エンドポイント導入のためのAMPでのオプトインおよびオービタル拡張検索の有効化（2020年1月8日現在の既存のお客様向け）

内容

シスコは最近、エンドポイント向けAMPのパッケージを2つ発表しました。EssentialsとAdvantage。オービタル高度な検索は、アドバンテージパッケージの重要な機能です。発売日（2020年1月8日）の時点で既存のお客様はすべて、契約期間の残りの期間は無料で利用できます。このFAQには、パッケージに関する詳細情報と、発売日の時点での既存のお客様への影響について説明しています。

Orbital Advanced Searchは、Cisco AMP for Endpointの新しい高度な機能で、100以上のカタログクエリを提供することで、セキュリティ調査と脅威の追跡をシンプルにします。これにより、任意またはすべてのエンドポイントで複雑なクエリを迅速に実行できます。また、現在の状態のスナップショットを取得することで、任意のエンドポイントで発生した事象をより詳細に把握できます。

オービタルの高度な検索を使用すると、次の重要なタスクをより良く、迅速に実行できます。

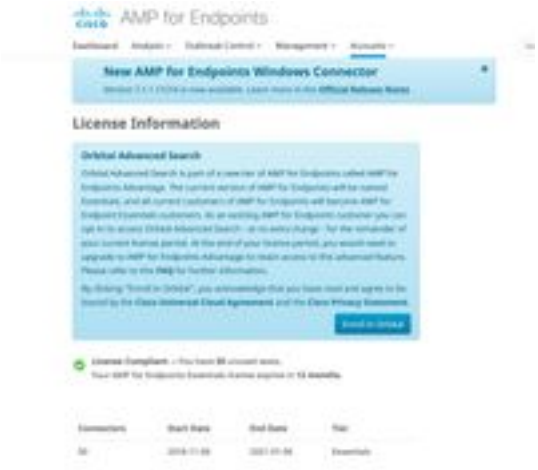
- **脅威追跡**。悪意のあるアーティファクトをほぼリアルタイムで検索し、脅威の発見を加速します。
- **インシデント調査**。インシデントの根本原因を迅速に把握し、修復を加速します。
- **IT運用**。ディスク領域、メモリ、およびその他のIT運用のアーティファクトを追跡するだけです。
- **脆弱性とコンプライアンス**。バージョンやパッチのアップデートなどのオペレーティングシステムのステータスをすばやくチェックし、エンドポイントが現在のポリシーに準拠していることを確認します。

このドキュメントは、新しい機能にオプトインし、エンドポイントで有効にする方法を説明する手順ガイドです。完全なオービジタルのユーザーガイドも利用できます。エンドポイント用AMPのお客様は、エンドポイントにすでにコネクタ(7.1.5以降)がインストールされている場合は、Orbital Advanced Searchを簡単に有効にできます。 最新のConnectorのバージョンやその他の情報については、OrbitalのAMP for Endpointsコンソールのヘルプトピックを参照してください。Orbital Advanced Searchは、現在、バージョン1703 (Creators Update)以降を実行している64ビットWindows 10ホストでサポートされています。

これらの手順を完了したら、オービタル高度な検索を使い始める方法の詳細については、クイックスタートガイドを参照してください。

ステップ 1：オービタル検索へのオプトイン

以前にOrbital Advanced Searchベータ版に登録していなかったり、明示的に登録されていない場合は、AMP for Endpointsコンソールのライセンス情報ページから登録できます。Orbital Advanced Searchにオプトインするには、AMP for Endpointsコンソールにログインし、[アカウント] > [ライセンス情報]のドロップダウン**を選択します**。このページでは、[Enroll in Orbital]をクリック**して、この機能**にアクセスすることができます。

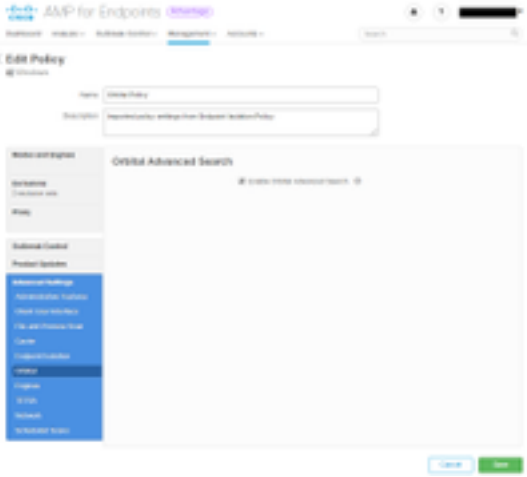


注：Orbital Advanced Searchにオプトインするには、特権（管理者）ユーザーである必要があります。

ステップ 2：既存のポリシーで軌道高度検索を有効にする

エンドポイントに既にコネクタがインストールされている場合(バージョン7.1.5以降)は、エンドポイントの既存のポリシーでOrbital Advanced Searchを有効にするだけです。

