

# IPS 5.x y posterior: NTP en el ejemplo de configuración IPS

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Configuración](#)

[Configure a un router Cisco para ser un servidor NTP](#)

[Configure el sensor para utilizar una fuente horaria NTP](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento proporciona una configuración de muestra para sincronizar el reloj seguro del Sistema de prevención de intrusiones (IPS) de Cisco con un servidor de tiempo de la red usando el Network Time Protocol (NTP). Configuran al router Cisco mientras que configuran a un servidor NTP y el sensor IPS para utilizar al servidor NTP (router Cisco) como la fuente horaria.

## [prerrequisitos](#)

### [Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El servidor NTP debe ser accesible del sensor del IPS de Cisco antes de que usted comience esta configuración del NTP.

### [Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo IPS de las Cisco 4200 Series que funciona con la versión de software 7.0 y posterior
- Versión 7.0.1 y posterior expresa del administrador del IPS de Cisco (IME)**Nota:** Mientras que

IME se puede utilizar para monitorear los dispositivos sensores que ejecutan el IPS de Cisco 5.0 y posterior, algo de las nuevas funciones y de las funciones entregadas en IME se soportan solamente en los sensores que ejecutan el IPS de Cisco 6.1 o más adelante.

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.

## Productos Relacionados

Usted puede también utilizar este documento con estas versiones de software y hardware:

- Dispositivo IPS de las Cisco 4200 Series que funciona con las versiones de software 6.0 y anterior
- Versión 6.1.1 expresa del administrador del IPS de Cisco (IME)

## Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## Configuración

### Configure a un router Cisco para ser un servidor NTP

El sensor requiere una conexión autenticada con un servidor NTP si va a utilizar al servidor NTP como la fuente horaria. El sensor soporta solamente el algoritmo de troceo MD5 para la encriptación de claves. Utilice el siguiente procedimiento para activar a un router Cisco para actuar como servidor NTP y para utilizar su reloj interno como la fuente horaria.

Complete estos pasos para configurar a un router Cisco para actuar como servidor NTP:

1. Inicie sesión al router.
2. Ingrese al modo de configuración.`router#configure terminal`
3. Cree la clave ID y el valor de la clave.`router(config)#ntp authentication-key key_ID md5 key_value` La clave ID puede ser un número entre 1 y 65535. El valor de la clave es texto (numérico o carácter). Se cifra más adelante. Por ejemplo:`router(config)#ntp authentication-key 12345 md5 123` **Nota:** El sensor soporta solamente las claves MD5. Las claves pudieron existir ya en el router. Utilice el **comando show running configuration** de marcar para saber si hay otras claves. Usted puede utilizar esos valores para la clave de confianza en el paso 4.
4. Señale la clave que usted acaba de crear en el paso 3 como la clave de confianza (o utilice una clave existente).`router(config)#ntp trusted-key key_ID` La clave de confianza ID es el mismo número que la clave ID en el paso 3. por ejemplo:`router(config)#ntp trusted-key 12345`
5. Especifique la interfaz en el router con quien el sensor comunicará.`router(config)#ntp source interface_name` Por ejemplo:`router(config)#ntp source FastEthernet 1/0`
6. Especifique el número de estrato del master NTP que se asignará al sensor como se muestra aquí:`router(config)#ntp master stratum_number` Por ejemplo:`router(config)#ntp`

`master 6` **Nota:** El número de estrato del master NTP identifica la posición relativa del servidor en la jerarquía NTP. Usted puede elegir un número entre 1 y 15. No es importante para el sensor que le numeran eligen.

