

# Выполните просмотры Индикации относительно компромисса (IOC) оконечной точки с AMP для оконечных точек или FireAMP

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Файлы цифровой подписи IOC](#)

[Выполните просмотр на Файле цифровой подписи IOC](#)

[Создайте Файл цифровой подписи IOC](#)

[Загрузите Файл цифровой подписи IOC](#)

[Иницилируйте просмотр](#)

## Введение

Этот документ описывает, как создать Файл цифровой подписи Индикации относительно компромисса (IOC) через редактора IOC Mandiant, как загрузить его к информационной панели Cisco FireAMP, и как инициировать просмотр IOC оконечной точки.

## Предварительные условия

### Требования

Cisco рекомендует иметь по крайней мере один гигабайт свободного дискового пространства, прежде чем вы попытаетесь выполнить просмотры IOC оконечной точки.

### Используемые компоненты

Сведения в этом документе основываются на сканере IOC оконечной точки, который доступен в Windows Connector Versions 4.0.2 Cisco FireAMP и позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Общие сведения

Функция сканера IOC оконечной точки является мощным программным средством реагирования на инциденты, которое используется для сканирования индикаторов посткомпромисса через несколько компьютеров.

**Примечание:** Несмотря на то, что FireAMP поддерживает IOCS с языком Mandiant, само программное обеспечение Mandiant IOC Editor не разрабатывается или поддерживается Cisco. Поддержка Cisco не устраняет неполадки созданный пользователями или сторонний IOCS.

## Файлы цифровой подписи IOC

Файл цифровой подписи IOC является расширяемой XML-схемой для описания технических характеристик, которые определяют известную угрозу, методологию атакующего или другое доказательство компромисса.

Можно импортировать IOCS оконечной точки через консоль от находящихся в OpenIOC файлов, которые записаны для включения свойств файла, таких как название, размер, и хэш, а также другие атрибуты и системные свойства, такие как информация о процессе, рабочие сервисы и Записи реестра Microsoft Windows. Синтаксис IOC может использоваться инцидентными респондентами для обнаружения определенных артефактов или для использования логики для создания сложных, коррелированных обнаружений для семейств вредоносного ПО.

## Выполните просмотр на Файле цифровой подписи IOC

Существует три шага, которые необходимо выполнить для выполнения просмотра на Файле цифровой подписи IOC:

1. Создайте Файл цифровой подписи IOC.
2. Загрузите Файл цифровой подписи IOC.
3. Иницилируйте просмотр.

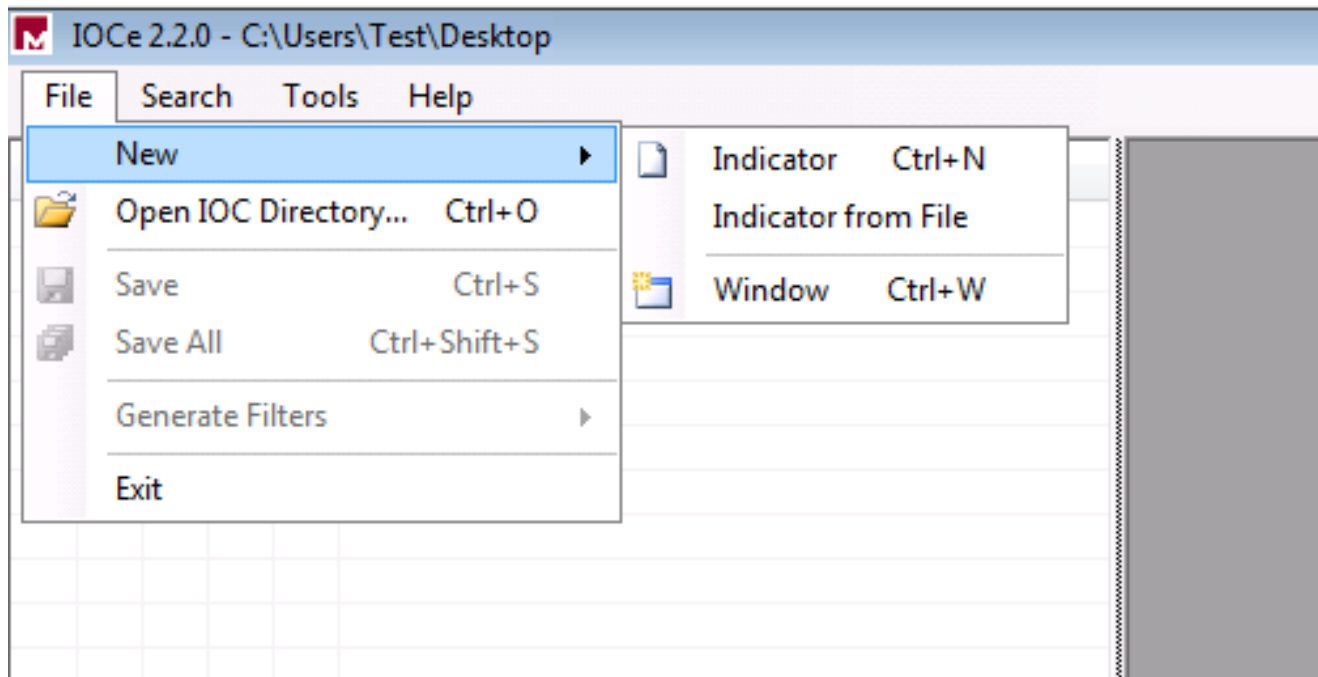
На этих шагах подробно останавливаются в разделах, которые придерживаются.

## Создайте Файл цифровой подписи IOC

**Примечание:** В данном примере редактор IOC Mandiant используется для построения Файла цифровой подписи IOC для текстового файла, названного **test.txt**.

Выполните эти шаги для создания Файла цифровой подписи IOC:

1. Откройте **IOCe** и перейдите к **Индикатору File> New>**. Это предоставляет пустую рабочую область так, чтобы можно было начать создавать IOC.



**Примечание:** Для создания IOC для чего-то определенного используйте бинарную логику со свойствами. Начальным оператором является OR, который является самым простым ядром для работы от. Это позволяет начальной функции IOC работать, таким образом, вы не обязаны изменять его. Требуется, что Файл цифровой подписи IOC имеет по крайней мере два свойства или условия для использования его успешно в просмотре.

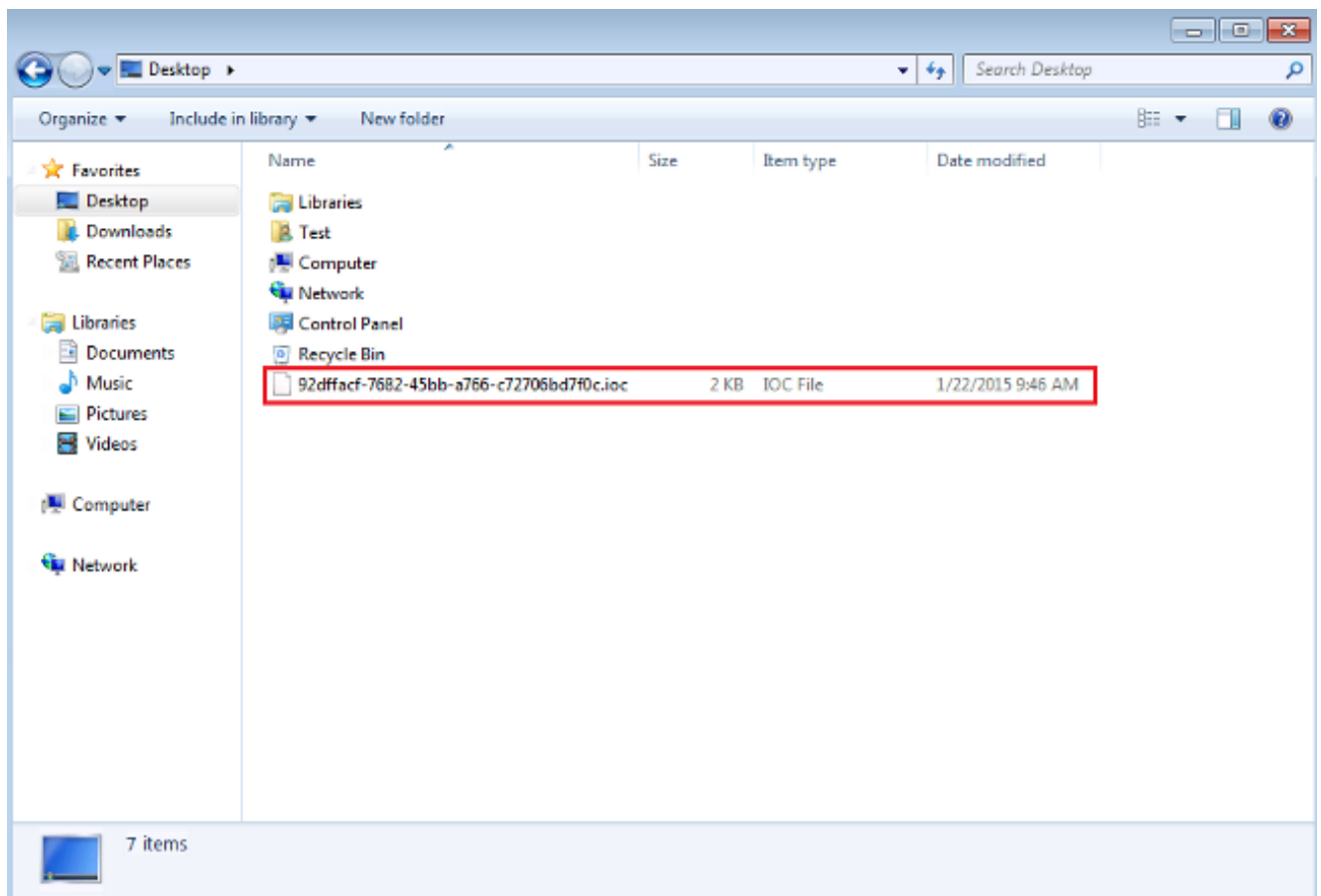
2. Нажмите раскрывающееся меню **Элементов** для добавления операторов. Первым свойством, которое необходимо добавить, является **Расширение файла, содержит**. Найдите свойство в меню дерева **Элементов** и нажмите его.
3. После добавления свойства нажмите маленький значок на дальней правой стороне экрана для открытия области Configuration. В этой области используйте поле **Content** для соответствия с расширением файла. Например, добавьте **текст** для соответствия с **test.txt** текстовым файлом:



4. Необходимо теперь добавить логический оператор. В данном примере вы будете совпадать с **тестовым** текстовым файлом. Для соответствия с этим используйте *операцию И* и добавьте следующее свойство. Найдите имя файла и выберите его из меню дерева **Элементов**. В Панели свойств добавьте название файла, который вы хотите найти. Например, добавьте **тест** в поле Content:



5. Так как никакие дополнительные свойства не необходимы для этого простого IOC, можно теперь сохранить файл. Нажмите **File> Save**, и Файл цифровой подписи с **.ioc** расширением сохранен в системе:



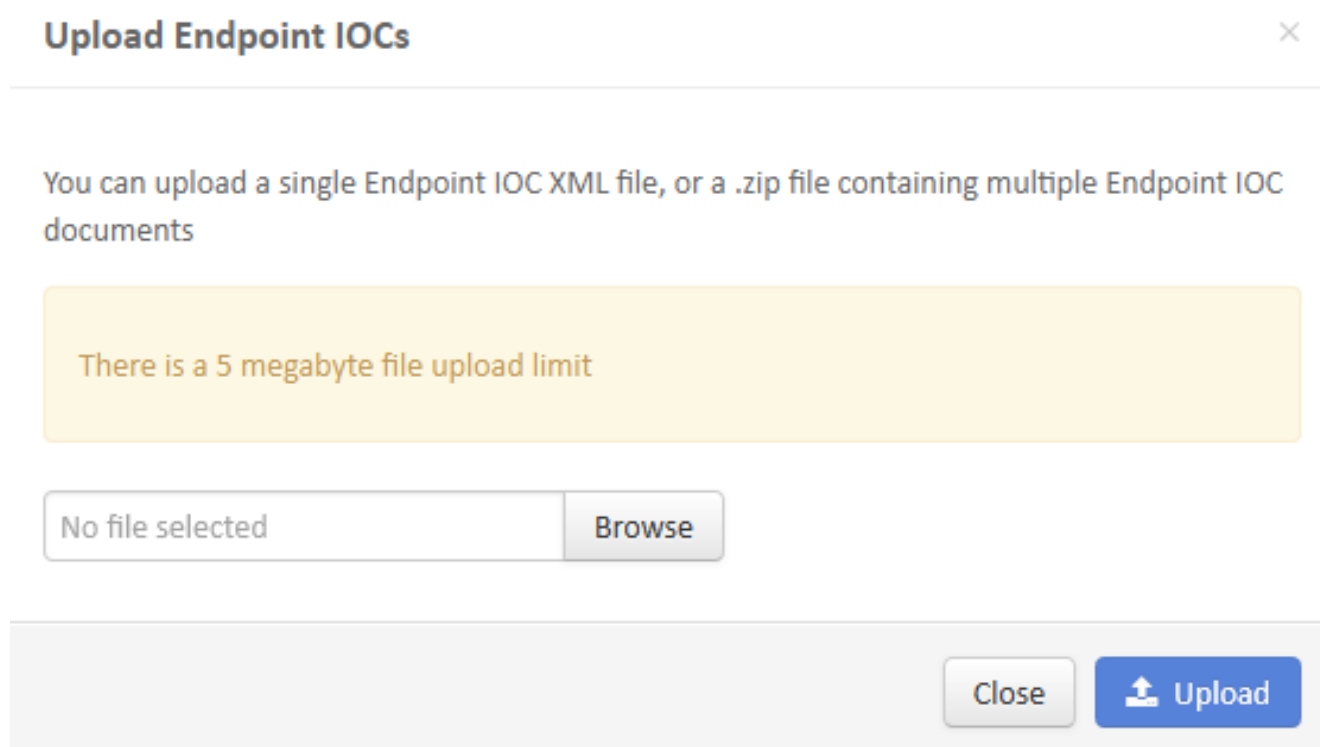
**Загрузите Файл цифровой подписи IOC**

Для выполнения просмотра необходимо загрузить файл IOC к информационной панели FireAMP. Можно использовать Файл цифровой подписи IOC, XML-файл или архив zip, который содержит множественные файлы IOC. Информационная панель распаковывает и анализирует файл с подписями IOC. Если неверный синтаксис или неподдерживаемое свойство используются, вы уведомлены.

**Совет:** Можно загрузить файлы, которые составляют до пяти мегабайтов в размере.

Выполните эти шаги для загрузки Файла цифровой подписи IOC к информационной панели FireAMP:

1. Войдите в Облачную Консоль FireAMP и перейдите к **Контролю за Вспышкой> Установленный IOC Оконечной точки**.
2. Нажмите **Upload**, и окно **Upload Endpoint IOCs** появляется:



После того, как Файл цифровой подписи IOC загружен успешно, подпись появляется в списке:

## Endpoint IOC - Installed Endpoint IOCs <sup>beta</sup>

Categories: All Categories + Groups: All Groups + Keywords: All Keywords +

Search by description Search Showing: All Active Inactive Valid Invalid ? Actions [ ]

Upload

Test 59c4cc2d-e1e7-489f-93fd-30596fda0052.ioc	Uploaded: 9:20 AM Eastern Standard Time, 1/22/2015	Active	View Edit [ ] [ ]
--	---	--------	-------------------

3. Нажмите **View** для просмотра фактических данных в XML подписи:

## Endpoint IOC <sup>beta</sup>

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="2015-01-22T14:18:48" xmlns="http://schemas.mandiant.co
4 /2010/ioc">
5   <short_description>Test</short_description>
6   <authoried_by>Test Author</authoried_by>
7   <authoried_date>2015-01-22T14:16:35</authoried_date>
8   <links />
9   <definition>
10     <Indicator operator="OR" id="325adecc-d75e-4fae-9cf4-cf8dcae84a36">
11       <IndicatorItem id="3311e18c-0e6a-4491-bba1-a63331a463a2" condition="contains">
12         <Context document="FileItem" search="FileItem/FileExtension" type="mix" />
13         <Content type="string">txt</Content>
14       </IndicatorItem>
15       <IndicatorItem id="017fc010-f0ea-4ede-b252-885bb85cfcf3">
16         <IndicatorItem id="6ac73c61-9e9f-43da-9317-38d09990c337" condition="contains">
17           <Context document="FileItem" search="FileItem/FileName" type="mix" />
18           <Content type="string">test</Content>
19         </IndicatorItem>
20       </IndicatorItem>
21     </Indicator>
22   </definition>
23 </ioc>
```

## Иницируйте просмотр

После того, как вы загружаете Файл цифровой подписи, выполняете *полный* просмотр. Первый просмотр должен быть полным просмотром, потому что он должен создать каталог метаданных для всего компьютера, который может занять 1–2 часа. Можно выполнить просмотр *флэш-памяти* после того, как система будет каталогизироваться посредством полного просмотра.



**Примечание:** Полный просмотр является очень сом интенсивной загрузкой ЦПУ. Cisco рекомендует не выполнять полный просмотр на ПК, в то время как она используется. Если вы планируете использовать функцию регулярно, можно выполнить полный

просмотр один раз в месяц для восстановления каталога.

Существует два других метода, которые можно использовать для выполнения просмотра IOC. Первый метод должен выполнить непосредственный просмотр от события или от информационной панели. Это инициировано в следующий раз, когда ПК передает биение к Облаку.

**Примечание:** Если это первоначально, что вы выполняете полный просмотр, вы не обязаны проверять **Перекаталог перед** опцией просмотра.

## 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

Второй метод должен создать запланированный просмотр IOC конечной точки от **Меню управления Вспышки** информационной панели. Когда вы желаете выполнить просмотры в течение непииковый часов, эта опция могла бы быть идеальной. Необходимо предоставить учетные данные учетной записи, которая имеет разрешения на данном компьютере, чтобы создать запланированные задачи и позволить **Вход в систему как Пакетные** разрешения групповой политики.

## Endpoint IOC - Initiate Scan beta

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

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

При планировании просмотра IOC конечной точки это предупреждающее сообщение появляется:

## 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

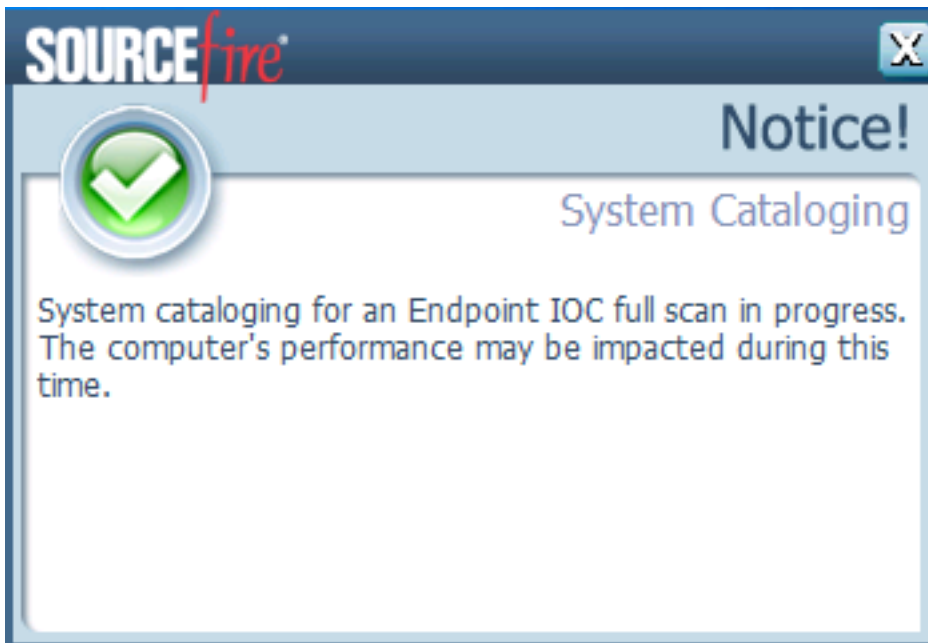
В следующий раз, когда ваш ПК передает биение, и если ваши учетные данные допустимы, необходимо видеть задание, подобное этому в Windows Task Scheduler:

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

Когда просмотр начинается, это сообщение появляется:

**Примечание:** Если GUI настроен, чтобы быть скрытым, то вы не видите, что Система Каталогизирует предупреждение.





Когда просмотр завершен, вы в состоянии просмотреть *Сводку Обнаружения Просмотра IOC Оконечной точки*. Данный пример показывает достойный **test.txt** Файла цифровой подписи IOC:

Win7 Scanned 16713078 objects. Found 655 matching objects and 0 malicious detections		Endpoint IOC Scan with Detections	11:55 AM Eastern Standard Time, 1/22/2015
Connector Info	Computer:	win7	
Comments	Connector GUID:	a088bbab-ef05-402c-e7c8-6bf0824e6638	
	Current User:		
	<a href="#">Run Scan</a>		<a href="#">Launch Device Trajectory</a>
Win7 Endpoint IOC Scan Detection Summary (matched 1 of 1 IOCs)		Endpoint IOC Scan Detection Summary	11:55 AM Eastern Standard Time, 1/22/2015
Endpoint IOC Summary	Matching Endpoint IOCs:	Test [Filename: 59c4cc26-e1a7-489f-93fd-3059685a0052.ioc]	
Connector Info	<a href="#">View All</a>		
Comments			