# Perform Endpoint Indication of Compromise (IOC) Scans with AMP for Endpoints or FireAMP

**Document ID: 118899**

Contributed by Nazmul Rajib and Alex Dipasquale, Cisco TAC
Engineers.

Apr 08, 2015

## Contents

## Introduction

This document describes how to create an Indication of Compromise (IOC) signature file via the Mandiant IOC editor, how to upload it to the Cisco FireAMP dashboard, and how to initiate an endpoint IOC scan.

## Prerequisites

### Requirements

Cisco recommends that you have at least one gigabyte of free drive space before you attempt to run the endpoint IOC scans.

### Components Used

The information in this document is based on the endpoint IOC scanner, which is available in the Cisco FireAMP Windows Connector Versions 4.0.2 and later.

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, make sure that you understand the potential impact of any command.

## Background Information

The endpoint IOC scanner feature is a powerful incident response tool that is used in order to scan post−compromise indicators across multiple computers.

***Note***: Although FireAMP supports IOCs with the Mandiant language, the Mandiant IOC Editor software itself is not developed or supported by Cisco. Cisco support does not troubleshoot user−created or third−party

IOCs.

### IOC Signature Files

The IOC signature file is an extensible XML schema for the description of technical characteristics that identify a known threat, an attacker methodology, or other evidence of compromise.

You can import endpoint IOCs through the console from OpenIOC−based files that are written in order to trigger on file properties such as name, size, and hash, as well as other attributes and system properties such as process information, running services, and Microsoft Windows Registry entries. The IOC syntax can be used by incident responders in order to find specific artifacts or in order to use logic to create sophisticated, correlated detections for families of malware.

## Run a Scan on an IOC Signature File

There are three steps that you must complete in order to run a scan on a IOC signature file:

1. Create an IOC signature file.
2. Upload the IOC signature file.
3. Initiate a scan.

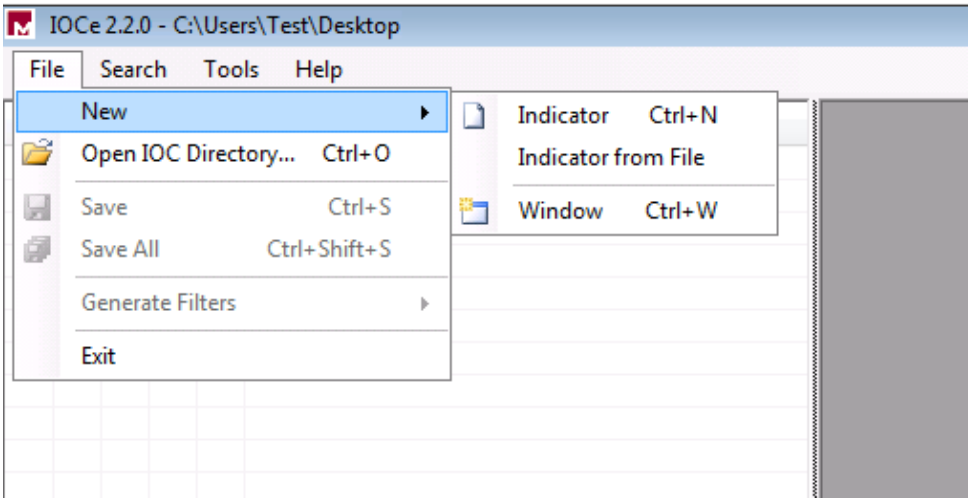
These steps are expanded upon in the sections that follow.

### Create an IOC Signature File

***Note***: In this example, the Mandiant IOC editor is used in order to build an IOC signature file for a text file named ***test.txt***.

Complete these steps in order to create an IOC signature file:

