# NAC 4.5: Policy Import−Export Configuration Example

### Document ID: 108332

## Contents



## Introduction

This document provides a step−by−step guide on how to configure the Policy Import−Export (PIE) feature on Cisco NAC Release 4.5. The purpose of this feature is to synchronize the device filters, traffic and remediation rules, and port profiles between NAC Managers (Clean Access Managers). When this feature is discussed, the NAC Manager where policies are defined is called the **Master**, which can push or synchronize the policies of as many as ten NAC Managers (Clean Access Managers), called **Receivers**. Policies can be synchronized automatically with a preset timer or through a manual sync.

## Prerequisites

Cisco recommends that you have familiarity with the Cisco NAC Manager (Clean Access Manager) web interface and the policies that are typically configured. Refer to the Release Notes for Cisco NAC Release 4.5 for information about what is supported and not supported with PIE.

### Requirements

Set up the NAC Manager(s) and Server(s) according to Cisco NAC Installation and Configuration Guide. Refer to Best Practice Recommendations for Configuring NAC Manager Policy Import−Export in order to identify which Manager must be used as Master and which one as Receiver. This document assumes that the Master and Receiver NAC Managers are identified and the best practice recommendations are used.

### Components Used

The information in this document is based on the Cisco NAC Software 4.5.0.

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.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

**Note:** Before you begin, confirm that the Master and Receiver(s) run the exact same versions. Also, ensure that the Ruleset Update settings under **Device Management > Clean Access > Updates > Update** match on the Master and all the Receivers.

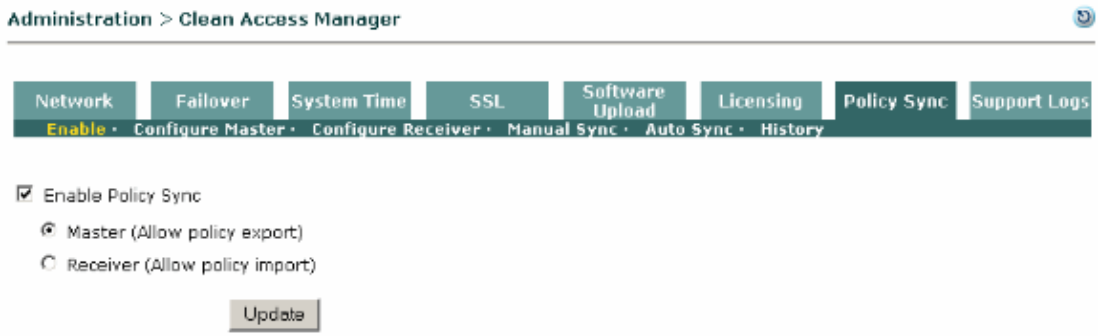
# NAC Configure

In this section, you are presented with the information to configure the features described in this document.

Complete these steps in order to configure Policy Import/Export between NAC Managers.

1. **Enable Policy Sync on Master NAC Manager:**

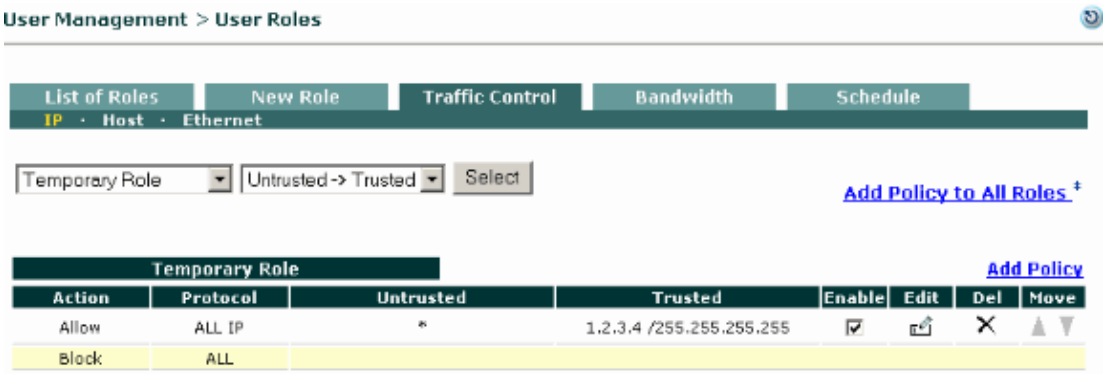
    a. On the Master NAC Manager, navigate to Administration > CCA Manager > Policy Sync > Enable.




    b. Check the **Enable Policy Sync** box. Choose the **Master (Allow policy export)** option, and click **Update**.

