Uninstall Orbital from Secure Endpoint

Contents

Introduction
Prerequisites
Requirements
Components Used
Problem
Solution
Uninstall via Control Panel
Uninstall via CMD
Uninstall via PowerShell
<u>Verify</u>

Introduction

This document describes how to effectively remove the Orbital completely from your endpoint running Cisco Secure Endpoint.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Windows Operating System
- Windows PowerShell
- Cisco Secure Endpoint
- Cisco Secure Endpoint Console

Components Used

The information in this document is based on these software verisons:

- Cisco Secure Endpoint 8.4.0.30201
- Windows Server 2019
- Windows PowerShell 5.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

Disabling Orbital for a policy halts and disables the service, yet it remains installed on endpoints. Reenabling the policy restarts the service and enables updates, but manual uninstallation of Orbital is also feasible when needed.

Solution

Disable the Orbital feature from the policy of those specific endpoints where you no longer want Orbital.

1. In the Secure Endpoint Console, navigate to the **Policies** page by selecting **Management > Policies**.

\equiv		Po	licies	() View	w All Changes +	- New Policy ~
55	Dashboard	Sea	ch by policy name, description, or GUID			
ı¦il Ø	Inbox	All	🛋 Windows 📽 Mac Å Linux 🗢 Android 🔲 IOS 🐨 Network		Show Descrip	rtions 😑 🕀
Ħ	Overview		Name	Modified	Groups	Computers
٢	Events		No description	2024-06-26 16:58:03 UTC		
ad	Analysis		No description	2024-06-26 16:53:24 UTC		
ж	Outbreak Control			2024-05-17 23:09:46 UTC		
-	Management			2024-06-26 17:08:37 UTC	1	
			No description			
30	Administration		e No description	2021-03-04 09:03:50 UTC		

2. Locate and select the policy that is applied to the endpoint(s). Click Edit.

Vo description		2024-07-18 10	0:52:55 UTC 1 1
Detection and Response	Exclusion Sets	Custom Detections	Groups 🖵
Files Quarantine Network Block Malicious Activity Protecti Quarantine System Process Protection Protect Script Protection Audit Exploit Prevention Audit Exploit Prevention Script Audit Behavioral Protection Protect TETRA Offline File Scanni Protect Orbital Enabled	Cisco-Maintained Microsoft Windows Default	Simple Not configured Advanced Not configured Application Control Allow Allow Not configured Block Telegram Network Control Network Control	
Device Control		Not configured	Provy
USB Mass Storage Not configured Windows Portable Not configured			proxy-wsa.esl.cisco.com:80
View Changes Serial Number 1499			d XML Edit Duplicate

3. Navigate to Advanced Settings > Orbital, Uncheck Enable Orbital. Save the changes.

_			Windows	
			Name	
55	Dashboard		Description	
.14	labov			
νø.	mbox			
#	Overview		Modes and Engines	Orbital
			Exclusions	Enable Orbital 🚯
÷	Events		1 exclusion set	Update Schedule Automatic With Connector
.14	Analysis	\$	Proxy	Orbital will update automatically when a new version is available.
	rinaryono			You must select a valid date range in Product Updates to set Orbital to undate with the connector. You can proceed with
*	Outbreak Control		Outbreak Control	your Orbital configuration after you select a valid date range.
	Management		Device Control	
	management		Product Updates	
•.	Administration		Advanced Settings	
-0	Administration	<i>´</i>	Administrative Features	
			Client User Interface	
			File and Process Scan	
			Cache	
			Endpoint Isolation	
			Orbital	
			Engines	
			TETRA	
			Network	
			Scheduled Scans	

Once the Orbital feature is disabled from the Secure Endpoint Console, you can choose any of the listed methods to uninstall Orbital completely.

Uninstall via Control Panel

Open **Control Panel**, navigate to **Programs and Features**, locate **Cisco AMP Orbital** in the list, rightclick, select **Uninstall**, proceed through the prompts in the uninstallation wizard, and restart if required.

Programs and Features						-	. 🗆	×
← → × ↑ 🖬 > Control P	anel > Programs > Programs and Features				> Ö Search	Programs a	and Features	P
Control Panel Home View installed updates 👽 Turn Windows features on or	Uninstall or change a program To uninstall a program, select it from the list and then	click Uninstall, Change, or Repair.						
off	Organize 👻 Uninstall Repair						800 -	?
	Name	Publisher	Installed On	Size	Version			
	🗟 Cisco AMP Orbital	Cisco Systems, Inc.	7/18/2024	86.1 MB	1.31.4	- Unir	nstall	
	Cisco Secure Endpoint Event Log Explorer 5.3	Cisco Systems, Inc. FSPro Labs	7/18/2024 1/20/2023	18.1 MB	8.4.0.30201 5.3	Repa	air	

Uninstall via CMD

- Open Command Prompt (CMD) with administrative privileges.
- Enter the command to uninstall Cisco AMP Orbital.

```
wmic product where "description='Cisco AMP orbital'" uninstall
```

Snippet of the Output:



Uninstall via PowerShell

- Open PowerShell with administrative privileges.
- Enter the command to uninstall Cisco AMP Orbital.

```
Uninstall-Package -Name "Cisco AMP Orbital"
```

Snippet of the Output:

Administrator: Windows PowerShell					
Windows PowerShell Copyright (C) Microsoft Co	rporation. All rig	nts reserved.			
PS C:\Users\Administrator>	Uninstall-Package	-Name "Cisco AMP	Orbital"		
Name	Version	Source	Summary		
Cisco AMP Orbital	1.31.4				

Verify

- Open services.msc from the Start menu or Run dialog.
- Search for any service related to Cisco AMP Orbital and ensure none exist in the list.



Note: These methods can also be used to automate the uninstallation of Orbital from multiple endpoints. However, re-enabling the Orbital feature via Secure Endpoint Console policy reinstalls the service on the endpoint.