NAC 4.5 ：策略导入导出配置示例

目录

简介

本文提供一分步指南关于怎样配置在思科美洲台版本4.5的策略进出口(饼)功能。此功能目的是设备过滤的同步，流量和修正规则和端口配置文件在美洲台管理器(Clean Access管理器)之间。当此功能讨论时，策略定义的美洲台管理器呼叫**万事达**，能推送或同步策略多达十个美洲台管理器(Clean Access管理器)，呼叫**Receivers**。策略可以自动地同步与预先设置计时器或通过一手工的同步。

先决条件

思科建议典型地配置的您有与思科美洲台管理器(Clean Access管理器) Web接口的熟悉和策略。参考思科美洲台版本的4.5版本注释关于什么的信息支持和不支持用饼。

要求

根据思科美洲台安装和配置指南设置美洲台管理器和服务器。配置的美洲台管理器策略进出口参考的最佳实践推荐为了识别哪个管理器一定使用的一样重要，并且哪个象接收方。本文假设，万事达和接收方美洲台管理器识别，并且使用最佳实践推荐。

使用的组件

本文档中的信息根据思科美洲台软件4.5.0。

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

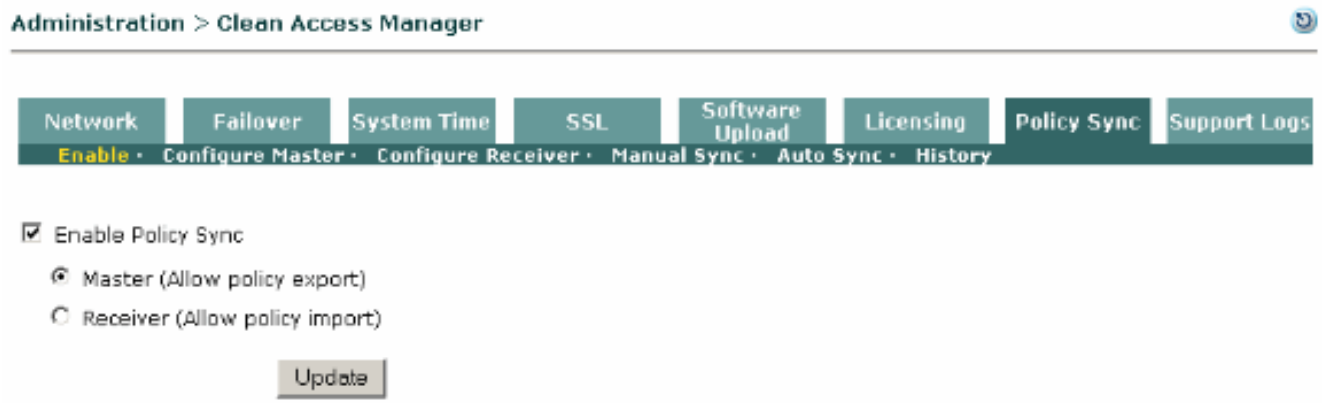
注意： 在您开始前，请确认万事达和接收方运行确切同样版本。并且，请保证规则集更新设置在万事达和所有接收方的**设备管理> Clean Access >更新>更新**匹配下。

美洲台配置

本部分提供有关如何配置本文档所述功能的信息。

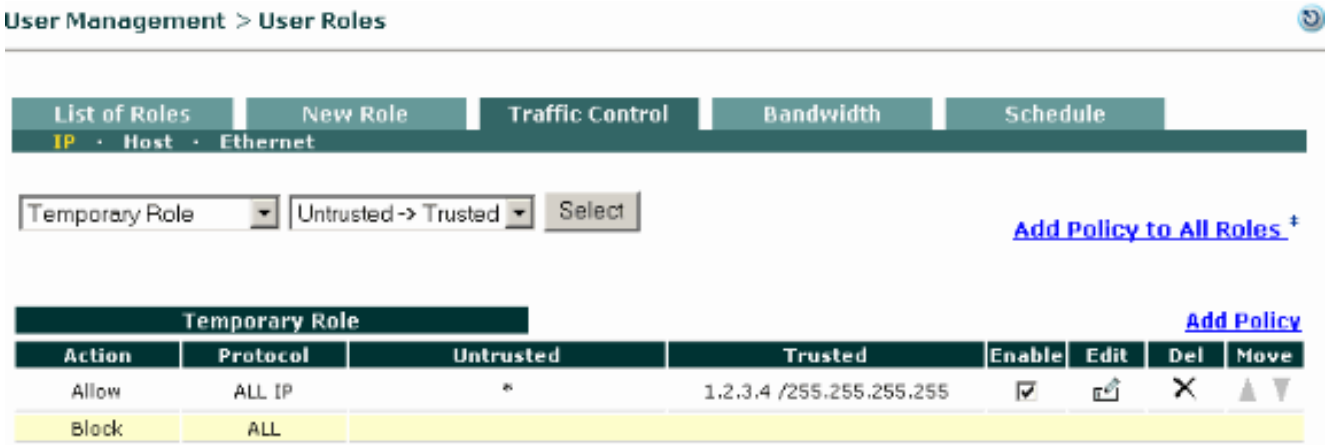
完成这些步骤为了配置在美洲台管理器之间的策略导入/导出。

1. **启用在重要的美洲台管理器的策略同步：**在重要的美洲台管理器，请导航对Administration > CCA Manager>策略同步>enable。

