NAC 4.5: Ejemplo de configuración de las importaciones/exportaciones de la directiva

Contenido

Introducción

Este documento proporciona un guía paso a paso en cómo configurar la característica de las importaciones/exportaciones de la directiva (EMPANADA) en la versión 4.5 del NAC de Cisco. El propósito de esta característica es sincronizar los filtros del dispositivo, las reglas del tráfico y de la corrección, y los perfiles del puerto entre los administradores del NAC (limpie a los administradores del acceso). Cuando se discute esta característica, llaman el administrador del NAC donde se definen las directivas el **master**, que puede avanzar o sincroniza las directivas de tanto como diez administradores del NAC (administradores limpios del acceso), llamado **Receivers**. Las directivas se pueden sincronizar automáticamente con un temporizador de la precolocación o a través de un manual sincronice.

prerrequisitos

Cisco recomienda que usted tienen familiaridad con la interfaz Web del administrador del NAC de Cisco (Access Manager limpio) y las directivas que se configuran típicamente. Refiera a los Release Note para la versión 4.5 del NAC de Cisco para la información sobre qué se soporta y no se soporta con la EMPANADA.

Requisitos

Configure los administradores y los servidores del NAC según la guía de instalación y configuración del NAC de Cisco. Refiera a las recomendaciones de la mejor práctica para configurar las importaciones/exportaciones de la directiva del administrador del NAC para identificar qué administrador debe ser tan principal usado y cuál como el receptor. Este documento asume que identifican a los administradores del NAC del master y del receptor y las

recomendaciones de la mejor práctica están utilizadas.

Componentes Utilizados

La información en este documento se basa en el software 4.5.0 del NAC de Cisco.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

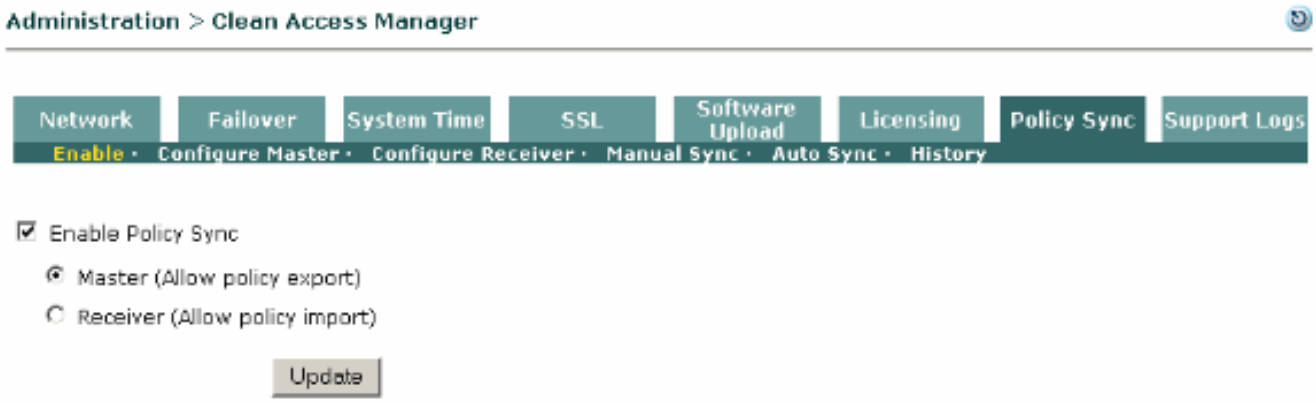
Note: Antes de que usted comience, confirme que el master y los receptores ejecutan el exacto las mismas versiones. También, asegúrese de que las configuraciones de la actualización de Ruleset bajo **Administración de dispositivos > acceso limpio > se pongan al día >** coincidencia de la **actualización** en el master y todos los receptores.

Configuración del NAC

En esta sección encontrará la información para configurar las funciones descritas en este documento.

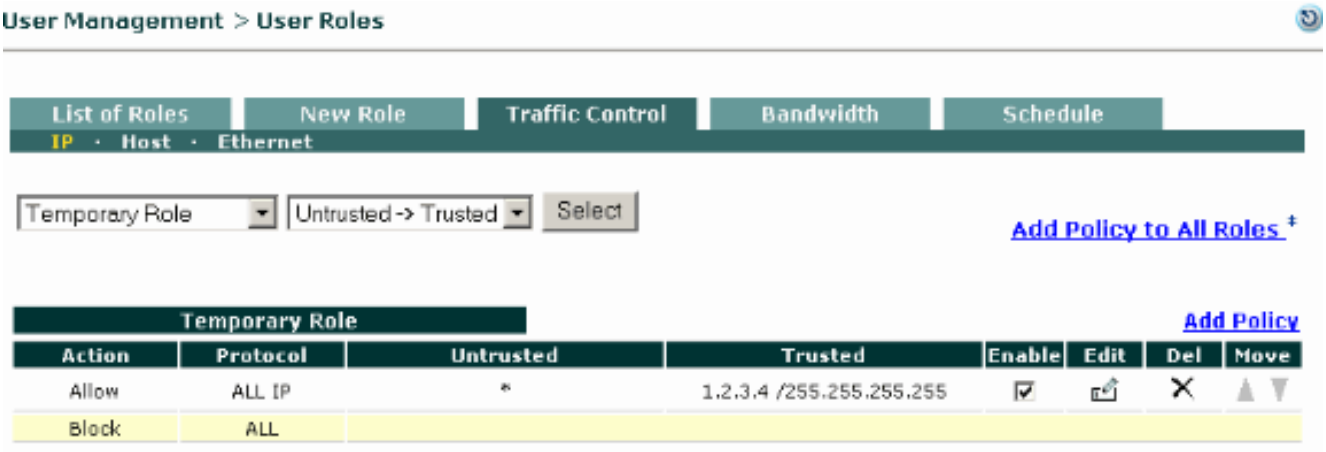
Complete estos pasos para configurar la importación/la exportación de la directiva entre los administradores del NAC.

