# 在面向终端的AMP部署中选择并启用轨道高级搜索(从2020年1月8日起面向现有客户)

#### 目录

o

步骤 1:选择进入轨道高级搜索

步骤 2: 在现有策略中启用轨道高级搜索

步骤 3: 在新策略和计算机组中启用轨道高级搜索(可选)

#### 步骤 4: 探索Orbital控制台

思科最近推出了两款面向终端的AMP软件包:<u>基本版和优势</u>。Orbital Advanced Search是 Advantage包中的一项关键功能。自发布之日(2020年1月8日)起,所有现有客户均可选择在其剩 余合同期内免费使用。本常<u>见问</u>题解答提供了有关产品包的更多信息,以及自发布之日起它对现有 客户的影响。

Orbital Advanced Search是面向终端的思科AMP中的一项新的高级功能,旨在通过提供100多个目录查询简化安全调查和威胁搜索。这允许您在任何或所有终端上快速运行复杂查询。这还使您能够通过拍摄任何终端当前状态的快照,更深入地了解任何终端在任何给定时间上发生的情况。

借助轨道高级搜索,您可以更好、更快地完成以下重要任务:

- •寻找威胁。近乎实时地搜索恶意项目,以加快您对威胁的搜索。
- •事故调查。快速找到事故的根本原因,加快补救速度。
- •IT运营。只需跟踪磁盘空间、内存和其他IT操作工件。
- •漏洞和合规性。快速检查操作系统的状态,了解版本和补丁更新,确保您的终端符合当前策略

本文档是分步指南,可指导您了解如何选择加入新功能并在终端上启用此功能。此外,还提供《全 <u>轨</u>道用户指南》。面向终端的AMP客户可以在终端已安装连接器(7.1.5或更高版本)的情况下轻松 启用Orbital Advanced Search。 有关最新连接器版本和其<u>他信息,请参</u>阅Orbital上面向终端的 AMP控制台帮助主题。运行版本1703(创建者更新)或更高版本的64位Windows 10主机当前支持 Orbital Advanced Search。

完成这些步骤后,请参阅快速入门指南,了解如何开始使用轨道高级搜索的更详细说明。

### 步骤 1:选择进入轨道高级搜索

如果您之前未注册Orbital Advanced Search beta或明确选择加入,则可以从面向终端的AMP控制台的"许可证信息"页面执行此操作。要选择加入Orbital Advanced Search,请登录面向终端的AMP控制台并选择Accounts > License Information**的下拉菜单**。在此页上,您可以单**击Enroll in Orbital**以访问此功能。

All for Designers The Designers of Status and Inc. The Designers Status (Lange - No. Status (Lange - No.	a salina ana A las sana Quas Alar Salinaka y	-		
		2		
to begins				
t ta Dagana Archego by		-		
etra de la composita de la comp	the side			
take behavior the		-		
of the local division of the local divisiono	-			
	-			
the party lands into		-		
and the Dans P	frang lines	-		
		-		
_				
	an per lan an and the Dans P		an par hann man and agree to be and the Chern Weinig Statements State (Street Statements	er pår hann mer att agen to for och för Orien Pfrang Kannann. Enterförstander

NOTE:您必须是特权(管理员)用户才能选择进入Orbital Advanced Search。

## 步骤 2: 在现有策略中启用轨道高级搜索

如果您的终端已安装连接器(版本7.1.5或更高版本),则只需在现有策略中为终端启用Orbital Advanced Search。

转至面向终端的AMP控制台。在管理>策略中,选择要在中启用轨道高级搜索的策略,然后单击编辑按钮以打开在高级设置下编辑策略,选择Orbital,并验证是否启用轨道高级搜索。应选中启用轨道高级搜索框。否则,选中复选框以启用它。

	And house - Mangalant - Antonia -	
dit Policy		
Tarte .	and here	
Description (	Institution with the Solar Solar Adap	
Note an Experi	Orbital Advanced Search	
Contention and	R cate the description (	
*140		
Indexed Sector		
Product Sprinker		

此时,使用此策略安装的任何连接器将自动在该终端上启用Orbital Advanced Search。

### 步骤 3: 在新策略和计算机组中启用轨道高级搜索(可选)

如上所述,在现有策略中启用Orbital Advanced Search后,使用该策略的所有连接器将启用Orbital Advanced Search,而您安装的任何新连接器也将启用Orbital Advanced Search。例如,如果您的 "保护"组中有1000台计算机,只要在该策略中启用轨道高级搜索,只要部署连接器版本7.1.5或更高版本,就会自动在这些终端上启用轨道高级搜索。

创建新策略和组是可选的。但是,如果您希望使用新策略和组对特定终端组使用轨道高级搜索,则 只需按照产品文档<u>创建</u>新策略和/或组,并确保在如上所述的策略中启用轨道高级搜索。

### 步骤 4: 探索Orbital控制台

一旦在至少一个终端上安装了连接器版本高于7.1.5的策略中启用了Orbital Advanced Search,您现 在就可以在终端上执行查询,以便从终端收集信息。

- •转到"管理">"计算机",找到具有"轨道高级搜索"的计算机展开窗格,然后单击"轨道查询"。(您也可以通过转到Analysis > Orbital Advanced Search (分析>轨道高级搜索)访问Orbital控制台。
  )
- Orbital控制台加载到新的浏览器选项卡中。如果需要,请点**击Log in with Cisco Security(使用 思**科安全登录)以使用现有AMP控制台凭证进行身份验证。

NOTE:您也可以直接访问Orbital Advanced Search(轨道高级搜索),网址为 https://orbital.amp.cisco.com

- 终端字段显示要查询的计算机。您可以输入特定GUID或在此字段中输入全部,以查询贵组织中 启用了轨道高级搜索的每个终端。如果要随机采样端点,请点击省略号(...)以打开"添加随机端 点"(Add Random Endpoints)对话框。
- •可以在SQL字段中输入自定义SELECT语句,或单击浏览查询目录以打开查询目录,该目录包 含可添加到查询的几十个查询。您不需要知道如何编写SQL SELECT语句来使用Orbital。



- 单击Query。查询针对指定的终端运行,结果显示在右窗格中。您可以编辑查询并重新运行。 您可以下载结果。您可以将查询另存为作业,以便按可配置的计划运行。
- 有关Orbital Advanced Search入门的详细信息,请浏览"快速入门"