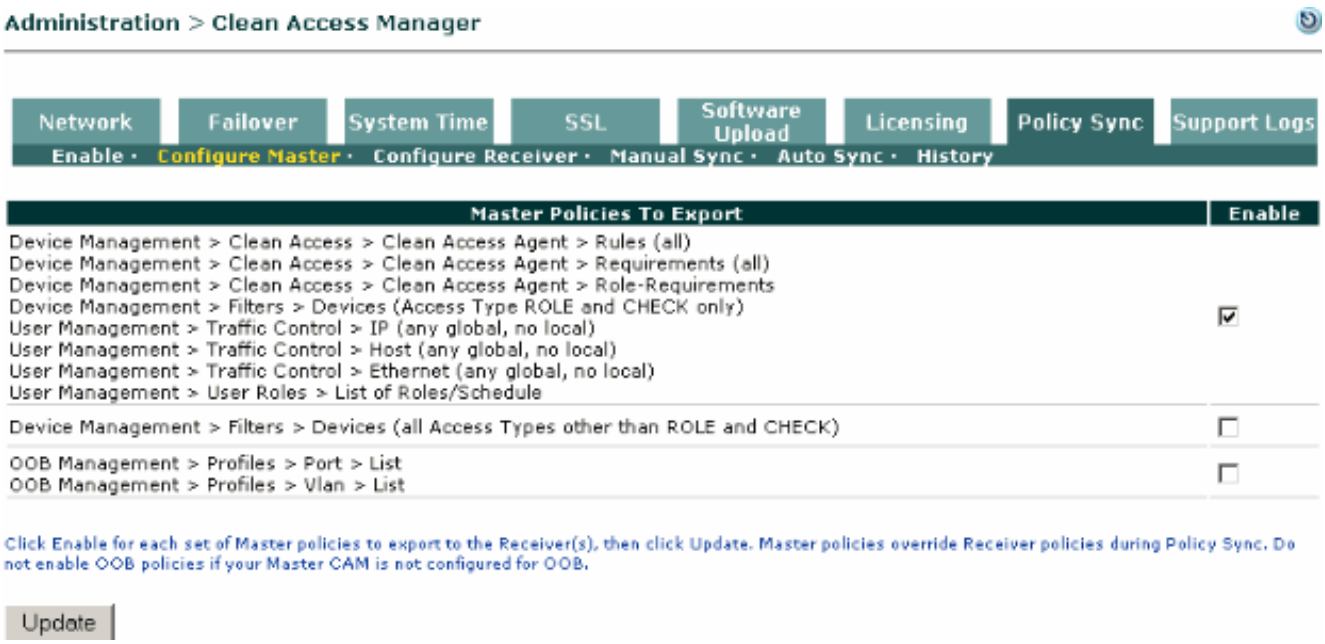


检查**Enable (event)策略同步**方框。选择**重要的(请允许策略出口)**选项，并且点击**更新**。

2. **了解将推送的具体政策：**在此步骤，您了解必须同步在主凸轮和接收方之间的具体政策。对于此示例，目标是同步在管理器之间的全局数据流交通控制策略。在这种情况下，必须选择全局基于IP的数据流策略在用户角色>数据流控制> IP下(请选择临时角色，不信任>委托在丢弃下来，如显示。单击**选择**。此规则在接收方不存在。



关于如何配置IP数据流策略的信息，参考请添加全局基于IP的数据流策略。选择Administration > Clean Access Manager>策略同步>配置主控并且检查Enable复选框如显示并且点击更新。

