします。.vbs ファイルを開き、以下のように変更します。
  - CURL_APP = " curlpath\curl.exe"

    ここで、curlpath は curl のインストール ディレクトリへのパスです。

- PROXY_SERVER = " http://x.x.x.x:yyyy"

  ここで、x.x.x.x はプロキシ サーバの IP アドレス、yyyy は使用するポートです（通常は 8080）。
- PROXY_USER_PASS = " Domain\username:password"

  ここで、Domain\username と password はプロキシ サーバに対する認証に使用するユーザ名とパスワードです。プロキシが認証を必要としない場合、このフィールドを空のままにして構いません。

以上の変更を行った後、次のコマンドを実行します。

```
cscript FireAMP_Helper.vbs testproxy
```

- 管理者としてコマンド プロンプトから `net start immunetprotect`（5.1.1 より古いバージョンの場合）および `net start ciscoamp_[version]`（[version] はインストールされているコネクタのバージョン（5.1.1 など）を実行して、AMP for Endpoints コネクタを起動します。
- 約 5 分間コネクタを実行させて、トラフィックを生成させます。
- AMP for Endpoints によりブロック 診断、AMP for Endpoints コネクタからプロキシへの PCAP、およびプロキシからインターネットへの PCAP を取得し、それらをサポート ケースに添付します。

コネクタの重複

場合によっては、AMP for Endpoints によりブロック コンソールの [コンピュータ（Computers）] ページに重複エントリが表示されることがあります。まず重複エントリの原因を特定することで、それらを削除するプロセスを進めることができます。

原因

実際の環境で重複するコネクタが発生する一般的な原因は 3 つあります。

ゴールド標準イメージ

AMP for Endpoints コネクタが含まれているゴールド標準イメージを使用してエンドポイントを導入する場合は、エンドポイントを導入するたびに重複するコネクタが AMP for Endpoints によりブロック コンソールに表示されます。ゴールド標準イメージを使用してエンドポイントを展開するときは、この記事を参照するか、サポートに連絡すると、コネクタの重複防止に役立ちます。

再イメージ化

エンドポイントを再イメージ化すると、常に重複コネクタ エントリが発生します。これは、再イメージ化されたコネクタに関して新しいデバイス トラジェクトリが開始されるとともに、古いコネクタのデバイス トラジェクトリが維持されるためです。セキュリティ侵害のためにコンピュータを再イメージ化した場合は、これにより、考えられる原因をより詳しく調べることができます。古いデバイス トラジェクトリが不要になったら、古いコネクタを削除できます。

仮想環境

仮想環境でも、新しい仮想セッションが開始されたとき、または仮想コンピュータが再イメージ化されたときに、重複コネクタ エントリが発生することがあります。ほとんどの場合、この記事を参照するか、サポートに連絡すると、コネクタの重複防止に役立ちます。

重複コネクタの削除

管理コンソール内では、重複コネクタを手動で削除します。重複を管理するには、[管理(Management)] > [コンピュータ(Computers)] に移動して、ページの上部にある [フィルタ(Filters)] セクションを展開し、[最後の確認日時(Last Seen)] ドロップダウンを目的の範囲に設定してから [フィルタの適用(Apply Filter)] をクリックします。フィルタ処理されたビューには、選択した期間で最後に確認されたすべてのコネクタが表示されます。リストのすべてのコンピュータを選択することも、それらを削除することもできます。コネクタが今もインストールされているコンピュータを削除すると、コンピュータのリブート時などにサービスが再起動され、コンピュータが管理コンソールに再登録されます。

シンプル カスタム検出

シンプル カスタム検出を使用すると、検出対象のファイルを手動でブラックリストに入れることができます。[モードとエンジン(Modes and Engines)] > [ファイル(Files)] を [監査(Audit)] に設定すると、検出の通知のみ行われますが、[検疫(Quarantine)] に設定した場合はファイルが検疫されます。最も一般的な問題として、ファイルを見つけてマシンにコピーし、そのファイルを [シンプルカスタム検出(Simple Custom Detection)] に追加したのに、どういうわけか、そのファイルが検出されないことがあります。それには以下の理由が考えられます。

