

# 使用面向终端的AMP或FireAMP执行终端IOC扫描

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[IOC签名文件](#)

[在IOC签名文件上运行扫描](#)

[创建IOC签名文件](#)

[上传IOC签名文件](#)

[启动扫描](#)

## 简介

本文档介绍如何通过Mandiant IOC编辑器创建危害表现(IOC)签名文件，如何将其上传到Cisco FireAMP控制面板，以及如何启动终端IOC扫描。

## 先决条件

### 要求

思科建议您在尝试运行终端IOC扫描之前至少拥有1GB的可用驱动器空间。

### 使用的组件

本文档中的信息基于终端IOC扫描程序，Cisco FireAMP Windows连接器版本4.0.2及更高版本中提供了该扫描程序。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 背景信息

终端IOC扫描程序功能是一个功能强大的事件响应工具，用于扫描多台计算机上的危害后指示器。

**注意：**尽管FireAMP支持Mandiant语言的IOC，但Mandiant IOC编辑器软件本身并不由思科开发或支持。思科支持不排除用户创建或第三方IOC故障。

## IOC签名文件

IOC签名文件是可扩展的XML架构，用于描述识别已知威胁、攻击者方法或其他危害证据的技术特征。

您可以通过控制台从基于OpenIOC的文件导入终端IOC，这些文件是为了在文件属性（如名称、大小和哈希）以及其他属性和系统属性（如进程信息、运行服务和Microsoft Windows注册表项）上触发而编写的。事件响应者可以使用IOC语法来查找特定的对象，或者使用逻辑来为恶意软件系列创建复杂的关联检测。