1. **La directiva del permiso sincroniza en el administrador principal del NAC:**En el administrador principal del NAC, navegue a la administración > CCA administrador > directiva sincronizan >
   permiso.

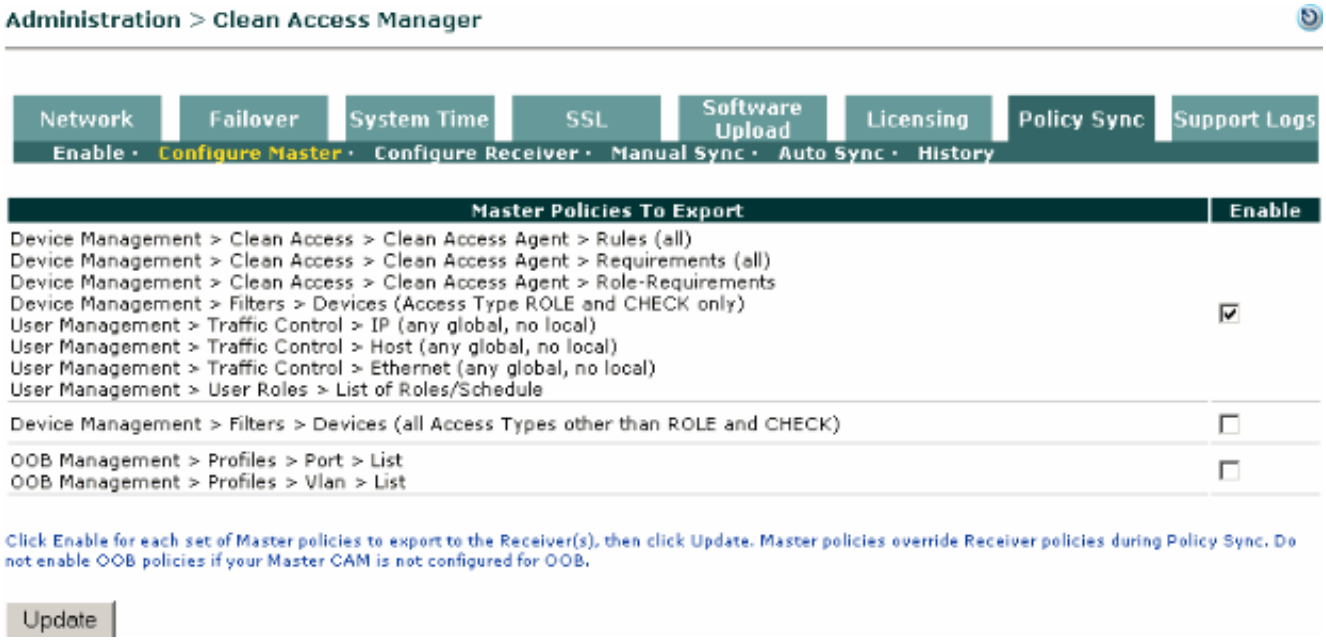


   Marque la **directiva del permiso sincronizan el** cuadro. Elija **(permita la exportación de la directiva) la** opción **principal**, y haga clic la **actualización**.
2. **Identifique las directivas que se avanzarán:**En este paso, usted identifica las directivas que se deben sincronizar entre el CAM principal y los receptores. Por este ejemplo, la meta es sincronizar las directivas de control del tráfico global entre los administradores. En este caso, la directiva global del tráfico basado en IP se debe elegir bajo los rol del usuario > el control

de tráfico > el IP (el papel temporal selecto, untrusted > confiaba en el descenso abajo, como se muestra. Tecleo selecto. Esta regla no existe en el receptor todavía.

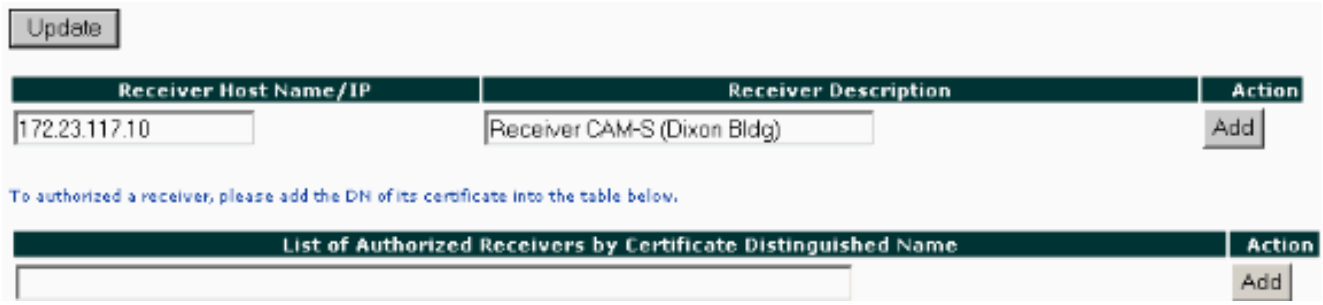


Refiérase agregan las políticas de información globales del tráfico basado en IP en cómo configurar las directivas del tráfico IP.Elija la administración > Access Manager limpio > directiva sincronizan > master de la configuración y marcan la casilla de verificación del permiso como se muestra y hacen clic la actualización.