1. ファイルが除外されています。実行元のパスを、policy.xml にリストされている除外項目のパスと比較してください。除外項目のファイル拡張子も調べる必要があります。
2. ファイルが署名済み Microsoft または Verisign Class 3 証明書に記載されています。ファイルを右クリックして、プロパティを参照してください。ファイルにデジタル署名が関連付けられているかどうかを調べ、関連付けられている場合はその発行元を調べます。署名が Verisign デジタル署名であり、マルウェアであると確信できる場合は、ファイルを [Virus Total] にアップロードした後、サポートに連絡してください。
3. ファイルに適切なポリシーが関連付けられていません。ファイルの SHA-256 が正しいシンプル カスタム検出リストに含まれていることを確認してください。そのシンプル カスタム検出リストが、コネクタで使用しているポリシーに関連付けられていることを確認します。
4. ファイルがキャッシュされています。これは、最も一般的な問題です。ファイルをコンピュータにコピーすると、cache.db にそのファイルのレコードが作成されます。このレコードを削除するには、以下の手順を実行します。
   - AMP for Endpoints コネクタのインストール フォルダから管理者としてコマンド プロンプトに「`sfc.exe -k "password"`」と入力して、AMP for Endpoints コネクタを停止させます。コネクタ保護が有効になっている場合にのみ、引用符で囲んだパスワードを入力する必要があります。

- インストール ディレクトリ（5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire\FireAMP、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP）に移動し、cache.* ファイルを削除します。
- 管理者としてコマンド プロンプトから `net start immunetprotect`（5.1.1 より古いバージョンの場合）および `net start ciscoamp_[version]`（[version] はインストールされているコネクタのバージョン（5.1.1 など）を実行して、AMP for Endpoints コネクタを起動します。
- 問題のファイルを再度コピーして、そのファイルが検出されないことを確認します。

カスタム ホワイトリスト

カスタム ホワイトリストを使用すると、ファイルをホワイトリストに入れて、ファイルの検出を回避できます。これは、「ゴールデン イメージ」からすべてのファイルを収集する一環として行うことも、誤検出に備えて行うこともできます。ここで最も一般的な問題となるのは、キャッシングです。それは、コンピュータ上に存在するファイルの cache.db をクリアする必要があるためです。

1. AMP for Endpoints コネクタのインストール フォルダから管理者としてコマンド プロンプトに「`sfc.exe -k "password"`」と入力して、AMP for Endpoints コネクタを停止させます。コネクタ保護が有効になっている場合にのみ、引用符で囲んだパスワードを入力する必要があります。
2. インストール ディレクトリ（5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire\FireAMP、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP）に移動し、cache.* ファイルを削除します。
3. 管理者としてコマンド プロンプトから `net start immunetprotect`（5.1.1 より古いバージョンの場合）および `net start ciscoamp_[version]`（[version] はインストールされているコネクタのバージョン（5.1.1 など）を実行して、AMP for Endpoints コネクタを起動します。
4. 作成したファイルを再度コピーして、そのファイルが検出されないことを確認します。

考えられる問題には、カスタム ホワイトリストが正しいポリシーに関連付けられていないか、またはファイルの SHA-256 がそのリストに追加されていないことも挙げられます。

アプリケーション ブロッキング

アプリケーション ブロッキングを使用すると、ファイルを検疫することなく、ファイルの実行を防ぐことができます。アプリケーション ブロッキング リストに SHA-256 を追加しても、それがまだ実行される場合、その原因には以下が考えられます。

1. ファイルが除外されています。実行元のパスを、policy.xml にリストされている除外項目のパスと比較してください。除外項目のファイル拡張子も調べる必要があります。
2. ファイルに適切なポリシーが関連付けられていません。ファイルの SHA-256 が正しいシンプル カスタム検出リストに含まれていることを確認してください。そのシンプル カスタム検出リストが、コネクタで使用しているポリシーに関連付けられていることを確認します。