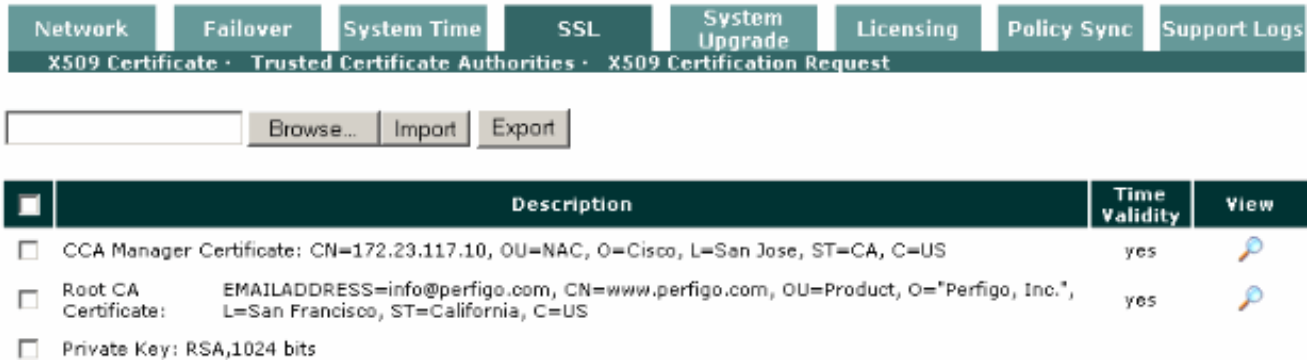


注意： 同步交通警也要求同步规则、需求、角色要求、设备过滤器(角色，检查类型)和角色。

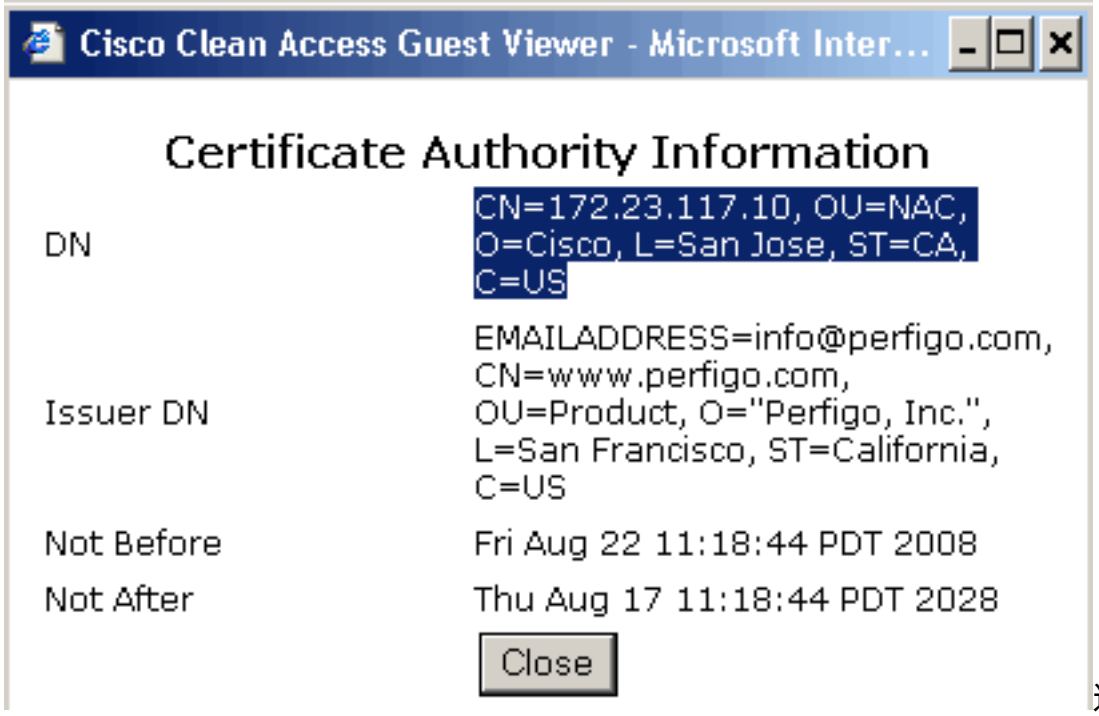
3. **添加/识别接收方：**您能加起来到十个支持的接收方到您的万事达。在本例中，您添加一个接收方到重要的美洲台管理器。选择Administration > Clean Access Manager>策略同步>配置万事达。在接收器主机名/IP下，请添加接收方的主机名(重要的美洲台管理器一定能解决主机名的DNS)或IP地址。添加一个可选说明并且单击添加。

一旦添加，新的接收方出现。您能添加多个接收器(支持的十)这样。在高性能的(HA)方案中，您需要添加虚拟/共享主机名或虚拟/共享HA对的IP地址对列表。

4. **授权接收方：**在您添加接收方后，巩固万事达和接收方之间的通信是重要的。仅已授权万事达能推送策略到接收方。同样地，万事达一定能用已授权接收方仅通信。并且，信任需要设立确保万事达，并且接收方是谁他们声称是。为此使用SSL。不仅万事达和接收方必须通过在证书的DN信息互相识别，但是他们也需要有他们的从委托权限(CA)的身份证书。简而言之，万事达和接收方需要委托彼此的证书。因为本文从实验室设置生成，自签名证书用于此示例。然而，请注意您在您的生产环境需要使用CA签名证书。参考配置的美洲台管理器策略进出口最佳实践推荐欲知更多信息。在接收方上，请选择Administration > CCA Manager> SSL > X509证书。



