在面向終端的AMP部署中選入並啟用Orbital Advanced Search（自2020年1月8日起針對現有客戶）

目錄

思科最近推出了兩個面向終端的AMP包：Essentials和Advantage。Orbital Advanced Search是Advantage軟體包中的一項關鍵功能。所有現有客戶在啟動之日（2020年1月8日）即可選擇在其剩餘合約期內免費使用該服務。本FAQ提供了有關軟體包的詳細資訊，以及自發佈之日起它如何影響現有客戶。

Orbital Advanced Search是思科面向終端的AMP中一項新的高級功能，旨在通過提供100多個目錄查詢，使安全調查和威脅搜尋變得簡單。這允許您對任何或所有端點快速運行複雜查詢。這還使您能夠通過獲取任何終端當前狀態的快照，從而更深入地瞭解任何終端在任意給定時間發生的情況。

使用Orbital Advanced Search，您可以更好、更快地執行以下重要任務：

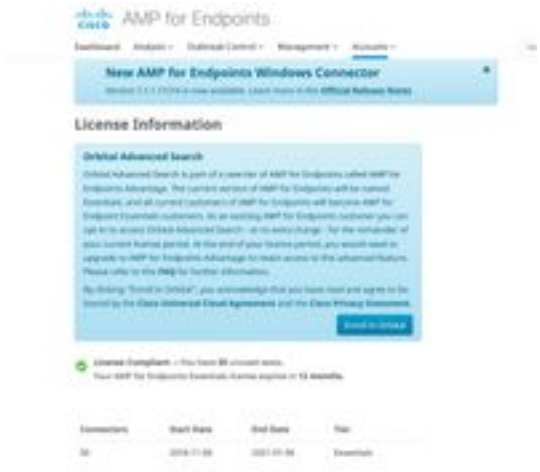
- **威脅搜尋**。近即時搜尋惡意物品，以加速對威脅的搜尋。
- **事故調查**。快速查明事件的根本原因，加快補救速度。
- **IT運營**。只需跟蹤磁碟空間、記憶體和其他IT操作工件。
- **漏洞和合規性**。快速檢查作業系統的狀態，以瞭解版本和修補程式更新等內容，確保您的終端符合當前策略。

本文檔是逐步指南，將指導您選擇使用新功能並在您的終端上啟用該功能。還有完整的軌道用戶指南可供使用。面向終端的AMP客戶可以輕鬆地啟用軌道高級搜尋(如果您的終端已經安裝聯結器（7.1.5或更高版本）。 請參閱軌道上的面向終端的AMP控制檯幫助主題，瞭解最新的聯結器版本和其他資訊。Orbital Advanced Search目前支援64位Windows 10主機運行1703版（建立者更新）或更高版本。

完成這些步驟後，請參閱快速入門指南，以獲取有關如何開始使用Orbital Advanced Search的更詳細說明。

第1步：進入軌道進階搜尋

如果您以前沒有註冊參加軌道高級搜尋試用版或明確選擇加入，您可以從面向終端的AMP控制檯的「許可證資訊」頁面進行註冊。要選擇加入Orbital Advanced Search，請登入到AMP for Endpoints控制檯，然後選擇**Accounts > License Information**下拉選單。在此頁面上，您可以按一下**Enroll in Orbital**以訪問此功能。