3. ファイルがキャッシュされています。これは、最も一般的な問題です。ファイルをコンピュータにコピーすると、cache.db にそのファイルのレコードが作成されます。このレコードを削除するには、以下の手順を実行します。
   - AMP for Endpoints コネクタのインストール フォルダから管理者としてコマンド プロンプトに「`sfc.exe -k "password"`」と入力して、AMP for Endpoints コネクタを停止させます。コネクタ保護が有効になっている場合にのみ、引用符で囲んだパスワードを入力する必要があります。
   - インストール ディレクトリ（5.1.1 より古いバージョンの場合はデフォルトで C:\Program Files\Sourcefire\FireAMP、5.1.1 以降のバージョンの場合は C:\Program Files\Cisco\AMP）に移動し、cache.* ファイルを削除します。
   - 管理者としてコマンド プロンプトから `net start immunetprotect`（5.1.1 より古いバージョンの場合）および `net start ciscoamp_[version]`（[version] はインストールされているコネクタのバージョン（5.1.1 など）を実行して、AMP for Endpoints コネクタを起動します。
   - 問題のファイルを再度コピーして、そのファイルが実行されないことを確認します。

サポートへの問い合わせ

トラブルシューティングで問題を解決できなかった場合は、サポートに連絡して問題を解決してください。サポート ケースの所要時間を短くするためには、ケースをオープンする際に以下の手順に従って情報を提供すると役立ちます。

1. [管理（Management）] > [ポリシー（Policies）] に移動し、トラブルシューティング対象のAMP for Endpoints コネクタが含まれるポリシーを編集します。
2. [詳細設定（Advanced Settings）] > [管理機能（Administrative Features）] > [コネクタ ログレベル（Connector Log Level）] を [デバッグ（Debug）] に設定します。
3. AMP for Endpoints コネクタで、[設定（Settings）] に移動し、[同期ポリシー（Sync Policy）] をクリックします。

   コネクタをインストールする際にコマンド ライン スイッチを使用してスタート メニュー項目を無効にした場合、コマンド プロンプトを開いて以下のコマンドを実行することで、ポリシー同期を強制できます。

   ```
   %PROGRAMFILES%\Sourcefire\FireAMP\x.x.x\iptray.exe -f
   ```

   ここで、x.x.x はAMP for Endpoints コネクタのバージョン番号です。
4. ポリシーが同期された後、コネクタを 5 ～ 10 分実行させるか、またはエラーを発生させている特定のアクションを実行します。
5. Windows のスタート メニューを開き、[AMP for Endpoints コネクタ] に移動して [サポート診断ツール（Support Diagnostic Tool）] をクリックします。これにより、デスクトップに Sourcefire_Support_Tool_2013_XX_XX_XX_XX_XX.7z という名前のファイルが作成されます。ここで、XX はツールを実行した月、日、時刻です。

   コネクタをインストールする際にコマンド ライン スイッチを使用してスタート メニュー項目を無効にした場合、コマンド プロンプトを開いて以下のコマンドを実行することで、サポート診断ツールを実行できます。

   ```
   %PROGRAMFILES%\Sourcefire\FireAMP\x.x.x\ipsupporttool.exe
   ```

   ここで、x.x.x はAMP for Endpoints コネクタのバージョン番号です。

6. AMP for Endpoints コネクタで接続の問題が発生している場合は、すべてのネットワーク アクティビティの PCAP を取得します。
7. サポートに連絡する際には、診断ファイルと PCAP をシスコ SSL サーバ（https://uploads.sourcefire.com/uploads/ed14f406d34f0fbd7c1af84fe024bd1d）にアップロードします。アップロードしたファイル名は、必ずメモしておいてください。
8. 問題がユーザインターフェイスのバグまたは AMP for Endpoints によりブロック コンソールの問題である場合、問題のスクリーンショットを電子メールに添付して送信してください。
9. 問題に関連するすべての情報と、アップロードしたファイルのファイル名をサポートに連絡し、必要な場合はスクリーンショットを添付してください。また、接続の問題の場合には、使用しているプロキシとファイアウォールのタイプに関する情報も記載してください。

付録 A
脅威の説明

AMP for Endpoints では、シスコ独自のネットワーク検出イベント タイプと侵害兆候を定義しています。ここでは、これらの検出タイプについて説明します。