## Configure el sensor para utilizar una fuente horaria NTP

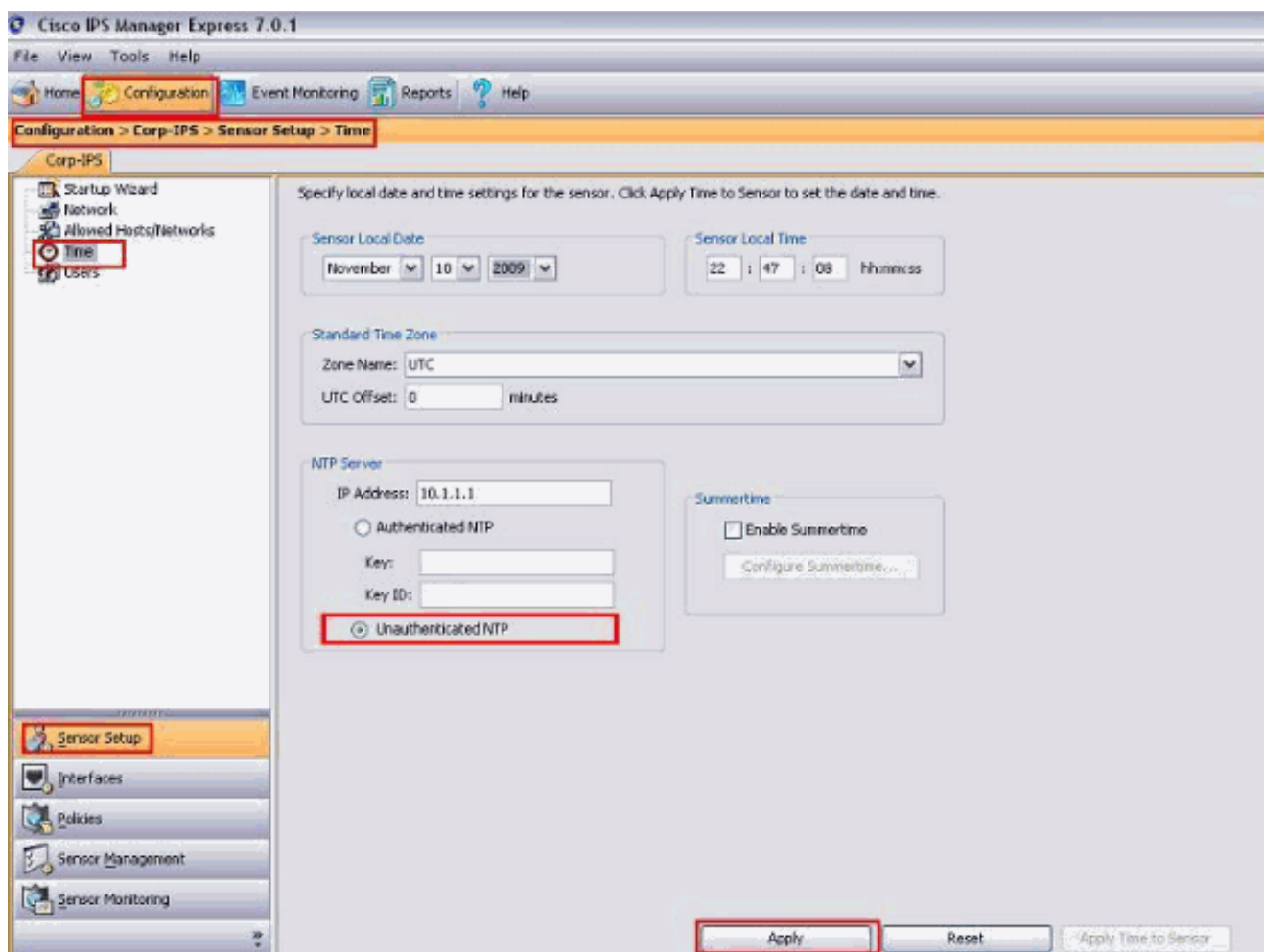
Complete los pasos en esta sección para configurar el sensor para utilizar la fuente horaria NTP (el router Cisco es la fuente horaria NTP en este ejemplo).

El sensor requiere una fuente horaria constante. Se recomienda para utilizar a un servidor NTP. Utilice el siguiente procedimiento para configurar el sensor para utilizar al servidor NTP como su fuente horaria. Usted puede utilizar autenticado o el unauthenticated NTP.