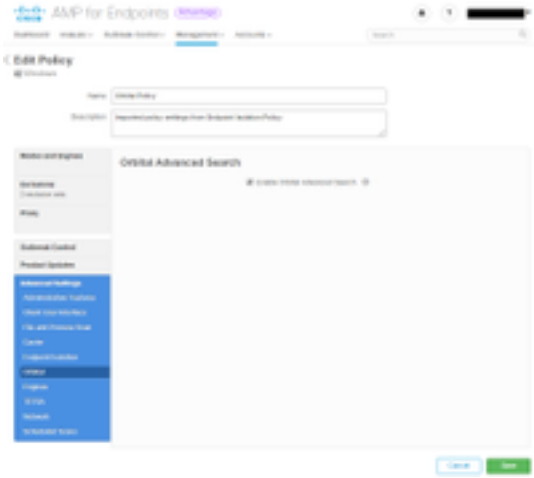


附註：您必須是特權（管理員）使用者才能選擇加入Orbital Advanced Search。

第2步：在現有策略中啟用軌道高級搜尋

如果您的終端已經安裝了一個聯結器（7.1.5版或更高版本），則只需在終端的現有策略中啟用軌道高級搜尋即可。

- 轉至AMP for Endpoints控制檯。在Management > Policies中，選擇要在中啟用Orbital Advanced Search的策略，然後點選**Edit**按鈕以開啟**Edit Policy**Under *Advanced Settings*下選擇**Orbital**，並驗證是否已啟用Orbital Advanced Search。應選中**Enable Orbital Advanced Search**框。如果不是，請選中該框以啟用它。



此時，使用此策略安裝的任何聯結器將自動在該終端上啟用Orbital Advanced Search。

步驟3:啟用新策略和電腦組的軌道高級搜尋（可選）

如上所述，一旦您在現有策略中啟用了Orbital Advanced Search，則使用該策略的所有聯結器都將啟用Orbital Advanced Search，而使用該策略安裝的任何新聯結器也將啟用Orbital Advanced Search。例如，如果您的「保護」組中有1000台電腦，只要在該策略中啟用Orbital Advanced Search，則只要部署了Connector 7.1.5版或更高版本，就會自動在這些端點上啟用Orbital Advanced Search。

建立新策略和組是可選的。但是，如果您要使用新策略和組對特定一組終端使用Orbital Advanced Search，則只需按照產品文檔建立新策略和/或組，並確保在策略中啟用Orbital Advanced Search（如上所示）。

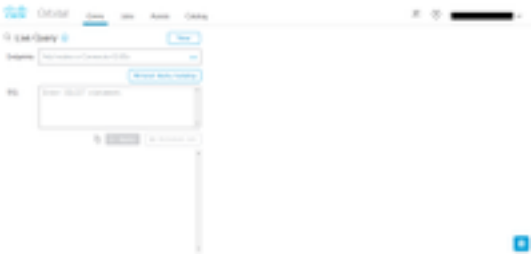
第4步： 探索軌道控制檯

在至少在一個端點上安裝了聯結器版本高於7.1.5的策略中啟用Orbital Advanced Search後，您現在可以在端點上執行查詢，以便從該端點收集資訊。

- 轉至**Management > Computers**，使用Orbital Advanced Search查詢電腦展開窗格，然後按一下**Orbital Query**。(也可以通過轉至**Analysis > Orbital Advanced Search**來訪問Orbital控制檯。)
- 軌道控制檯被載入到一個新的瀏覽器頁籤中。如果需要，請點選**Log in with Cisco Security**，使用現有的AMP控制檯憑證進行身份驗證。

附註：您也可以直接訪問https://orbital.amp.cisco.com上的Orbital Advanced Search

- **Endpoints**欄位顯示將查詢的電腦。您可以輸入特定的GUID或在此欄位中輸入**all**，以查詢組織中啟用了Orbital Advanced Search的每個終端。如果要對端點進行隨機取樣，請按一下省略號(...)以開啟「新增隨機端**點」**對話方塊。
- 您可以在**SQL**欄位中輸入自定義SELECT語句，或按一下**瀏覽查詢目錄**以開啟**查詢目錄**，其中包含可以新增到查詢中的幾十個查詢。**您不必知道如何編寫SQL SELECT語句以使用Orbital。**



- 按一下「**Query**」。查詢針對指定的端點運行，結果顯示在右窗格中。您可以編輯查詢並重新運行。您可以下載結果。您可以將查詢另存為可以配置的計畫運行作業。
- 有關Orbital Advanced Search入門的詳細資訊，請瀏覽快速入門