# Cisco AMP的配置终端的与身份持续时间

## 目录



## 简介

本文描述在Cisco的身份持续时间功能如何提前全体地允许计算机对象唯一标识符(UUID)重新使用Malware保护(AMP)终端的，当计算机或虚拟机被再镜像或被调遣时。这防止复制计算机对象的创建在显示板的，并且维护连续数据为那些计算机对象。这在检查也帮助维护终端连接器，提供数据连续性和保留许可证计数。

## 先决条件

### 要求

Cisco建议您有知识此题目：

- 对Cisco AMP的访问终端显示板的
- 在您最初配置连接器前，请配置身份持续时间
- Windows操作系统(OS)只支持身份持续时间

**Note**:必须启用身份持续时间功能Cisco技术支持中心(TAC)。

### 使用的组件

本文的信息根据终端显示板的Cisco AMP。

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。如果您的网络实际，请保证您了解所有命令的潜在影响。

## 工作流

当这是enable (event)时，身份持续时间选项使用这些工作流：

1. 身份持续时间选项在策略被配置。

2. 终端安装程序的AMP从显示板在一台新的计算机或VM生成并且配置。
3. 一个新的计算机对象用UUID和身份持续时间标志位创建。

- 注册检查

当连接器服务开始时，网云注册检查被执行。注册检查评估当前机器例如，主机名-和MAC地址的信息。它也评估在策略的身份持续时间设置网云为了确定新的UUID是否需要生成。

- 注册标准

对应于使用的身份持续时间设置的计算机对象有一隐藏的标志设置。此标志位，与唯一信息(主机名-或MAC地址)一起用于提供现有的UUID给匹配标准的所有机器。 如果标志位和机器的唯一信息与任何现有的计算机对象不配比，一个新的UUID和对象为机器生成。

> **Note**:当您使用主机名-时，使用完全合格的域名(FQDN)。如果有一台机器名为**测试的**和名为**test.domain.com的**另一台机器，他们不配比，并且没有重新使用UUID。

- 移动计算机

计算机的移动在组之间的用不同的身份持续时间设置创建重复项。这归结于与每个身份持续时间设置产生关联的一个隐藏的标志位。 当设置不配比时，重复项生成。当他们与**在策略**设置间一起使用时，两个组必须安排同一个策略被运用。如果设置是相同的，但是策略是不同的，重复项被创建。

> **Note**:如果要克隆或有Cisco AMP的一台计算机终端的配置的镜像，请读本文。

- MAC地址选择

机器可能有多MAC地址，然而，在连接器注册时手工影响MAC地址选择进程是不可能的。您必须使用MAC地址设置，只有当能保证您的机器只有一MAC地址，否则使用主机名-。

- 默认组

必须为策略也配置身份持续时间被运用于您的默认组。在策略或组用一台活动机器情况下删除，机器被放置到默认组，当注册检查被执行下次时。如果身份持续时间没有为默认组被配置，则复制对象生成。