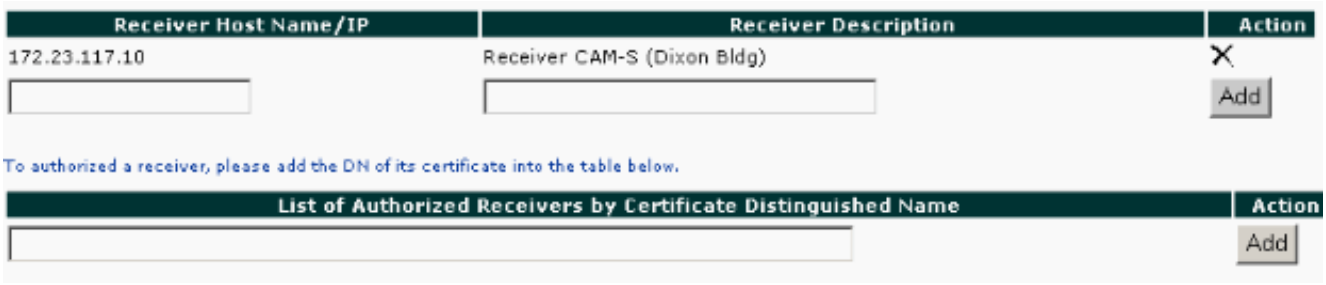


Note: La sincronización del tráfico limpia también requiere la sincronización de las reglas, de los requisitos, de los requisitos del papel, de los filtros del dispositivo (los tipos del PAPEL, del CONTROL) y de los papeles.

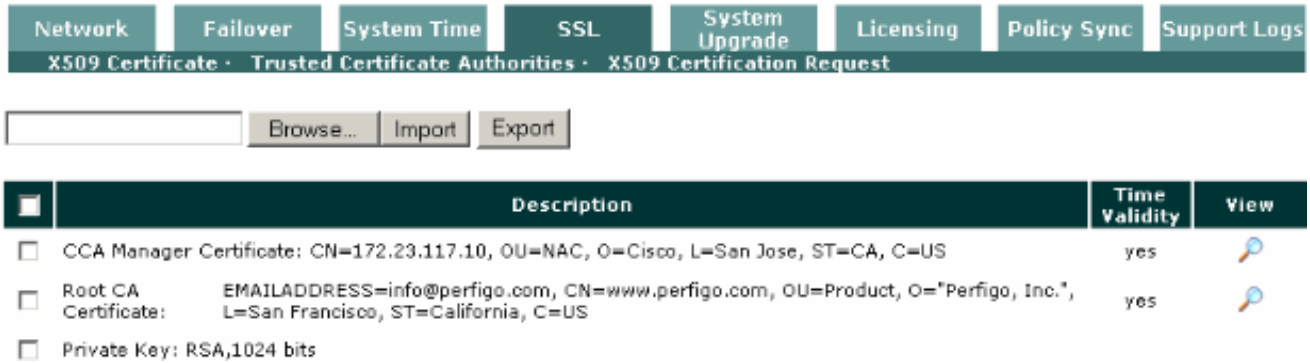
3. **Agregue/identifique los receptores:**Usted puede agregar hasta diez receptores soportados a su master. En este ejemplo, usted agrega un receptor al administrador principal del NAC.Elija la administración > Access Manager limpio > directiva sincronizan > master de la configuración. Bajo host Name/IP del receptor, agregue el nombre de host (el administrador principal del NAC debe poder resolver el DNS para el nombre del host) o la dirección IP del receptor. Agregue una descripción opcional y el haga click en Add