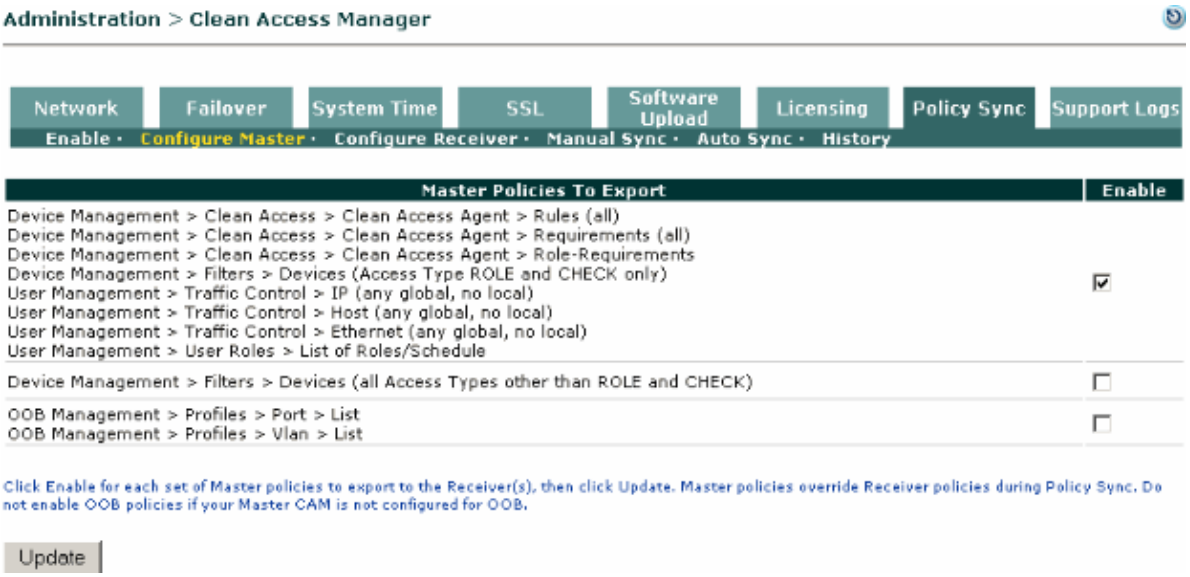
2. **Identify the policies to be pushed:**

    In this step, you identify the Policies that must be synchronized between the Master CAM and the Receivers. For this example, the goal is to synchronize the Global Traffic Control policies between the managers. In this case, the Global IP−Based Traffic Policy must be chosen under User Roles > Traffic Control > IP (Select Temporary Role, Untrusted > Trusted in the drop down, as shown. Click Select. This rule does NOT exist on the receiver yet.




    Refer to Add Global IP−Based Traffic Policies for information on how to configure IP Traffic Policies.

Choose Administration > Clean Access Manager > Policy Sync > Configure Master and check the Enable check box as shown and click Update.

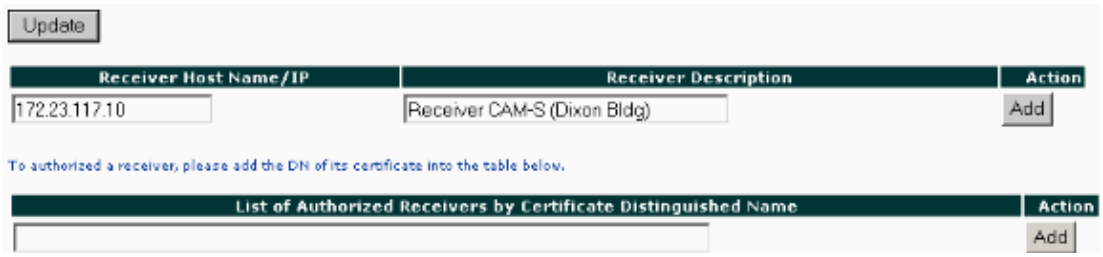



**Note:** Synchronizing Traffic Polices also requires synchronizing Rules, Requirements, Role Requirements, Device Filters (ROLE, CHECK types) and Roles.

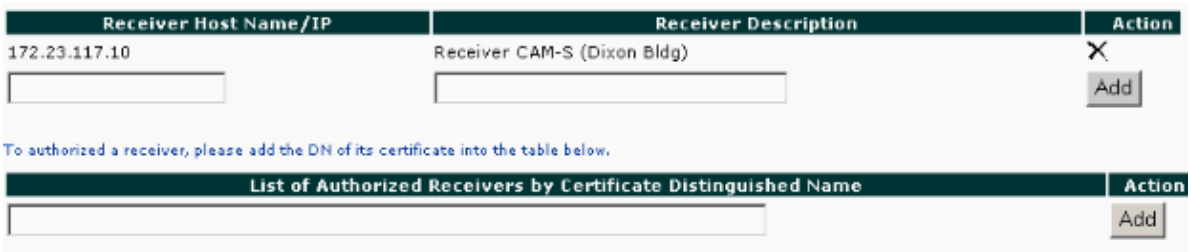
3. **Add/Identify the Receiver(s):**

   You can add up to ten supported Receivers to your Master. In this example, you add one Receiver to the Master NAC Manager.

   a. Choose Administration > Clean Access Manager > Policy Sync > Configure Master. Under Receiver Host Name/IP, add the Hostname (the Master NAC Manager must be able to resolve DNS for the host name) or IP address of the Receiver. Add an optional Description and click Add.




   b. Once added, the new Receiver appears. You can add multiple Receivers (up to ten supported) this way. In High Availability (HA) scenarios, you need to add the Virtual/Shared Host Name or Virtual/Shared IP address of the HA Pair to the list.



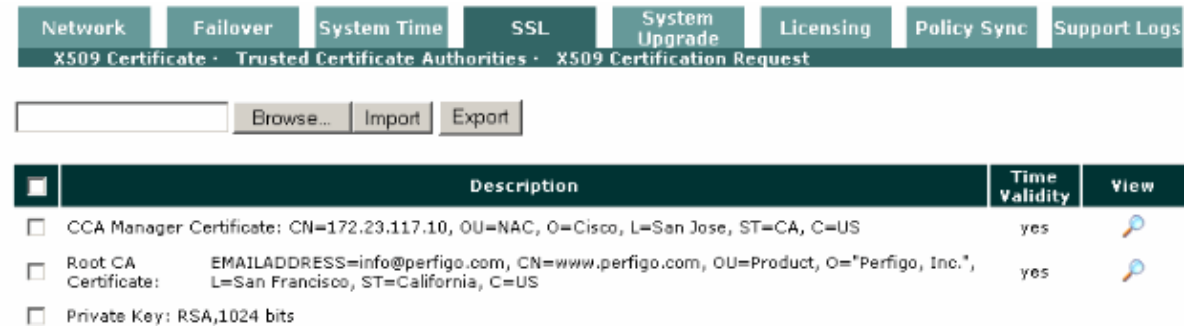

4. **Authorize the Receiver(s):**

   After you add the Receiver(s), it is important to secure the communication between the Master and Receiver(s). Only an Authorized Master is able to push policies to a Receiver. Similarly, the Master