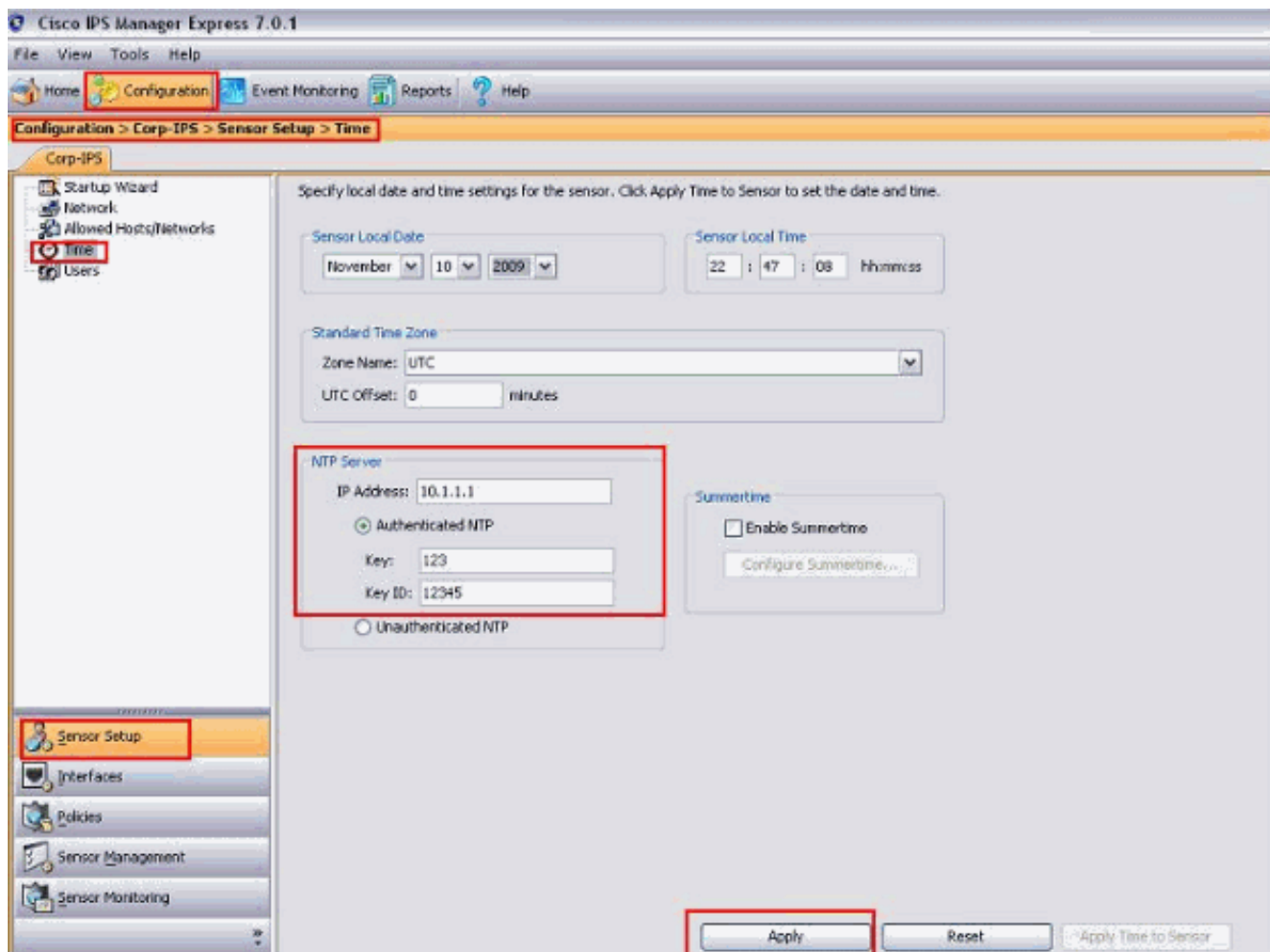
**Nota:** Para el NTP autenticado, usted debe obtener la dirección IP del servidor NTP, el servidor NTP ID dominante, y el valor de la clave del servidor NTP.