重要! 脅威の名前の説明については、AMP の命名規則を参照してください。

侵害の兆候

AMP for Endpoints は、過去 7 日間にわたって観察されたイベントに基づく侵害の兆候を使用してデバイスを評価します。悪意のあるファイルの検出、悪意のあるファイルを繰り返しダウンロードしている親ファイル（ドロッパー感染の可能性）、悪意あるファイルをダウンロードしている複数の親ファイル（複数の感染したファイル）などのイベントすべてが要因です。侵害の兆候には以下が含まれます。

- 脅威を検出（Threat Detected）：コンピュータ上で 1 つ以上のマルウェア検出がトリガーされました。
- ドロッパー感染の可能性（Potential Dropper Infection）：1 つのファイルが繰り返しマルウェアをコンピュータにダウンロードしようとしていることを示します。
- 複数の感染したファイル（Multiple Infected Files）：複数のファイルがマルウェアをダウンロードしようとしていることを示します。
- 実行されたマルウェア（Executed Malware）：既知のマルウェア サンプルがコンピュータ上で実行されました。この場合は、マルウェアがペイロードを実行した可能性があるため、単純な脅威検出よりも深刻です。
- 疑わしいボットネット接続（Suspected botnet connection）：コンピュータが疑わしいボットネットコマンドと制御システムへのアウトバウンド接続を確立しました。

- [アプリケーション]侵害([Application] Compromise):疑わしいポータブル実行ファイルが「Adobe Reader Compromise」などの名前のアプリケーションによってダウンロードされ、実行されました。
- [アプリケーション] により起動されたシェル([Application] launched a shell):指定したアプリケーションが不明なアプリケーションを実行し、コマンド シェルを起動しました(Java によるシェルの起動など)。
- 汎用 IOC(Generic IOC):コンピュータが侵害された可能性を示す疑わしい動作。
- 疑わしいダウンロード(Suspicious download):疑わしい URL から実行可能ファイルをダウンロードしようとしました。ただし、必ずしも URL やファイルに悪意がある(またはエンドポイントが侵害されている)とは限りません。動作の原因を理解するために、ダウンロードの背景やダウンロードしようとしたアプリケーションを詳細に調査する必要があります。
- 疑わしい Cscript の起動(Suspicious Cscript Launch):Internet Explorer がコマンドプロンプトを起動し、cscript.exe を実行しました(Windows スクリプト ホスト)。この一連のイベントは一般に、ブラウザのサンドボックス エスケープを示唆します。これは悪意のある Visual Basic スクリプトの実行につながります。
- 疑わしいランサムウェア(Suspected ransomware):既知のランサムウェアに関連付けられた特定のパターンを含むファイル名がコンピュータ上で確認されました。たとえば、help_decrypt.<filename> という名前のファイルが検出されました。
- WebShell の可能性(Possible webshell):IIS ワーカー プロセス(w3wp)が、powershell.exe などの別のプロセスを起動しました。これは、コンピュータがセキュリティ侵害を受けており、攻撃者へのリモート アクセスが許可されたことを示唆する可能性があります。
- 認識可能な脅威(Cognitive Threat):シスコ Cognitive Threat Analytics は高度なアルゴリズム、機械学習、および人工知能を使用して、ユーザおよびネットワークデバイスによって生成されたネットワークトラフィックを関連付けて、指揮および統制トラフィック、データ漏洩、および悪意のあるアプリケーションを識別します。認識可能な脅威による侵害の兆候イベントは、組織で検出された疑わしいトラフィックまたは異常なトラフィックが検出されると生成されます。CTA により重大度 7 以上を割り当てられた脅威のみが AMP for Endpoints に送信されます。

重要! 正規のアプリケーションのアクティビティが侵害兆候として判断される場合があります。正規のアプリケーションは検疫/ブロックされませんが、再び侵害兆候として判断されることを防止するため、アプリケーションを Application Control - Whitelisting に追加してください。

DFC 検出

デバイス フロー コリレーション(DFC)を使用すると、疑わしいネットワーク アクティビティにフラグを立てたり、ブロックしたりできます。Policies を使用すると、疑わしい接続が検出されたときのAMP for Endpoints Connectorの動作に加え、コネクタがアドレスを使用すべき場所(シスコ Intelligence Feed、作成したカスタム IP リスト、またはその両方の組み合わせ)を指定できます。DFC 検出には以下が含まれます。