## 在IOC签名文件上运行扫描

要在IOC签名文件上运行扫描，必须完成三个步骤：

1. 创建IOC签名文件。
2. 上传IOC签名文件。
3. 启动扫描。

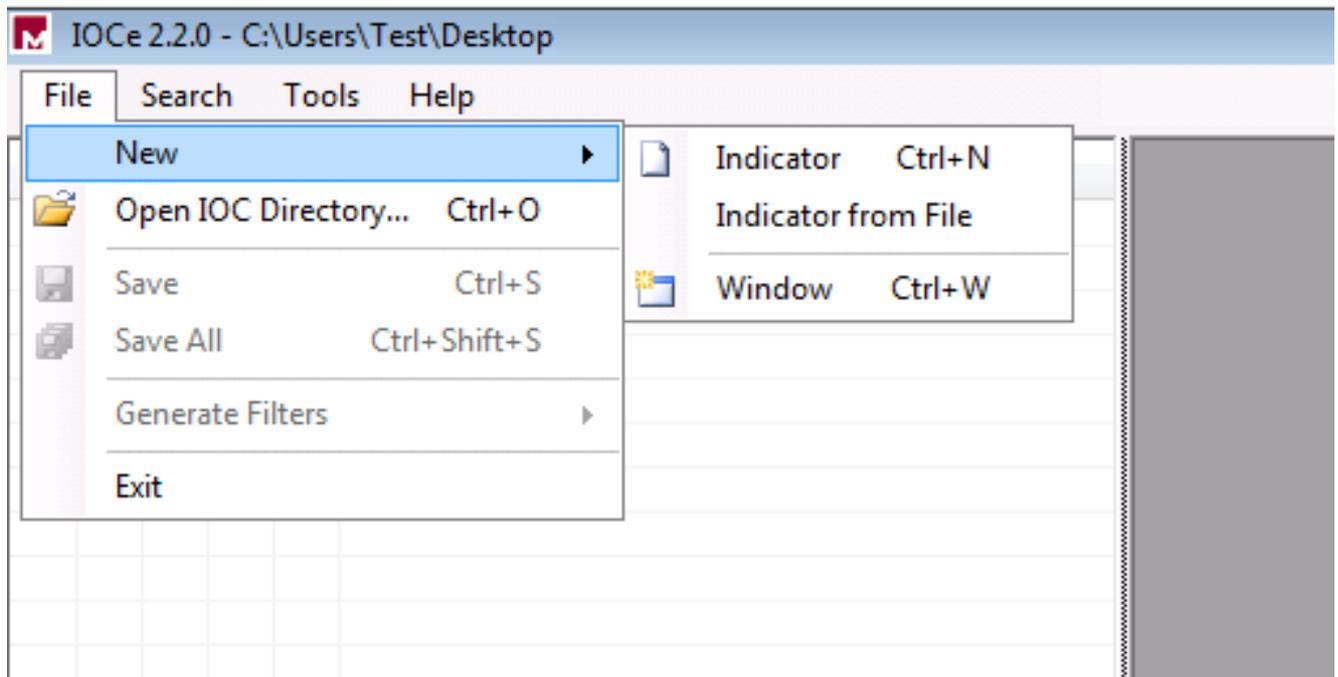
以下各节将对这些步骤进行扩展。

### 创建IOC签名文件

**注意：**在本例中，使用Mandiant IOC编辑器为名为test.txt的文本文件构建IOC签名文件。

要创建IOC签名文件，请完成以下步骤：

1. 打开IOCe，然后导航到**File > New > Indicator**。这将提供一个空白工作区，以便您开始构建IOC。



**注意：**要为特定内容创建IOC，请将二进制逻辑与属性一起使用。初始运算符是OR，它是最简单的基。这样，IOC的初始功能就可以工作，因此您无需更改它。IOC签名文件必须至少具有两个属性或条件才能在扫描中成功使用。

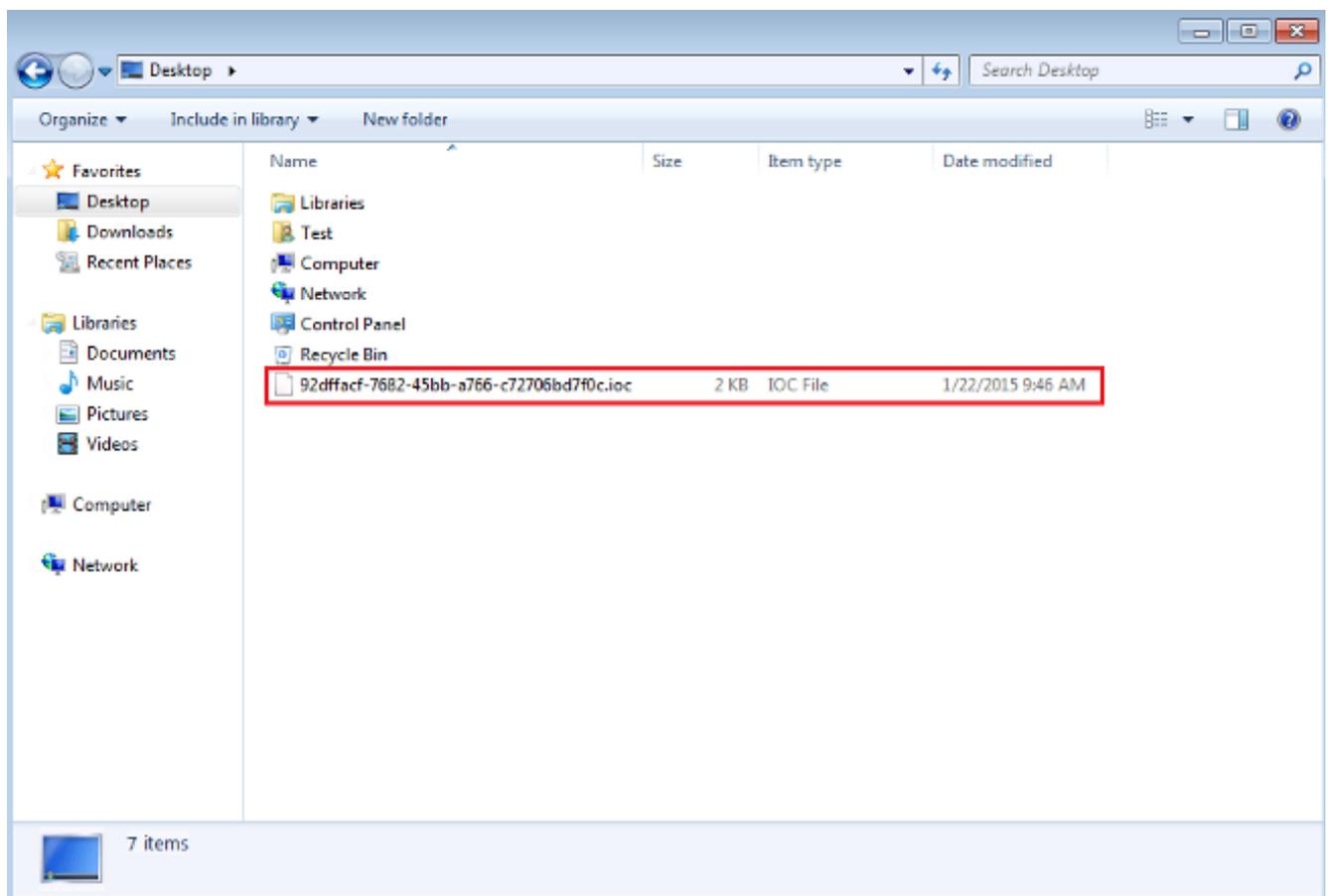
2. 单击**项目**下拉菜单以添加运算符。您应添加的第一个属性是“**文件扩展名包含**”。在“项目”树菜单中找到该属性，然后单击它。
3. 添加属性后，单击屏幕最右侧的小图标以打开“配置”窗格。在此窗格中，使用**Content**字段以匹配文件扩展名。例如，添加**txt**以匹配test.txt文件：