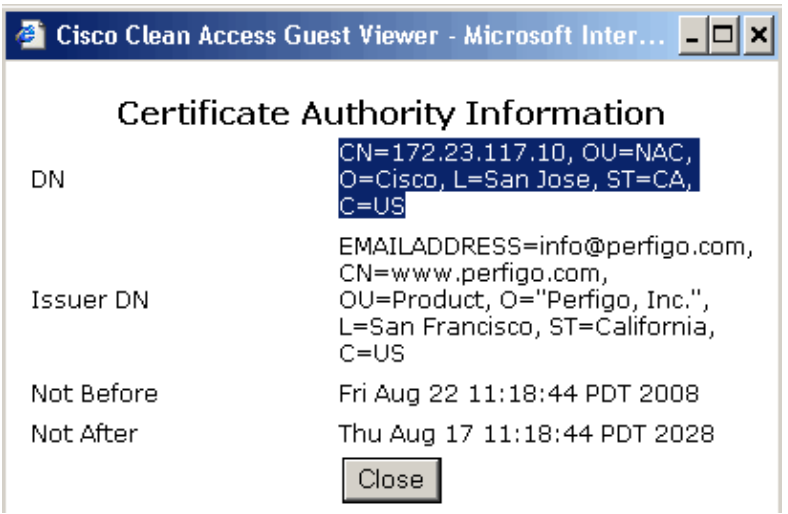
must be able to communicate only with authorized Receivers. Also, a trust needs to be established to make sure the Master and Receivers are who they claim to be. SSL is used for this purpose. Not only do the Master and Receiver have to identify each other through the DN information in the certificate, but they also need to have their identity certificate from a Trusted Authority (CA). In short, Master and Receiver need to trust each other s certificates.

Since this document is generated from a lab setup, self−signed certificates are used in this example. However, note that you need to use a CA signed certificate in your production environment. Refer to Best Practice Recommendations for Configuring NAC Manager Policy Import−Export for more information.

a. On the Receiver, choose Administration > CCA Manager > SSL > X509 Certificate.




b. Identify the CCA Manager Certificate and click on the icon under View. In the Window that appears, select and copy (right−click and copy) the DN information.




c. Return to the Master NAC Manager under Administration > CCA Manager > Policy Sync > Configure Master. At the bottom, under List of Authorized Receivers by Certificate Distinguished Name, paste the certificate DN information that you copied from the Receiver in the previous step and click Add.


5. **Enable Policy Sync on Receiver NAC Manager:**

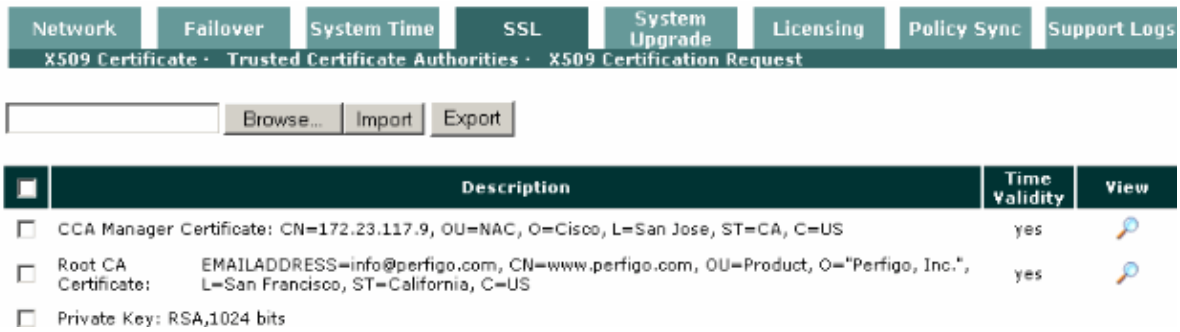
a. On the Receiver NAC Manager, navigate to Administration > CCA Manager > Policy Sync > Enable.

b. Check the **Enable Policy Sync** box. Choose the **Receiver (Allow policy import)** option, and click **Update**.

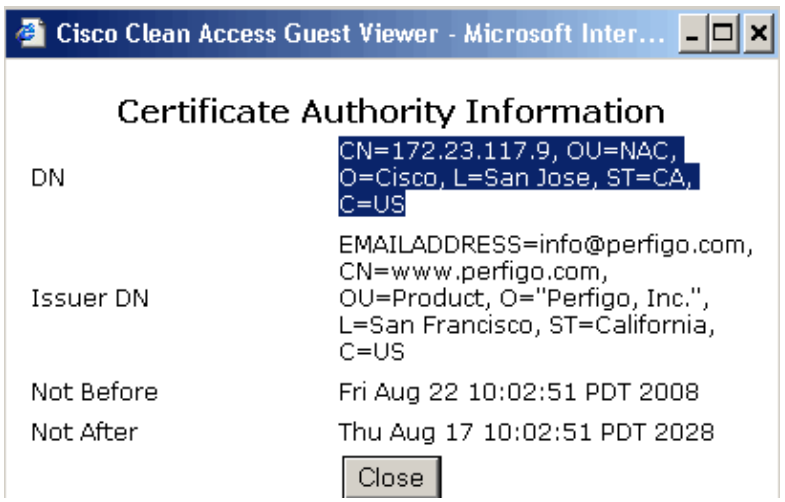
**Note:** Notice that the banner on top turns red, which indicates this NAC Manager is a enabled to be a Receiver.


6. **Authorize the Master:**

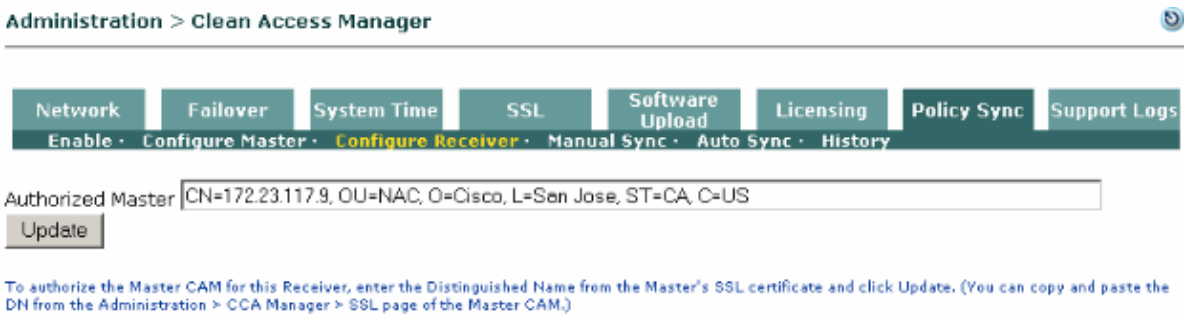
a. On the Master, choose Administration > CCA Manager > SSL > X509 Certificate.




b. Identify the CCA Manager Certificate and click on the icon under View. In the Window that appears, select and copy (right−click and copy) the DN information.



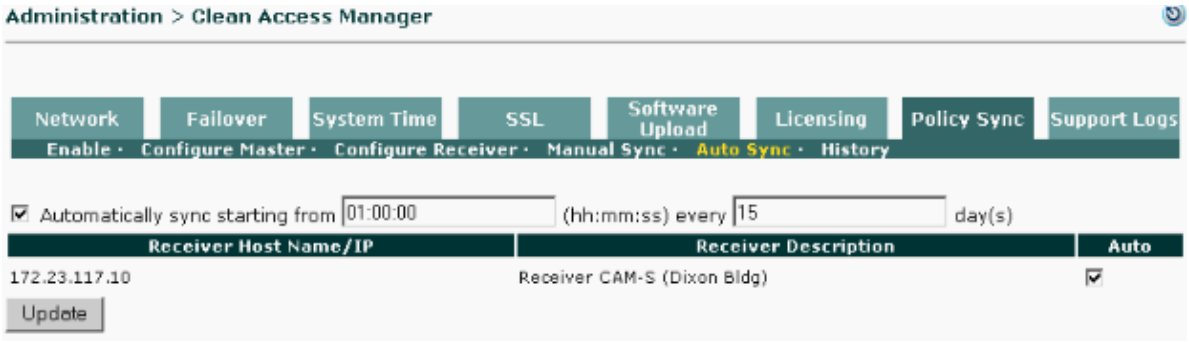

c. Return to the Receiver NAC Manager under Administration > CCA Manager > Policy Sync > Configure Receiver. Next to Authorized Master, paste the certificate DN information that you copied from the Master in the previous step and click Update.




7. **Configure Auto Sync (Optional):**

   Policy Sync can be manual or automated. A manual sync can be performed on an as−needed basis, while an Auto Sync Timer can be setup to automatically execute a policy sync between the NAC Managers once every *x* number of days (minimum is one day) at a predetermined time. Cisco strongly recommends you perform a Manual sync and verify that the sync works successfully before you enable Auto sync between your NAC Managers. See Troubleshoot in order to understand how you can use Manual Sync to troubleshoot issues related to PIE.

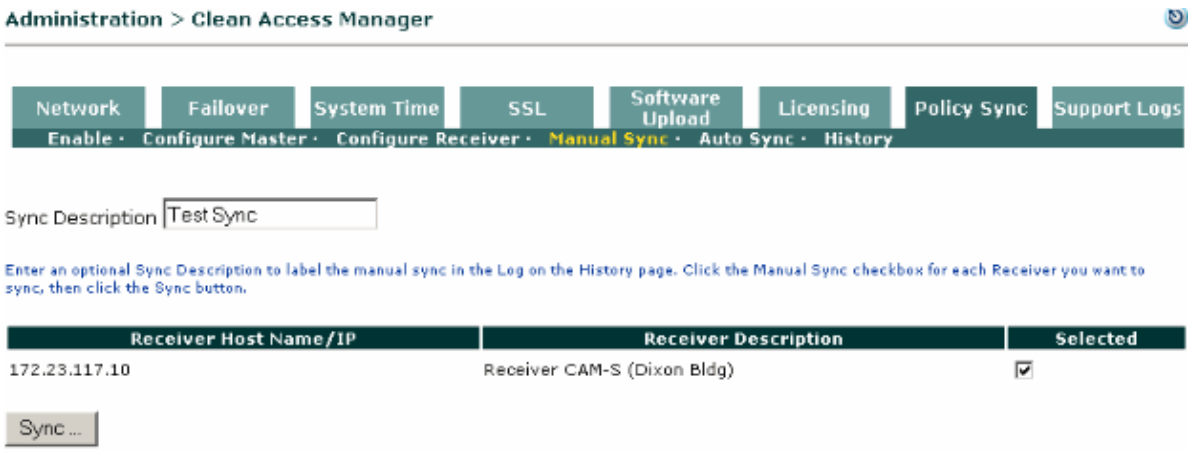
   a. In order to enable Auto sync, navigate to Administration > CCA Manager > Policy Sync > Auto Sync on the Master NAC Manager.
   b. Check the **Automatically sync starting from ___ (hh:mm:ss) every ___ day(s)** check box.
   c. Enter the time of sync (1:00 AM in this example) and how often (every 15 days in this example) that you want to run the Auto Sync.
   d. Check the box under **Auto** in order to select the Receiver(s) that automatically receive policies on a periodic basis, and click **Update**.




# Verify

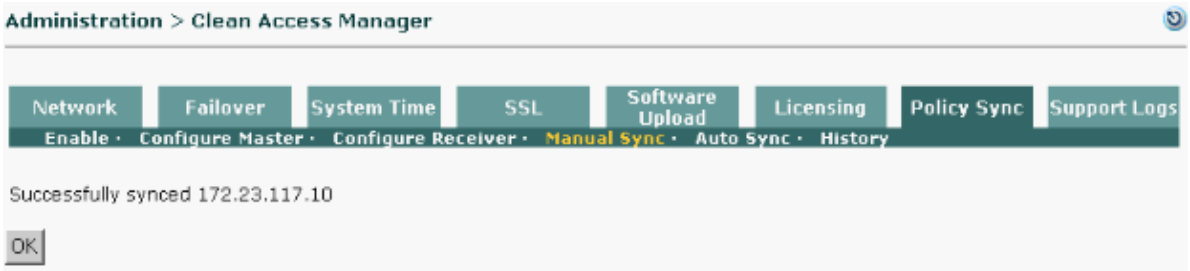
Use this section in order to confirm that your configuration works properly.

1. Navigate to Administration > CCA Manager > Policy Sync > Manual Sync on the Master.
2. Type a name (optional) for the Synchronization under Sync Description
3. Select the Receiver(s) on which you want to perform the Sync action. Check the box under Selected, and click **Sync**. In this example, you have only one Receiver, 172.23.117.10, so it is chosen.

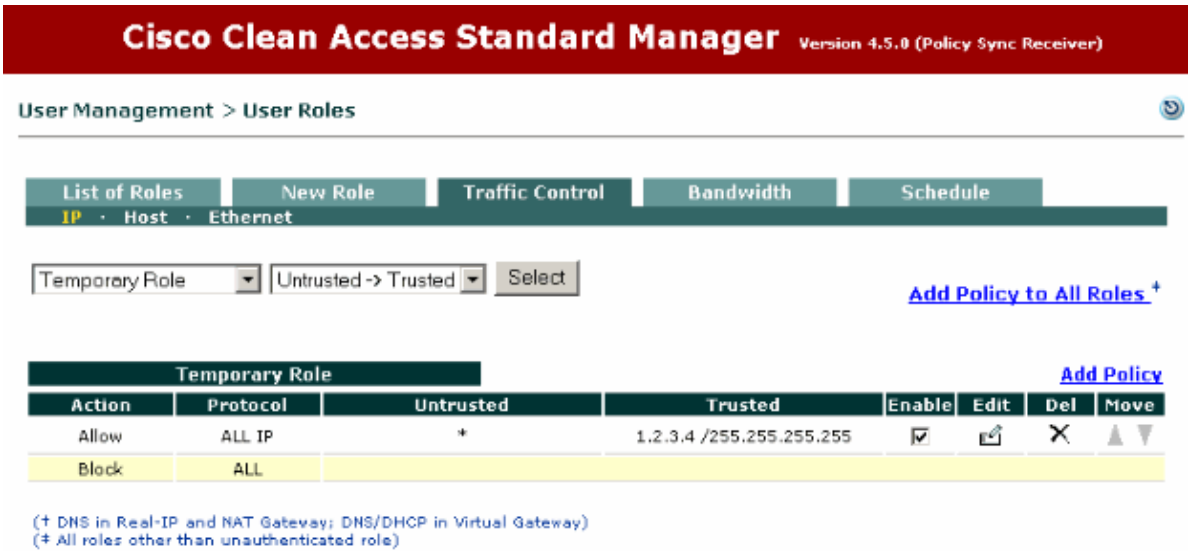



4. At this point, the Master performs a pre−sync sanity check against the Receiver. The pre−sync check ensures that the Master and Receiver NAC managers are configured correctly (to Push and Receive policies), and that authorization information is correct, etc. If there are any configuration or Authorization errors, the pre−sync check fails with appropriate error messages. See the Troubleshoot section.
5. If there are no configuration or authorization issues, the Master displays a successful pre−sync check.


6. Hit continue to successfully complete the sync.




7. Go to the Receiver NAC Manager and verify that the Traffic rule is synchronized.




# Troubleshoot

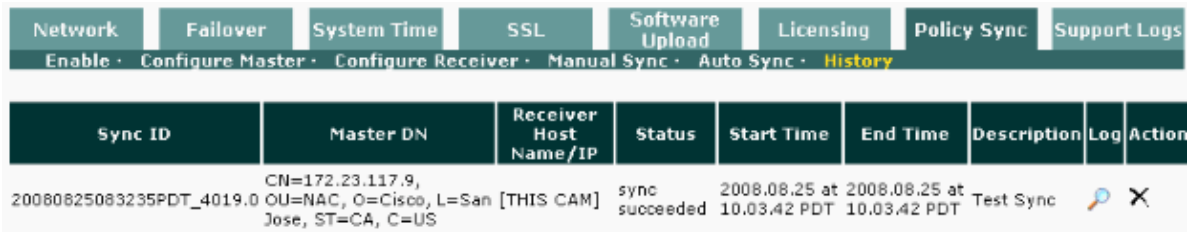
This section provides information you can use to troubleshoot your configuration.

## Logging

The Sync summary is logged under CCA Manager > Policy Sync > History on the Master and the Receiver(s).

On the Master NAC Manager:


On the Receiver NAC Manager:




Click the Magnifying Glass Icon under Log in order to view detailed transaction logs:

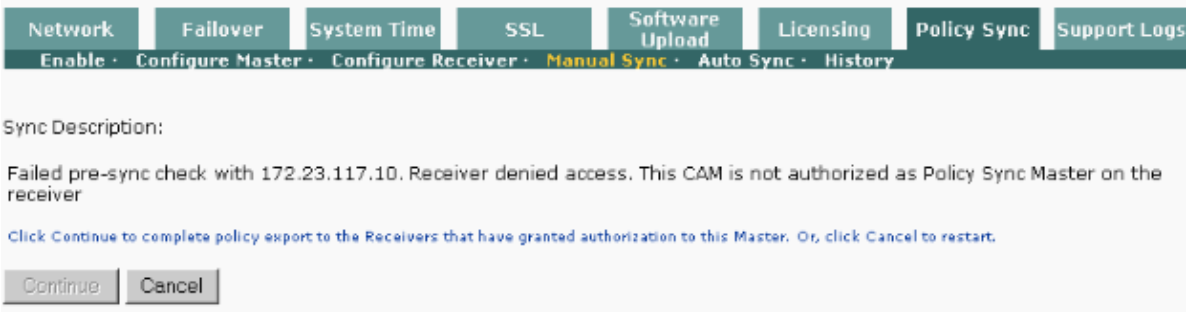
```
*************** Master Log ***************

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
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.
```

**Policy import/export successfully completed on Policy Sync Receiver.**

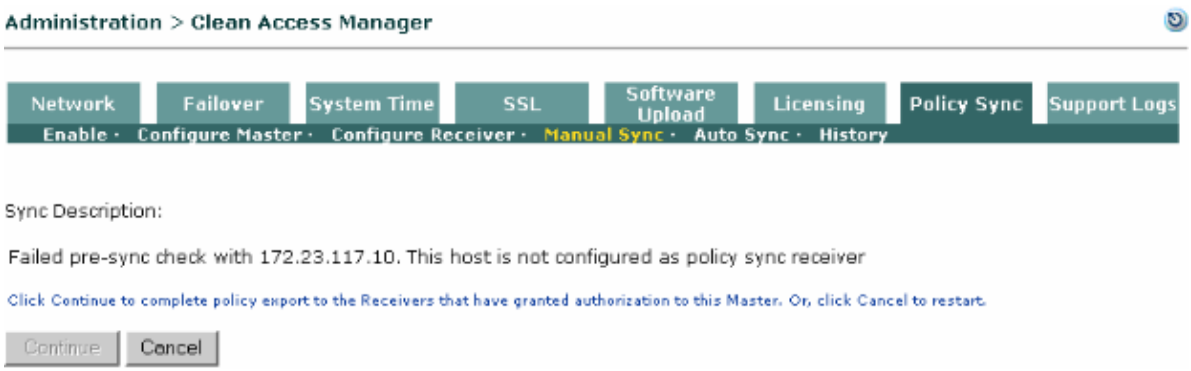
## Issues

1. **Receiver denied access. This CAM is not authorized as Policy Sync Master on the receiver.**




   This error typically means that the Receiver rejects the policy sync because the Master DN information is misconfigured on the Receiver NAC Manager. Choose Administration > CCA Manager > Policy Sync > Configure Receiver on the Receiver and make sure that the  Authorized Master  information is configured correctly.
2. **This receiver is not authorized**


   This message typically means that the Receiver is not setup for Authorization or the Authorization parameters (Receiver s DN information) configured on the Master NAC Manager is incorrect. Choose Administration > CCA Manager > Policy Sync > Configure Master on the Master and make sure the DN information of the Receiver s certificate exists under List of Authorized Receivers by Certificate Distinguished Name and is configured correctly.
3. **This host is not configured as policy sync receiver.**




This message typically means that the Master tries to sync to a host that is either not enabled for Policy Sync or it is not configured to be a Receiver. Choose Administration > CCA Manager > Policy Sync > Settings on the NAC Manager which is chosen to be the Receiver and ensure that the Policy Sync Enabled box is checked and that the Radio button is set to Receiver (Allow Importing Policy).

## Related Information

- **Technical Support & Documentation − Cisco Systems**



Updated: Nov 20, 2008 Document ID: 108332