- DFC.CustomIPList:コンピュータが、DFC IP ブラックリストで定義された IP アドレスへの接続を確立しました。
- Infected.Bothost.LowRisk:コンピュータが、ボットネットへの既知の参加者であるコンピュータに属していると見られる IP アドレスへの接続を確立しました。
- CnC.Host.MediumRisk:コンピュータが、過去にボット コマンドと制御チャネルとして使用されたことが判明している IP アドレスへの接続を確立しました。このコンピュータのデバイス トラジェクトリをチェックして、このホストからファイルがダウンロードされ、その後実行されたかどうかを確認してください。
- ZeroAccess.CnC.HighRisk:コンピュータが、既知の ZeroAccess コマンドと制御チャネルへの接続を確立しました。
- Zbot.P2PCnC.HighRisk:コンピュータが、ピアツーピア コマンドと制御チャネルを使用して既知の Zbot ピアへの接続を確立しました。
- Phishing.Hoster.MediumRisk:コンピュータが、フィッシング サイトをホストしている可能性のある IP アドレスへの接続を確立しました。フィッシング サイトが他の多くの無害な Web サイトもホストしている場合も多くあり、このようなサイトのいずれかに接続された可能性もあります。

付録 B
関連資料

ダウンロード可能な関連資料は次のとおりです。

シスコ AMP for Endpoints ユーザ ガイド

次のリンクから、ユーザ ガイドの最新バージョンをダウンロードできます。

ユーザ ガイドのダウンロード

シスコ AMP for Endpoints クイックスタートガイド

このガイドでは、グループ、ポリシー、除外の設定、およびAMP for Endpoints コネクタの展開について段階的に説明します。このガイドは、AMP for Endpoints を評価するのに役立ちます。

クイック スタート ガイドのダウンロード

シスコ AMP for Endpoints 導入戦略ガイド

このガイドでは、AMP for Endpoints の本番導入に向けた準備と計画の詳細に加えて、ベスト プラクティスとトラブルシューティングのヒントについても説明します。

導入戦略ガイドのダウンロード

Cisco Endpoint IOC の属性

エンドポイント IOC の属性に関するドキュメントには、AMP for Endpoints コネクタに搭載されているエンドポイント IOC スキャナでサポートされる IOC の属性が詳しく説明さ

れています。AMP for Endpoints コンソールにアップロードできるサンプルの IOC ドキュメントも含まれています。

エンドポイント IOC の属性のダウンロード

Cisco AMP for Endpoints API ドキュメンテーション

API を 使用すると、コンソールにログインせずに、AMP for Endpoints のデータやイベントにアクセスできます。このドキュメンテーションには、使用可能なインターフェイス、パラメータ、および使用例が記載されています。

API ドキュメンテーションの表示

シスコ AMP for Endpoints リリース ノート

このリリース ノートには AMP for Endpoints の変更ログが含まれています。

リリースノートのダウンロード

シスコ AMP for Endpointsデモ データのシナリオ

デモ データのシナリオでは、AMP for Endpoints で Demo Data が有効になっている場合に表示される一部の例について説明します。

SFEICAR ドキュメントのダウンロード

ZAccess ドキュメントのダウンロード

ZBot ドキュメントのダウンロード

CozyDuke ドキュメントのダウンロード

Upatre ドキュメントのダウンロード

PlugX ドキュメントのダウンロード

Cryptowall ドキュメントのダウンロード

Low Prevalence Executabl のドキュメントのダウンロード

コマンド ライン キャプチャのドキュメントのダウンロード

Cognitive Threat Analytics（CTA）のドキュメントのダウンロード

WannaCry ランサムウェアのドキュメントのダウンロード

シングル サインオンの設定

AMP for Endpoints コンソールでシングル サインオンを有効にする際に、一部の ID プロバイダーでは追加の設定手順が必要になります。手順については、次のドキュメントを参照してください。

Active Directory セットアップ ガイドのダウンロード

Okta セットアップ ガイドのダウンロード

PingFederate セットアップ ガイド

シスコ ユニバーサル クラウド契約

クラウド オファーの利用規約