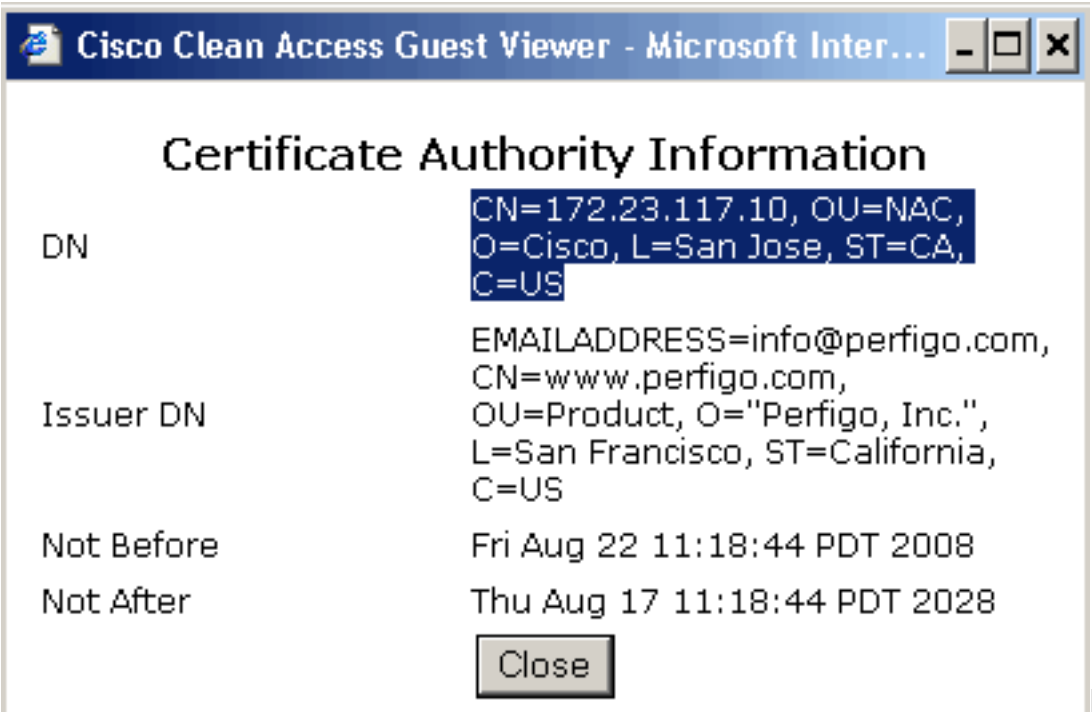
Una vez que está agregado, el nuevo receptor aparece. Usted puede agregar a los receptores múltiples (hasta diez soportados) esta manera. En los escenarios de gran disponibilidad (HA), usted necesita agregar el nombre del host virtual/compartido o la dirección IP virtual/compartida de los pares HA a la lista.



4. **Autorice los receptores:**Después de que usted agregue los receptores, es importante asegurar la comunicación entre el master y los receptores. Solamente un master autorizado puede avanzar las directivas a un receptor. Semejantemente, el master debe poder comunicar solamente con los receptores autorizados. También, una confianza necesita ser establecida para aseegurarse al master y los receptores son quién demandan ser. El SSL es para este propósito usado. No sólo el master y el receptor tienen que identificarse con la información DN en el certificado, pero también necesitan tener su certificado de identidad de una autoridad de confianza (CA). En fin, el master y el receptor necesitan confiar en los Certificados de cada uno.Puesto que este documento se genera de una configuración de laboratorio, los certificados autofirmados se utilizan en este ejemplo. Sin embargo, observe que usted necesita utilizar un certificado firmado de CA en su entorno de producción. Refiera a las [recomendaciones de la mejor práctica para configurar las importaciones/exportaciones de la directiva del administrador del NAC] para más información.En el receptor, elija la administración > CCA administrador > el certificado SSL > X509.



Identifique CCA el certificado del administrador y haga clic en el icono bajo visión. En la ventana que aparece, seleccione y copie (click derecho y copia) la información

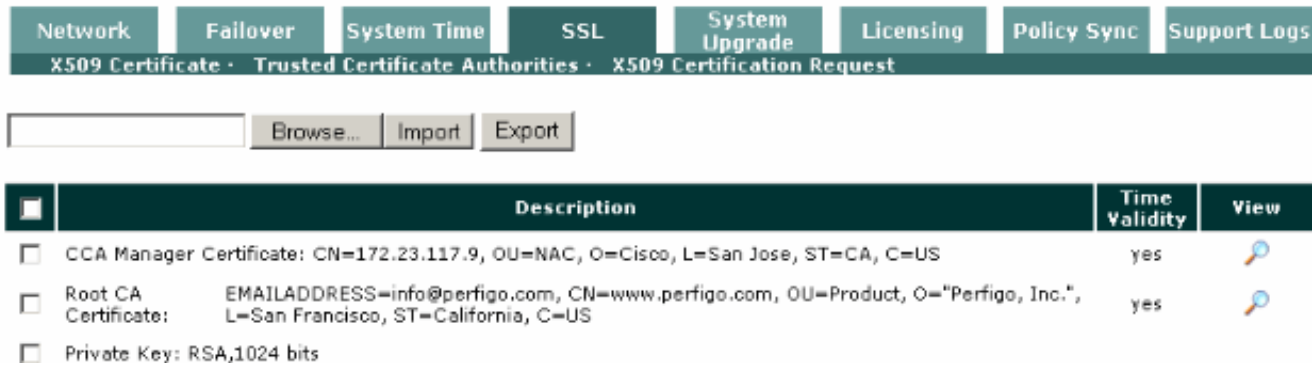


DN. La vuelta al administrador principal del NAC bajo administración > CCA administrador > directiva sincroniza > master de la configuración. En la parte inferior, bajo la lista de receptores autorizados por el nombre distintivo del certificado, goma la información DN del certificado que usted copió del receptor en el paso anterior y el haga click en Add