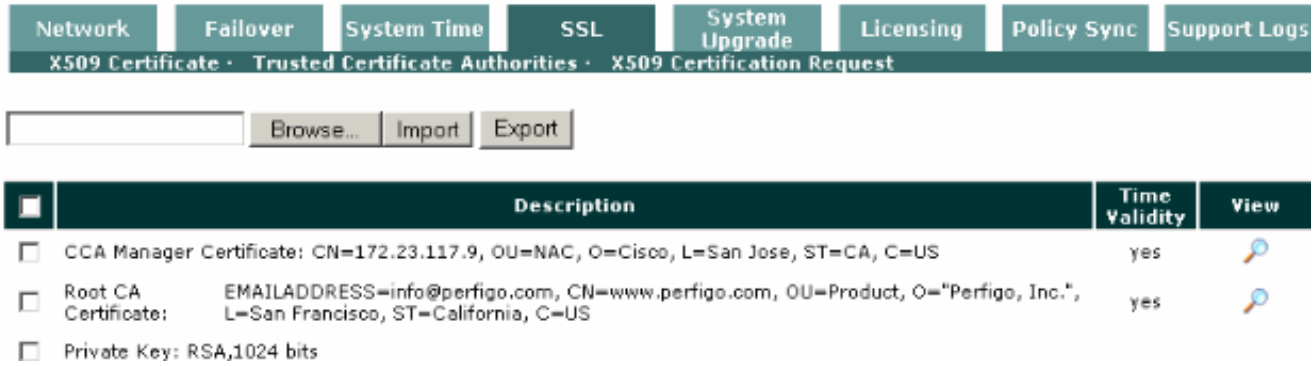
识别CCA管理器证书并且点击图标在视图下。在出现的窗口，请选择并且复制(右键单击和复制) DN信息。



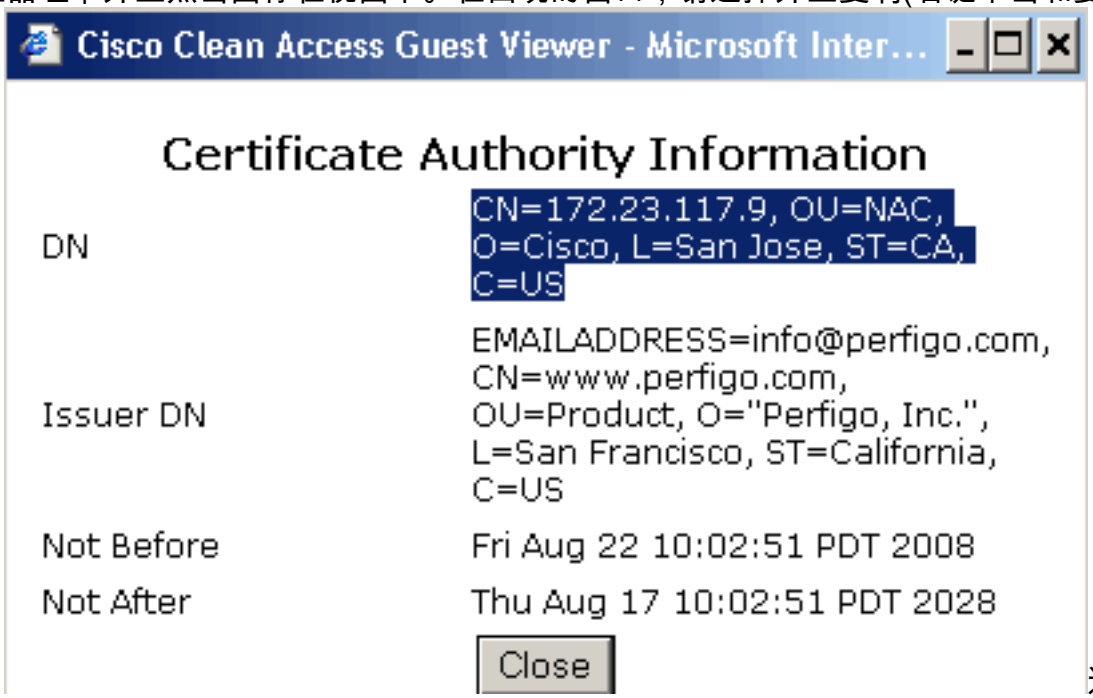
返回到在Administration下的重要的美洲台管理器> CCA Manager>策略同步>配置万事达。在底部，在已授权接收方下列表由证书辨别名称的，证书DN信息您从在上一步的接收方复制并且点击添加的粘贴。

5. **Enable (event)在接收方美洲台管理器的策略同步：**在接收方美洲台管理器，请导航对Administration > CCA Manager>策略同步>enable。检查**Enable (event)策略同步**方框。选择**接收方(请允许策略导入)**选项，并且点击**更新。注意：** 注意在上面的标语变红灯，指示是此美洲台的管理器已启用接收方。

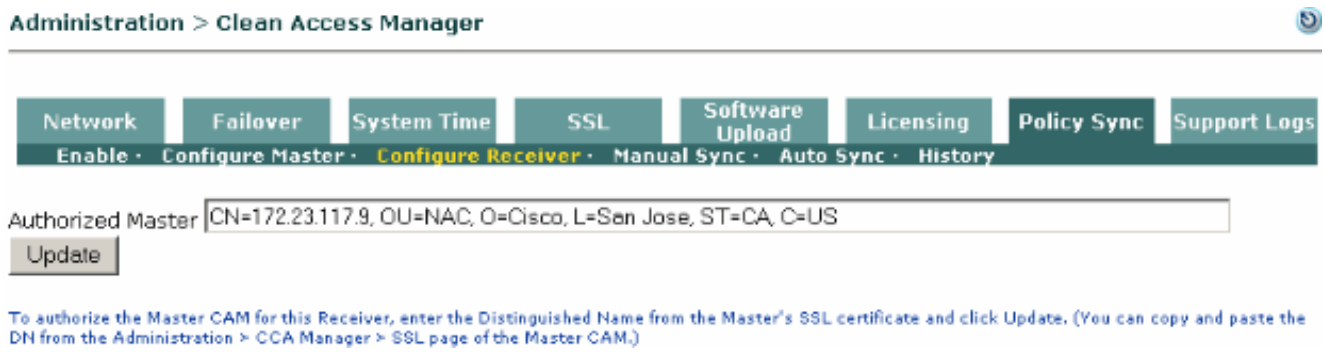
6. **授权万事达**：在万事达，请选择Administration > CCA Manager> SSL > X509证书。



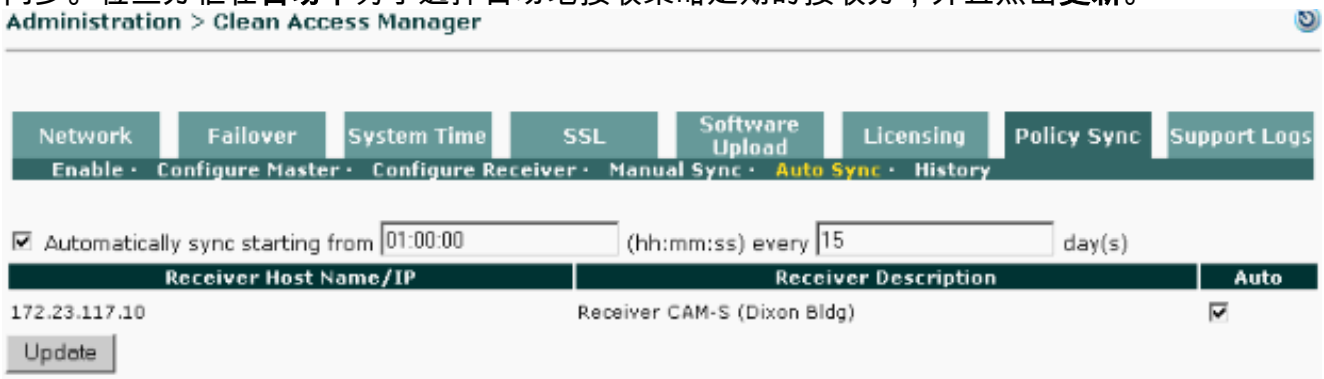
识别CCA管理器证书并且点击图标在视图下。在出现的窗口，请选择并且复制(右键单击和复



制) DN信息。返回到在Administration下的接收方美洲台管理器> CCA Manager>策略同步>配置接收方。在已授权万事达旁边，请粘贴您从在上一步的万事达复制并且点击更新的证书DN信息。



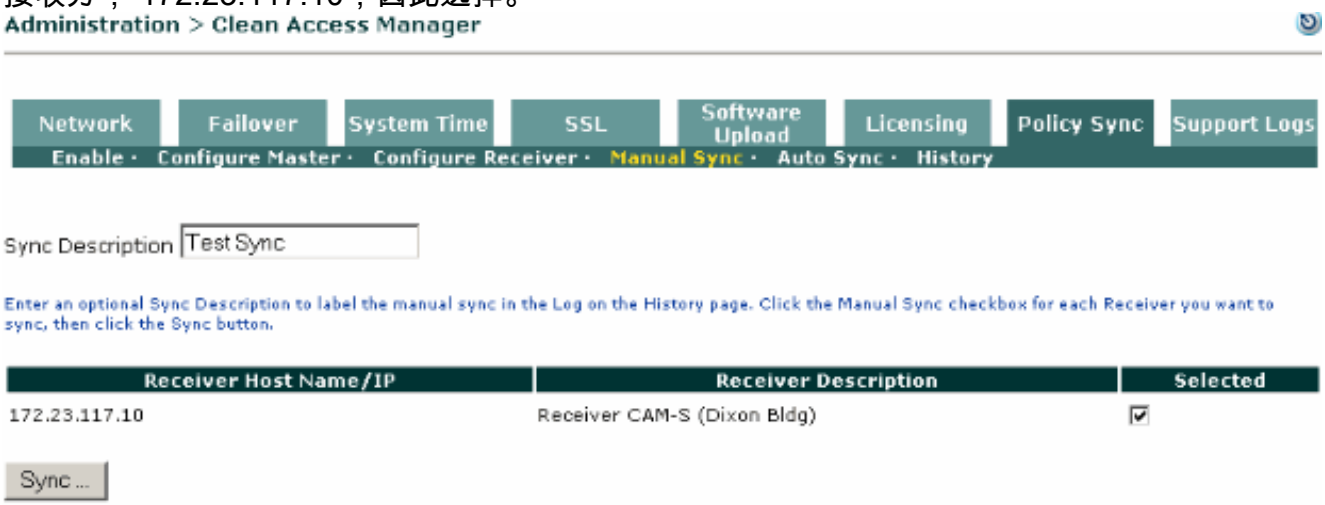
7. **配置自动同步(可选)**：策略同步可以手工或自动化。一手工的同步可以根据需要执行，而一个自动同步计时器可以设置一次自动地执行在美洲台管理器之间的一策略同步几天每个*x*编号(最低是一天)在预定时间。思科强烈建议您执行一手工的同步并且验证同步顺利地运作，在您启用在您的美洲台管理器之间前的自动同步。请参阅排除故障为了知道您如何能使用手工的同步排除故障与饼涉及的问题。为了启用自动同步，请导航对Administration > CCA Manager>策略同步>在重要的美洲台管理器的自动同步。**从_(hh开始自动地**检查**同步：mm:ss)每个_天**复选框。进入同步(上午1:00的时期在本例中)，并且(在本例中的每15天)该您多频繁要运行自动同步。检查方框在**自动下**为了选择自动地接收策略定期的接收方，并且点击**更新**。



验证

使用本部分可确认配置能否正常运行。

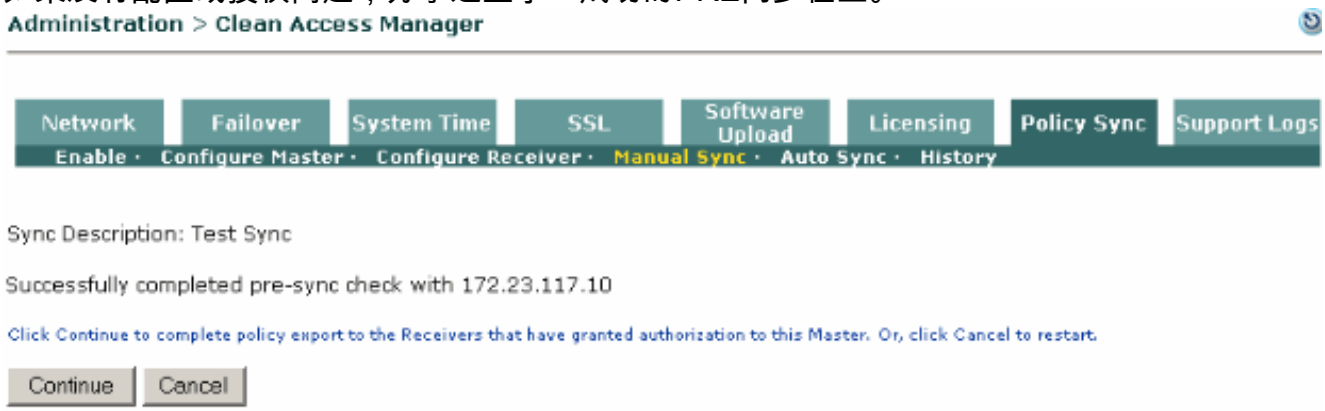
1. 导航对Administration > CCA Manager>策略同步>在万事达的手工的同步。
2. 键入一名称(可选)对于同步在同步说明下
3. 选择您要进行同步操作的接收方。检查方框在选定下，并且点击**同步**。在本例中，您只有一个接收方， 172.23.117.10，因此选择。



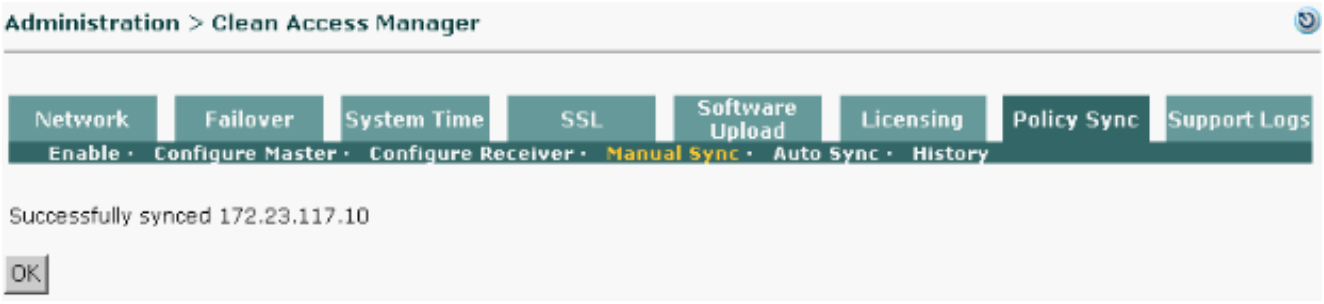
4. 这时，万事达执行一个PRE同步健全性检查接收方。PRE同步检查保证万事达和接收方美洲台管理器正确地配置(推送和接收策略)，并且验证信息正确等等。如果有任何配置或授权错误，

PRE同步检查失效与appropriate错误信息。请参阅Troubleshoot部分。

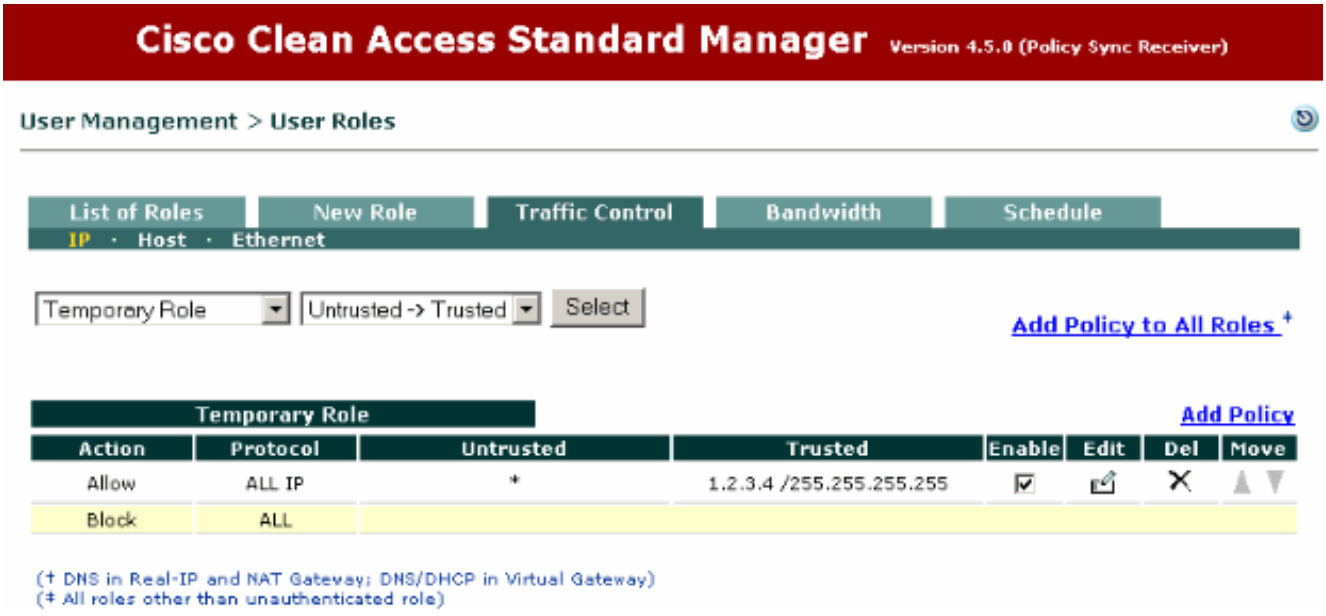
5. 如果没有配置或授权问题，万事达显示一成功的PRE同步检查。



6. 命中数继续成功地完成同步。



7. 去接收方美洲台管理器并且验证交通规则同步。



故障排除

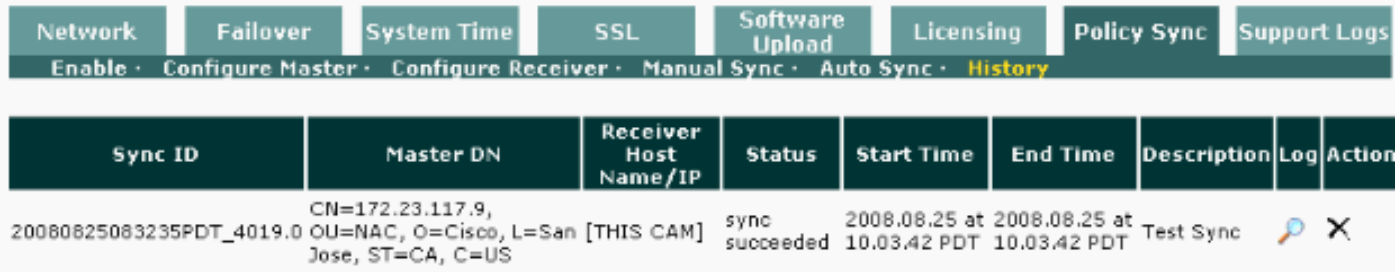
本部分提供的信息可用于对配置进行故障排除。

记录

同步摘要被记录在CCA Manager>在万事达和接收方的策略同步>历史记录下。

在重要的美洲台管理器：

在接收方美洲台管理器：



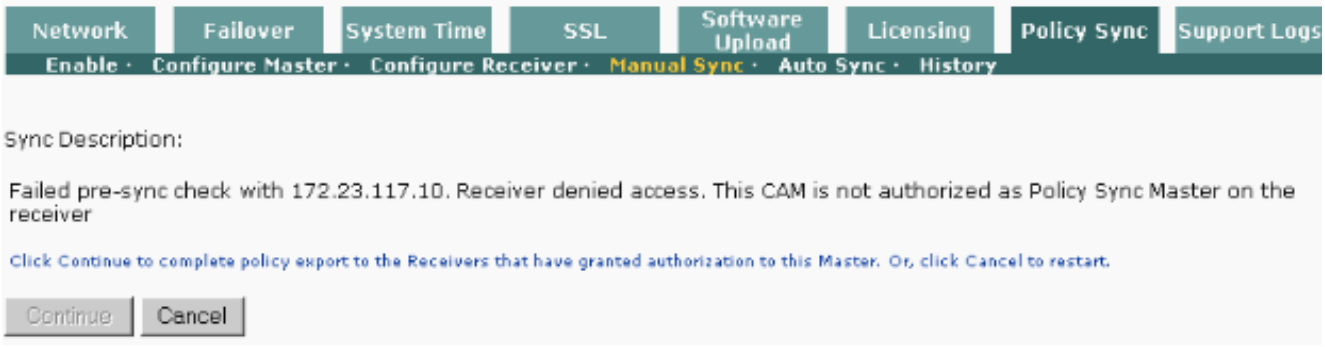
单击放大镜图标在洛金定货查看详细的处理日志下：

```
************** Master Log **************

Starting policy import/export on Policy Sync Master.
Created dump file for policy: User Management -> User Roles -> List of Roles/Schedule
Created dump file for policy: Device Management > Clean Access > Clean Access Agent > Role-
Requirements
Created dump file for policy: Device Management > Filters > Devices
Created dump file for policy: User Management->Traffic Control->IP
Created dump file for policy: User Management->Traffic Control->Host
Created dump file for policy: User Management->Traffic Control->Ethernet
Dump file creation is complete.
Created policy import/export dump file.
Created  policy import/export header file.
Created policy import/export tar file.


************** Receiver Log **************

Starting policy import on Policy Sync Receiver.
Hash value is a match.
Policy Sync Master and Receiver CAM versions match.
All SQL statements successfully executed
All requirements are valid.
All rules are valid.
Role tables integrity check is successful.
```

策略导入/出口在策略同步接收方顺利地完成。

问题

1. **接收方拒绝访问。此CAM没有授权作为在接收方的策略同步万事达。**

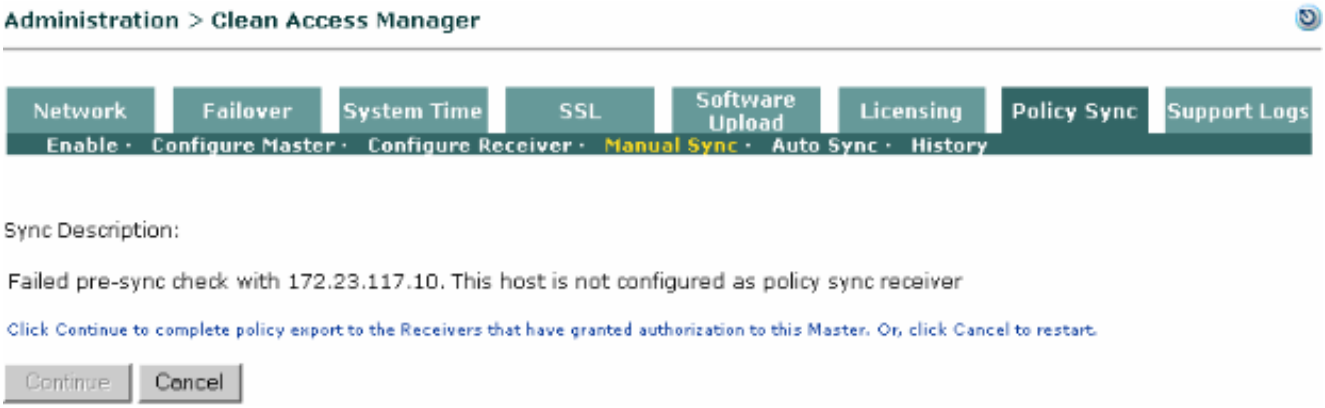


此错误典型地意味接收方拒绝策略同步，因为万事达DN信息在接收方美洲台管理器被不正确配置。选择Administration > CCA Manager>策略同步>配置在接收方的接收方并且确保，“授权万事达”信息正确地配置。

2. **此接收方没有授权**

此消息典型地意味着接收方没有为授权设置或在万事达美洲台管理器(接收方的DN信息)配置的授权参数不正确。选择Administration > CCA Manager>策略同步>配置在万事达的万事达并且确保接收方的证书的DN信息存在已授权接收方下列表由证书辨别名称和正确地配置。

3. **此主机没有配置作为策略同步接收方。**



此消息典型地意味着万事达设法同步到或者没有为策略同步启用的主机或没有配置是接收方。选择Administration > CCA Manager>在选择是接收方和保证的美洲台管理器的策略同步>设置策略同步启用的方框被检查，并且单选按钮设置为接收方(请允许导入策略)。

相关信息

- 技术支持和文档 - Cisco Systems