Complete estos pasos para configurar el sensor para utilizar a un servidor NTP como su fuente horaria:

1. Inicie sesión al CLI usando una cuenta con los privilegios de administrador.
2. Ingrese al modo de configuración como se muestra aquí:`sensor#configure terminal`
3. Ingrese el modo del host del servicio.`sensor(config)# service host`
4. El NTP se puede configurar según lo autenticado y el unauthenticated NTP. Complete estos pasos para configurar el unauthenticated NTP: Ingrese el modo de la configuración del NTP.`sensor(config-hos)#ntp-option enabled-ntp-unauthenticated` Especifique la dirección IP del servidor NTP.`sensor(config-hos-ena)#ntp-server ip_address` En este ejemplo la dirección IP del servidor NTP es 10.1.1.1.`sensor(config-hos-ena)#ntp-server 10.1.1.1` Éste es el procedimiento para configurar el unauthenticated NTP usando el administrador del IPS de Cisco expreso: Elija la **configuración > el Corp-IPS > el sensor puesto > tiempo**. Entonces, haga clic el botón de radio al lado del **unauthenticated NTP** después de que usted proporcione la dirección IP del servidor NTP tal y como se muestra en del tiro de pantalla. Haga clic en Apply (Aplicar).



Esto completa la configuración del NTP del unauthenticated. Complete estos pasos para configurar el NTP autenticado: Ingrese el modo de la configuración del NTP. `sensor(config-hos)#ntp-option enable` Especifique la dirección IP del servidor NTP y el ID dominante. La clave ID es un número entre 1 y 65535. Ésta es la clave ID esa usted configura ya en el servidor NTP. `sensor(config-hos-ena)#ntp-servers ip_address key-id key_ID` En este ejemplo la dirección IP del servidor NTP es 10.1.1.1. `sensor(config-hos-ena)#ntp-server 10.1.1.1 key-id 12345` Especifique al servidor NTP del valor de la clave. `sensor(config-hos-ena)#ntp-keys key_ID md5-key key_value` El valor de la clave es texto (numérico o carácter). Éste es el valor de la clave ese usted configura ya en el servidor NTP. Por ejemplo: `sensor(config-hos-ena)#ntp-keys 12345 md5-key 123` Éste es el procedimiento para configurar el NTP autenticado usando el administrador del IPS de Cisco expreso: Elija la **configuración > el Corp-IPS > el sensor puesto > tiempo**. Entonces, haga clic el botón de radio al lado del **NTP autenticado** después de que usted proporcione la dirección IP del servidor NTP tal y como se muestra en del tiro de pantalla. Proporcione la clave y la clave ID que deben ser lo mismo como se menciona en el servidor NTP. En este ejemplo la clave es 123 y la clave ID es 12345. Haga clic en Apply (Aplicar).



Esto completa la configuración del NTP autenticada.

5. Dé salida al modo de la configuración del NTP.`sensor(config-hos-ena)# exit`

```
sensor(config-hos)# exit
```

```
Apply Changes:[yes]
```

6. Presione ENTER para aplicar los cambios o a ingresar **no** para desecharlos. Esto completa la tarea de configuración.

## Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

Verifique las configuraciones autenticadas NTP. Esto se asegura que la configuración del NTP autenticada está hecha correctamente.

```
sensor(config-hos-ena)#show settings enabled -----
ntp-keys (min: 1, max: 1, current: 1) ----- key-id:
12345 ----- md5-key: 123 -----
----- ntp-servers (min: 1, max: 1,
current: 1) ----- ip-address: 10.1.1.1 key-id: 12345 -
-----
sensor(config-hos-ena)#
```

Para visualizar el contenido de la configuración contenida en el submode actual, utilice las [configuraciones de la demostración](#) ordenan en cualquier modo de comando `service`. Esto verifica que la configuración del NTP del unauthenticated esté hecha correctamente.

```
sensor(config-hos-ena)#show settings enabled-ntp-unauthenticated -----  
----- ntp-server: 10.1.1.1 -----  
sensor(config-hos-ena)#
```

Para visualizar el reloj del sistema, utilice el [comando show clock](#) en el modo EXEC como se muestra. Este ejemplo muestra el NTP configurado y sincronizado:

```
sensor#show clock detail 11:45:02 CST Tues Jul 20 2011 Time source is NTP sensor#
```

## [Troubleshooting](#)

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## [Información Relacionada](#)

- [Página de soporte del Cisco Intrusion Prevention System](#)
- [Página de soporte expresa del administrador del IPS de Cisco](#)
- [Network Time Protocol \(NTP\)](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)