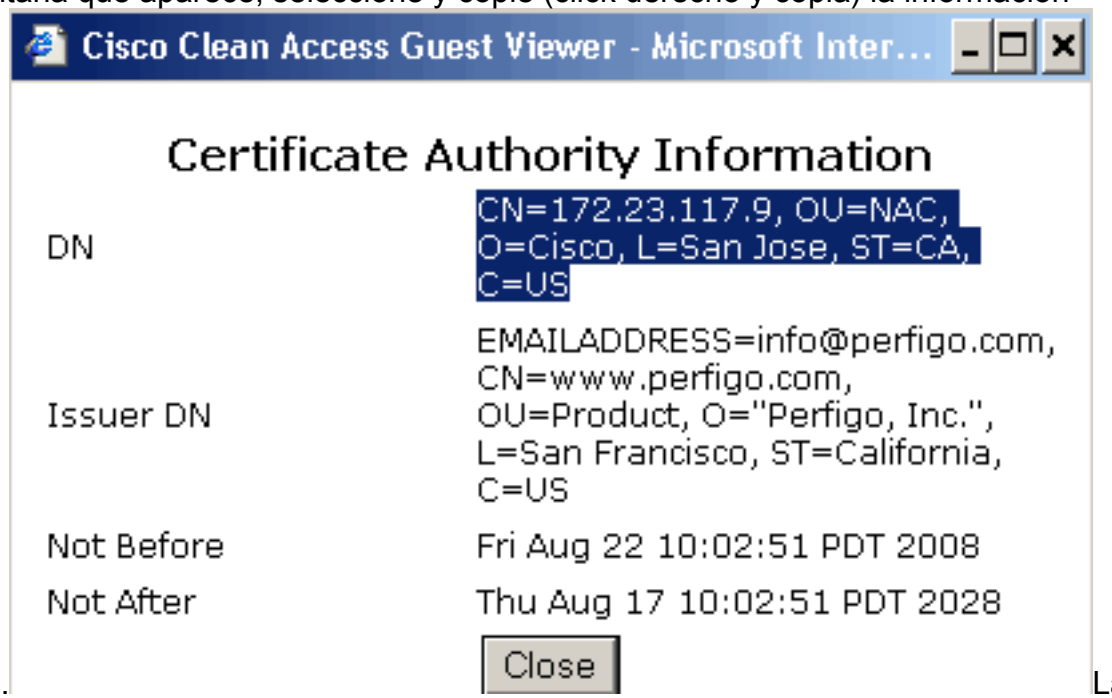
5. **La directiva del permiso sincroniza en el administrador del NAC del receptor:**En el administrador del NAC del receptor, navegue a la administración > CCA administrador > directiva sincronizan > permiso.Marque la **directiva del permiso sincronizan el** cuadro. Elija la opción del **receptor (permita la importación de la directiva)**, y haga clic la **actualización**.**Note**: Note que el banner en el top da vuelta al rojo, que indica que este administrador del NAC es un habilitado a ser un receptor.

6. **Autorice al master:**En el master, elija la administración > CCA administrador > el certificado SSL >

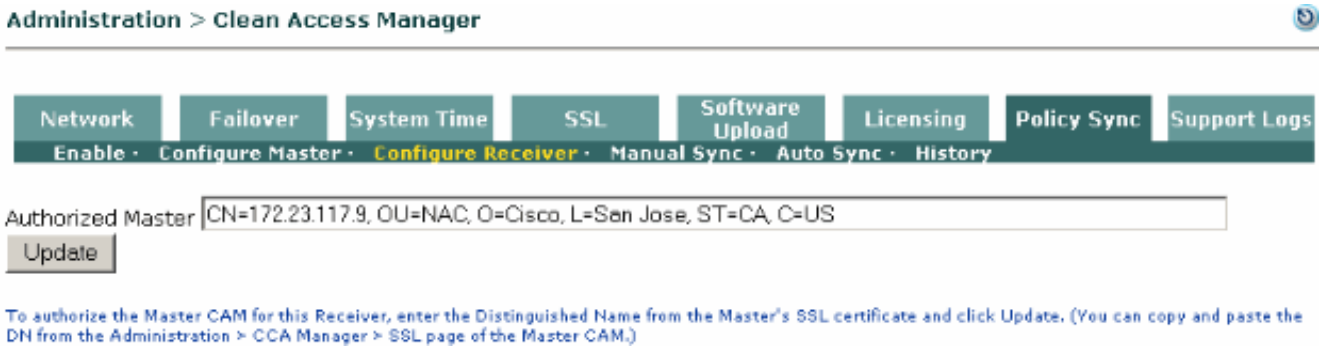
X509.



Identifique CCA el certificado del administrador y haga clic en el icono bajo visión. En la ventana que aparece, seleccione y copie (click derecho y copia) la información DN.