4. 现在必须添加逻辑运算符。在本例中，您将匹配**测试**文本文件。要匹配此项，请使用**AND**运算符并添加下一个属性。找到文件名，然后从“项目”树菜单中选择它。在“属性”窗格中，添加要查找的文件的名称。例如，在“内容”(Content)字段中添加“**测试**”(test):



5. 由于此简单IOC不需要其他属性，因此现在可以保存文件。单击File > Save，系统上将保存扩展名为.ioc的签名文件：



## 上传IOC签名文件

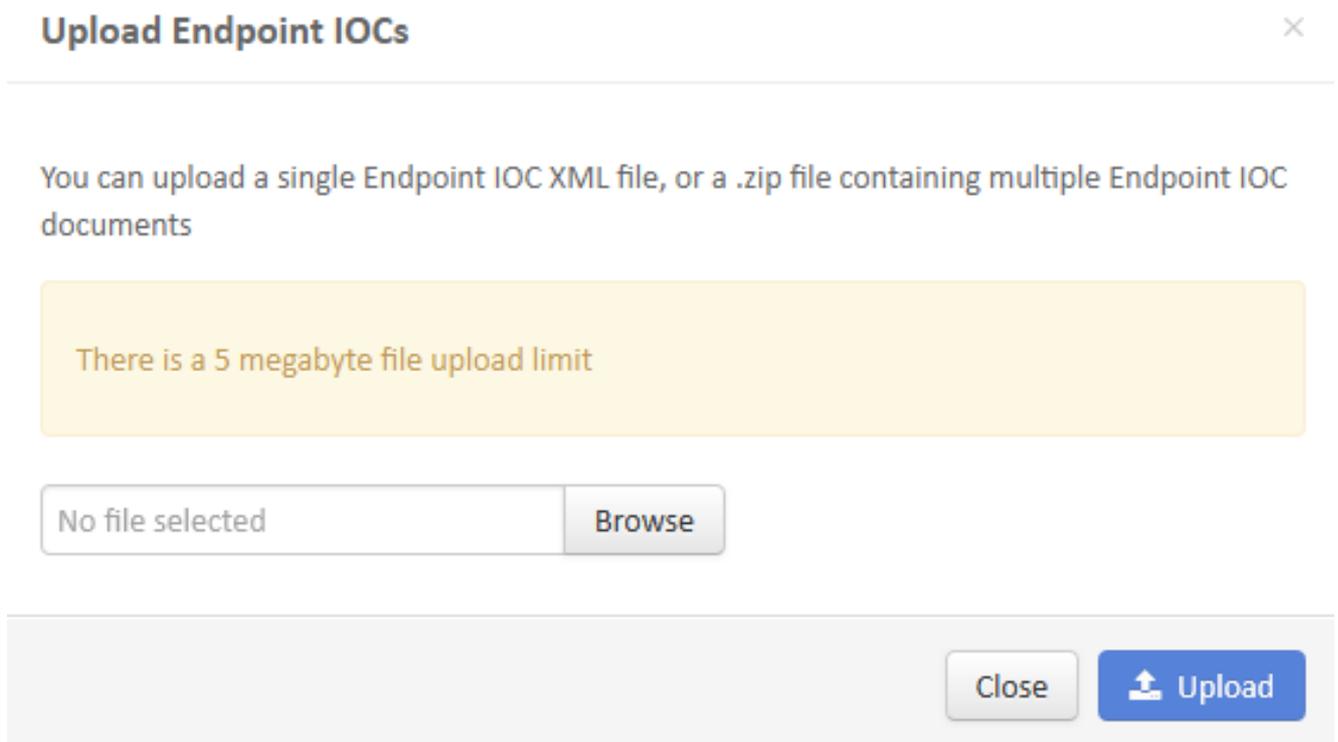
要执行扫描，必须将IOC文件上传到FireAMP控制面板。您可以使用IOC签名文件、XML文件或包含多个IOC文件的压缩存档。控制面板使用IOC签名解压缩并解析文件。如果语法不正确或使用了不受支持的属性，系统会通知您。

**提示：**您可以上传大小最大为5 MB的文件。

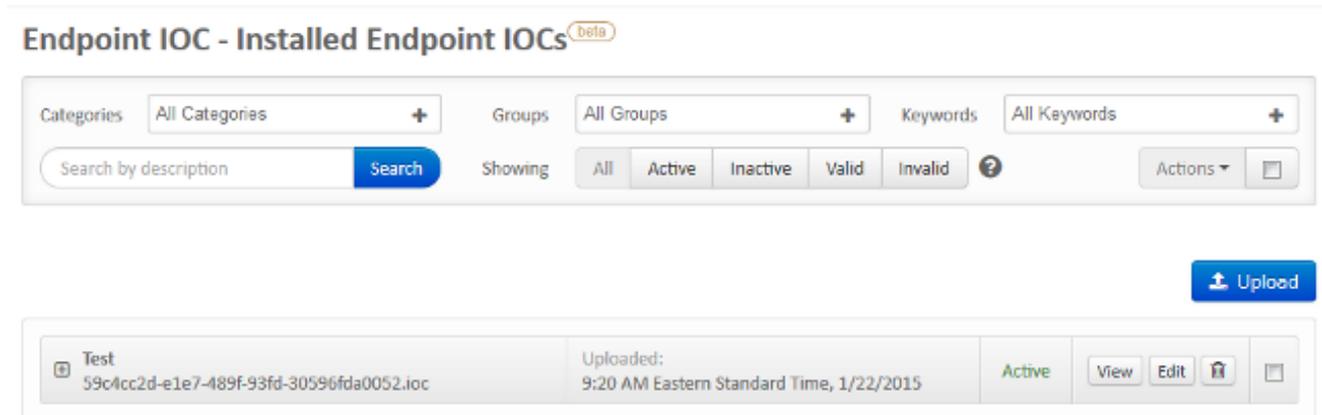
要将IOC签名文件上传到FireAMP控制面板，请完成以下步骤：

1. 登录FireAMP云控制台并导航至Outbreak Control > **Installed Endpoint IOC**。

2. 单击**Upload**，并出现Upload Endpoint IOCs窗口：



成功上传IOC签名文件后，该签名将显示在列表中：



3. 单击**View**以查看签名的实际XML数据：

## Endpoint IOC beta

File name: 59c4cc2d-e1e7-489f-93fd-30596fda0052.ioc

View All

View

Edit

Active

### Short Description:

Test

### Description

No description given

### Categories

No Categories to display

### IOC Groups

No IOC Groups to display

### Keywords

No Keywords to display

### Source [Download]

```
1 <?xml version="1.0" encoding="us-ascii"?>
2 <ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
3 id="59c4cc2d-e1e7-489f-93fd-30596fda0052" last-modified="2015-01-22T14:16:48" xmlns="http://schemas.mandiant.co
4 /2010/ioc">
5   <short_description>Test</short_description>
6   <authored_by>Test Author</authored_by>
7   <authored_date>2015-01-22T14:16:35</authored_date>
8   <links />
9   <definition>
10    <Indicator operator="OR" id="325adeacd-d75e-4fae-9cf4-cf8dcae84a36">
11      <IndicatorItem id="5311e18c-0e6a-4491-bb1a-a63331a463a2" condition="contains">
12        <Context document="FileItem" search="FileItem/FileExtension" type="mir" />
13        <Content type="string">txt</Content>
14      </IndicatorItem>
15      <IndicatorItem id="6ac73c61-9e9f-43da-9317-38d09990c337" condition="contains">
16        <Context document="FileItem" search="FileItem/FileName" type="mir" />
17        <Content type="string">test</Content>
18      </IndicatorItem>
19    </Indicator>
20  </definition>
21 </ioc>
```

## 启动扫描

上传签名文件后，执行完整扫描。第一次扫描必须是完全扫描，因为它必须为整个计算机构建元数据目录，这可能需要1-2个小时。通过完全扫描对系统进行编目后，可以执行闪存扫描。

**注意：**完全扫描占用的CPU非常多。思科建议在PC使用时不要运行完全扫描。如果您计划定期使用该功能，则可以每月执行一次完全扫描以重建目录。

有两种不同的方法可用于运行IOC扫描。第一种方法是从事件或控制面板执行即时扫描。下次PC向云发送心跳时会触发此信号。

**注意：**如果这是您第一次运行完全扫描，则无需检查扫描前**重新编录**选项。

## Run Scan on win7



Windows 7, SP 1.0 Device in  
IOC Test using IOC Test

1 Endpoint IOC active.

Scan Engine:

File

Endpoint IOC

Scan Depth:

Flash

Full

Re-catalog before scan

Running a full scan is **time consuming and resource intensive**. On endpoints with a large number of files a full scan can take multiple days to run. You should only run a full scan during non-business hours otherwise consider running a flash scan.

Close

Start Scan

第二种方法是从控制面板的爆发控制菜单创建计划的终端IOC扫描。当您希望在非高峰时段执行扫描时，此选项可能是理想之选。您必须提供对给定计算机具有权限的帐户的凭据，才能创建计划任务并允许以批处理组策略权限登录。

## Endpoint IOC - Initiate Scan <sup>beta</sup>

Policy:

IOC Test

Scheduled Scan User Name:

Test

Scheduled Scan Password:

••••••••

Run Scan On:

2015-01-22

09

:

30

Flash scan

Full scan

Re-catalog before scan

Schedule Scan

1 Active Endpoint IOC

1 group using IOC Test with 1 Endpoint IOC capable connector out of 1 total connector

- loc test with 1 Endpoint IOC capable connector out of 1 total connector

当您安排终端IOC扫描时，将显示以下警告消息：

## Warning



Running a full scan is **time consuming and resource intensive**. On endpoints with a large number of files a full scan can take multiple days to run. You should only run a full scan during non-business hours otherwise consider running a flash scan.

You have selected to re-catalog before a full scan, which can take longer to complete. You may not need to re-catalog if you recently ran a full scan with re-catalog.

Are you sure you want to schedule a full scan ?

Close

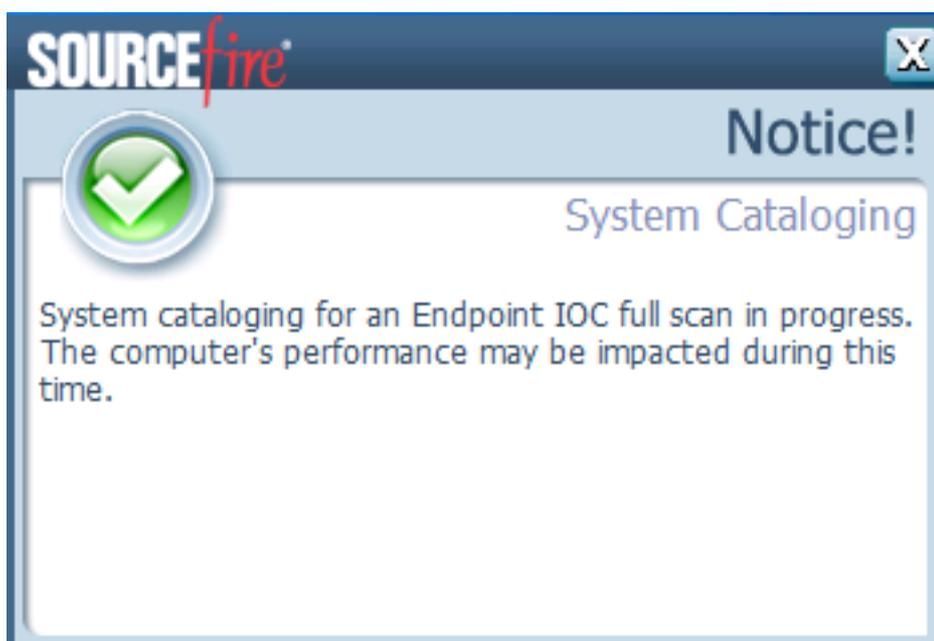
Schedule

下次PC发送心跳信号时，如果凭据有效，您应在Windows任务调度程序中看到类似于此的作业：

Name	Status	Triggers	Next Run Time
Immunet Scan 1421937278	Ready	At 9:40 AM on 1/22/2015	1/22/2015 9:40:00 AM

扫描开始时，显示以下消息：

**注意：**如果GUI配置为隐藏，则您看不到系统编录通知。



扫描完成后，您可以查看终端IOC扫描检测摘要。此示例显示test.txt IOC签名文件的匹配项：

<b>Connector Info</b>	Computer:	win7
Comments	Connector GUID:	s068bbab-af05-402e-a7c8-6bf0824a6638
	Current User:	
<a href="#">Run Scan</a>		<a href="#">Launch Device Trajectory</a>

<b>Endpoint IOC Summary</b>	Matching Endpoint IOCs:	Test (Filename: 5f04cc2d-e1a7-489f-93fd-305968da0052.ioc)
Connector Info	<a href="#">View All</a>	
Comments		