- AMP for Endpointsコンソールに移動します。Management > Policiesで、Orbital Advanced Searchを有効にするポリシーを選択し、**Editボタンをクリックして**Edit Policyを開きます*Advanced Settings*でOrbitalを選択し、Orbital Advanced Searchが有効になっていることを確認します。[Enable Orbital Advanced Search]**ボックスにチェック**を入れる必要があります。有効になっていない場合は、チェックボックスをオンにして有効にします。



この時点で、このポリシーを使用して取り付けられたコネクタは、そのエンドポイントでOrbital Advanced Searchを自動的に有効にします。

ステップ 3：新しいポリシーとコンピューターのグループで軌道高度検索を有効にする（オプション）

前述のように、既存のポリシーでOrbital Advanced Searchを有効にすると、そのポリシーを使用するすべてのコネクタでOrbital Advanced Searchが有効になり、そのポリシーを使用して新しくインストールしたコネクタでもOrbital Advanced Searchが有効になります。たとえば、「保護」グループに1000台のコンピュータがある場合、そのポリシーでOrbital Advanced Searchを有効にするだけで、Connectorバージョン7.1.5以降が展開されている限り、それらのエンドポイントでOrbital Advanced Searchが自動的に有効になります。

新しいポリシーとグループの作成はオプションです。ただし、新しいポリシーとグループを使用してエンドポイントの特定のグループでOrbital Advanced Searchを使用する場合は、製品のドキュメントに従って新しいポリシーやグループを作成し、上記のようにポリシーでOrbital Advanced Searchが有効になっていることを確認してください。

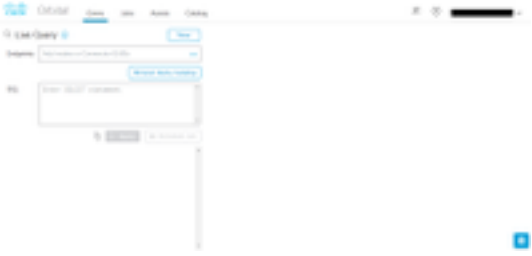
ステップ 4： 軌道コンソールの探索

少なくとも1つのエンドポイントに7.1.5よりも高いコネクタバージョンがインストールされているポリシーでOrbital Advanced Searchを有効にすると、エンドポイントでクエリを実行して情報を収集できるようになります。

- [**Management**] > [Computers]**に移動**し、[Orbital Advanced Search]を使用するコンピュータを探します。ペインを展開し、[**Orbital Query**]をクリック**します**。([**Analysis**] > [**Orbital Advanced Search**]に移動して、オービタル**コンソールにアクセスすることも**できます)。
- オービタルのコンソールが新しいブラウザタブにロードされます。必要に応じて、[Log in with **Cisco Security]をクリックし**て、既存のAMPコンソールの認証情報を使用して認証します。

注：また、https://orbital.amp.cisco.comからOrbital Advanced Searchに直接アクセスすることもでき[ます](#)

- [エン**ドポイン**ト]フィールドには、照会するコンピュータが表示されます。特定のGUIDを入力するか、このフィールドに**allと入力**して、Orbital Advanced Searchが有効になっている組織内のすべてのエンドポイントを照会できます。端点のランダムなサンプリングを行う場合は、省略記号(...)をクリックして、「ランダム端点を追加」(**Add Random Endpoints)ダイアログボ**ックスを開きます。
- カスタムSELECT文を**SQL**フィールドに入力するか、[クエリのカタログの参**照]をクリックし**て、クエリに追加できる多数のクエリを含む**クエリカタログを開**きます。**Orbitalを使用するためにSQL SELECT文を書く方法を知る必要はありません。**



- [Query] を選択します。クエリーが指定したエンドポイントに対して実行され、結果が右ペインに表示されます。クエリーを編集して再実行できます。結果をダウンロードできます。設定できるスケジュールに基づいて実行するジョブとしてクエリを保存できます。
- オービタルの高度な検索を開始する方法の詳細については、クイックスタートをご覧[ください](#)