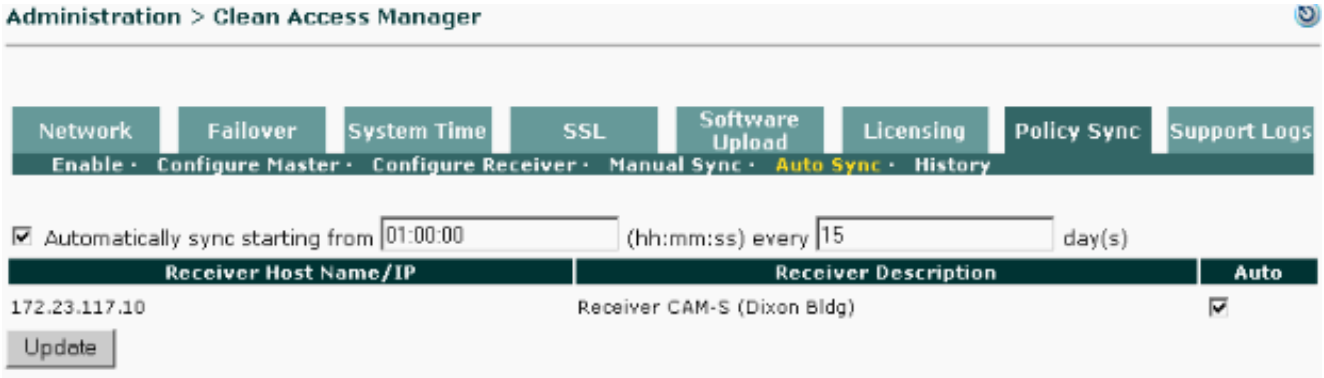


La vuelta al administrador del NAC del receptor bajo administración > CCA administrador > directiva sincroniza > receptor de la configuración. Al lado del master autorizado, pegue la información DN del certificado que usted copió del master en el paso y la actualización anteriores del
tecleo.



7. **El auto de la configuración sincroniza (opcional):**La directiva Synchronization puede ser manual o automatizó. Un manual sincroniza se puede realizar según sea necesario, mientras que un auto sincroniza el temporizador se puede poner para ejecutar automáticamente una directiva sincroniza entre los administradores del NAC una vez cada número *x de* días (el mínimo es un día) en una hora predeterminada. Cisco le recomienda fuertemente realiza un manual sincroniza y verifica que el sincronizar trabaja con éxito antes de que usted habilite el auto sincronice entre sus administradores del NAC. Vea que

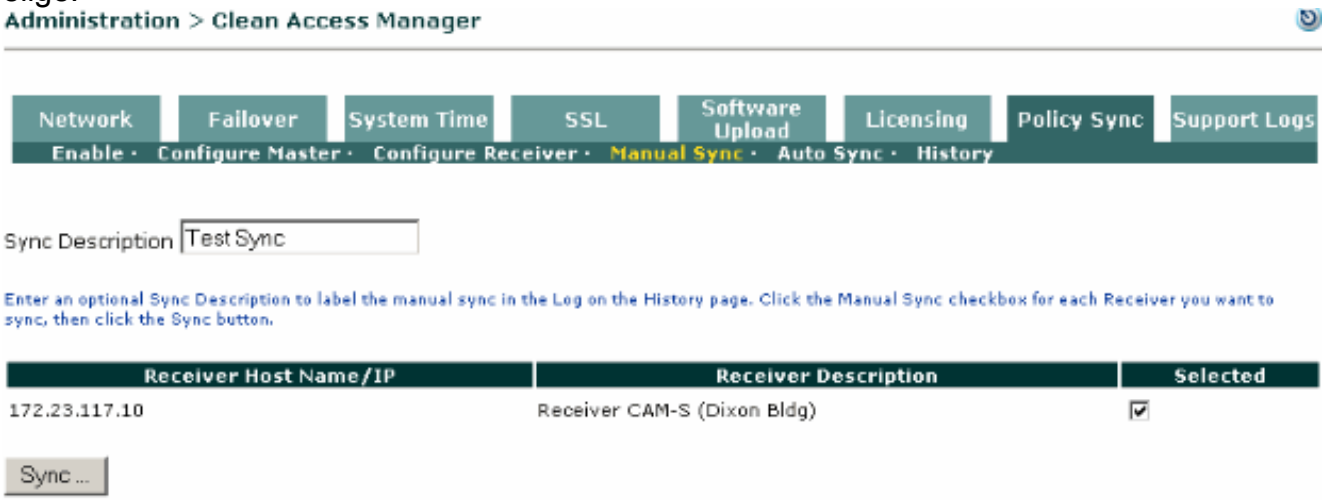
Troubleshooting para entender cómo usted puede utilizar el manual sincronice para resolver problemas los problemas relacionados con la EMPANADA.Para habilitar el auto sincronice, navegue a la administración > CCA administrador > directiva sincronizan > auto sincronizan en el administrador principal del NAC.Marque **automáticamente el sincronizar a partir del _(hh: milímetro: ss) cada** casilla de verificación de los **días del** _.Ingrese la época de sincronizan (1:00 en este ejemplo) y cuantas veces (cada 15 días en este ejemplo) ese usted quiere funcionar con el auto sincronice.Marque el cuadro bajo el **auto** para seleccionar los receptores que reciben automáticamente las directivas en una forma periódica, y haga clic la
actualización.



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Navegue a la administración > CCA administrador > directiva sincronizan > manual sincronizan en el master.
2. Teclee un nombre (opcional) para la sincronización debajo sincronizan la descripción
3. Seleccione los receptores en los cuales usted quiere realizar la acción del sincronizar. Marque el cuadro bajo seleccionado, y el tecleo **sincroniza**. En este ejemplo, usted tiene solamente un receptor, 172.23.117.10, así que se
elige.