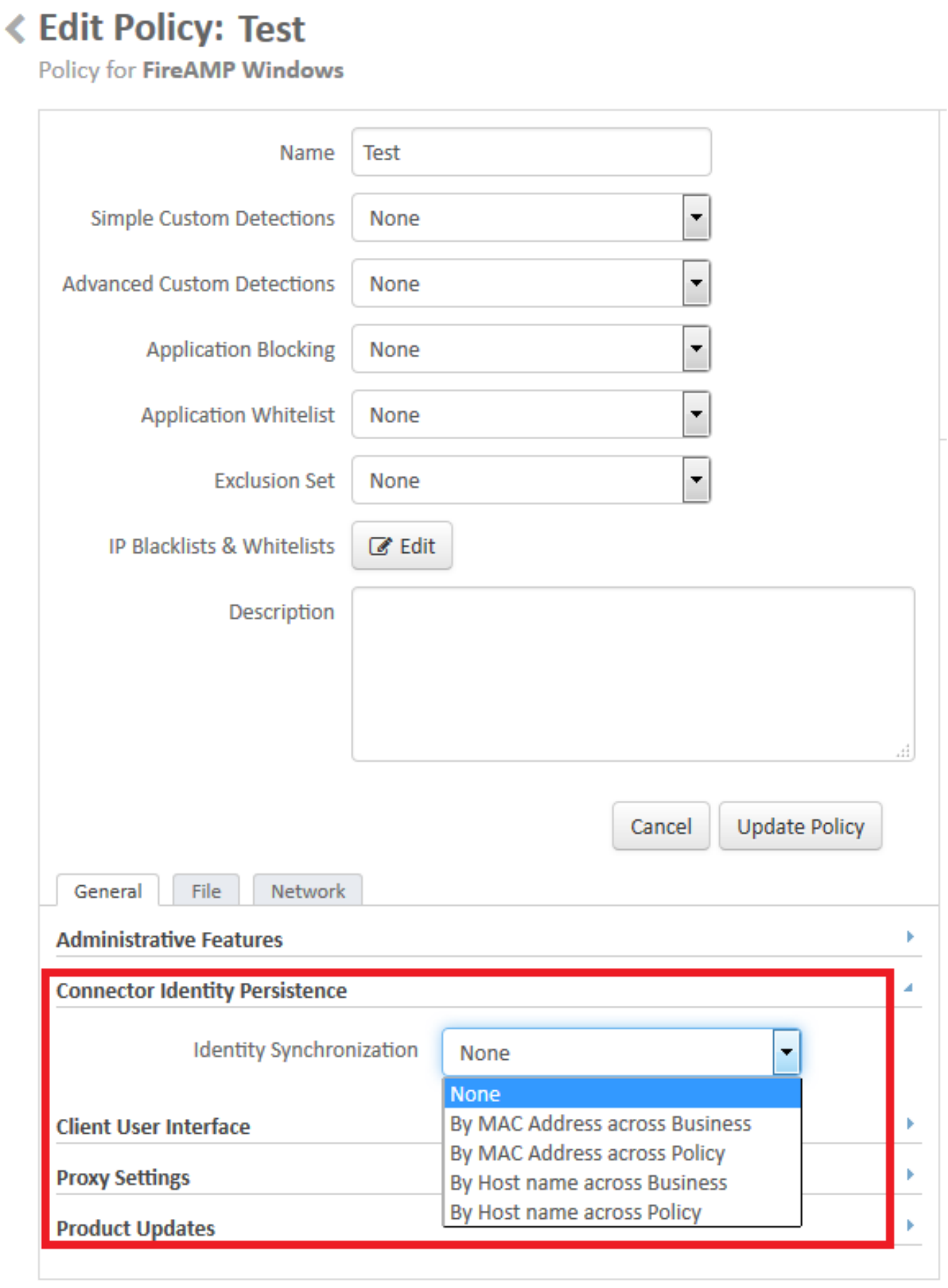
> **Note**:有时，被克隆从的被克隆的VM在默认组也许安置而不是组。如果这发生，请搬入VM在FireAMP控制台的正确的组。

# 配置

遵从步骤这里为了配置有身份持续时间的连接器：

步骤1.应用期望身份持续时间设置于您的策略：

- 连接对**Management>策略**
- 选择期望策略。点击**编辑**
- 连接对**一般**选项。它选择，默认情况下
- 选择**连接器身份持续时间**。如镜像所显示，**身份同步**下降下来出现。




Note:功能的启动，在终端的安装能造成复制对象为每台机器后生成。

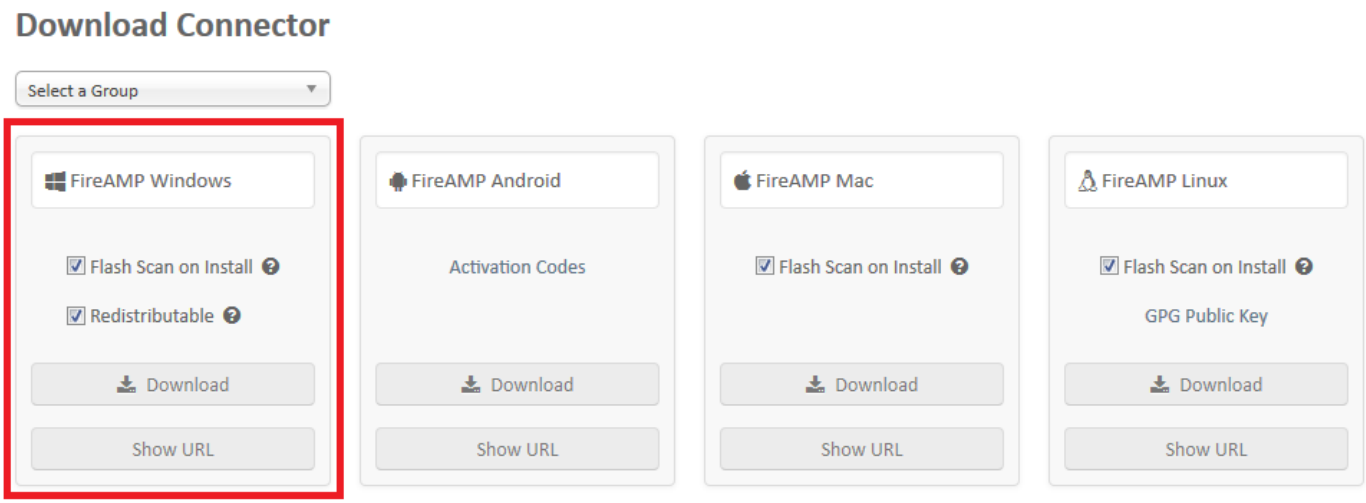
选择您的环境的是最佳的一个**身份同步**选项。这些选项是可用的：

- 无：功能不是启用的。连接器UUIDs没有与新的连接器同步在任何情况下安装。每新的安装生成一个新的机器对象。
- 由在事务间的MAC地址：新的连接器寻找有同一MAC地址为了在事务的所有策略间同步有身份同步设置为值除无之外的最近连接器。当选择，机器对象被创建并且被标记与使用在整个帐户间的该MAC地址的所有机器同步。
- 由在策略间的MAC地址：新的连接器寻找有同一MAC地址为了与在同一个策略内同步的最近连接器。当选择，机器对象被创建并且被标记与使用该MAC地址的所有机器同步和分配注册特定策略。
- 由在事务间的主机名：新的连接器寻找有同样主机名-为了与在事务的所有策略间同步有身份同步设置为值除无之外的最近连接器。当选择，机器对象被创建并且被标记与使用该主机名-在整个帐户间的所有机器同步。 **Note**:如果选择使用身份持续时间， Cisco建议您**由在事务间的主机名**使用。机器有一个主机名-，但是能有超过一MAC地址。 当使对象全球可用而不是每个策略，在您的事务间的配置可以减少配置的复杂性。
- 由在策略间的主机名：新的连接器寻找有同样主机名-为了与在同一个策略内同步的最近连接器。当选择，机器对象被创建并且被标记同步到使用该主机名-和注册对特定策略的所有机器。

步骤2.如镜像所显示，从网云显示板下载安装包：

- 连接到**Management>下载连接器**
- 选择期望组名和选项
- 点击**下载**
- 请使用**Redistributable**第三方部署软件或者脱机安装

**Note**:Cisco不支持使用第三方部署软件的建立程序包或安装。




步骤3.配置连接器到在您的组织的机器。

## 验证

使用本部分可确认配置能否正常运行。

为了验证身份持续时间工作，是否遵从这些步骤：

1. 安装连接器为了生成为身份同步被标记的计算机对象。

2. 在对象被创建了后，请记录下来**<uuid>**从local.xml文件在安装目录C:\Program Files\Sourcefire\fireAMP\local.xml里。**您**必须发现线路类似于此：
   ```
   <uuid>1234567890-abcd-efgh-ijkl-mnopqrst</uuid>
   ```
3. 之后，请卸载连接器。选择**没有**从安装路径删除的所有文件。
4. 重新启动PC并且重新安装终端的AMP与程序包和前一样。
5. 根据初始步骤再检查**local.xml文件**并且保证匹配从原始local.xmlfile的UUID。

## 故障排除

本部分提供了可用于对配置进行故障排除的信息。

- 保证安装程序包和身份持续时间设置一致。
- 如果您enable (event)身份持续时间POST配置，和使用一个更旧的程序包为了安装连接器，不用被启用的身份持续时间，连接器生成重复项，当他们注册，并且更新与当前设置的策略。
- 如果您的机器看上去共享UUID，请保证他们不共享唯一信息，例如在虚拟化的环境内的MAC地址。

## 相关信息

- 先进的Malware保护终端
- **技术支持和文档 - Cisco Systems**