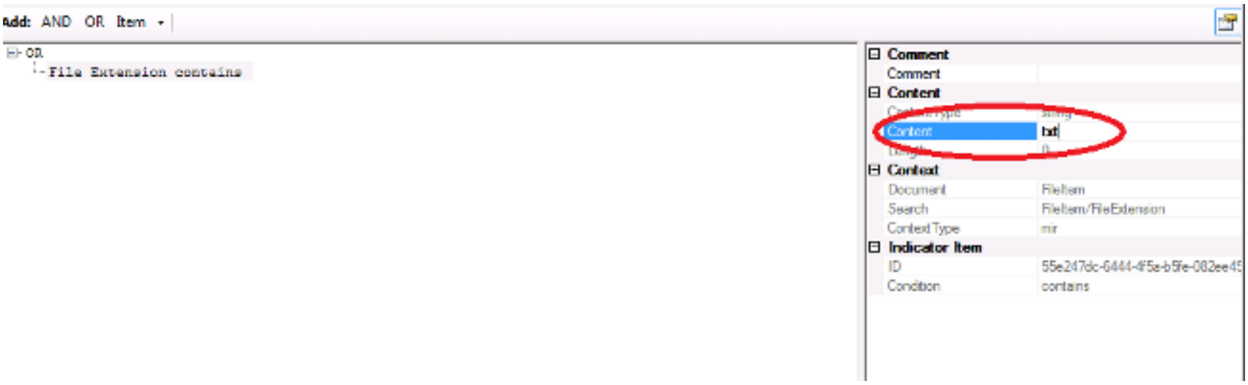
1. Open the ***IOCe*** and navigate to ***File*** > ***New*** > ***Indicator***. This provides a blank workspace so that you can begin to build an IOC.



***Note***: In order to create an IOC for something specific, use binary logic with the properties. The initial operator is an OR, which is the simplest base to work from. This allows the initial function of the IOC to work, so you are not required to change it. It is required that an IOC signature file has at least two properties or conditions in order to use it successfully in a scan.

2. Click the ***Items*** drop−down menu in order to add operators. The first property that you should add is ***File Extension contains***. Find the property in the ***Items*** tree menu and click it.

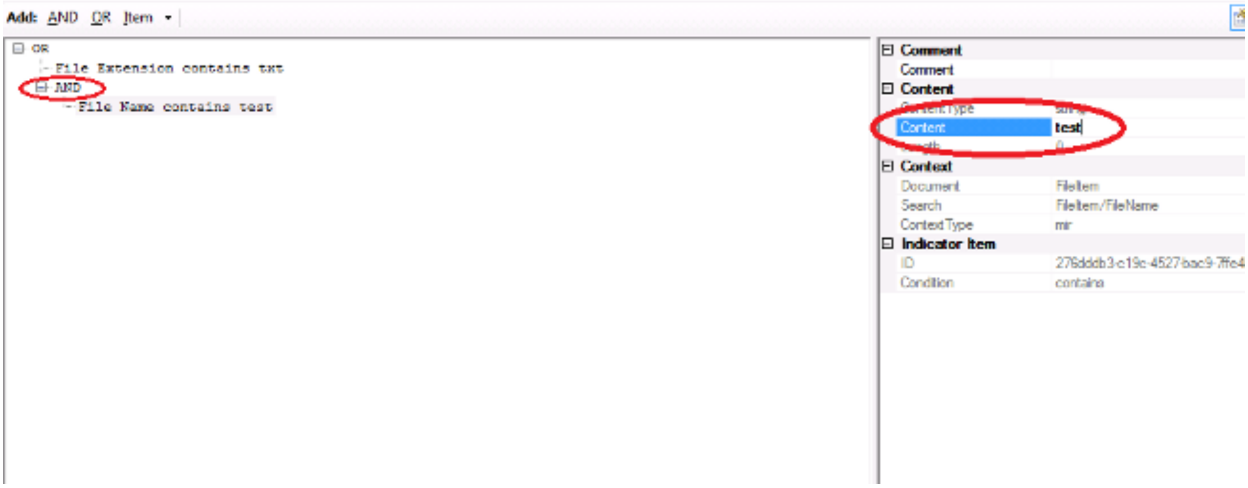
3. After you add a property, click the small icon on the far right side of the screen in order to open the Configuration pane. Within this pane, use the ***Content*** field in order to match a file extension. For example, add ***txt*** in order to match the ***test.txt*** text file:



```
⊟ OR
  └- File Extension contains
```

| | |
|---|---|
| ⊟ **Comment** | |
| Comment | |
| ⊟ **Content** | |
| Content Type | string |
| Content | txt |
| Length | 0 |
| ⊟ **Context** | |
| Document | FileItem |
| Search | FileItem/FileExtension |
| Context Type | mir |
| ⊟ **Indicator Item** | |
| ID | 55e247dc-6444-4f5e-b5fe-082ee45 |
| Condition | contains |