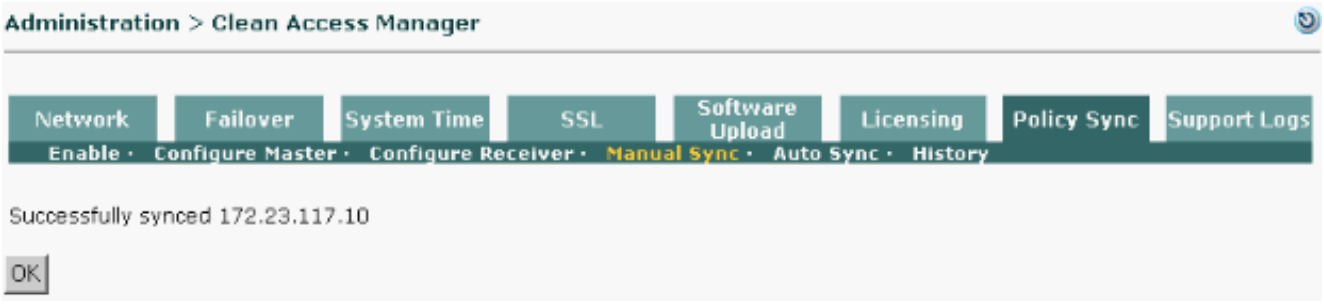


4. En este momento, el master realiza una verificación de integridad del PRE-sincronizar contra el receptor. El control del PRE-sincronizar se asegura de que configuren a los administradores del NAC del master y del receptor correctamente (avanzar y recibir las directivas), y que la información de autorización está correcta, etc. Si hay alguna configuración o errores de la autorización, el control del PRE-sincronizar falla con los

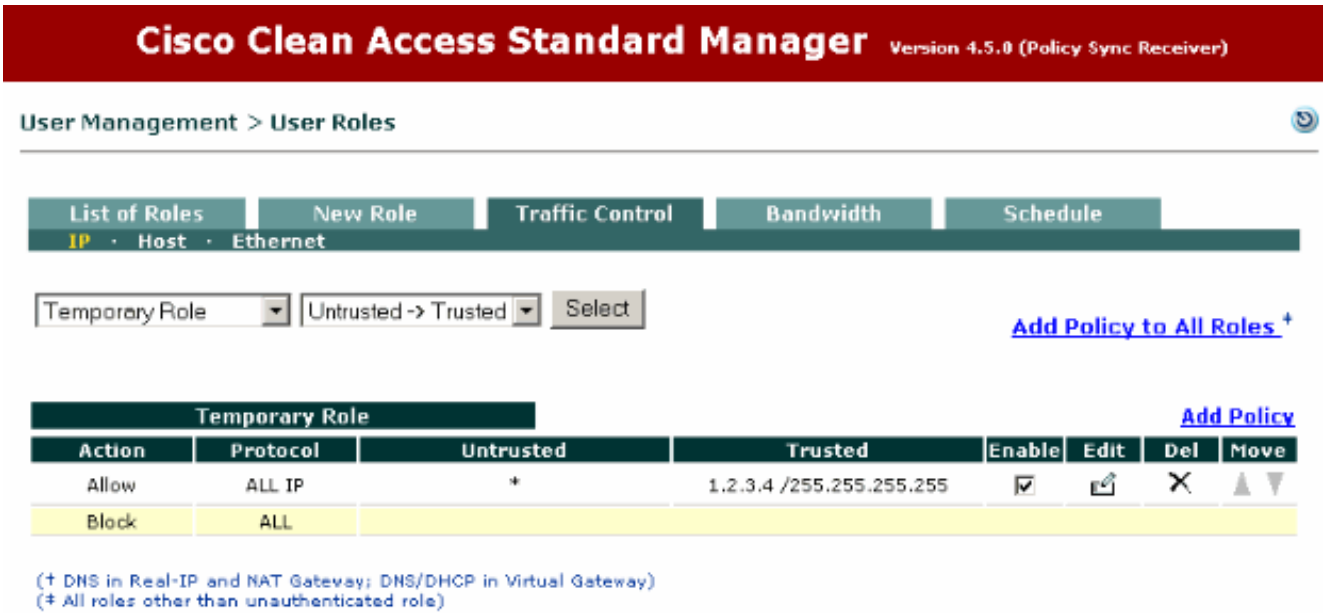
mensajes de error apropiados. Vea la sección del Troubleshooting.

5. Si no hay problemas de la configuración o de la autorización, el master visualiza un acertado PRE-sincroniza el
control.

6. El golpe continúa completando con éxito el
sincronizar.



7. Vaya al administrador del NAC del receptor y verifique que la regla de tráfico está sincronizada.



Troubleshooting

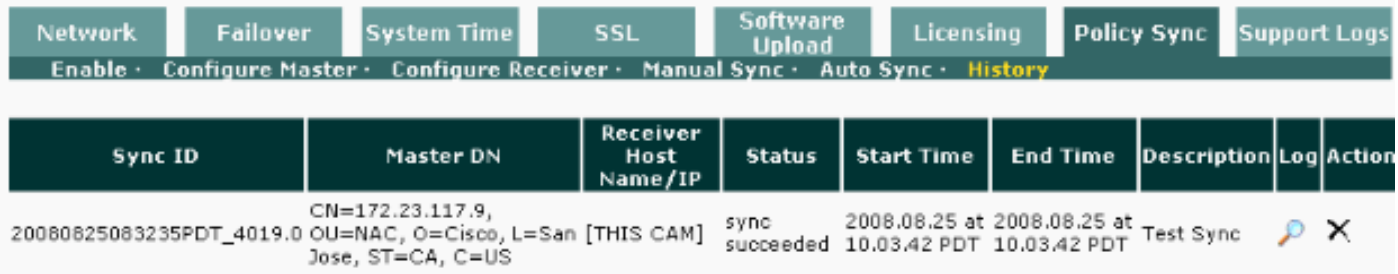
En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Registro

El resumen del sincronizar se registra bajo CCA el administrador > directiva sincroniza > historial en el master y los receptores.