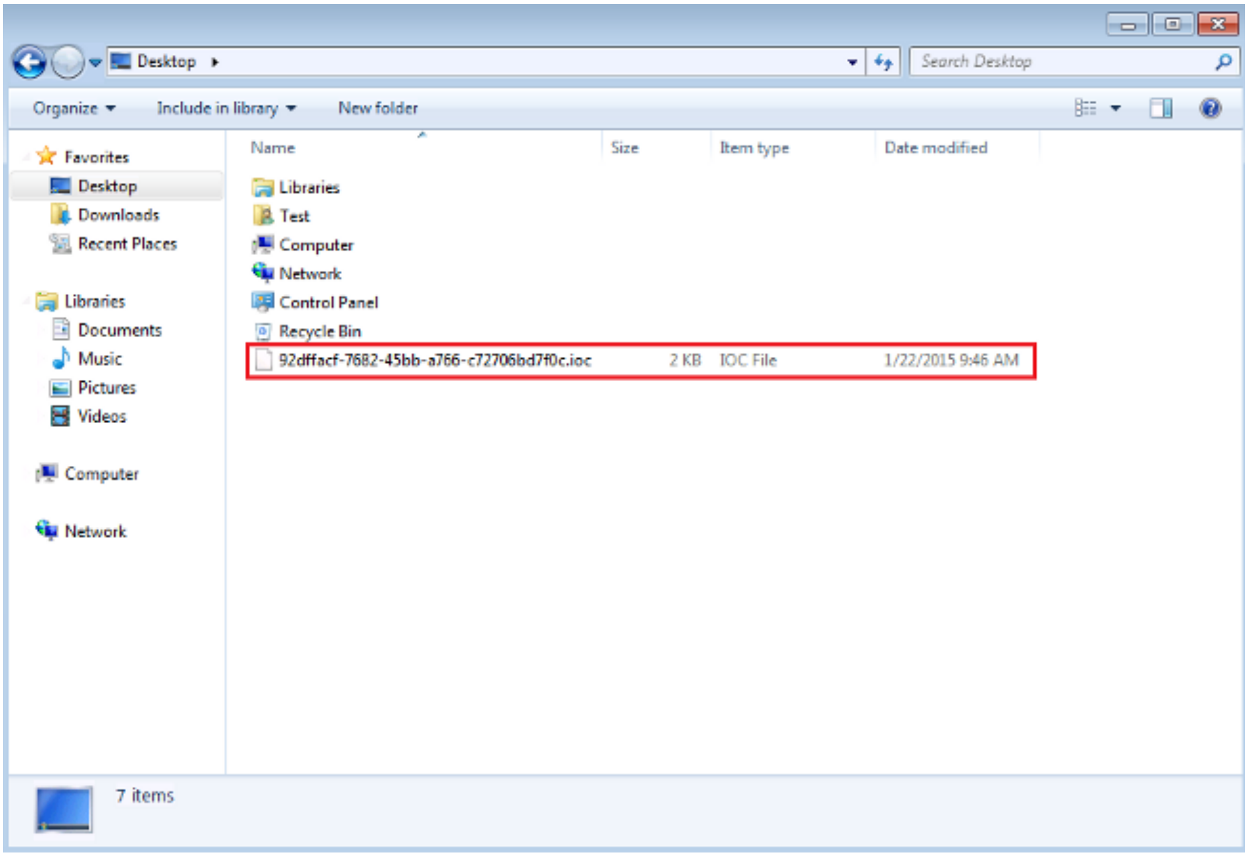
4. You must now add a logic operator. In this example, you will match the ***test*** text file. In order to match this, use an *AND* operator and add the next property. Locate the file name and select it from the ***Items*** tree menu. In the Properties pane, add the name of the file that you want to find. For example, add ***test*** in the Content field:



```
⊟ OR
  - File Extension contains txt
  ⊟ AND
    - File Name contains test
```

| | |
|---|---|
| ⊟ **Comment** | |
| Comment | |
| ⊟ **Content** | |
| Content Type | string |
| Content | test |
| Length | 0 |
| ⊟ **Context** | |
| Document | FileItem |
| Search | FileItem/FileName |
| Context Type | mir |
| ⊟ **Indicator Item** | |
| ID | 276dddb3-c19c-4527-bac9-7ffe4 |
| Condition | contains |

5. Since no additional properties are necessary for this simple IOC, you can now save the file. Click ***File > Save***, and a signature file with a ***.ioc*** extension is saved on the system:



| Name | Size | Item type | Date modified |
|---|---|---|---|
| Libraries | | | |
| Test | | | |
| Computer | | | |
| Network | | | |
| Control Panel | | | |
| Recycle Bin | | | |
| 92dffacf-7682-45bb-a766-c72706bd7f0c.ioc | 2 KB | IOC File | 1/22/2015 9:46 AM |

## Upload an IOC Signature File

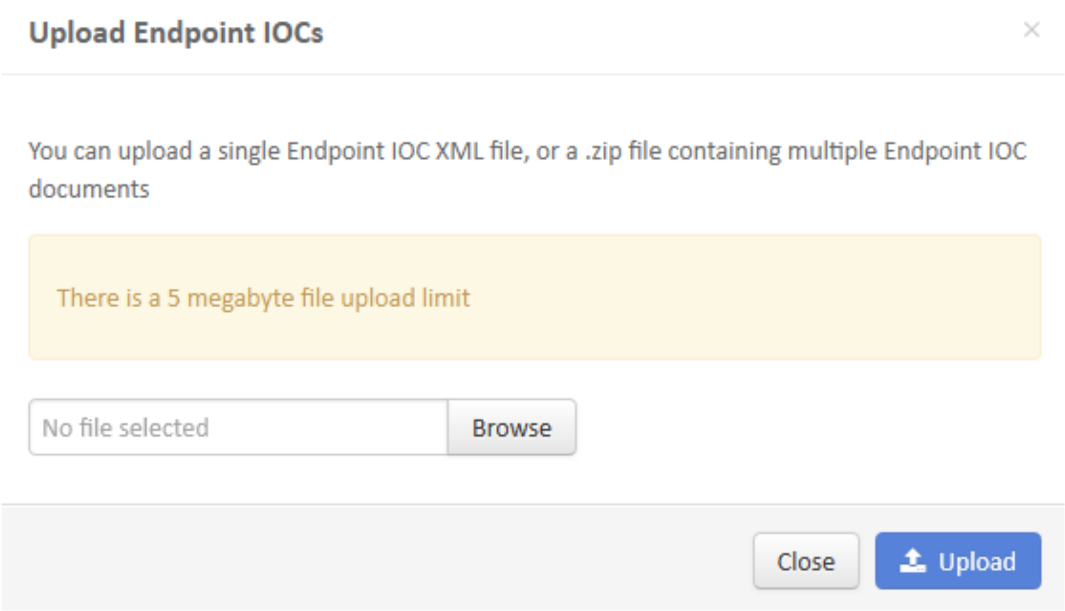
In order to perform a scan, you must upload an IOC file to the FireAMP dashboard. You can use an IOC signature file, an XML file, or a zip archive that contains multiple IOC files. The dashboard decompresses and parses the file with the IOC signatures. You are notified if an incorrect syntax or an unsupported property is used.

***Tip***: You can upload files that are up to five megabytes in size.

Complete these steps in order to upload the IOC signature file to the FireAMP dashboard:

1. Log into the FireAMP Cloud Console and navigate to ***Outbreak Control*** > ***Installed Endpoint IOC***.

2. Click ***Upload***, and the ***Upload Endpoint IOCs*** window appears:



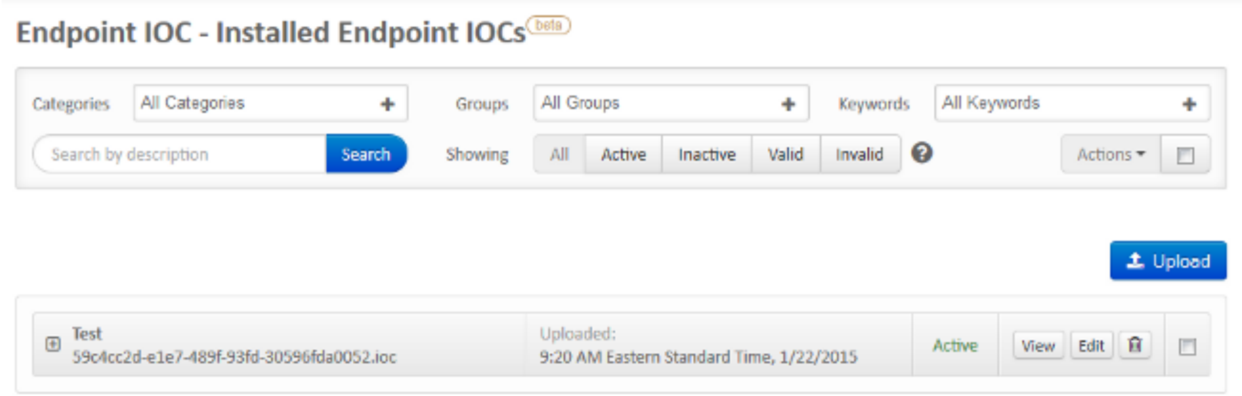
Upload Endpoint IOCs

You can upload a single Endpoint IOC XML file, or a .zip file containing multiple Endpoint IOC documents

There is a 5 megabyte file upload limit

No file selected

After an IOC signature file is uploaded successfully, the signature appears on the list:



Endpoint IOC - Installed Endpoint IOCs beta

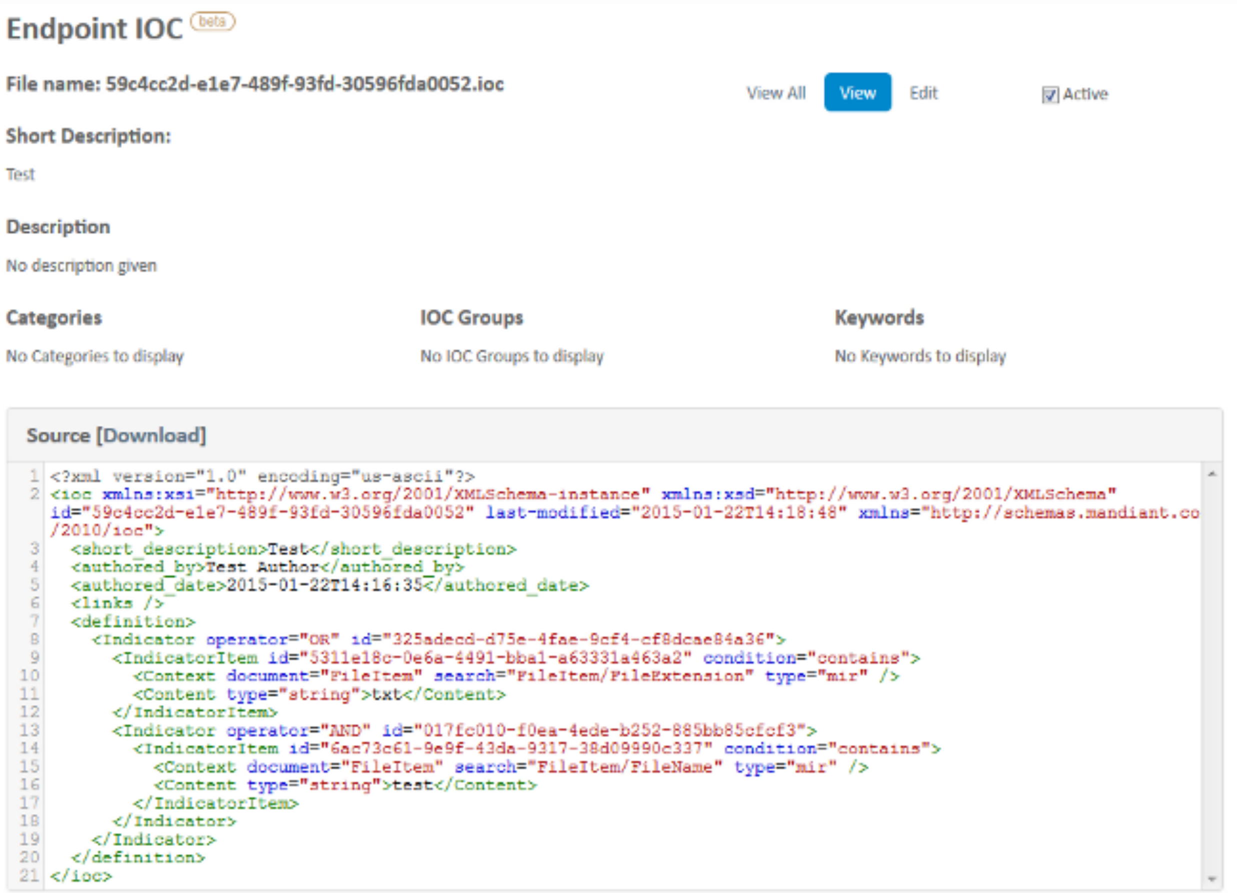
| Categories | All Categories | Groups | All Groups | Keywords | All Keywords |
|---|---|---|---|---|---|

Search by description

Showing: All | Active | Inactive | Valid | Invalid

| Test<br>59c4cc2d-e1e7-489f-93fd-30596fda0052.ioc | Uploaded:<br>9:20 AM Eastern Standard Time, 1/22/2015 | Active |
|---|---|---|

3. Click ***View*** in order to view the actual XML data of the signature:



Endpoint IOC

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

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]

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
id="59c4cc2d-e1e7-489f-93fd-30596fda0052" last-modified="2015-01-22T14:18:48" xmlns="http://schemas.mandiant.co
/2010/ioc">
  <short_description>Test</short_description>
  <authored_by>Test Author</authored_by>
  <authored_date>2015-01-22T14:16:35</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="325adecd-d75e-4fae-9cf4-cf8dcae84a36">
      <IndicatorItem id="5311e18c-0e6a-4491-bba1-a63331a463a2" condition="contains">
        <Context document="FileItem" search="FileItem/FileExtension" type="mir" />
        <Content type="string">txt</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="017fc010-f0ea-4ede-b252-885bb85cfcf3">
        <IndicatorItem id="6ac73c61-9e9f-43da-9317-38d09990c337" condition="contains">
          <Context document="FileItem" search="FileItem/FileName" type="mir" />
          <Content type="string">test</Content>
        </IndicatorItem>
      </Indicator>
    </Indicator>
  </definition>
</ioc>
```

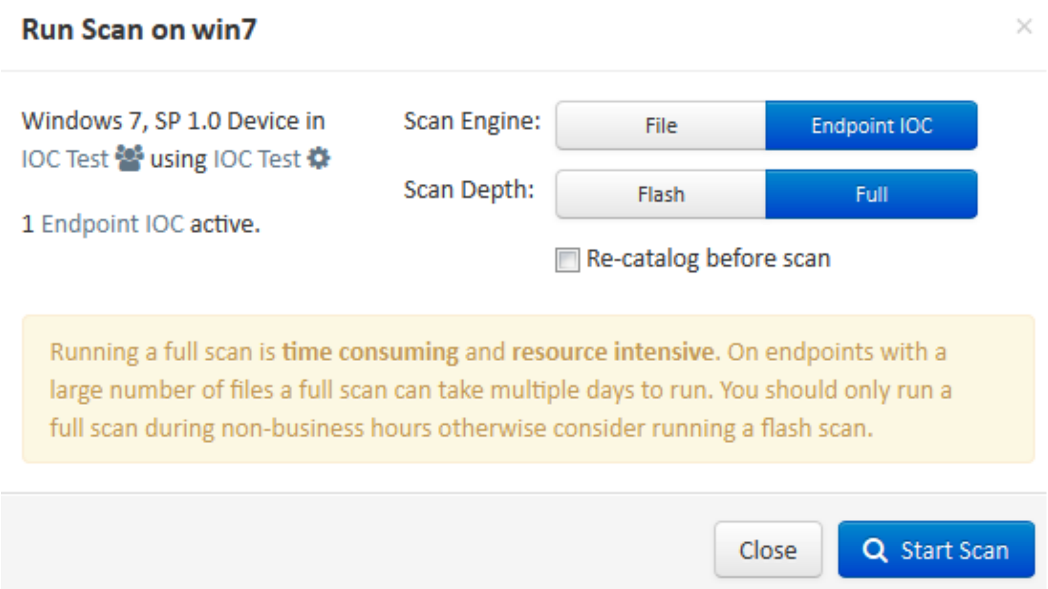
## Initiate a Scan

After you upload a signature file, perform a *full* scan. The first scan must be a full scan because it must build a catalog of metadata for the entire computer, which can take 12 hours. You can perform a *flash* scan after the system is cataloged through a full scan.

***Note***: The full scan is very CPU intensive. Cisco recommends that you do not run a full scan on a PC while it is in use. If you plan to use the feature regularly, you can perform a full scan once a month in order to rebuild the catalog.

There are two different methods that you can use in order to run an IOC scan. The first method is to perform an immediate scan from an event or from the dashboard. This is triggered the next time that a PC sends a heartbeat to the Cloud.

***Note***: If this is the first time that you run the full scan, you are not required to check the ***Re−catalog before scan*** option.



Run Scan on win7

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

1 Endpoint IOC active.

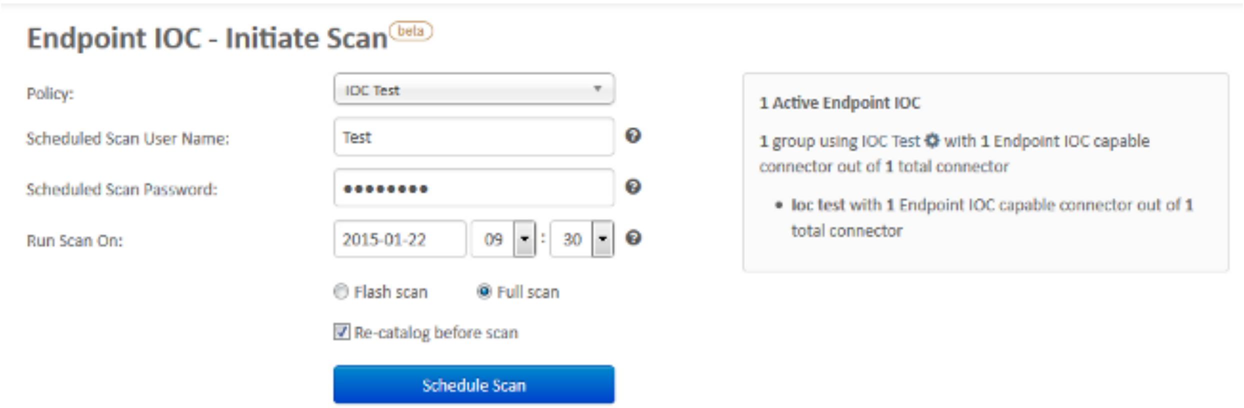
Scan Engine: File | **Endpoint IOC**

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.

The second method is to create a scheduled endpoint IOC scan from the ***Outbreak Control*** menu of the dashboard. This option might be ideal when you desire to perform scans during off−peak hours. You must provide the credentials of an account that has permission on the given computer in order to create scheduled tasks and allow the ***Log on as Batch*** group policy permission.



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

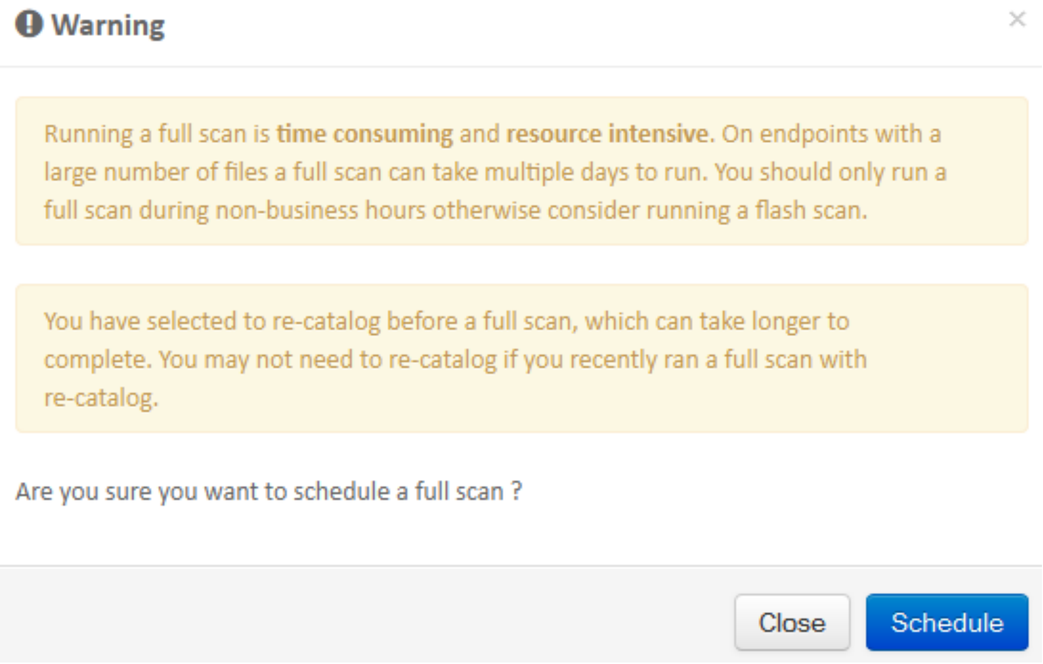
☑ Re-catalog before scan

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

When you schedule an endpoint IOC scan, this warning message appears:



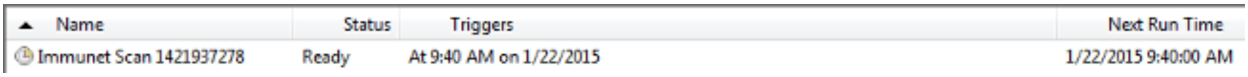
**Warning**

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 ?

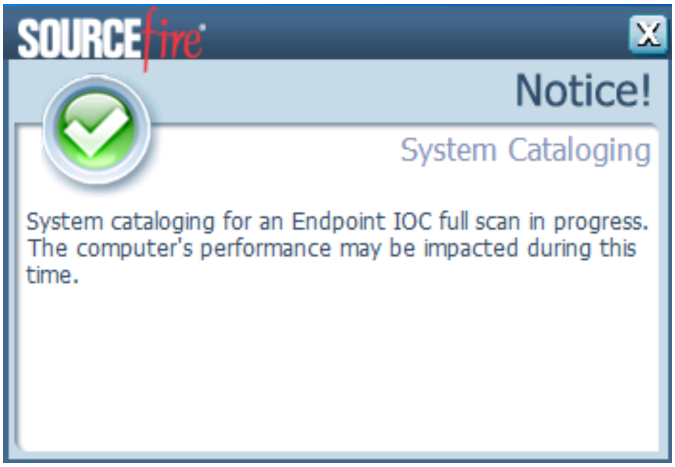
The next time that your PC sends a heartbeat, and if your credentials are valid, you should see a job similar to this in the Windows Task Scheduler:



| 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 |

When the scan begins, this message appears:

***Note***: If the GUI is configured to be hidden, then you do not see the ***System Cataloging*** notice.

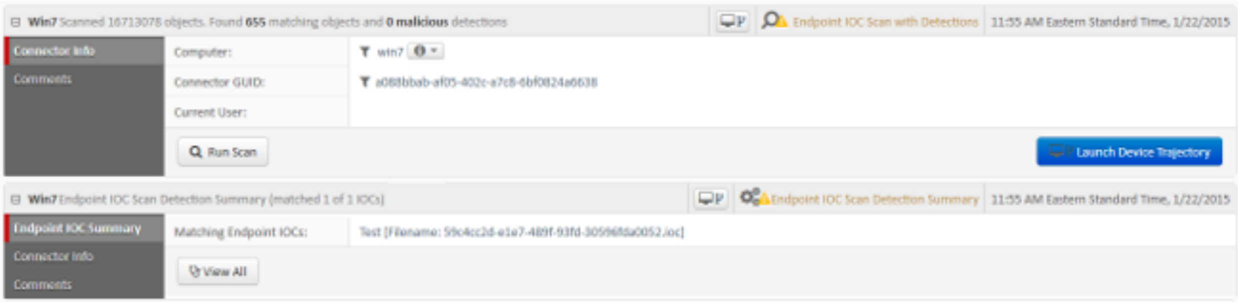


Notice!

System Cataloging

System cataloging for an Endpoint IOC full scan in progress. The computer's performance may be impacted during this time.

When the scan is complete, you are able to view the *Endpoint IOC Scan Detection Summary*. This example shows a match for the ***test.txt*** IOC signature file:



⊟ **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

Computer: win7

Connector GUID: a088bbab-af05-402c-a7c8-6bf0824a6638

Current User:

⊟ **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

Matching Endpoint IOCs: Test [Filename: 59c4cc2d-e1e7-489f-93fd-305968da0052.ioc]

Updated: Apr 08, 2015 Document ID: 118899