En el administrador principal del NAC:

En el administrador del NAC del receptor:



Haga clic el icono de la lupa bajo orden del login para ver los registros de transacciones detallados:

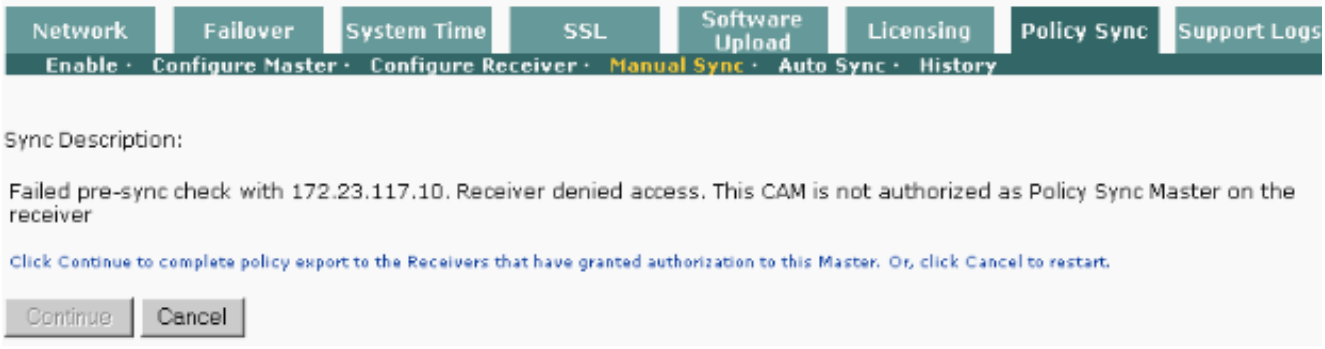
```
*************** Master Log ***************

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.
```

La importación/la exportación de la directiva completada con éxito en la directiva sincroniza el receptor.

Problemas

1. **Acceso negado receptor. Este CAM no se autoriza mientras que la directiva sincroniza al**

master en el receptor.

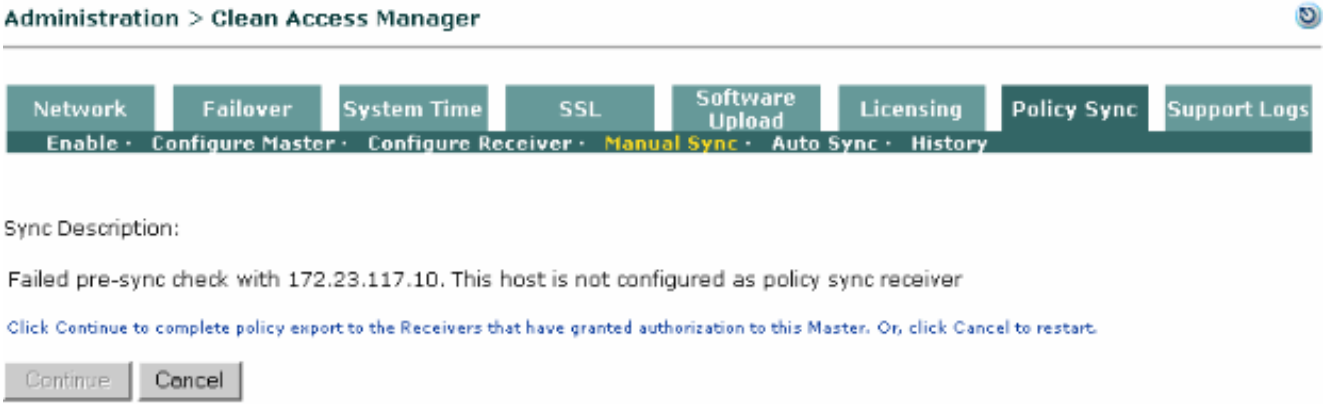


Este error significa típicamente que el receptor rechaza la directiva sincroniza porque la información DN principal se configura mal en el administrador del NAC del receptor. Elija la administración > CCA administrador > directiva sincronizan > receptor de la configuración en el receptor y se aseeguran que “autorizó la información al master” está configurado correctamente.

2. **Este receptor no se autoriza**

Este mensaje significa típicamente que el receptor no está puesto para la autorización o los parámetros de autorización (la información DN del receptor) configurados en el administrador principal del NAC son incorrectos. Elija la administración > CCA administrador > directiva sincronizan > master de la configuración en el master y se aseeguran la información DN del certificado del receptor existe bajo la lista de receptores autorizados por el nombre distintivo del certificado y se configura correctamente.

3. **Este host no se configura mientras que la directiva sincroniza el receptor.**



Este mensaje significa típicamente que el master intenta sincronizar a un host que o no se habilite para la directiva sincronice o no se configura para ser un receptor. Elija la administración > CCA administrador > directiva sincronizan > las configuraciones en el

administrador del NAC que se elige para ser el receptor y asegurar que la directiva sincroniza el cuadro habilitado se marca y que el botón de radio está fijado al receptor (permite la directiva de importación).

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems