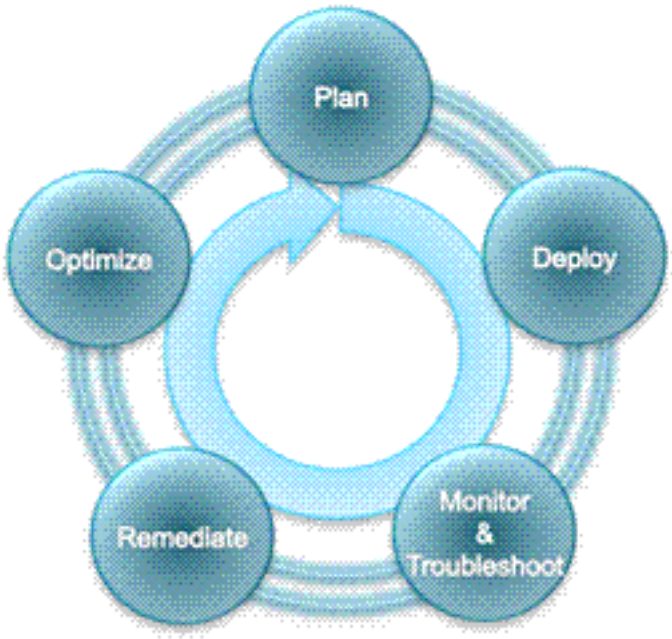
# Guía de despliegue de la prima NCS 1.1 de Cisco

## Contenido

# Introducción

Cisco Prime Network Control System (NCS) es la próxima generación de la plataforma de administración de red de Cisco para gestionar redes de acceso de red alámbrica/inalámbrica.




Administración del ciclo vital de la red inalámbrica (WLAN): La Administración completa del ciclo vital de la red inalámbrica (WLAN) incluye una gama completa de hojas de operación (planning), de despliegue, de supervisión y de troubleshooting, de corrección y de optimización.

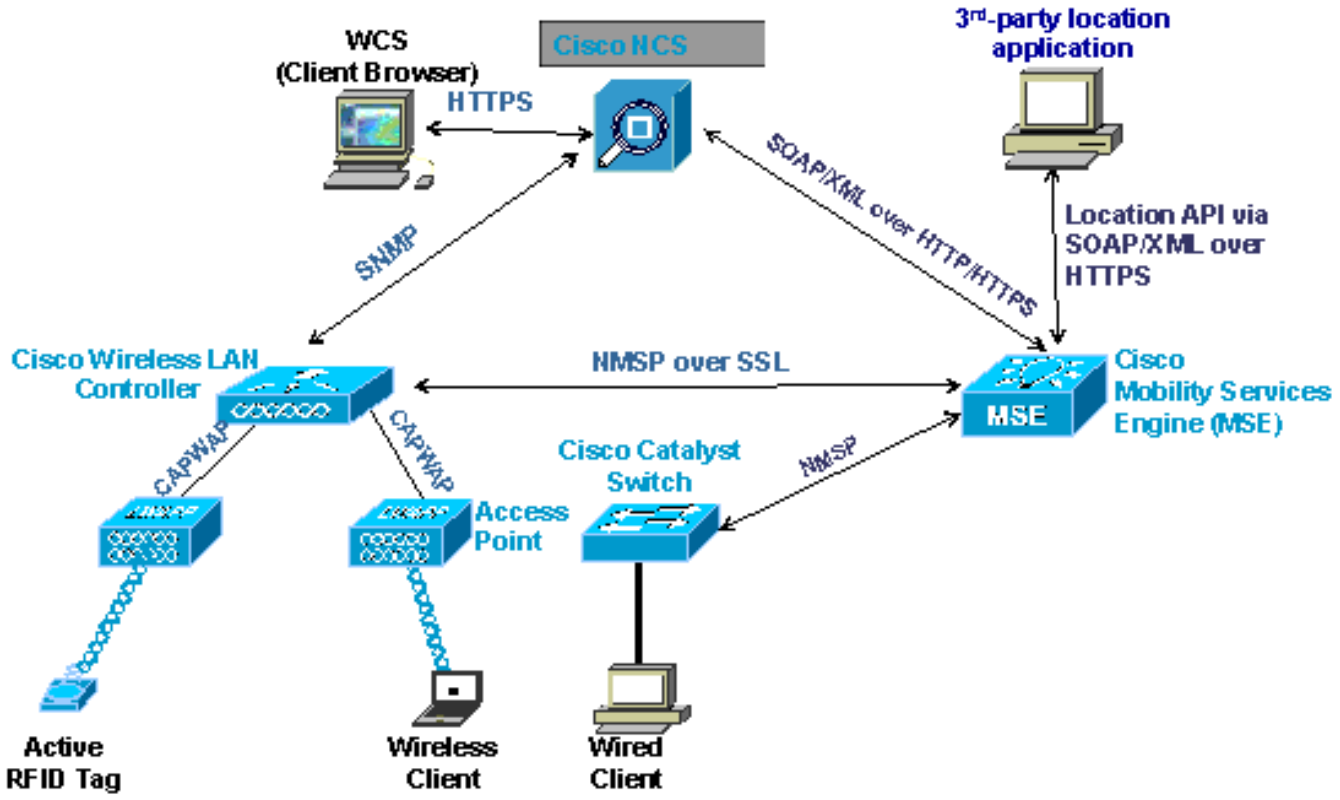
- Planificación — Las hojas de operación (planning) incorporadas y las herramientas de diseño simplifican la definición de la colocación y de la cobertura del Punto de acceso. Además, la información de las herramientas de tercera persona del estudio sobre el sitio se puede

importar en Cisco NCS para ayudar en el diseño de WLAN y el despliegue.

- Despliegue — Un conjunto amplio de las plantillas integradas del regulador y de la Configuración de punto de acceso entrega las implementaciones rápidas y rentables. La auditoría de la red se utiliza para la administración de la configuración eficaz. NCS también proporciona a las herramientas para ayudar en la supervisión, actualizando, y los Puntos de acceso (autónomos) independientes de la migración Cisco Aironet para actuar como los Puntos de acceso ligeros y funcionamiento CAPWAP. el control de acceso Papel-basado proporciona a la flexibilidad para dividir la red inalámbrica en segmentos en uno o más dominios virtuales controlados por una sola plataforma de Cisco NCS.
- Supervisión y troubleshooting — La supervisión centralizada de las ayudas enteras de la red inalámbrica (WLAN) mantiene el funcionamiento robusto de la red inalámbrica (WLAN) y una experiencia inalámbrica óptima. Cisco CleanAir proporciona a la información detallada sobre los eventos de interferencia RF, la calidad del aire, y las amenazas de seguridad de interferencia para ayudar más eficientemente a evaluar, a dar prioridad, y a manejar a los problemas de interferencia RF. Las visualizaciones gráficas fáciles de usar sirven como punto de partida para el mantenimiento, la Seguridad, el troubleshooting, y la planificación de capacidad futura. Los gráficos, las cartas, y las tablas son interactivos para la configuración rápida y la reconfiguración. Los árboles jerárquicos, la codificación policromática, y los iconos de la asignación utilizan las evaluaciones rápidas de la visualización y del estatus de la red, de los dispositivos, y de la calidad del aire. El resumen omnipresente de la alarma proporciona al incidente, al evento, y a la Administración de alarma robustos. La Herramienta de búsqueda persistente facilita el acceso de la cruz-red a la información inmediata e histórica sobre los dispositivos y los activos situados dondequiera en la red de acceso, incluyendo los atributos de la punto final y de sesión, el historial de la asociación, la Ubicación de punto final, el funcionamiento RF, las estadísticas, el Administración de recursos de radio (RRM), y la calidad del aire. Una herramienta incorporada del troubleshooting del cliente proporciona a un método gradual para analizar los problemas para toda la haber atado con alambre y dispositivos de red inalámbrica de cliente. Las ayudas robustas de esta del cliente herramienta del troubleshooting reducen los costos operativos apresurando la resolución de los ticketes de problemas para una variedad de tipos de dispositivo cliente del Wi-Fi.

### El papel de NCS en la red

Esta figura representa la arquitectura de red inalámbrica de Cisco con la prima NCS de Cisco. Las interacciones entre los diversos elementos de red, que son regulador inalámbrico LAN, AP, conmutador del Cisco Catalyst, Servicios de movilidad motor, Sistema de control de redes, estación de administración del Client Network, y aplicación de terceros.




## Puertos usados por NCS

| Source Device | Destination Device | Protocol | Destination Port | Description |
|---|---|---|---|---|
| NCS | WLC and MSE | TCP | 21 | FTP - Used to transfer files to/from devices |
| Various Management Stations | NCS Host Server OS-Linux | TCP | 22 | SSH - Used for remote Host Access |
| NCS | a IOS AP | TCP | 23 | Telnet - Used for a IOS AP Configuration |
| NCS | SMTP mail servers | TCP | 25 | SMTP – used for fault notifications |
| AAA Servers | NCS | TCP/UDP | 49 | TACACS+ |
| NCS | a IOS AP | UDP | 53 | DNS – used for a IOS AP Configuration |
| WLC | NCS | UDP | 69 | TFTP - Used to transfer files to/from devices |
| Various Management Stations | NCS | TCP | 80 | HTTP (Configurable at install time) |
| NTP Server | WLC | UDP | 123 | NTP |
| WLC and MSE | NCS | UDP | 161 | SNMP discovery, inventory a IOS AP and others |
| WLC and MSE | NCS | UDP | 162 | SNMP Trap Receiver |
| Various Management Stations | NCS | TCP | 443 | HTTPS (Configurable at install time) |
| MSE | NCS | TCP | 443 | SOAP/XML (Simple Object Access Protocol Used for MSE Management |
| WLC | NCS | UDP | 514 | Syslog (Optional) |
| NCS HA Server | NCS | TCP | 1522 | HA DB Port |
| AAA Servers | NCS | UDP | 1812 / 1645 | RADIUS |
| AAA Servers | NCS | UDP | 1813 / 1646 | RADIUS |
| MSE | NCS | TCP | 8001 | MSE Data Sync. Communication Port |
| HA Web Server | NCS | TCP | 8082 | HA Web Server Port: Health Monitor for NCS HA |
| Various Management Stations | NCS | TCP | 8456 | HTTP Connector |
| Various Management Stations | NCS | TCP | 8457 | HTTP Redirect |
| Various Management Stations | NCS | TCP | 16113 | NMSP TLS Port |

## Ayuda y versiones de software del dispositivo

| Tipo de dispositivo | Software admitido Version* |
|---|---|
| Cisco Catalyst 2000 Series Switch: 2960, 2975 | Independiente de la versión de software del ® del Cisco IOS |
| Cisco Catalyst 3000 Series Switch: 3560, 3750-E, 3750-X | Independiente de la versión de software del Cisco IOS |

| | |
|---|---|
| Cisco Catalyst 4500 Series Switch | Independiente de la versión de software del Cisco IOS |
| Cisco Catalyst 6000 Series Switch | Independiente de la versión de software del Cisco IOS |
| Cisco 2x00, 4x00, red inalámbrica (WLAN) integrada de 5500 reguladores inalámbricos (WLCM, WiSM, WiSM2) | 4.2.x, 6.x, 7.x |
| Cisco Aironet APs autónomos | Cisco IOS Software Release 12.3(7)JA y Posterior |

* - las versiones de software utilizadas del regulador se enumeran en los Release Note NCS.

NCS tiene dos Opciones de instrumentación:

1. dispositivo de la dotación física
2. dispositivo virtual

El dispositivo virtual es un fichero de los HUEVOS que se puede desplegar en VMware ESX/ESXi 4.x y 5.0. Esta tabla proporciona a los números de la escala para los dispositivos manejados por NCS.

| Escala de plataforma | | | | |
|---|---|---|---|---|
| | AP unificados | aIOS AP | Switches | Reguladores inalámbricos LAN |
| Pequeño dispositivo virtual | 3,000 | 1,000 | 1,000 | 240 |
| Dispositivo virtual medio | 7,500 | 2,500 | 2,500 | 600 |
| Dispositivo virtual grande | 15,000 | 5,000 | 5,000 | 1,200 |

Note: La escala de plataforma numera para los reguladores inalámbricos LAN (WLC; s) es escala máxima. WLCs no cuenta contra la cuenta de la licencia NCS.

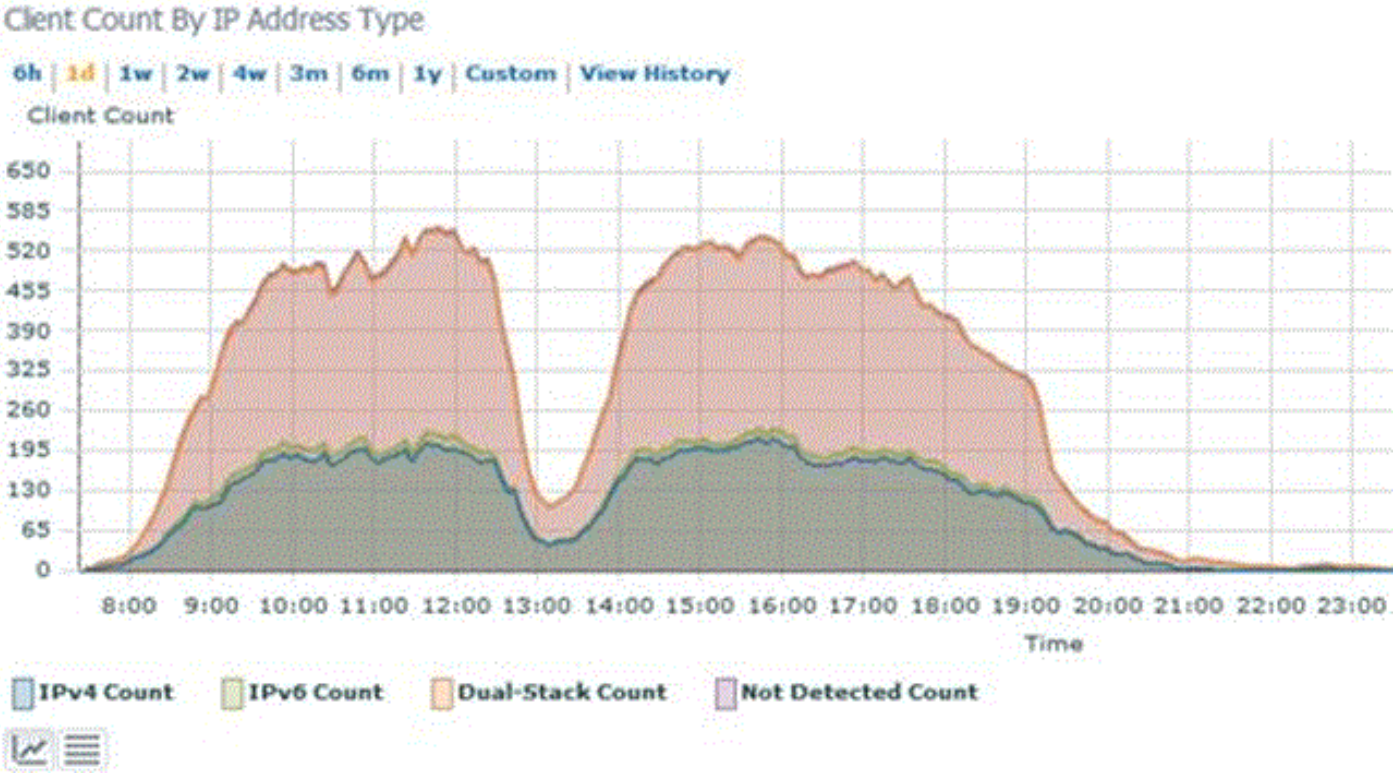
Esta tabla enumera los requisitos de hardware para el dispositivo virtual basado en la escala atada con alambre/inalámbrica.

| Dispositivo virtual – Requisitos de hardware | | | |
|---|---|---|---|
| | Procesador | DRAM | Disco duro |

| | | | |
|---|---|---|---|
| **Pequeño dispositivo virtual** | 2 memorias @ 2.93GHz | 8 GB | 200 GB |
| **Dispositivo virtual medio** | 4 memorias @ 2.93GHz | 12 GB | 300 GB |
| **Dispositivo virtual grande** | 8 memorias @ 2.93GHz | 16 GB | 400 GB |

### Home Page NCS

NCS 1.1 proporciona a la capacidad de vigilar a los clientes del IPv6. Un nuevo dashlet del Home Page, cuenta del cliente por el tipo de la dirección IP, proporciona a un indicador visual de los clientes basados en el tipo de la dirección IP. `No detectado` refiere a los clientes cuya dirección IP no puede ser resuelta; clientes típicamente atados con alambre en caso de que la vigilancia del tráfico del IPv6 no sea disponible/utilizada en el dispositivo.




### Ayuda del navegador

NCS 1.1 utiliza a estos navegadores:

- 3.6 y posteriores de Firefox
- Google Chrome 12.0.742.x
- Microsoft Internet Explorer con el enchufe de Chrome**Note**: No apoyan al Internet Explorer nativo.

Este documento proporciona a la comprensión y a la guía para el diseño arquitectónicas para las implementaciones NCS.

## Prerequisites

## Requisitos

No hay requisitos específicos para este documento.

## Componentes usados

La información en este documento se basa en la prima NCS 1.1 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

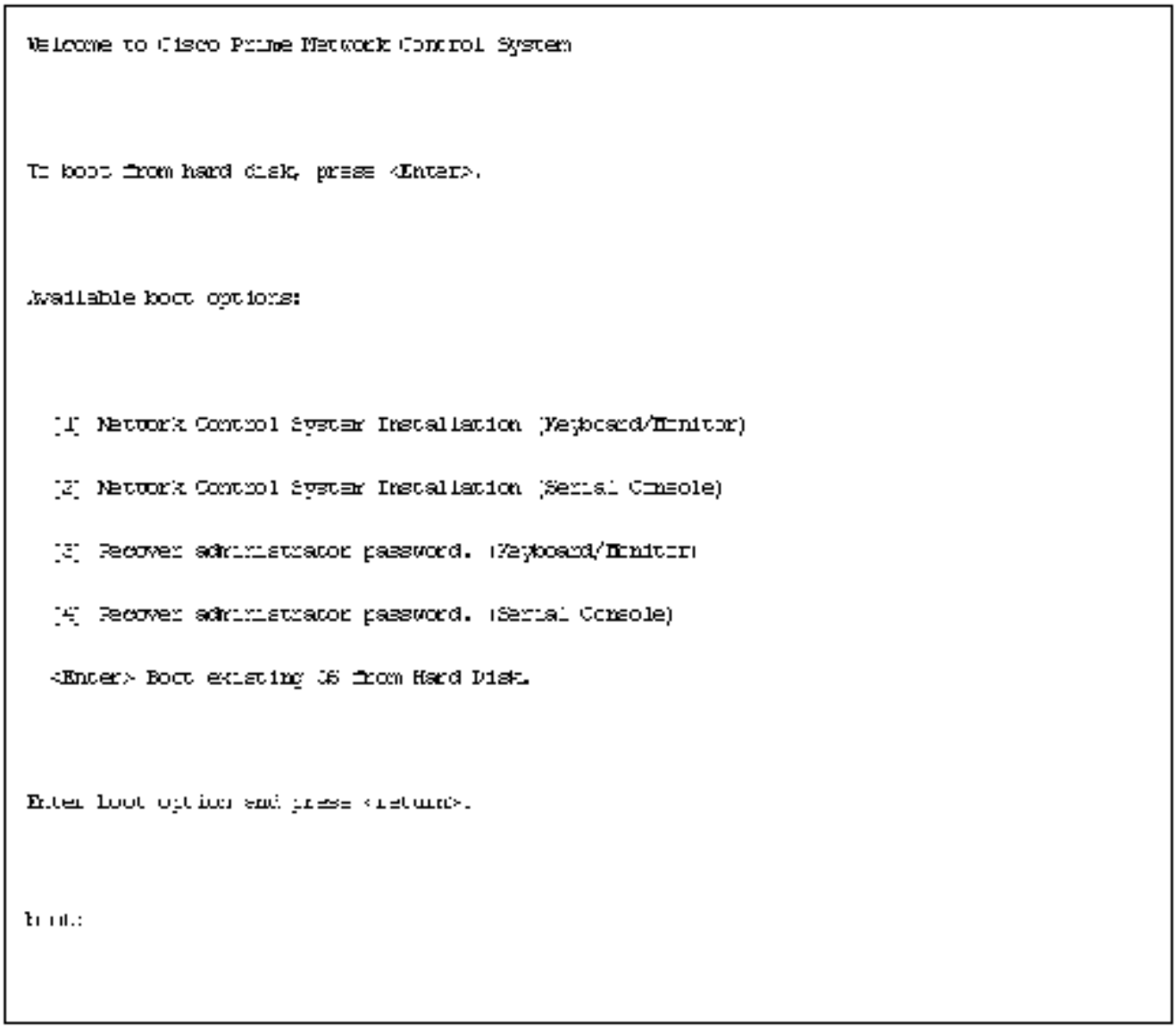
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

# Instalación

## Dispositivo físico: Instalación ISO

NCS está disponible como dispositivo físico y virtual. Esta sección proporciona a los pasos para instalar la imagen ISO en un dispositivo físico.

1. Transferencia directa y quemadura ISO al DVD. El ISO se fija en el software de la transferencia directa (clientes registrados solamente). Utilice su nombre de usuario y contraseña de Cisco.com.
2. Instale el ISO. Reinicie la máquina con el ISO insertado. Esta ventana aparece. Elija la opción 1 o 2, que depende de cómo usted está conectado con el dispositivo




3. La instalación tarda aproximadamente 30 minutos para completar. Después de que la imagen ISO esté instalada, el servidor reinicia. Después de que su dispositivo reinicie, vaya a la sección de configuración física/virtual del dispositivo.

## Dispositivo virtual: Instalación de los HUEVOS de VMware

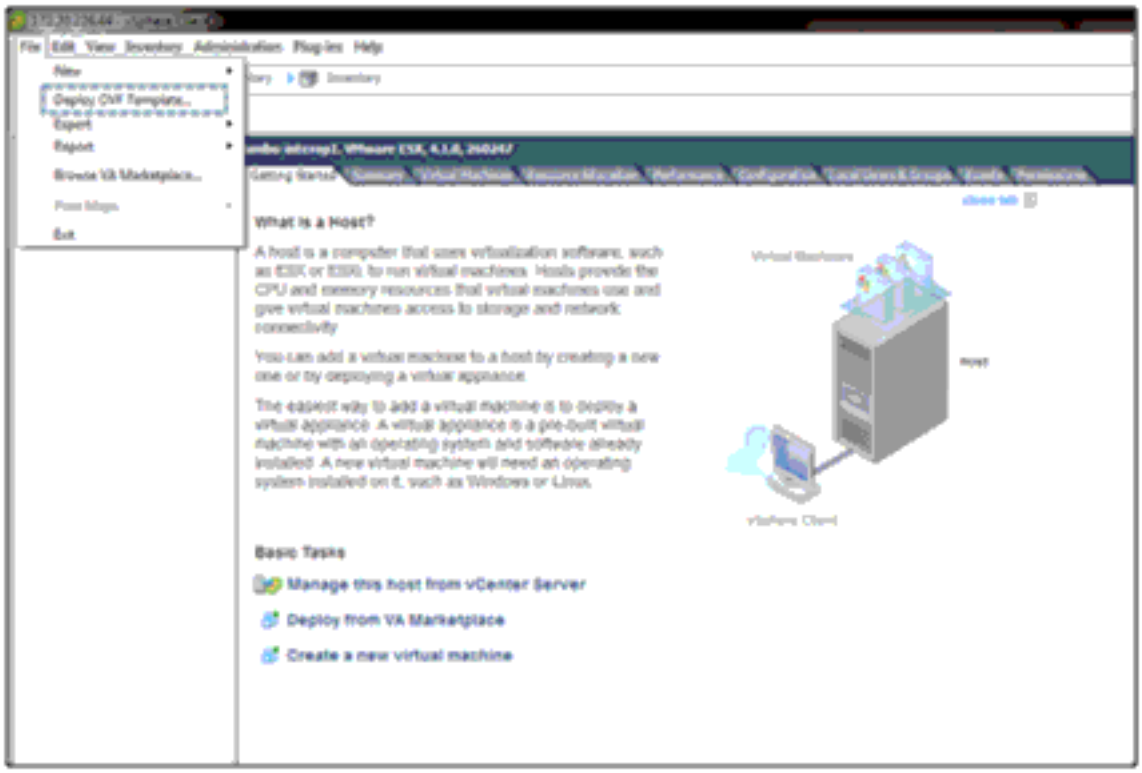
Complete estos pasos en esta sección para desplegar los HUEVOS en VMware ESX/ESXi 4.x. Después de que los HUEVOS hayan estado instalados, continúe con la sección de configuración física/virtual del dispositivo. El tiempo que toma para desplegar varía basado sobre la velocidad de la conexión de la red al host ESX.

Despliegue el fichero de los HUEVOS. Los HUEVOS se fijan en el software de la transferencia directa (clientes registrados solamente). Descargue los HUEVOS apropiados basados en el número de dispositivos que es manejado por este servidor NCS.

## Utilice al cliente del vSphere para instalar los HUEVOS

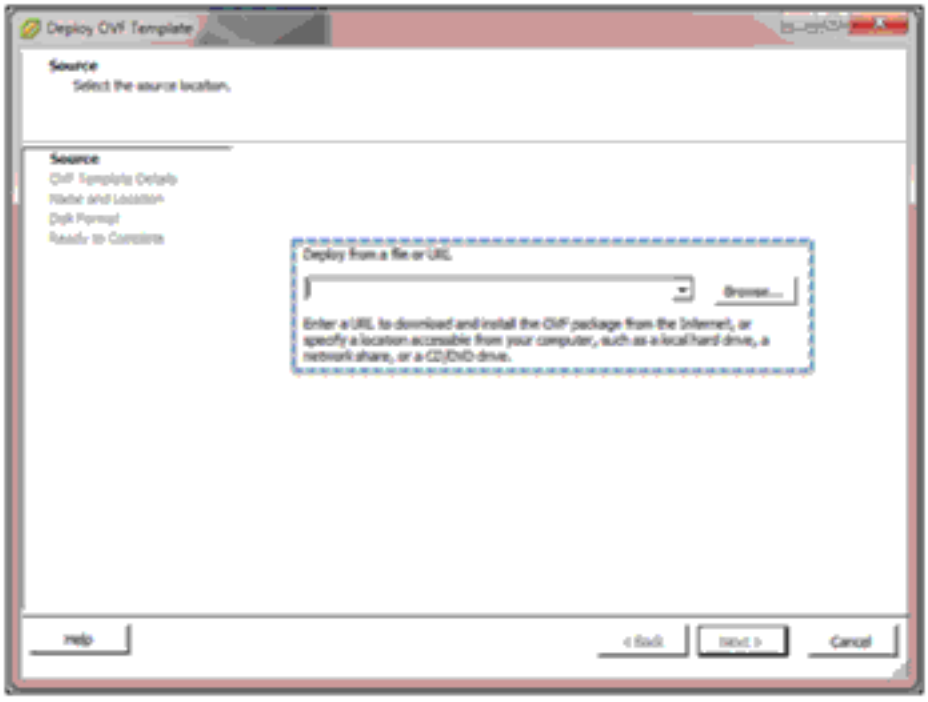
Complete estos pasos:

1. Lance al cliente del vSphere de VMware. Elija el **fichero > despliegan la plantilla**



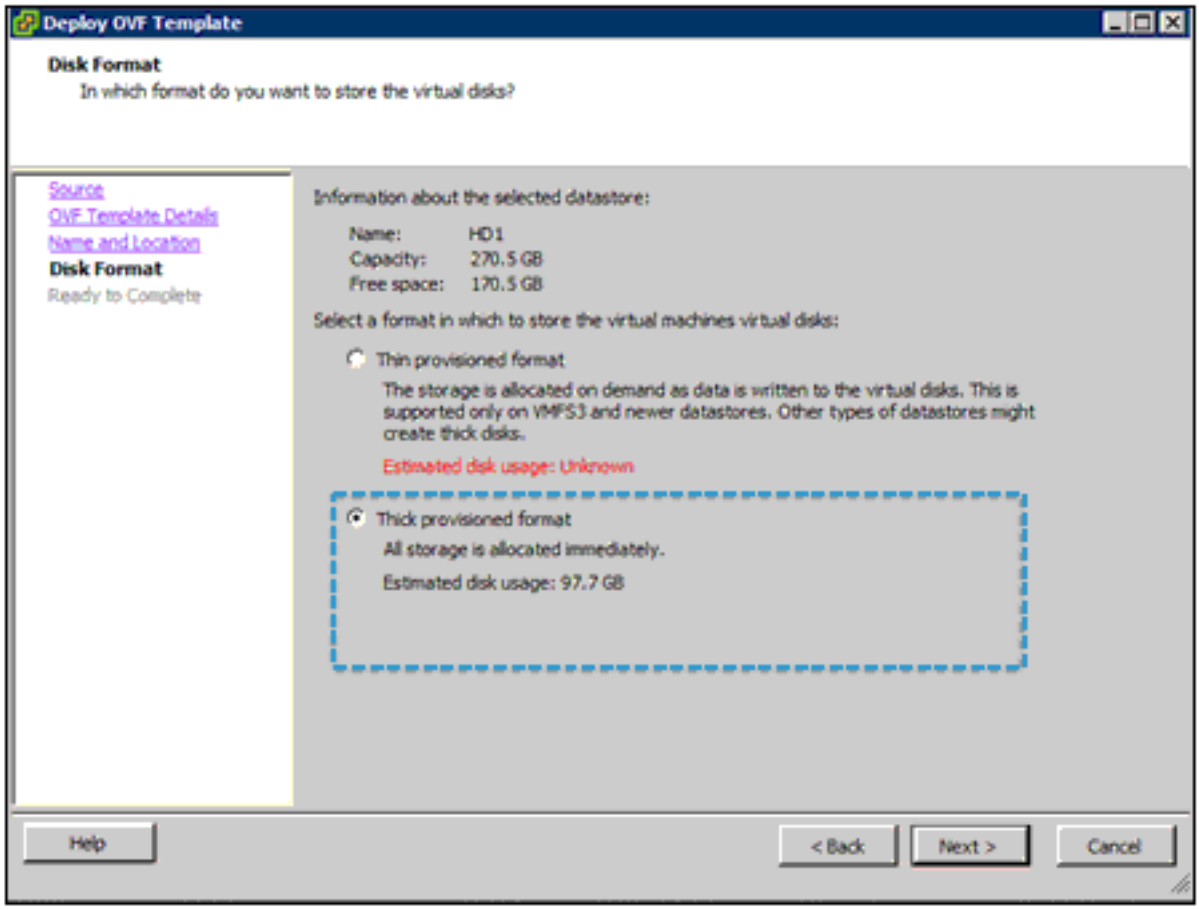

**OVF**. Se empaqueta la imagen NCS VMware mientras que los HUEVOS (archivo abierto de la virtualización) clasifían. El elemento de menú en el tiro de pantalla anterior está para una plantilla OVF. Los HUEVOS son una colección de items en un solo archivo. Estos items consisten en típicamente un fichero de la descripción de la máquina virtual (*.ova), un archivo de manifiesto (*.mf), y el fichero virtual de la unidad de disco duro (*.vmdk).

2. Elija **hojean** y localizan el fichero de los HUEVOS NCS. Haga clic en Next




(Siguiente).

3. Después de que se seleccione el fichero de los HUEVOS, VMware ESX/ESXi lee los atributos del archivo de los HUEVOS. Continúe con los pasos para eligió los HUEVOS clasifían que usted quiere instalar en ESX/ESXi. En la página del formato del disco, elija la opción **disposición gruesa del formato**.




4. La página de resumen enumera las opciones que fueron elegidas. Haga clic en Next (Siguiente). Reinicializaciones NCS. Después de que se haya construido la máquina virtual, aparece en el lado izquierdo de la ventana. Para lanzar la máquina virtual, elíjala del menú izquierdo que enumera las máquinas virtuales instaladas y haga clic el icono **abierto de la consola**. A este punto, NCS está instalado como máquina virtual. El resto de los pasos de la disposición es idéntico para una máquina física y virtual.

## Mejora física/virtual del dispositivo

Complete estos pasos:

1. Obtenga el URL de la ubicación del fichero en donde la imagen de actualización NCS se salva en el servidor. Funcione con estos comandos para actualizar la instalación NCS:
```
ncs1/admin# ncs stop
Stopping Network Control System...
This may take a few minutes...
Network Control System successfully shutdown.
```
2. Una vez que se ha parado NCS, ingrese el modo de la configuración y coloque el URL de la ubicación del fichero en el depósito:
```
ncs1/admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ncs1/admin(config)# repository NCS58
ncs1/admin(config-Repository)# url http://xxxx/sanity/1.X.X.10/wcs-cars-appbundle/
ncs1/admin(config-Repository)# exit
ncs1/admin(config)# exit
```
3. Verifique que el repositorio tenga acceso al archivo especificado con el URL anterior:
```
ncs1/admin# show repository NCS58
ncs-upgrade-bundle-1.1.0.58.tar.gz
```
4. Funcione con estos comandos para iniciar el proceso de actualización del repositorio.
```
ncs1/admin# application upgrade ncs-upgrade-bundle-1.1.0.58.tar.gz NCS58
```

```
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
```

5. Un mensaje debe aparecer que indica que el proceso de actualización es completo ahora.

### Comenzar NCS

Después de que el servidor reinicie, registre en el sistema como admin usando la contraseña a que usted proporcionó como parte del paso de la disposición. Después de que usted haya registrado en el servidor, encienda el servidor NCS con `admin@ncs-server para optar] # comando start de los ncs`.

Los mensajes de la consola indican cuando NCS se está ejecutando. Registro en su servidor NCS vía el buscador Web como raíz de usuario con la contraseña que usted eligió durante la instalación. La contraseña de raíz puede ser cambiada después de que usted registre en NCS con la clave del navegador.

### Migración del WCS a NCS

Usted debe actualizar su servidor de Cisco WCS a una de estas versiones antes de que usted intente realizar el proceso de migración a NCS 1.1.x.x.

- 7.0.164.3
- 7.0.172.0
- 7.0.220.0

Esta sección proporciona a las instrucciones para que cómo emigre el WCS en Windows o el servidor Linux a NCS. La versión NCS es una versión principal a prever la Administración convergida de atado con alambre y los dispositivos de red inalámbrica, y capacidad de conversión a escala creciente. La plataforma NCS se basa en el OS del bit de Linux 64, y la base de datos backend es el Oracle DBMS. Las Plataformas existentes WCS son o Windows o Linux 32 mordido y la base de datos backend es DB sólido.

## Migración de datos del WCS

### Datos de la exportación del WCS

Exporte los datos de WCS 7.x con el CLI. El comando CLI del **userdata de la exportación** está disponible en la versión 7.x WCS y más adelante, que crea el fichero .zip que contiene el archivo de datos WCS. El CLI no proporciona a ninguna opción para personalizar qué puede ser exportada; se exportan todos los items definidos por el usario no-globales. Complete estos pasos para exportar los datos WCS:

1. Pare el servidor WCS.
2. Funcione con el comando de la **exportación** a través del archivo de secuencia de comandos y proporcione a la trayectoria y exporte el nombre de fichero cuando está incitado.
3. Para Linux, ejecute export.sh todo el comando de /data/wcs.zip. Para Windows, funcione con el export.bat todo \ el comando de los datos \ wcs.zip.

### Datos de la migración WCS a NCS

Complete estos pasos para emigrar los datos WCS:

1. Coloque el fichero de la exportación .zip WCS (por ejemplo, wcs.zip) en un repositorio o una carpeta (por ejemplo, los repositorios).
2. Ábrase una sesión como usuario admin y pare el servidor NCS ingresando el **comando stop de los ncs**. Configure el repositorio FTP en el dispositivo NCS con el **comando repository**:
   ```
   ncs-appliance/admin#configure
   ncs-appliance/admin(config)# repository ncs-ftp-repo
   ncs-appliance/admin(config-Repository)# url ftp://209.165.200.227//
   ncs-appliance/admin(config-Repository)# user ftp-user password plain ftp-user
   ```

   **Note**: Asegúrese de que el fichero de archivo esté disponible con el comando del **repositoryname del repositorio de la demostración**.
3. Ingrese los **ncs emigran el** comando para restablecer la base de datos WCS.
   ```
   ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
   ```

4. Por abandono, no se emigra ningunos eventos WCS. Ingrese el **comando start de los ncs** para encender el servidor NCS después de que se complete la mejora. Ábrase una sesión a la interfaz de usuario NCS con el inicio de sesión en la raíz y la contraseña de raíz.Estos datos no se emigran del WCS a NCS:Subconjunto de informes — Imagen Predownload AP, estatus del perfil AP, resumen AP, cuenta del cliente, resumen del cliente, tráfico del cliente, informe PCI, informe del resumen detallado y informes del resumen, preferido de la conformidad PCI de la llamada de la red, APs no fiables, granujas ad hoc, nuevos granujas ad hoc y informes del resumen de la Seguridad.Arreglo para requisitos particulares del panelLa información sobre estadísticas de la estación del cliente no se puebla con los viejos datos WCS en las cartas de los clientes, la página de los detalles del cliente, los paneles y los informes.La información de sesión histórica del cliente consigue actualizada.El historial de los eventos salvado en la base de datos WCS no se emigra a NCS.El RADIUS/TACACS IP del servidor y las credenciales no se emigran y necesitan ser agregados otra vez después de que la migración sea completa. Usted necesita copiar los últimos atributos personalizados de NCS e incluirlo en la autenticación de servidor para el usuario AAA/la autorización en el TACACS+/RADIUS.**Note**: Asegúrese de que servidor RADIUS/TACACS esté activado como modo AAA en la página de las configuraciones de modo de la administración >AAA >AAA.Solamente las alarmas con el dominio virtual de la raíz se emigran de la versión 7.0 a NCS.La contraseña de raíz no se emigra de la versión 7.0.164.3 o 7.0.172.0 a la versión 1.1.x.x NCS. El usuario debe cambiar la contraseña de raíz durante la instalación de la aplicación. No emigran a los usuarios raíz y sus credenciales durante la migración.Las categorías y las subcategorías de la alarma no se restablecen después de la migración al resumen de la alarma NCS.

## Mejora NCS de NCS 1.0.x a 1.1

Usted puede actualizar de las versiones 1.0.0.96, 1.0.1.4, 1.0.2.28, y 1.0.2.29 NCS a NCS 1.1.x.x.

Estos items se deben observar antes del proceso de actualización:

- Asegúrese de que usted realice una salvaguardia antes de que usted intente actualizar.
- Alta disponibilidad de la neutralización antes de que usted realice la mejora.
- Cierre NCS antes de que usted realice la mejora. Funcione con el **comando stop de los ncs**

para parar NCS.

Utilice este comando para actualizar de NCS 1.0 a NCS 1.1.x.x:

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

En el comando anterior, **NCS-upgrade-bundle-1.1.x.x.tar.gz** es el fichero del manojo de la mejora, que está disponible en el software de la transferencia directa (clientes registrados solamente). El repositorio usado en el ejemplo, WCS-ftp-**repo**, puede ser cualquier repositorio válido. Éstos son ejemplos de las configuraciones repositorias:

Repositorio FTP:

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

Repositorio SFTP:

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

Repositorio TFTP:

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

## Correspondencias de la importación del WCS

La exportación/la función importar de la correspondencia está disponibles en WCS 7.0. Esta característica se describe detalladamente en la guía de configuración WCS 7.0.

Después de que usted exporte las correspondencias de su servidor WCS, usted puede importar este conjunto de las correspondencias en su servidor NCS. Los pasos para importar sus correspondencias se cubren en la guía de configuración WCS 7.0.

**Note**: Es importante que los APs en su servidor WCS primero están agregados a su servidor NCS antes de importar las correspondencias puesto que los APs en sus correspondencias WCS también se incluyen durante el proceso de la exportación. Los APs que no se han agregado a su NCS sino están presentes en el resultado exportado de las correspondencias del suelo en los errores se visualizan que cuando usted importa esas correspondencias en NCS.

## Alta disponibilidad - Teoría básica de la operación

La puesta en práctica NCS ha en NCS permite para que hasta dos sistemas primarios NCS fallen encima a un (salvaguardia) NCS secundario. Se requiere un segundo servidor que tiene los recursos suficientes (CPU, unidad de disco duro, conexión de red) para asumir el control la operación NCS en caso que el NCS primario falle. Cada instancia de la base de datos en el NCS secundario es un recurso seguro caliente para el NCS primario correspondiente.

La notación que se utiliza para describir primario y los sistemas secundarios es **N: M**, donde N = número de sistemas primarios en funcionamiento y M = número de sistemas secundarios que

están sosteniendo los sistemas primarios.

En NCS, se utilizan estas configuraciones ha:

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

El tamaño del servidor secundario debe ser más grande que o igual al servidor primario, por ejemplo si el servidor primario NCS es HUEVOS medios, después el servidor secundario NCS debe ser HUEVOS medios o grandes.

El primario y el servidor secundario pueden ser una mezcla de un dispositivo físico y virtual. Por ejemplo, si el servidor primario NCS es un dispositivo físico, el servidor secundario puede ser o dispositivo físico o el dispositivo virtual de los HUEVOS grandes, por ejemplo, la Configuración del servidor y el apresto de los HUEVOS grandes es lo mismo que el dispositivo físico.

El control de salud (HM) es un nuevo proceso ejecutado en NCS, eso es el componente primario que maneja la operación ha del sistema. Dividen al HM en estos submódulos múltiples, que manejan un conjunto específico de las funciones:

- HM de la base — responsable de estas tareas:configuración del sistema total hamantiene la máquina de estado para el sistema hapartida/parada del HM y del NCS JVMpartida/parada y monitor de otros submódulos dentro del HMmaneja el registro de los pares primarios/secundariosautentica la sesión del específico del HMtoma todas las decisiones sobre la falla y recuperación
- Golpe de corazón — El submódulo del golpe de corazón es responsable de mantener la comunicación entre el HMs primario y secundario. La comunicación ocurre sobre el HTTPS (el puerto predeterminado es 8082). El valor de agotamiento del tiempo es 2 segundos. Un mecanismo de reintentos se ha ejecutado para revisar el establecimiento de la Conectividad entre el P-HM y el S-HM. Si el HM no recibe una respuesta después de enviar una petición del latido del corazón dentro del período de agotamiento del tiempo de espera, revisa el establecimiento de la comunicación enviando otra petición del latido del corazón. El número total de recomprobaciones es 3. Después de que la comunicación tenga no ser establecida después de que 3 recomprobaciones, la acción apropiada de la toma HMs según los decorados definidos:el servidor primario va abajo: éste es el caso clásico de la Conmutación por falla. En este decorado, cuando el S-HM no recibe los pedidos del latido del corazón 6 segundos (3 recomprobaciones x 2 segundos), inicia el mecanismo de la Conmutación por falla en el NCS secundario.el servidor secundario va abajo: en este decorado, el P-HM no recibe la respuesta del latido del corazón del S-HM por 6 segundos (3 recomprobaciones x 2 segundos). Cuando sucede esto, el P-HM cambia su estado a PRIMARY_ALONE, aumenta las alarmas y cambia en el modo que escucha – esperando para recibir cualquier mensaje del secundario para restablecer el link entre P-HM y el HM del - S.
- Monitor de la aplicación — El submódulo del monitor de la aplicación es responsable de la comunicación con el marco NCS (NCS JVM) en el servidor local extraer la información de estatus. La comunicación está vía el JABÓN sobre el HTTPS.
- Monitor DB — El submódulo del monitor DB configura el DB para la replicación. No es responsable de la replicación sí mismo DB pues esto es realizado vía el protocolo propietario de la replicación de la base de datos.
- Sincronización del fichero — El submódulo de la sincronización del fichero tiene 4 subcomponentes:Fichero Archiver: analiza periódicamente los directorios que buscan los

ficheros se han modificado que. Recoge tales ficheros y los agrega a un archivo comprimido TARAgente de la transferencia de archivos (FTA): responsable de transferir el archivo comprimido TAR de la compresa al destino (el otro servidor, es decir primario a secundario o a secundario a primario).File Upload (Subir archivo) Servlet (FUS): los funcionamientos en el servidor secundario y son las contrapartes al FTA. Cuando recibe un fichero, el FUS lo fluye directamente al extractor del ALQUITRÁN bastante que el fichero en el disco local (evita la actividad del disco innecesaria). El FTA y los FUS comunican sobre el HTTPS.Recolector de estadísticas: guarda las estadísticas de las operaciones de la transferencia de archivos a partir del tiempo que el servidor comienza.

La base de datos NCS es el elemento de almacenamiento de datos de la base del sistema y se debe replicar entre los sistemas primarios y de reserva en el tiempo real del - sin la pérdida de datos. Esto es fundamental a la operación de NCS ha. Los datos se salvan en 1 de 2 maneras:

1. Base de datos NCS
2. Datos de aplicación

Los datos de aplicación son un conjunto de los archivos planos que contiene estos datos:

- fichero de la contraseña de la base de datos: replicado en el tiempo real (11 segundos)
- Archivos de licencia NCS: replicado vía el Batch Processing (Procesamiento por lote) (cada 500 segundos)
- todos los ficheros conforme al directorio raíz de tftp: replicado vía el Batch Processing (Procesamiento por lote) (cada 500 segundos)
- informes creados programados: replicado en el tiempo real (11 segundos)

Control de salud: el control de salud (HM) es el componente primario que maneja/vigila la Disponibilidad ha del sistema. Hay los submódulos múltiples que manejan las diversas funciones con el HM.

HM de la base: responsable de estas negociaciones:

- Configura el sistema ha
- Mantiene la máquina de estado para el sistema HW
- HM partida/parada
- Partida/parada y vigile otros submódulos dentro del HM
- Maneja el registro de los pares primario-secundarios
- Toma todas las decisiones con respecto a la falla y recuperación

## Operación de la Conmutación por falla

Después de la implementación inicial de NCS, la configuración entera de NCS primario se replica al host del NCS secundario. Durante el funcionamiento normal (es decir NCS primario es operativo), la base de datos de primario se replica a NCS secundario.

Además de la replicación de la base de datos, los ficheros de los datos de aplicación también se replican al NCS secundario. La frecuencia de la replicación es 11 segundos (el tiempo real del - clasifía) y 500 segundos (archivos por lote).

## Requisitos NCS para usar la característica NCS ha

El cliente debe funcionar con la misma versión NCS en los servidores primarios y secundarios

NCS. La característica NCS ha es transparente al regulador inalámbrico, es decir no hay requisito de versión de software para WLC, los AP y MSE.

## Configuración de la característica ha

Estos parámetros se deben configurar en el NCS primario:

- nombre/dirección IP de NCS secundario
- dirección de correo electrónico del administrador de la red para la notificación del sistema
- opción del manual o de la falla automática

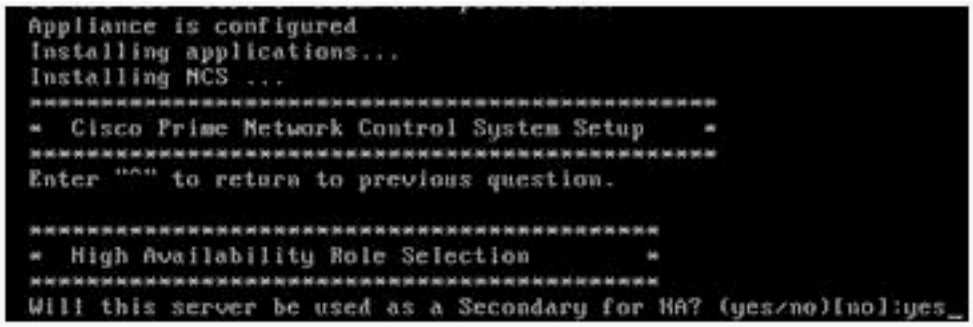
NCS secundario debe siempre ser una nueva instalación y esta opción se debe seleccionar durante NCS instala el proceso. Por ejemplo, NCS independiente o primario no se puede convertir a NCS secundario. NCS independiente se puede convertir a la ha primaria.

**Note**: La replicación de la base de datos entre P-NCS y S-NCS utiliza el puerto 1522, así que asegúrese de que este puerto esté abierto en todos los dispositivos de red, tales como Firewall, Switches, Routers y así sucesivamente, a lo largo del trayecto de red entre los servidores primarios y secundarios NCS.

## Ejemplo – Instalación y proceso de configuración

En este ejemplo, esto es un sistema de 1:1 NCS ha

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```



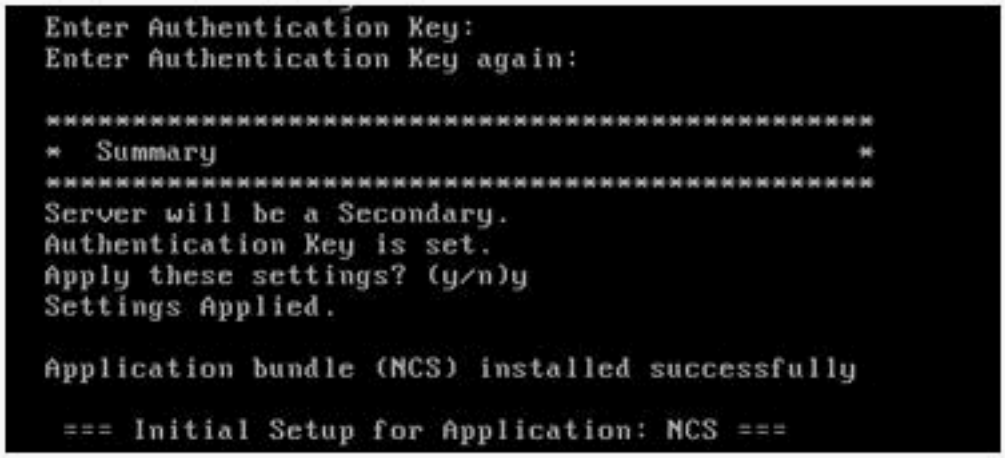

El primer paso es instalar y configurar el NCS secundario. Al configurar el NCS primario para la ha, el NCS secundario necesita ser instalado y accesible por el NCS primario.

**Note**: Un punto clave a recordar es que cuando P-NCS se está ejecutando/operativo, S-NCS no se está ejecutando. Cuando el servidor secundario está en el modo de reserva, estos servicios se están ejecutando en el servidor secundario: HM, Apache y base de datos. Cuando P-NCS va a un estado inactivo, el HM en el servidor secundario comienza el proceso NCS JVM. Entonces hace solamente S-NCS llegan a ser accesible.

El puerto del control de salud necesita poner en la máquina de la instalación de la blanco NCS. El valor de puerto predeterminado es el puerto 8082. Este número del puerto tiene solamente significación de la máquina local (puerto de la máquina local).

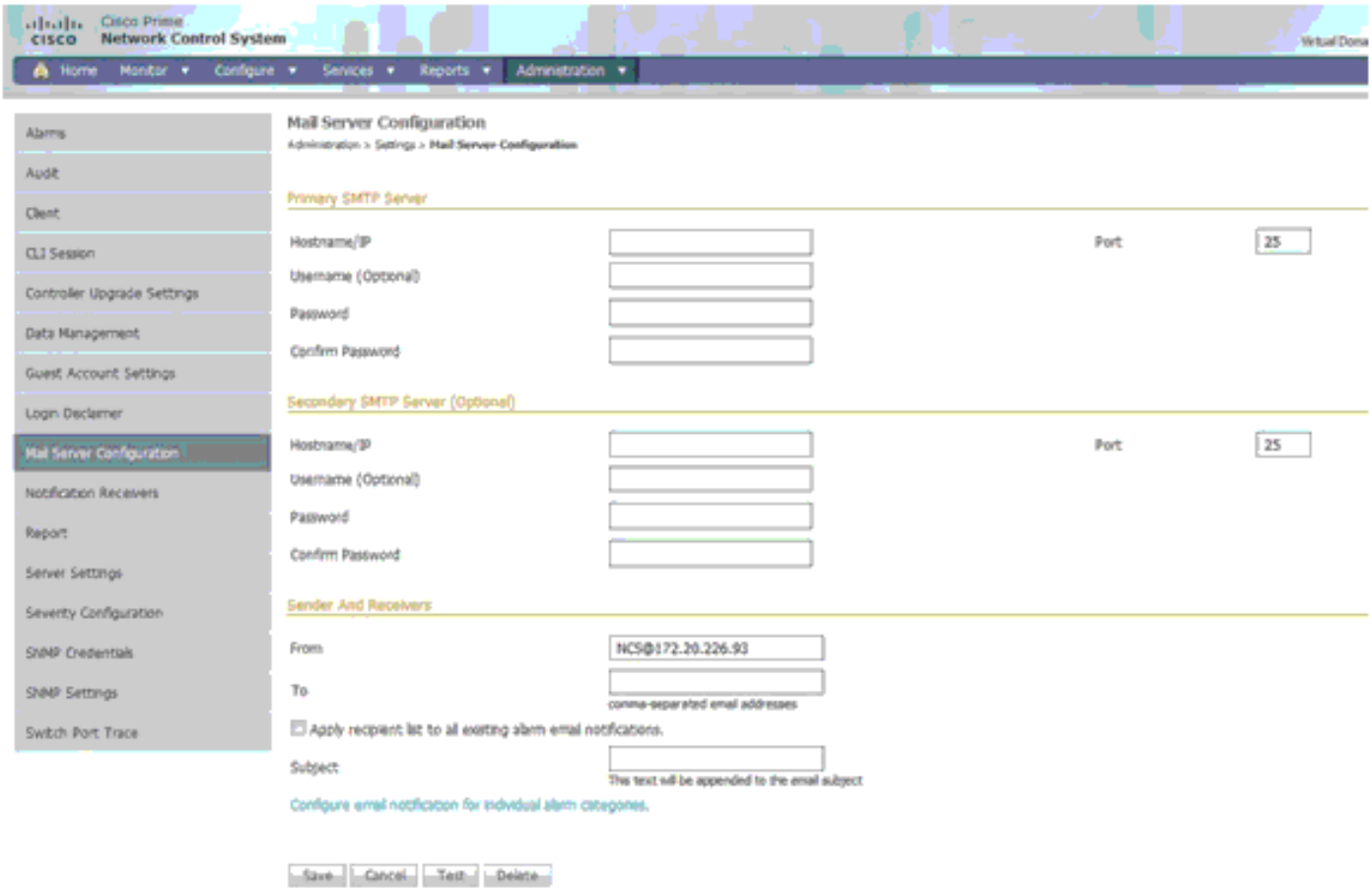
```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

La clave de la autenticación para el control de salud se debe también crear durante el proceso de instalación. Esta clave es utilizada solamente internamente por el HM del - P y el HM del - S para la autenticación. Debe ser la misma clave en el primario y los servidores secundarios.




Según lo expuesto anterior, solamente una licencia del servidor NCS necesita ser comprada. Por ejemplo, una licencia separada NCS no necesita ser comprada para el NCS secundario. El mismo archivo de licencia NCS reside en el NCS primario y secundario. Puesto que el NCS JVM se está ejecutando solamente en el primario o secundario (no ambos), el archivo de licencia es solamente activo en un sistema en una punta dada a tiempo.

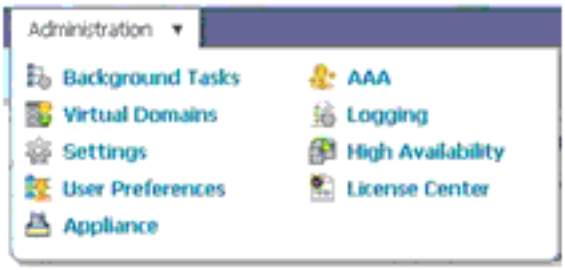
El administrador de la red también necesita proporcionar a los servidores establezca del correo electrónico para el correo electrónico de notificación para el proceso ha. Esto se requiere para la operación manual ha (intervención del administrador del sistema). Navegue a esta página como sigue: **>Settings > mail server de la administración**

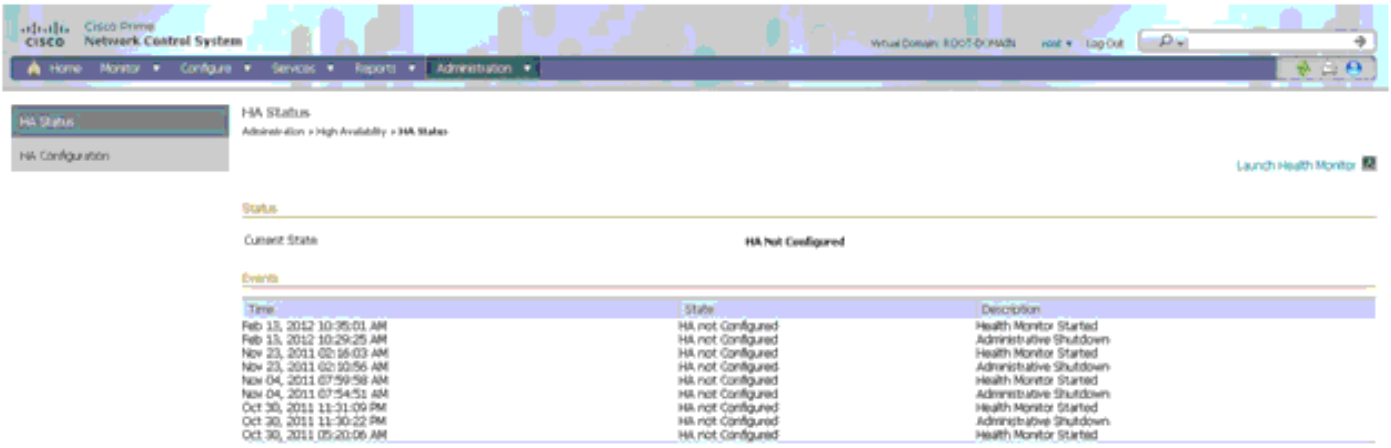



## Configuración en NCS primario secundario

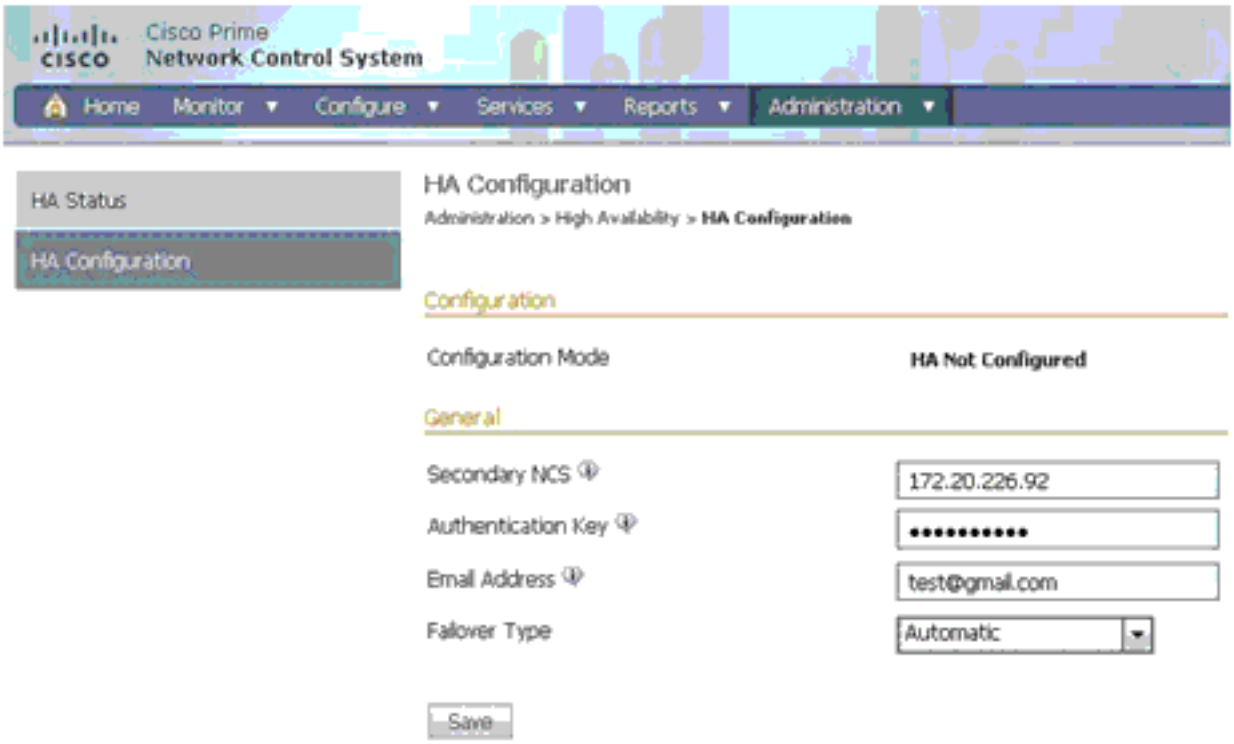
Configuraciones NCS

Elija la **administración > la Alta disponibilidad**. Según lo destacado, la ha no se configura actualmente en este sistema.



Del menú en el lado izquierdo de la pantalla, elija la **configuración ha**. Esto le lleva a esta ventana. Cuando usted ingresa la información pedida en la sección general del título y hace clic la **salvaguardia y el botón Enable Button**, se salva la configuración y se activa la ha.



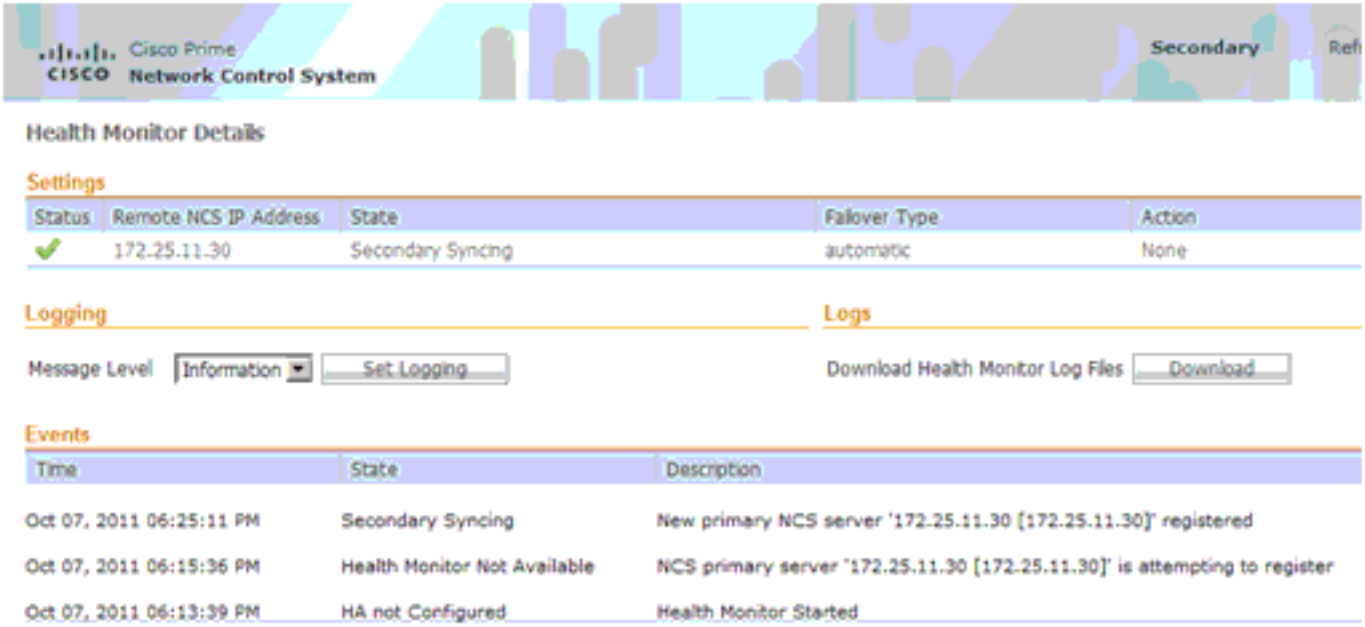

Usted necesita entrar esta información: Dirección IP de S-NCS, clave de la autenticación, dirección de correo electrónico para que notificaciones sean enviadas, tipo de la Conmutación por falla. Usted puede elegir salvar esta información sin la activación de la ha, o salve y active la ha.

## Vigilar la operación NCS ha

Después de que usted complete el paso anterior, la información de estado de mensaje en NCS proporciona a la información en la configuración ha y si está activada.

## Control de salud – NCS secundario

En la pantalla de control de salud en el NCS secundario, usted puede ver la información del estado de NCS secundario y del tipo de la Conmutación por falla se ha configurado que. También esto permite que el administrador de la red fije el tipo del nivel de mensaje de registración y la capacidad de capturar/los archivos del registro de la transferencia directa. Usted puede también ver los eventos vistos por S-HM con los grupos fecha/hora asociados.




## Ejemplo de la falla primaria – Failover manual

En este ejemplo, el NCS secundario fue configurado con el failover manual. Por ejemplo, notifican al administrador de la red a través del correo electrónico que el NCS primario había experimentado `abajo una` condición. El control de salud en NCS secundario detecta la condición del error de NCS primario. Puesto que se ha configurado el failover manual, el administrador de la red necesita accionar manualmente S-NCS para asumir el control las funciones NCS de NCS primario. Se hace esto si usted registra en S-HM. Aunque S-NCS no se está ejecutando, S-HM se puede conectar con directo este sintaxis:

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

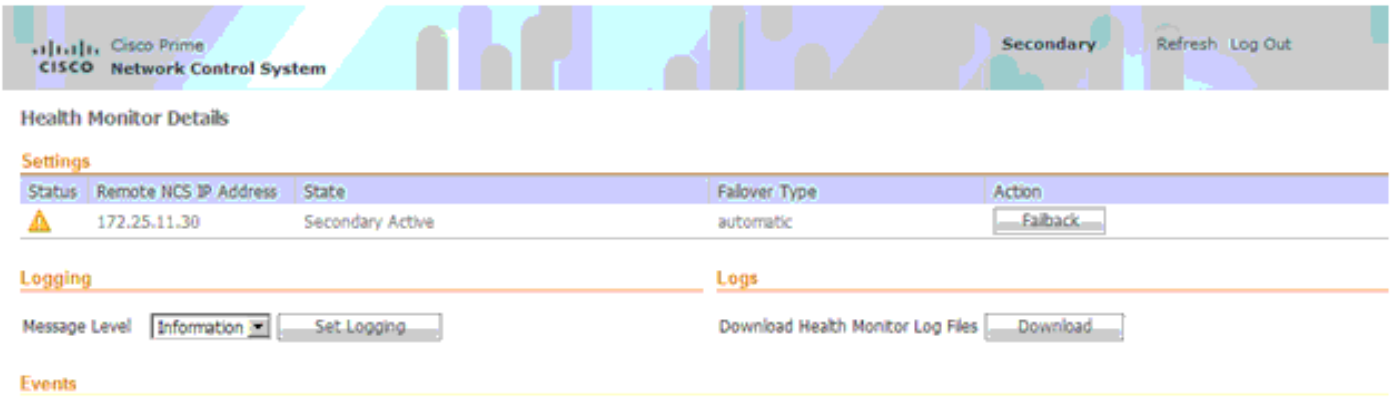
El S-HM visualiza los mensajes con respecto a los eventos se consideran que. Puesto que se ha configurado el failover manual, el S-HM espera al administrador de sistema para invocar el proceso de la Conmutación por falla. Una vez que se ha elegido el failover manual, se visualiza este mensaje mientras que S-NCS comienza. Una vez que se ha completado el proceso de la Conmutación por falla, así que significa que el proceso de replicación de la base de datos NCS está completado y proceso S-NCS JVM ha comenzado, después S-NCS es el NCS activo.

El control de salud en NCS secundario proporciona a la información de estatus de NCS primario y de los servidores secundarios. Failback se puede iniciar con S-HM una vez que P-NCS se ha recuperado de la condición del error. *El proceso de Failback se inicia siempre manualmente* en cuanto a evita una condición del aleteo que pueda ocurrir a veces cuando hay un problema de conectividad de red.

## Failback

Cuando los problemas en el servidor que reciben P-NCS se han resuelto, el failback puede ser iniciado manualmente. Una vez que se hace esto, la pantalla se visualiza en S-NCS. Cuando usted inicia el failback, la base de datos NCS en S-NCS y cualquier otros ficheros que han cambiado desde que S-NCS asumió el control la operación NCS se sincronizan entre S-NCS y P-NCS. Una vez que se ha completado la sincronización de la base de datos, P-NCS JVM es comenzado por P-HM. Cuando P-NCS JVM se está ejecutando, esta pantalla se visualiza en S-

HM.




## Falla automática

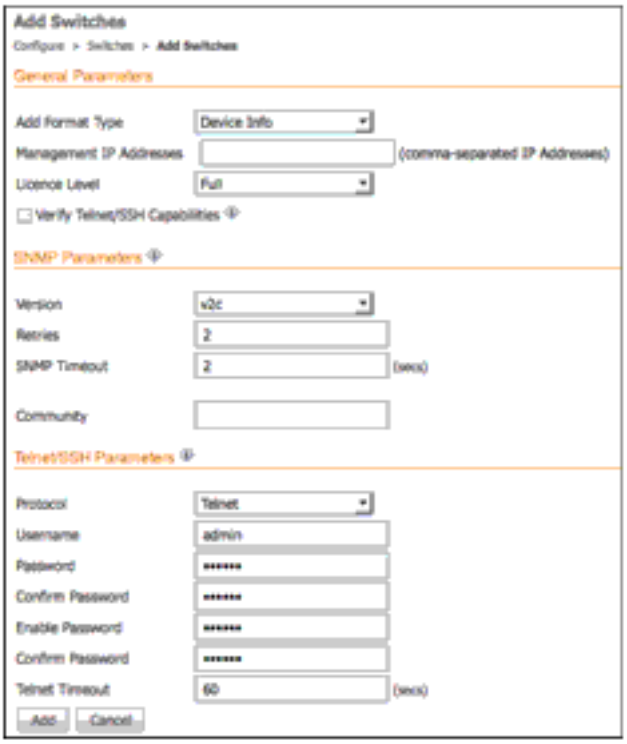
La falla automática es un proceso mucho más simple. Todos los pasos para la configuración son lo mismo a menos que seleccionen a la *falla automática*. Una vez que está configurado, el administrador de la red no necesita obrar recíprocamente con el HM del - S para que la operación de la Conmutación por falla ocurra. Solamente durante el failback es la Intervención requerida humana.

## Agregue un regulador a NCS

- Elija **configuran > los reguladores > agregan el regulador** para agregar un conmutador. Los reguladores inalámbricos de Cisco (WLCs) se pueden agregar en manualmente o con archivo CSV.
- Después de que usted agregue los reguladores, se colocan temporalmente en la página del monitor > de los dispositivos desconocidos mientras que NCS intenta comunicar con los reguladores que usted ha agregado. La comunicación con el regulador ha sido una vez acertada, los movimientos del regulador de la página del monitor > de los dispositivos desconocidos a la página del monitor > de los reguladores. Si NCS no puede comunicar con éxito con un regulador, permanece en el monitor > los dispositivos desconocidos y se visualiza una condición de error.

## Agregue un conmutador a NCS

Elija **configuran > Switches > agregan el Switches** para agregar un conmutador. El Switches puede ser agregado individualmente o los switches múltiples se pueden importar con archivo CSV.




Después de que se agregue un conmutador, se pone temporalmente en la página del monitor > del Switches mientras que NCS intenta comunicar con este conmutador. La comunicación con el conmutador ha sido una vez acertada, NCS mueve el conmutador desde la página del monitor > de los dispositivos desconocidos a la página del monitor > del Switches. Si NCS no puede comunicar con éxito con un conmutador, permanece en el monitor > los dispositivos desconocidos y se visualiza una condición de error.

## Configuración del switch del catalizador

Hay tres pasos para la configuración de Seguridad del cliente en el Switches del Cisco Catalyst: Autenticación AAA, RADIUS y 802.1x/MAC.

| Configuración AAA |
| --- |
| ncs-appliance/admin# **ncs migrate wcs-data wcs.zip repository ncs-ftp-repo** |

Refiera a la descripción AAA para más información.

Esta configuración es configuración del switch de Cisco para la autenticación de RADIUS para Cisco ISE/ACS y los servidores de RADIUS de no-Cisco.

| Configuración IOS |
| --- |
| ncs-appliance/admin# **ncs migrate wcs-data wcs.zip repository ncs-ftp-repo** |

Si desea más información, consulte estos documentos:

- El servidor de RADIUS reordena en el error
- Atributo de RADIUS 8 (Framed-IP-direccionamiento) en las peticiones del acceso

- Referencia de Comandos de Seguridad de Cisco IOS

802.1x y configuración auténtica MAC — Esta configuración del switch proporciona a tres funciones: la autenticación para los clientes del 802.1x, permite que los clientes continúen en la red que fallan la autenticación del 802.1x (el evento se genera/se envía a NCS para la autenticación fallada del 802.1x), puente de la autenticación MAC (MAB) para los dispositivos IP que no tienen el suplicante del 802.1x.

| Configuración del Cisco IOS |
| --- |
| ncs-appliance/admin# **ncs migrate wcs-data wcs.zip repository ncs-ftp-repo** |

Refiera a configurar la autenticación Puerto-basada 802.1x de IEEE para más información.

Notificación MAC para los desvíos (clientes de la no-identidad) — este del Cisco IOS de la función del switch SNMP traps adelante del conmutador al NMS, por ejemplo, servidor NCS, para las notificaciones MAC, clientes non-802.1x.

| Configuración del Cisco IOS |
| --- |
| ncs-appliance/admin# **ncs migrate wcs-data wcs.zip repository ncs-ftp-repo** |

Paquetes snmp de la depuración de los comandos Debug

Cambio de la notificación de la direccionamiento-tabla del mac de la demostración de los comandos show

Refiera a configurar los desvíos de la notificación de cambio MAC para más información.

Configuración de syslog (clientes de la identidad solamente) — Los mensajes de Syslog de esta configuración adelante del catalizador cambian al servidor NCS.

| Configuración IOS |
| --- |
| ncs-appliance/admin# **ncs migrate wcs-data wcs.zip repository ncs-ftp-repo** |

# Hojas de operación (planning) de red inalámbrica

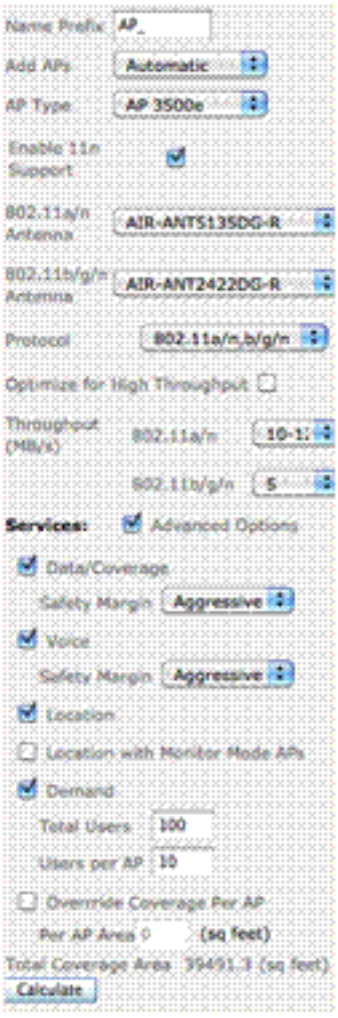
## Herramienta de planificación

La herramienta incorporada de las hojas de operación (planning) proporciona a una manera para los administradores de la red en la determinación de qué se requiere en el despliegue de una red inalámbrica. Como parte del proceso de hojas de operación (planning), los diversos criterios se entran en la herramienta de las hojas de operación (planning). Complete estos pasos:

1. Especifique el método del prefijo AP y de la colocación AP (automático contra el manual).
2. Elija el tipo AP y especifique la antena para la banda 2.4GHz y 5GHz.
3. Elija el protocolo (banda) y la producción deseada mínimo por la banda que se requiere para

este plan

4. Active el modo de las hojas de operación (planning) para las opciones anticipadas para los datos, Voz, ubicación. Los datos y la Voz proporcionan a los márgenes de seguridad para la ayuda del diseño. Los márgenes de seguridad ayudan a diseñar con certeza los umbrales RSSI, que se detalla en la ayuda en línea. La ubicación con el modo monitor descompone en factores en el AP que se podría desplegar para aumentar la exactitud de la ubicación. La ubicación requiere típicamente un despliegue más denso que los datos y el checkbox de la ubicación ayuda al plan para la exactitud de divulgación de la ubicación.
5. Las opciones de la *demanda* y de la *invalidación* permiten planear para cualquier caso especial donde hay una alta densidad de la presencia del cliente tales salas de conferencia




o las salas de conferencias. La oferta generada contiene éstos:Detalles del plan de pisoNegación/alcance/suposicionesColocación propuesta APTarifa Heatmap de la cobertura y de datosAnálisis de la cobertura

## Editor de la correspondencia

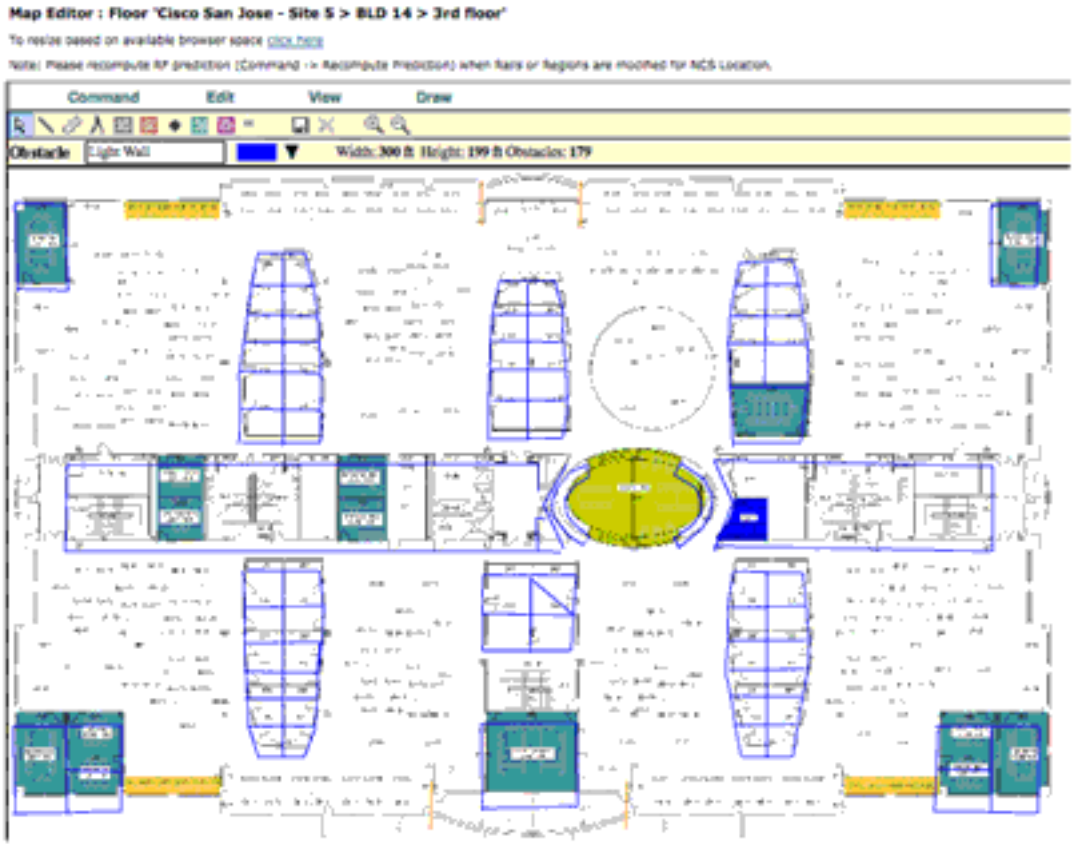
El editor integrado de la correspondencia en NCS explica los objetos y los obstáculos en un suelo. La modificación de las características de la correspondencia del suelo da lugar a un modelo más exacto de la propagación RF que se visualice en las correspondencias proféticas del calor. Las características de la atenuación para los objetos y el motor profético de la ayuda de los obstáculos visualizan una correspondencia profética más realista del calor. corrige hecho para solar las ayudas de la correspondencia especifican las áreas y las regiones por ejemplo:

- Área de cobertura y etiquetas de plástico — usadas para las notificaciones de la ubicación
- Perímetro — define el límite externo

- Regiones de la inclusión y de la exclusión de la ubicación — usadas para los eventos y las notificaciones de la ubicación

Objetos y obstáculos que pueden ser especificados:

- Paredes (luz y pesado) — 2dB y 13dB
- Cubículo (paredes) — 1dB
- Puertas (luz y pesado) — 4dB y 15dB
- Vidrio (puertas, ventanas, paredes) — 1.5dB




## Correspondencias de la importación del WCS a NCS

La exportación/la función importar de la correspondencia está disponibles en WCS 7.0. Esta característica se describe detalladamente en la guía de configuración WCS 7.0.

Después de la exportación de las correspondencias del servidor de la fuente WCS, este conjunto de las correspondencias se puede importar en el servidor del destino NCS. Los pasos para importar sus correspondencias se cubren en la guía de configuración NCS.

**Note**: Es importante que los APs en el servidor WCS primero están agregados al servidor NCS antes de importar las correspondencias puesto que los APs en las correspondencias WCS también se incluyen durante el proceso de la exportación. Los APs que no se han agregado a su NCS sino están presentes en el resultado exportado de las correspondencias del suelo en los errores que son visualizados cuando usted importa esas correspondencias en NCS.

# Utilice NCS para desplegar un LAN de la Tecnología inalámbrica

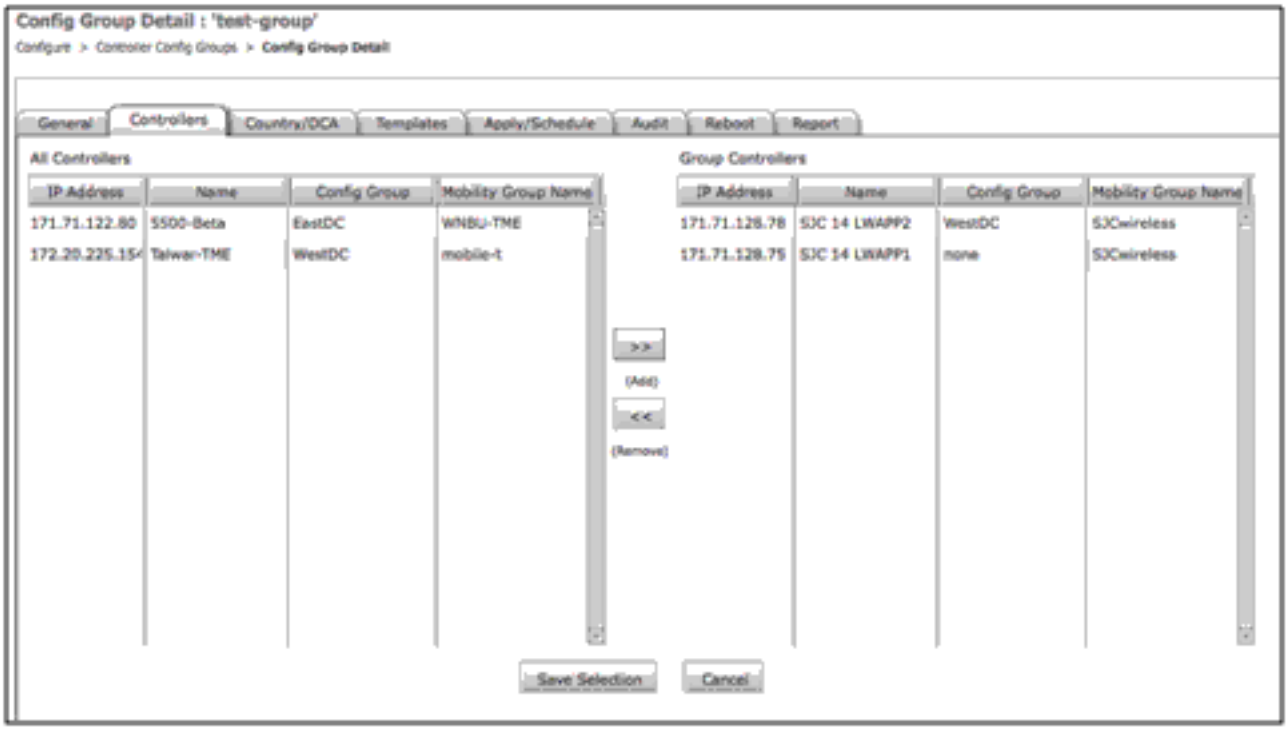
## Plantillas de la configuración

Las plantillas de la configuración son conjuntos de las configuraciones que se pueden aplicar a los dispositivos en un sistema o un nivel global. Pueden ser reutilizadas para modificar las configuraciones existentes. Las plantillas se pueden también utilizar para replicar la configuración a los otros dispositivos agregados posteriormente. Las plantillas de la configuración se pueden utilizar para programar los cambios de los config en la fecha y hora predefinida. Las capacidades de la auditoría en NCS pueden también leverage las plantillas de los config para determinar las diferencias de los config entre NCS y la configuración existente del regulador.

## Grupos de configuración (Config-grupos)

los Config-grupos son una forma sencilla de agrupar los reguladores lógicamente. Esta característica proporciona a una manera de manejar los reguladores con las configuraciones similares. Las plantillas se pueden extraer del regulador existente para provision los nuevos reguladores o los reguladores existentes con los parámetros adicionales de la configuración. Los grupos de los Config pueden también ser utilizados para programar los conjuntos de la configuración de provisioned. Las reinicializaciones del regulador se pueden también programar/conectar en cascada dependiendo de los requisitos de funcionamiento. Los Grupos de movilidad, el DCA, y la auditoría de la configuración del regulador pueden también ser manejados usando los config-grupos.

Utilizan a los Config-grupos al agrupar los sitios juntos para una Administración más fácil (Grupos de movilidad, DCA y configuraciones reguladoras del dominio) y para programar los cambios de configuración remota. Sitios de los grupos para asegurar la conformidad con las directivas de configuración.




- Agregando los reguladores — Los reguladores en el WCS se presentan y se pueden mover encima nuevamente al grupo de los config
- Aplicando las plantillas — Descubierto o presente ya las plantillas puede entonces ser aplicado al regulador
- Auditoría — Ensure plantilla-basó la auditoría se selecciona en las configuraciones de la auditoría y después auditoría los reguladores en el grupo para asegurarse que cumplen con las directivas

# Utilice vigilar/Troubleshooting NCS una red inalámbrica

## RRM /CleanAir

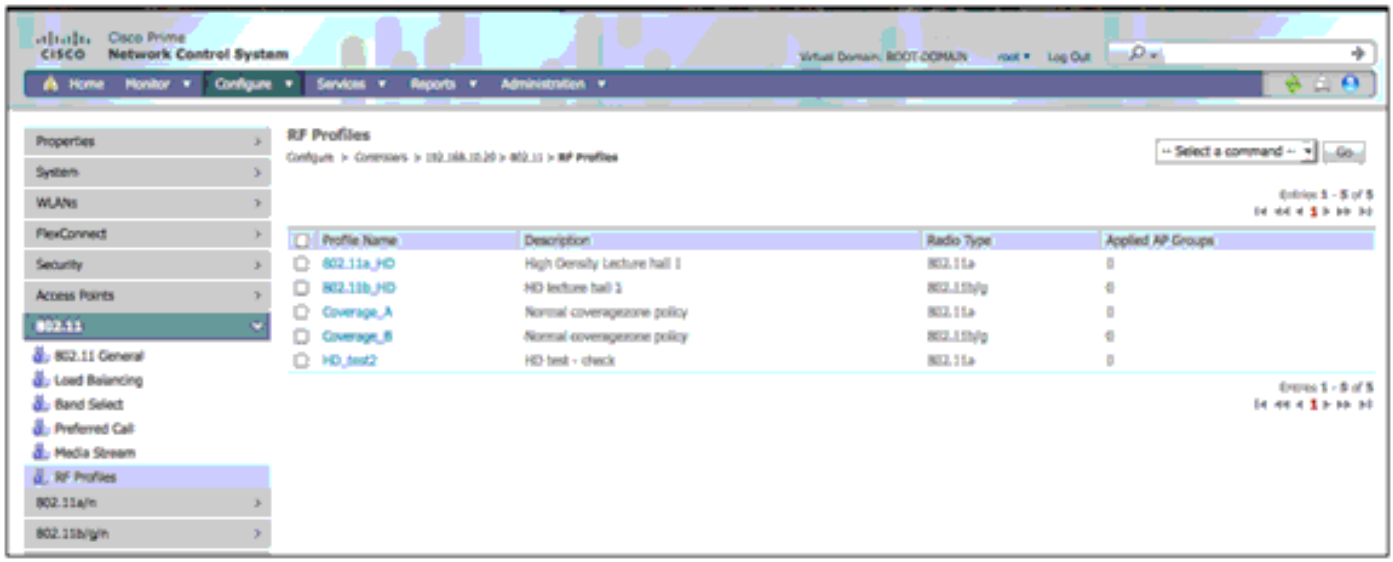
Utilizan los perfiles y a los grupos RF en la versión 1.1 NCS para ambas plantillas de la creación del perfil RF, y las plantillas del grupo AP. Si usted utiliza NCS 1.1 para crear los perfiles RF a través de la creación de las plantillas, esto da a administrador un método simple de crear y de aplicar las plantillas constantemente a los grupos de reguladores. Los flujos del proceso lo mismo que era discutido previamente en la característica del regulador fijaron con algunas diferencias de menor importancia pero importantes.

El proceso es lo mismo que discutido previamente en que usted primero crea los perfiles RF, después aplica los perfiles a través de los grupos AP. Las diferencias están en cómo esto se hace de NCS y en el uso de las plantillas de desplegar a través de la red.

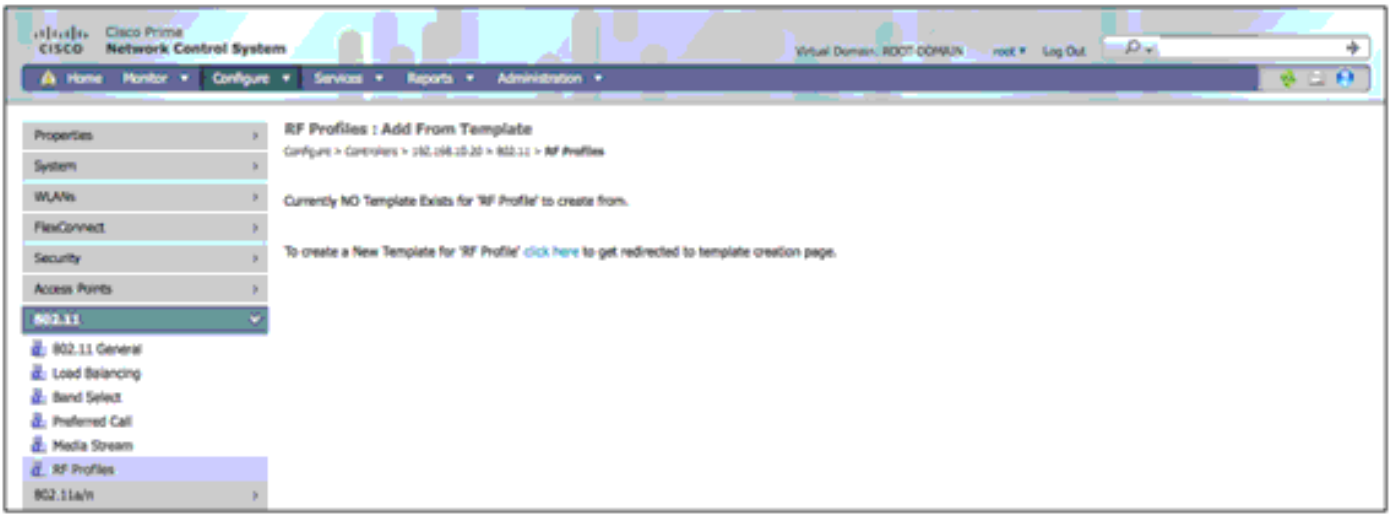
## Construya un perfil RF con la prima NCS 1.1 de Cisco

En la prima NCS de Cisco hay dos maneras que usted puede acercarse al edificio o a manejar un perfil RF. Elija **configuran > los reguladores > (dirección IP del regulador) > 802.11 > RF perfila** para tener acceso a los perfiles para un regulador individual.

Esto visualiza todos los perfiles RF actualmente presentes en el regulador elegido y permite que usted realice los cambios a las asignaciones de los perfiles o del grupo AP. Las mismas limitaciones con respecto a un perfil que se aplique actualmente a un grupo AP están en efecto como con el GUI del regulador. Usted tiene que inhabilitar la red u O.N.U-asignar el perfil RF del grupo AP.




Cuando usted crea un nuevo perfil, NCS le incita elegir una plantilla existente. Si esto está la primera vez está siendo alcanzada, usted se dirige al diálogo de la creación de la plantilla para una plantilla del regulador del 802.11.

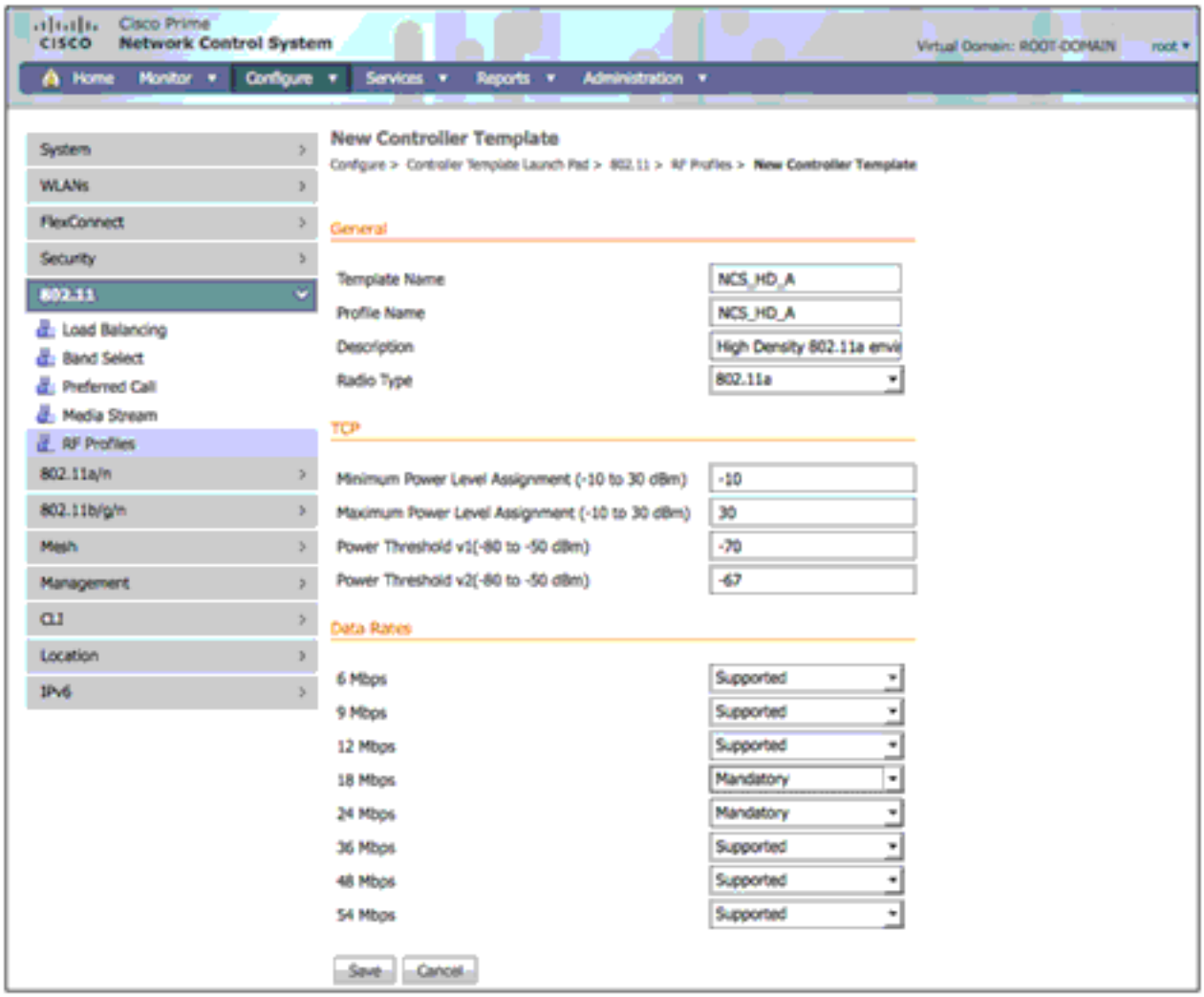



Elija **configuran > plataforma de lanzamiento de la plantilla del regulador > 802.11 > los perfiles RF** para ir a la plataforma de lanzamiento de la plantilla del regulador directamente.

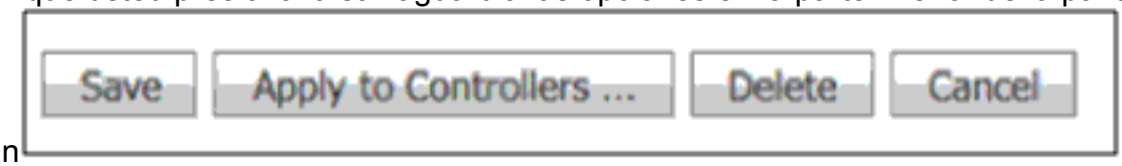
En ambos casos, un nuevo perfil RF se crea en NCS con el uso de una plantilla. Esto es un método preferido, puesto que permite que el administrador leverage el flujo de trabajo de NCS y aplique las plantillas y las configuraciones a todos los o a los grupos selectos reguladores y reduzca los Errores de configuración y las discordancías.

Complete estos pasos:

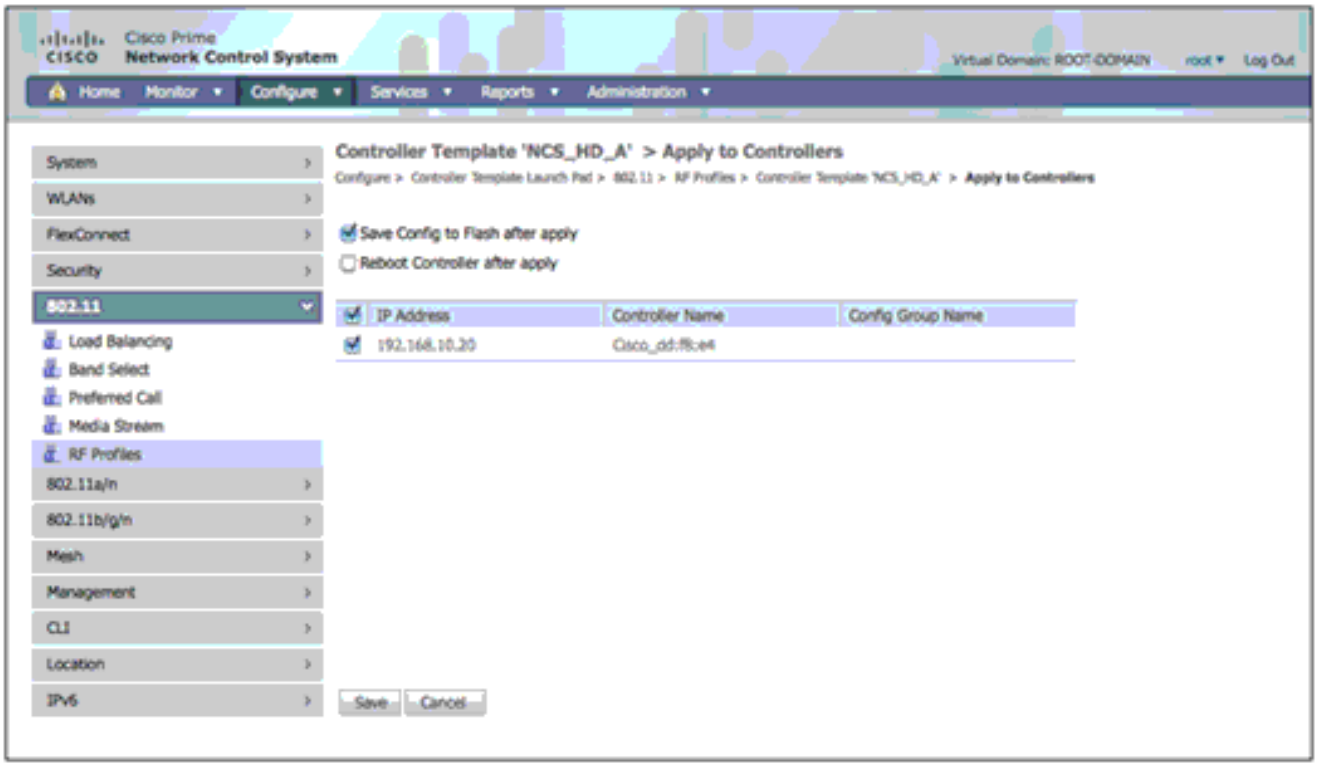
1. Para crear las plantillas de perfiles RF, elija **nuevo**:



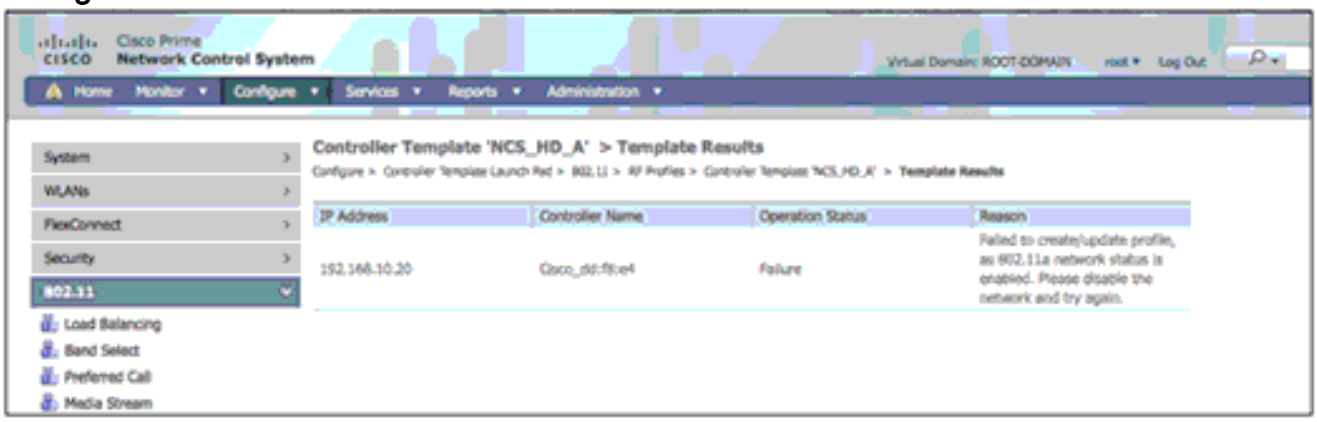

2. La configuración de la plantilla/de las configuraciones es casi idéntica con la adición de un nombre de la plantilla. Haga esto descriptivo para el reconocimiento fácil en el futuro. Cambie las configuraciones según las necesidades o requerido y elija la **salvaguardia**.**Note**: Si usted elige un valor de umbral para TPCv2 y no es el algoritmo elegido TPC para el grupo RF, después se ignora este valor.**Note**: Una configuración simple a cambiar para la validación es la potencia del mínimo TPC. La potencia mínima puede ser aumentada si usted elige un valor del dBm que sea más que el nivel de potencia actual asignado por RRM. Esto ayuda a validar la operación de los perfiles RF.
3. Una vez que usted presiona la salvaguardia las opciones en la parte inferior de la pantalla




cambian Elija **se aplican a los reguladores** y el cuadro de diálogo del regulador aparece visualizar la lista de reguladores manejados por este servidor
NCS.




4. Elija los config de la salvaguardia para contellear, elija el regulador que usted desea tener el perfil disponible encendido, y elige la **salvaguardia.**



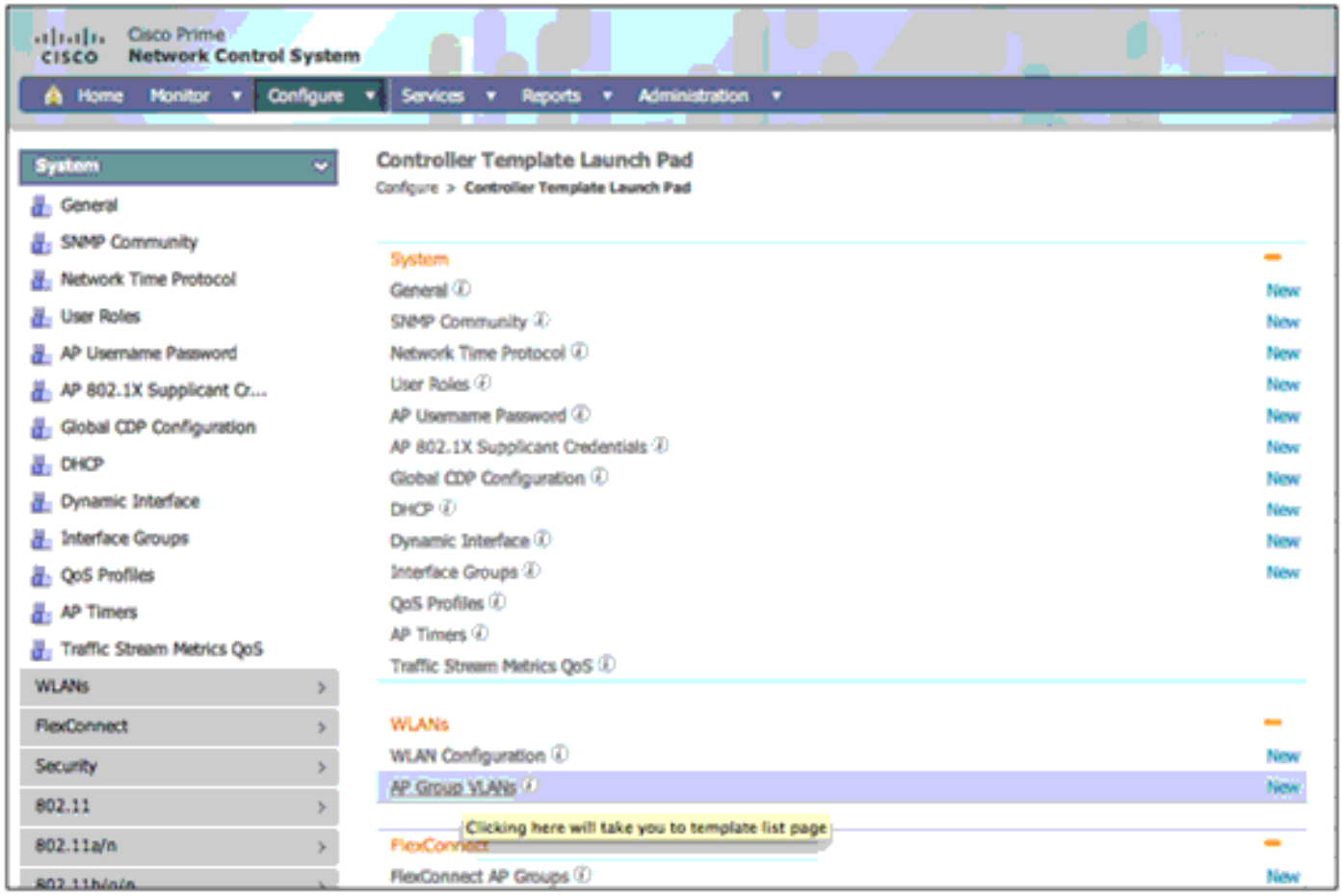

5. Ahora en que usted ve el RF perfila la pantalla, usted puede considerar la nueva plantilla creada.


Los pasos anteriores se pueden relanzar para crear y aplicar las plantillas adicionales como sea necesario, por ejemplo, para el 802.11b.

## Aplique los perfiles RF a los grupos AP con NCS

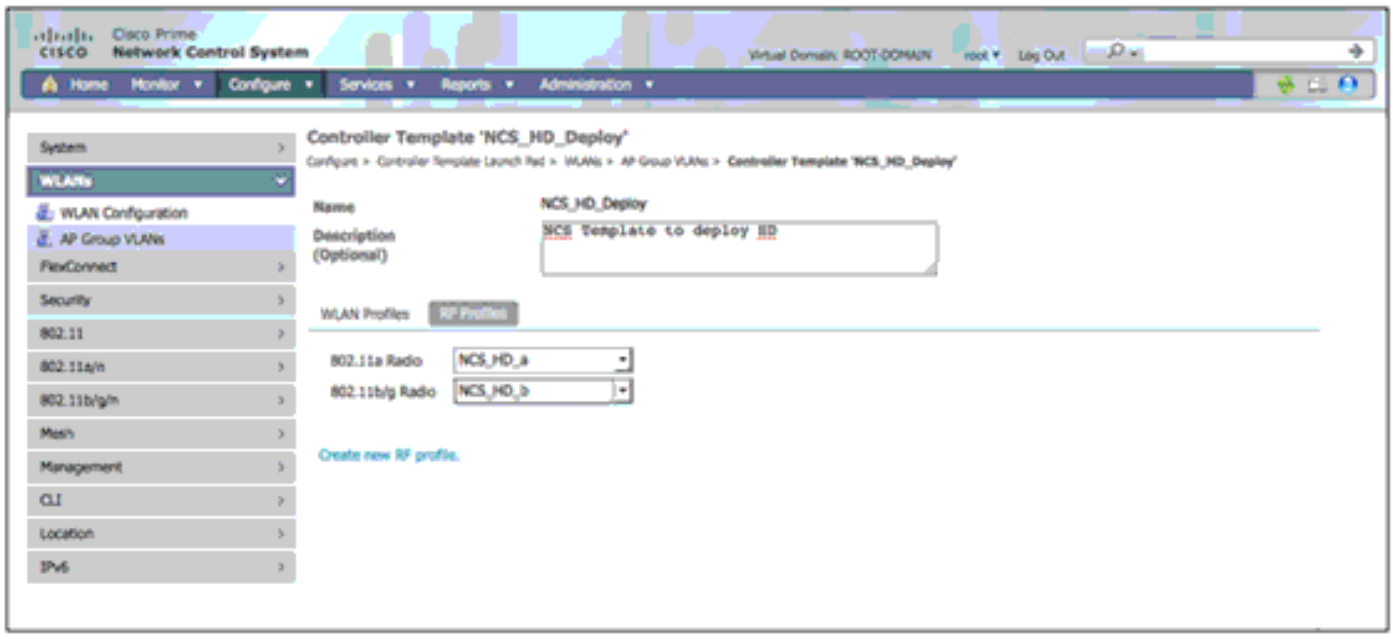
Como con la configuración WLC para los perfiles RF, los perfiles creados recientemente se pueden aplicar a un regulador con el uso de los grupos AP que se asignan a. Para hacer esto, o guardó previamente la plantilla de los VLA N del grupo AP o la plantilla creada recientemente puede ser utilizada.

Elija **configuran > plataforma de lanzamiento de la plantilla del regulador** y eligen los **VLA N del grupo AP**.

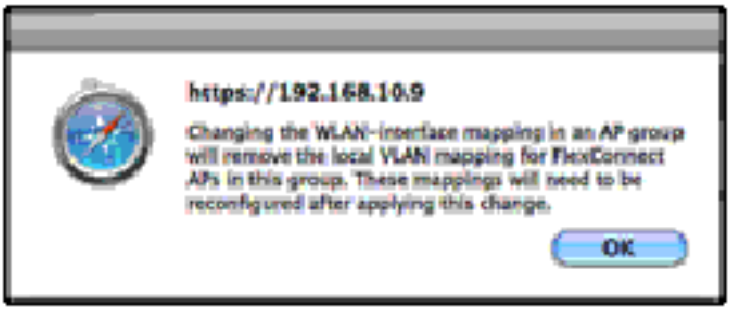



Para crear una nueva plantilla, elija **nuevo** y complete la Información requerida.

Elija la tabulación de los **perfiles RF** para agregar los perfiles RF.



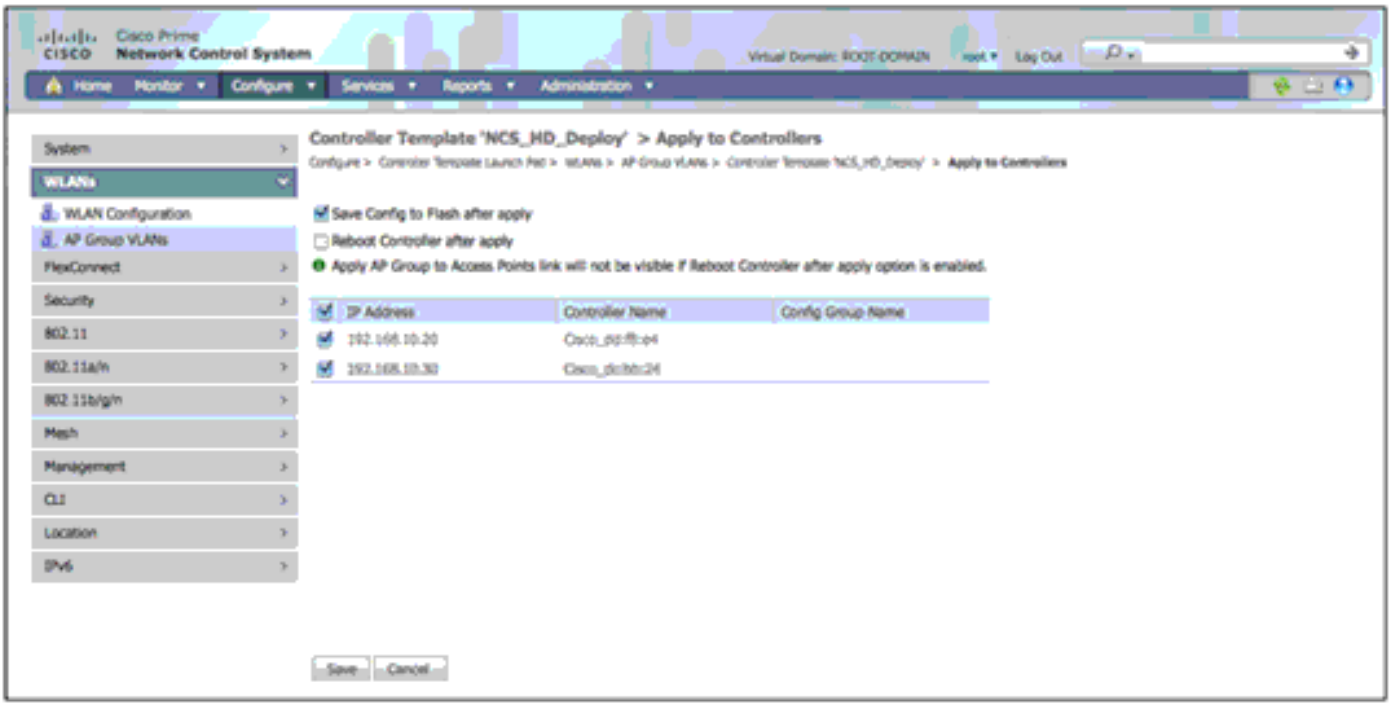

Si usted salva la plantilla, un mensaje de advertencia aparece.




Como se afirma en el mensaje anterior, el cambio del interfaz que la red inalámbrica (WLAN) asignada utiliza interrumpe las asignaciones del VLA N para FlexConnect APs aplicado en este grupo. Asegúrese de que el interfaz sea lo mismo antes de que usted proceda.

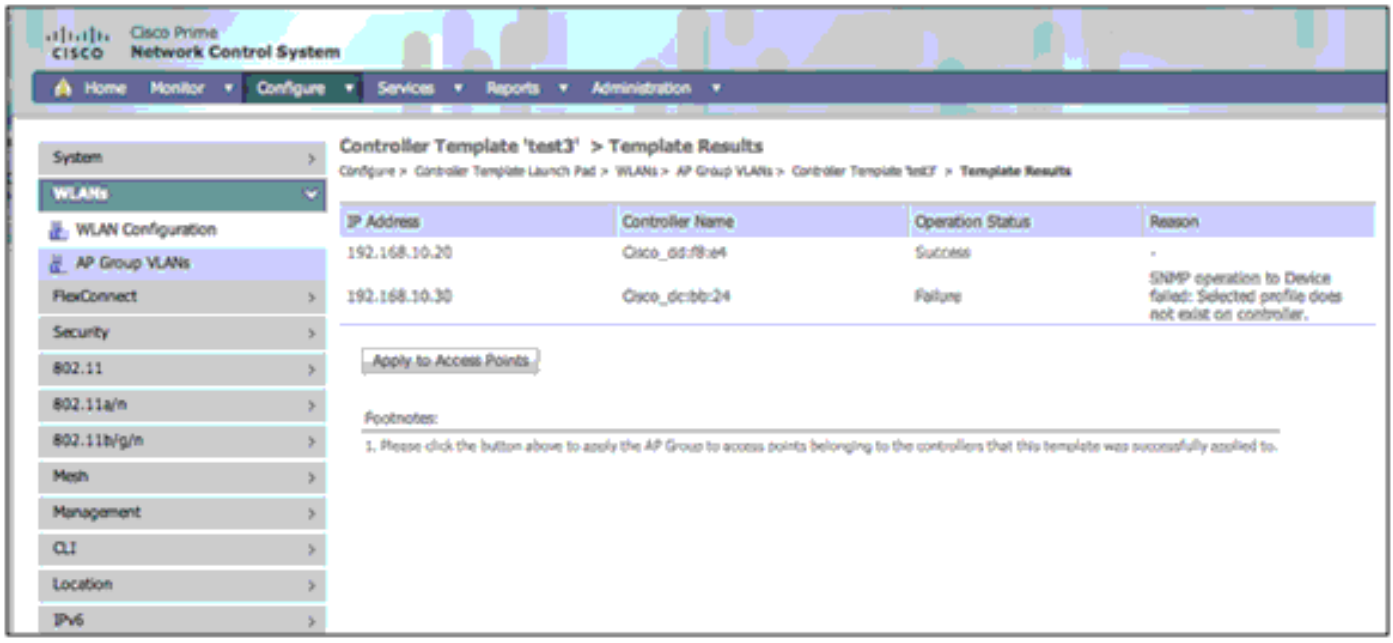
Una vez que usted elige **OK**, el diálogo se substituye por la opción **para aplicarse a los reguladores**. Elija esta opción.


Elija los reguladores a los cuales la plantilla necesita ser aplicada.




NCS responde con el estado operacional encendido si la plantilla fue aplicada con éxito a los reguladores seleccionados.


Si la plantilla no fue empujada con éxito, NCS proporciona a un mensaje que estado la razón del error. En este ejemplo, el perfil RF que se aplica al grupo no está presente en uno de los reguladores a los cuales la plantilla era aplicada.

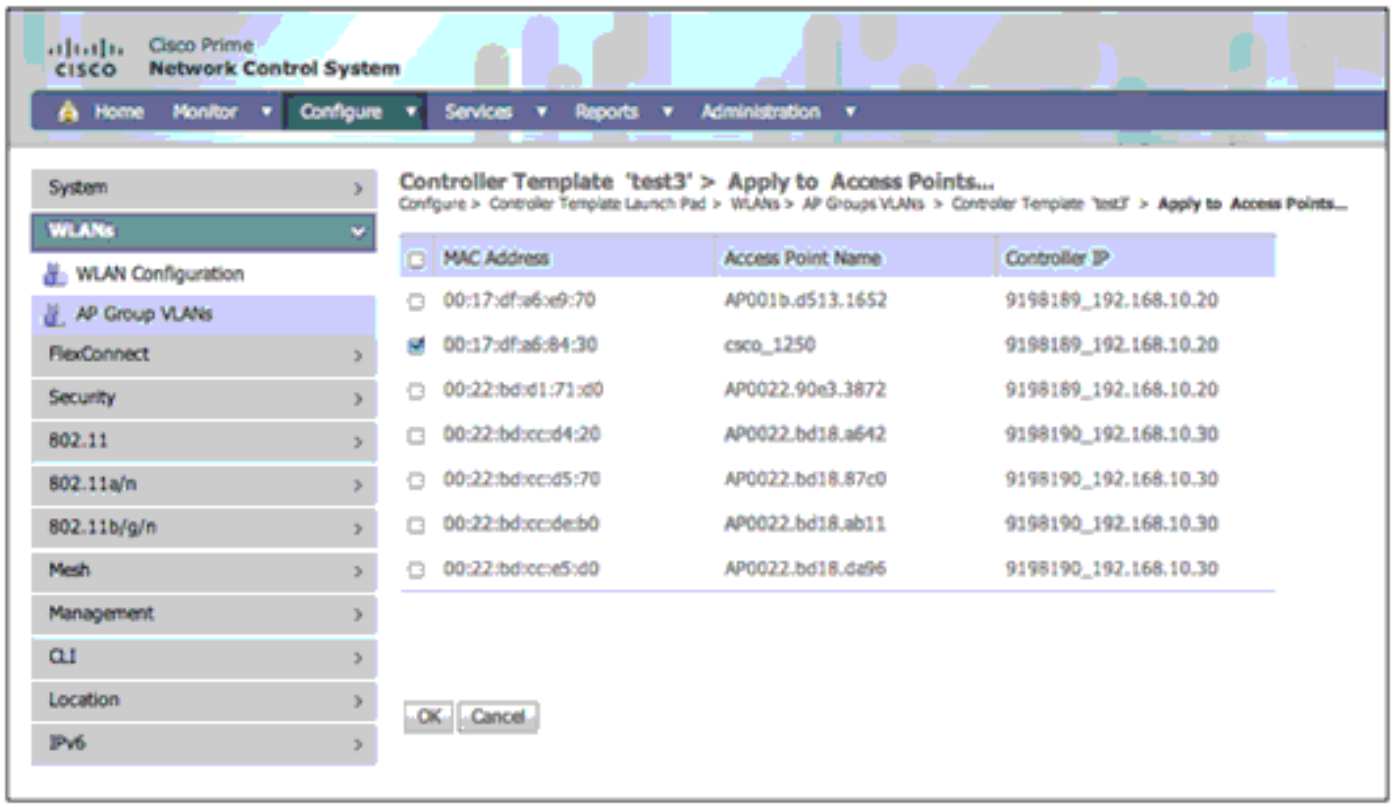



Aplique el perfil RF otra vez, específicamente a ese regulador y después reaplique al grupo AP para generar un mensaje acertado.

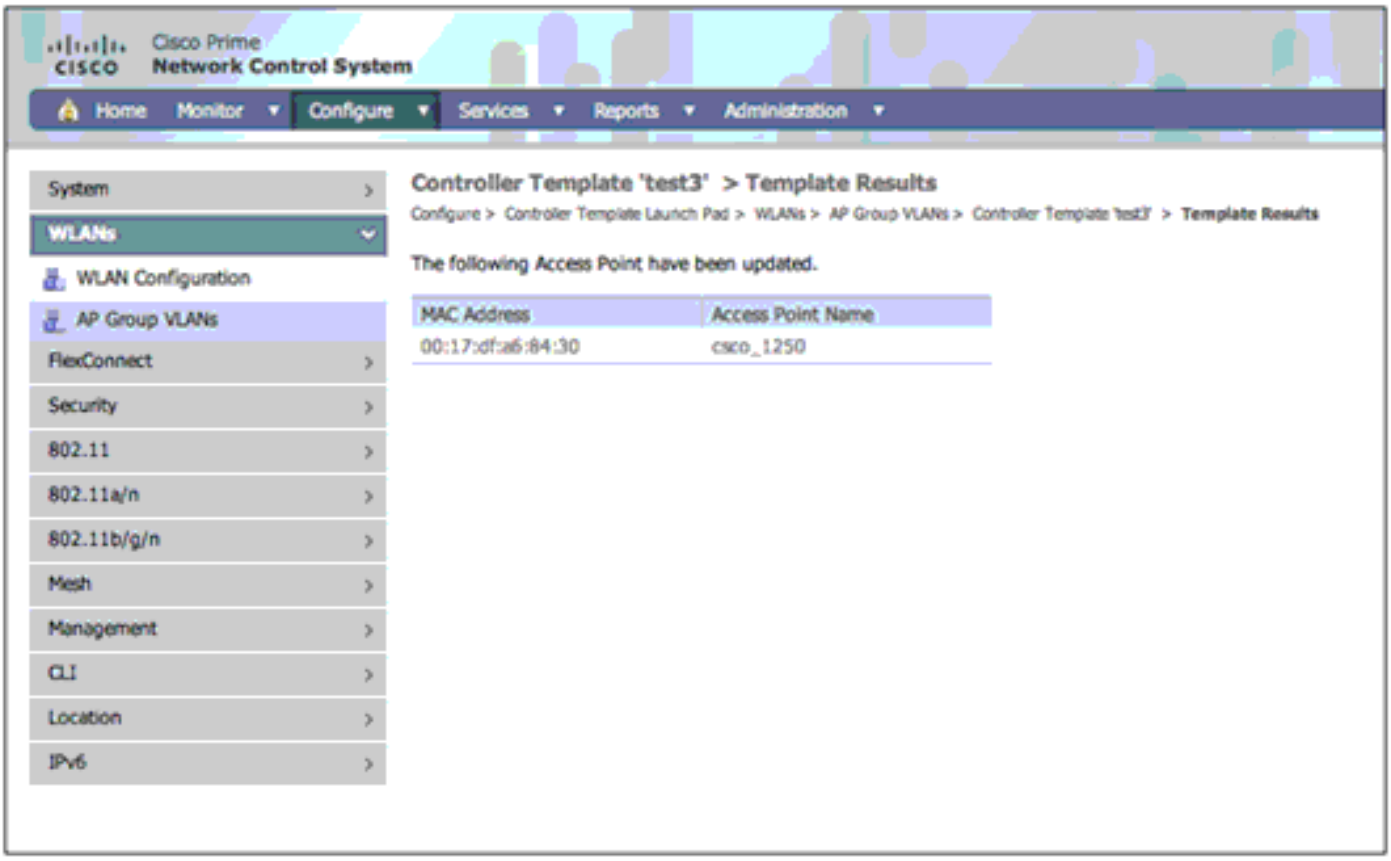
Una vez que han desplegado al grupo AP con los perfiles RF aplicados (elija la **aplicación al** botón de los **Puntos de acceso**), sólo los Puntos de acceso asociados a los reguladores donde desplegaron al grupo AP con éxito están disponibles seleccionar de.

**Note**: Hasta esta punta, no se realizó ningunos cambios reales a la infraestructura RF, pero éste cambia cuando los APs se trasladan al grupo que contienen los nuevos perfiles RF. Cuando un AP se mueve en o de un grupo AP, las reinicializaciones AP para tomar la nueva configuración.

Elija los APs para agregar al grupo AP y elegir **OK**. Un mensaje de advertencia aparece.




NCS visualiza el estatus del cambio.




## Utilice NCS a los problemas de Remediate

- CleanAir
- troubleshooting del cliente
- herramienta de auditoría
- panel de la Seguridad
- SPT

## Utilice NCS para optimizar la operación de la red inalámbrica

- informes
- funcionamiento de red inalámbrica (RRM)
- funcionamiento (ancho de banda WAN)

## Panel

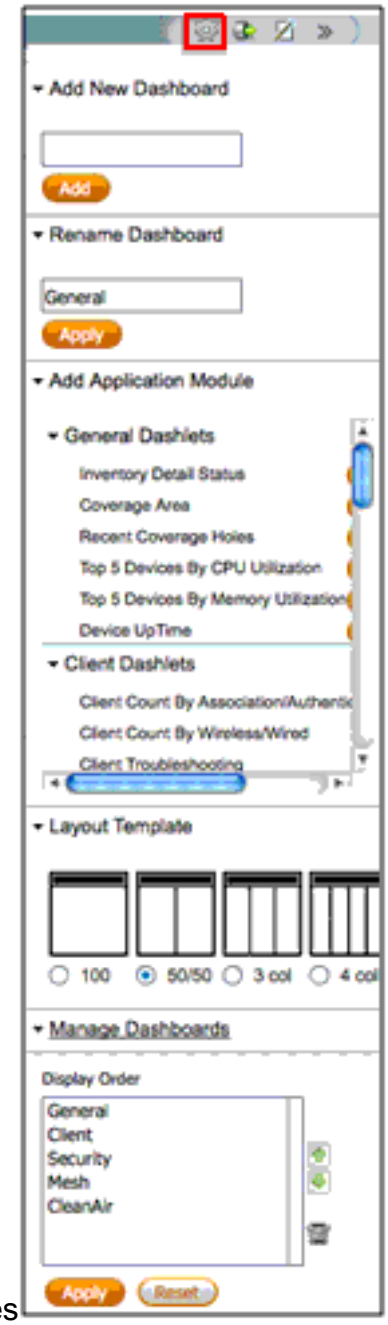
Los componentes del panel se han aumentado en NCS 1.0 allí son varias mejoras a los componentes del Home Page:

- integración atada con alambre/inalámbrica: los componentes ahora también visualizan la información atada con alambre del cliente y del conmutador
- flujo de trabajo componente del arreglo para requisitos particulares: qué puede ser personalizada, cómo personalizar
- los componentes individuales pueden ser restaurados. La velocidad de actualización se puede configurar individualmente también.

- facilidad del arreglo para requisitos particulares del componente y del Home Page: todo el corregir se completa directamente en el Home Page (ninguna necesidad de navegar para corregir la página). Arrastrar y soltar para agregar/los componentes móviles
- flujo de trabajo intuitivo: los enlaces hipertexto componentes proporcionan a la facilidad de la navegación, e.g distribución auténtica del cliente a la página filtrada de la lista del cliente

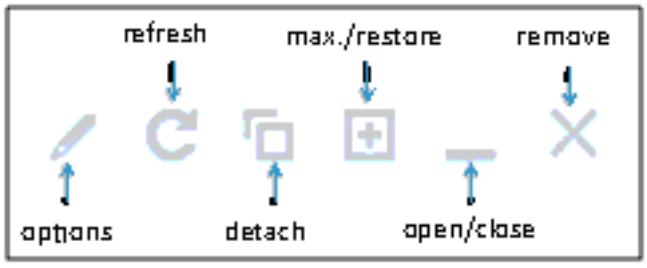

Éstas son las personalizaciones del usuario principales para el panel:

- arrastrar y soltar del dashlet: los componentes se pueden cambiar en la página
- agregue/suprimiendo los paneles: agregue/las nuevas tabulaciones de la cancelación
- el reordenar del panel
- retitulación del panel
- corregir la disposición: puede especificar el número de columnas para los dashlets, el agregar/que suprime los dashlets
- retitulación de los dashlets
- instancias múltiples del dashlet: el usuario puede agregar el mismo dashlet y personalizar el contenido en cada uno
- disposición usuario-configurable del panel: número de columnas en la página para los

componentes 


Arreglo para requisitos particulares de Dashlet:

- el manual restaura: permite que los usuarios restauren el contenido individual del dashlet
- corrija el nombre del dashlet
- vuelva a clasificar según el tamaño: minimice (reduzca para titular y barra de estado), restablezca (los restores al tamaño original), maximice (el dashlet activo ocupa el área del panel)
- separe: contenido del dashlet separe/de los redespliegues en la nueva ventana
- cierre: quita el dashlet del panel. Puede ser agregado otra vez vía “agregan la pantalla de Dashlet”
- opciones múltiples de la visualización: gráfico o tabla
- indicador visual a visualizar si se ha personalizado el

dashlet. 


Escoja la opinión atado con alambre/los clientes de red inalámbrica en el dashlet

Hay once componentes del dashlet que proporcionan a la información en atado con alambre/los clientes de red inalámbrica:

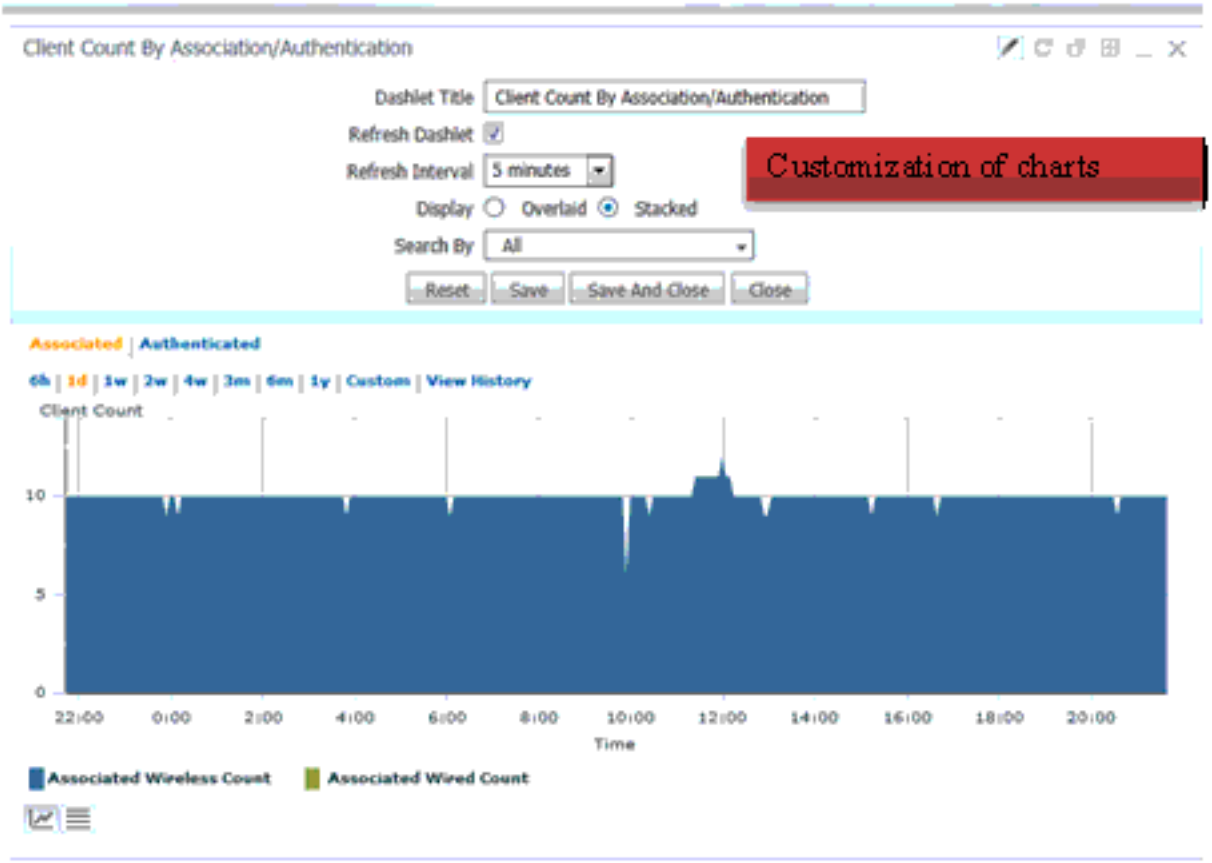
- Cuenta del cliente por la asociación/la autenticación
- Cuenta del cliente por la Tecnología inalámbrica/atada con alambre
- Tráfico del cliente
- Alarma y eventos del cliente sumarios
- Tráfico del cliente
- Troubleshooting del cliente
- Estatus de la postura del cliente
- Estatus del detalle del inventario
- Uptime del dispositivo
- Dispositivos del top 5 por la utilización CPU
- Dispositivos del top 5 por la utilización de la memoria

Dashlets atados con alambre-solamente

- Distribución atada con alambre de la velocidad del cliente
- 5 Switch superiores por la cuenta del cliente

## Arreglo para requisitos particulares de las cartas de área

Las cartas en los dashlets como la cuenta del cliente por la Tecnología inalámbrica/la cuenta atada con alambre y del cliente por la autenticación de la asociación tienen cartas de área múltiple que dependan de la selección de barra ad hoc del filtro de las cartas que tenga todos/Tecnología inalámbrica/alambre" y asociado/autenticado respectivamente pues las opciones en la barra del filtro. Las cartas de área consideradas pueden ser sobrepuestas (cruz de las áreas múltiples) o ser empiladas (las áreas múltiples se empilan verticalmente – una sobre la otra). La indicación de si está empilada o sobrepuesta se muestra junto al título de y-AXIS. La razón de los diversos tipos de visiones (empiladas o sobrepuestas) es dar al usuario una mejor indicación del conjunto de datos que es mostrado.

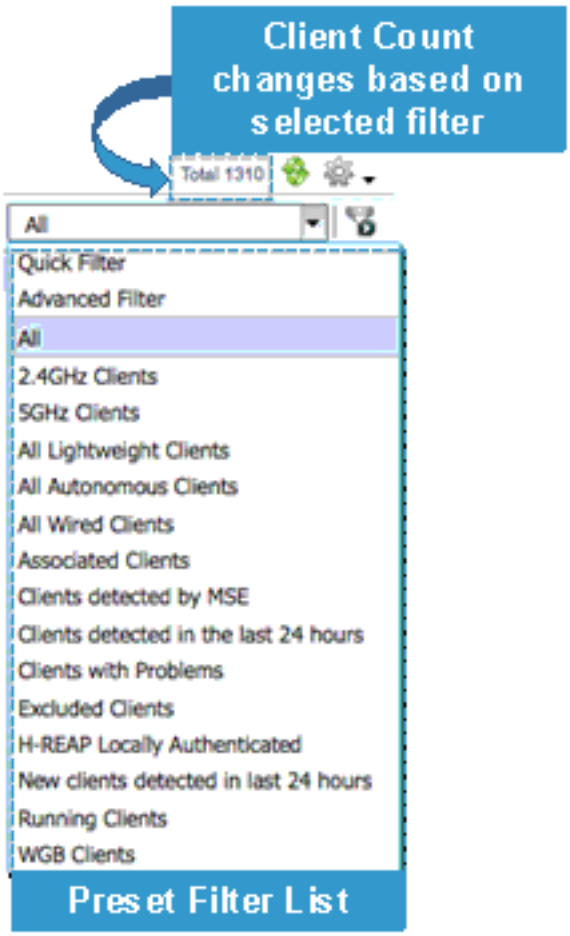



## Vigilar los clientes y a los usuarios

NCS proporciona a la capacidad de vigilar atado con alambre y los clientes de red inalámbrica (**monitor > clientes y usuarios**). Esto proporciona a una opinión unificada todos los clientes en la red. Estos filtros están disponibles.

Durante la navegación la página a la lista de los clientes y de usuarios, todos los clientes asociados se visualiza por abandono. Hay 14 actuales filtros que permiten que el usuario vea un subconjunto de clientes. Los detalles se proporcionan en la tabla. Además, hay la opción para crear los filtros de encargo:

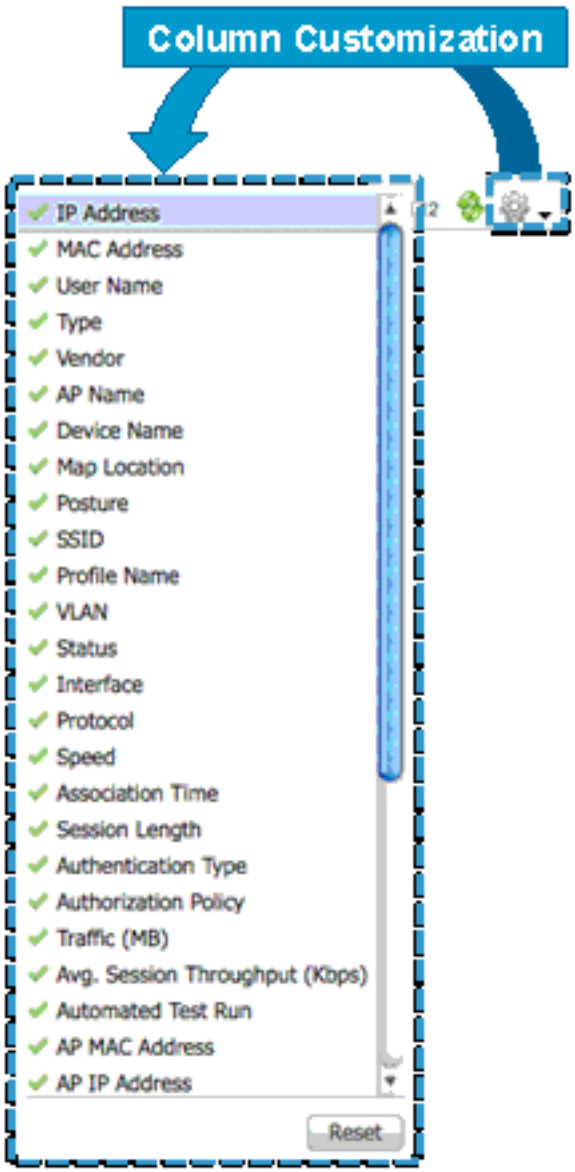
- Filtro rápido
- Filtro avanzado




| Filtros de la lista del cliente | |
|---|---|
| **Filtro** | **Resultados** |
| Todos | Todos los clientes incluyendo inactivo |
| clientes 2.4GHz | Todos los clientes de red inalámbrica activos que usan la banda de la radio 2.4 gigahertz |
| clientes 5GHz | Todos los clientes de red inalámbrica activos que usan la banda de la radio 5.0 gigahertz |
| Todos los clientes ligeros | Todos los clientes conectados con los AP ligeros |
| Todos los clientes autónomos | Todos los clientes conectados con los AP autónomos |
| Todos los clientes atados con alambre | Todos los clientes conectados directamente para cambiar manejado por NCS |
| Clientes asociados | Todos los clientes conectados sin importar si está autenticado o no |
| Clientes detectados por MSE | Todos los clientes detectados por MSE incluyendo atado con alambre y Tecnología inalámbrica |
| Clientes detectados en 24 horas pasadas | Todos los clientes detectados en 24 horas pasadas |

| | |
|---|---|
| Clientes con los problemas | Los clientes que son asociados, pero no han completado la directiva. |
| Clientes excluidos | Todos los clientes de red inalámbrica ligeros que son excluidos por el regulador |
| H-REAP localmente autenticado | Los clientes conectaron con H-REAP AP y autenticaron localmente |
| Nuevos clientes detectados en 24 horas pasadas | Todos los nuevos clientes detectados en 24 horas pasadas |
| Clientes corrientes | Clientes que han completado todas las directivas del conjunto y están en el estado de ejecución. |
| Clientes WGB | Todos los clientes WGB |

Las columnas en la tabla de la lista del cliente se pueden personalizar directamente en esta página.




Las columnas en la tabla de la lista del cliente se pueden personalizar directamente en página de

la lista de los **clientes y de usuarios**. Seleccione o las columnas del unselect para visualizar u ocultar la columna inmediatamente.

Omita el conjunto de las columnas visualizadas y su orden se puede reajustar al valor predeterminado a través del **botón reset**.

En la orden o reordene las columnas, arrastre la columna directamente en la página y muévala a la orden/a la ubicación deseadas.

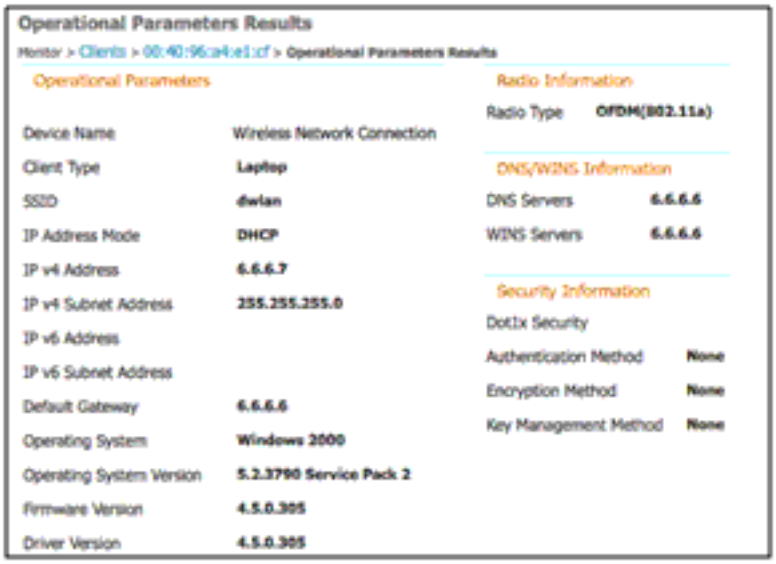
| Cliente y página del usuario: Detalles de la columna | |
|---|---|
| **Atributo** | **Comentarios** |
| IP Address | Dirección IP del cliente |
| Dirección MAC | Dirección MAC del cliente |
| Username | Username basado en la autenticación del 802.1x. El desconocido se visualiza para el cliente conectado sin un username |
| Tipo | El icono representa un peso ligero, a un cliente autónomo o atado con alambre. |
| Vendedor | Vendedor del dispositivo derivado de OUI |
| Nombre AP | Tecnología inalámbrica solamente |
| Nombre del dispositivo | Nombre del dispositivo de la autenticación de red, e.g. WLC, conmutador. |
| Ubicación de la correspondencia | Ubicación de la correspondencia del dispositivo conectado. |
| Postura | El último estatus de la postura del cliente |
| SSID | Tecnología inalámbrica solamente |
| Nombre del perfil | Tecnología inalámbrica solamente |
| VLA N | El dispositivo del VLA N está prendido |
| Estatus | Estatus del cliente actual |
| Interfaz | El interfaz del regulador (Tecnología inalámbrica) o la interfaz del switch (atada con alambre) ese cliente es conecta con. |
| Protocolo | 802.11 - Tecnología inalámbrica 802.3 - atado con alambre. |
| Velocidad | Velocidad del puerto Ethernet - atada con alambre solamente. Visualización “N/A” para la Tecnología inalámbrica |
| Tiempo de la asociación | La hora de inicio pasada de la asociación AP, Tecnología inalámbrica solamente |
| Longitud de la sesión | Longitud de la sesión |
| Tipo de autenticació | WPA, WPA2, 802.1x, etc. |

| | |
|---|---|
| n | |
| Tipo de autorización | Tipo de autorización atado con alambre de ISE |
| Tráfico (MB) | Trafique (transmitido/recibido) en esta sesión en el MB |
| Producción media de la sesión (Kbps) | Producción media de la sesión en el Kbps |
| Prueba ejecutada automatizada | Indica si el cliente está en el modo de prueba auto |
| Dirección MAC AP | Tecnología inalámbrica solamente |
| Dirección IP AP | Tecnología inalámbrica solamente |
| Regulador del ancla | Tecnología inalámbrica ligera solamente |
| Ejecutándose | El cliente ha completado todas las directivas del conjunto. |
| CCX | Tecnología inalámbrica ligera solamente |
| Nombre de host del cliente | Atado con alambre y Tecnología inalámbrica. Resultado de la búsqueda inversa DNS. |
| Dirección IP del dispositivo | Dirección IP del dispositivo conectado (WLC, conmutador o aIOS AP). |
| Puerto | Switchport en WLC |
| E2E | Tecnología inalámbrica ligera solamente. |
| Cifra del cifrado | Tecnología inalámbrica solamente |
| MSE | Servidor MSE que maneja a este cliente |
| RSSI | Tecnología inalámbrica solamente |
| SNR | Tecnología inalámbrica solamente |
| ID de Sesión | Auditoría-sesión-identificación usada en ISE y el conmutador |
| Tiempo de la sesión | Hora de inicio de la sesión por la hora de inicio de la sesión de la sesión activa – tiempo del final de la sesión para la sesión inactiva |
| Nombre del vendedor | Nombre del vendedor derivado de OUI |

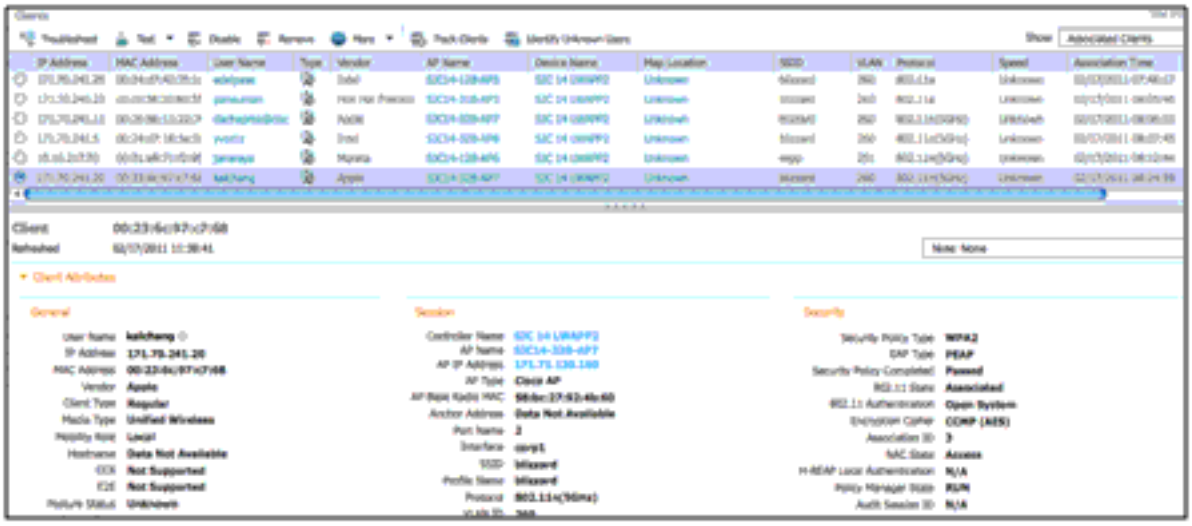
La barra de herramientas el cliente/la lista de usuario proporciona a un conjunto de las herramientas que se pueden invocar en los clientes seleccionados (uno o más).


| Monitor > clientes y usuarios: Comandos admitidos | |
|---|---|
| **Comando** | **Tipo de cliente** |
| Resolución de problemas | Todos |
| **Menú Prueba** | |
| Prueba del link | Tecnología inalámbrica ligera solamente |
| Medidas de radio | Tecnología inalámbrica ligera solamente |
| Estadísticas V5 | Tecnología inalámbrica v5 del peso ligero CCX solamente |
| Parámetros del funcionamiento | Tecnología inalámbrica v5 del peso ligero CCX solamente |
| Neutralización | Tecnología inalámbrica ligera solamente |
| Quite | Tecnología inalámbrica ligera solamente |
| **Más menú** | |
| Perfiles | Peso ligero (CCXv5) |
| Vague por la razón | Tecnología inalámbrica ligera solamente |
| Correspondencia reciente | Tecnología inalámbrica ligera solamente |
| Actual correspondencia | Tecnología inalámbrica ligera solamente |
| Sesiones | Todos |
| Detección de los APs | Tecnología inalámbrica ligera solamente |
| Historial de la ubicación | Tecnología inalámbrica ligera solamente |
| Modo del espejo del permiso | Tecnología inalámbrica ligera solamente |
| Métrica de la Voz | Tecnología inalámbrica ligera solamente |
| Clientes de la pista | Tecnología inalámbrica ligera solamente |
| Identifique a los clientes desconocidos | Todos |

**Acción del ejemplo: Parámetros del funcionamiento**



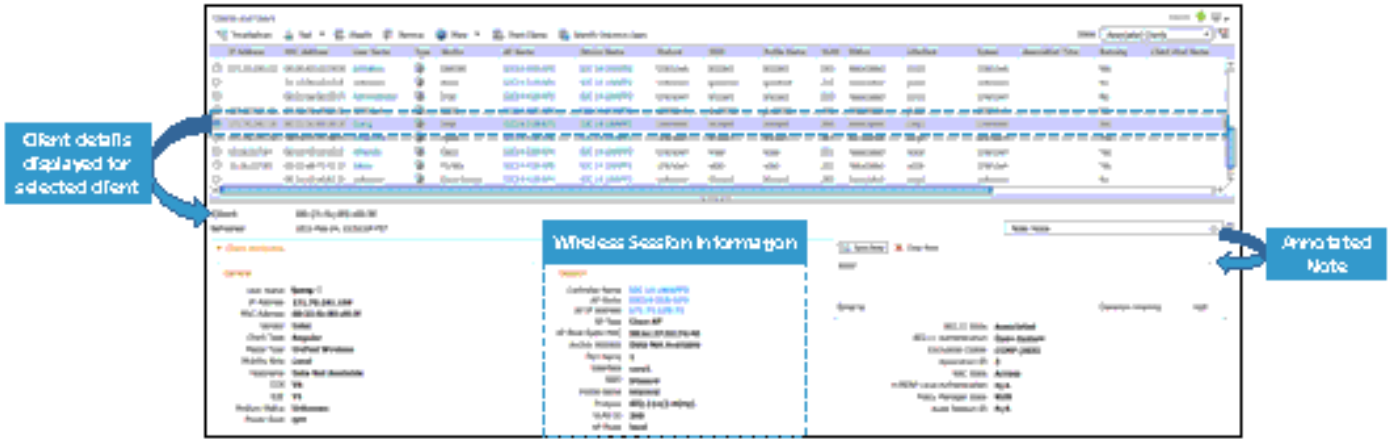

El botón de radio encendido al lado izquierdo elige a un cliente particular para visualizar a los detalles del cliente en esta lista del cliente.



cliente de red inalámbrica ligero

cliente atado con alambre

En este tiro de pantalla, el cliente en la parte inferior de la lista es un cliente de red inalámbrica del peso ligero (tipo: Tecnología inalámbrica ligera).



El ejemplo está para el cliente atado con alambre.

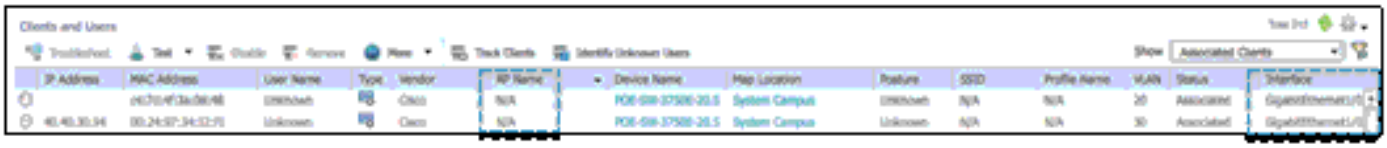

## Troubleshooting atada con alambre/del cliente de red inalámbrica

En la supervisión atada con alambre y inalámbrica NCS 1.0, y el troubleshooting se ha integrado con los servicios de la identidad. La integración entre la Administración atada con alambre/de la red inalámbrica se ha alcanzado vía tres elementos de red:

- Reguladores inalámbricos LAN de Cisco (WLC)
- Funciones de seguridad del conmutador del Cisco Catalyst: AAA, RADIUS, 802.1x y autenticación MAC, desvíos de la notificación MAC (clientes de la no-identidad), Syslog (clientes de la identidad solamente)
- Cisco Identity Services Engine (ISE)

Visualizan a todos los clientes – atados con alambre y Tecnología inalámbrica – en la página de los clientes y de los usuarios (**monitor > clientes y usuarios**).

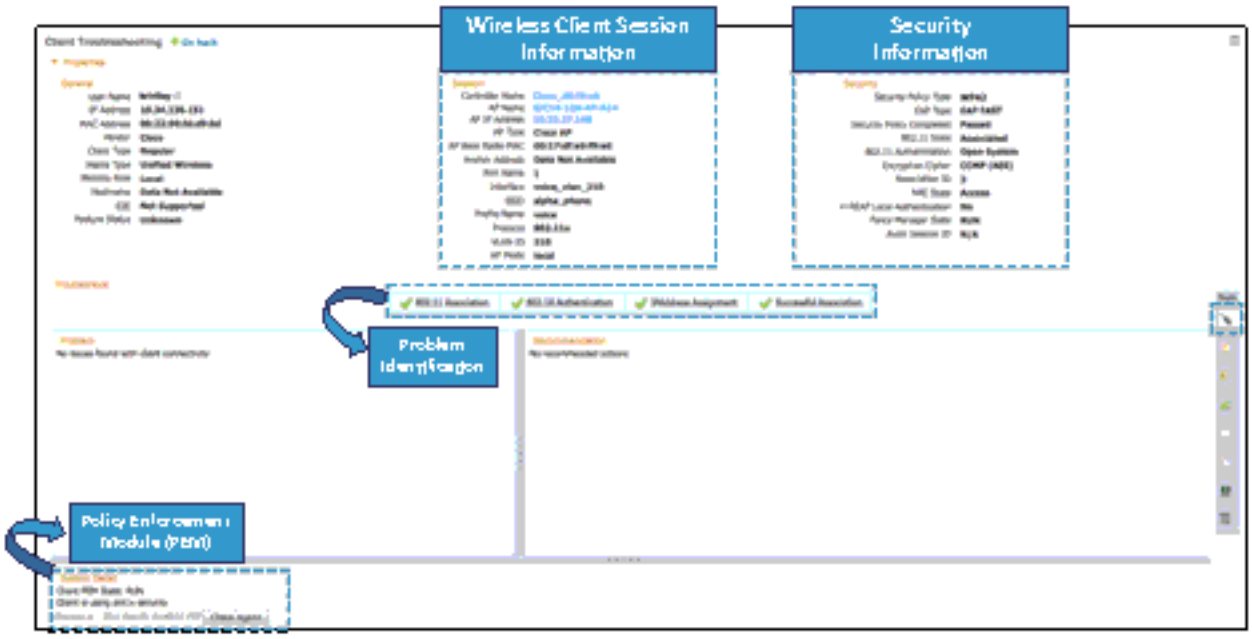
**El nombre** atado con alambre de la visualización **AP de los** clientes como información de puerto del switch *N/A.* se proporciona en los **interfaces**.



### Troubleshooting del cliente de red inalámbrica

Para lanzar la herramienta del troubleshooting del cliente, haga clic en el botón de radio a la izquierda del elemento de lista del cliente. Una vez que seleccionan al cliente, haga clic en el icono del **troubleshooting** en la barra de herramientas.

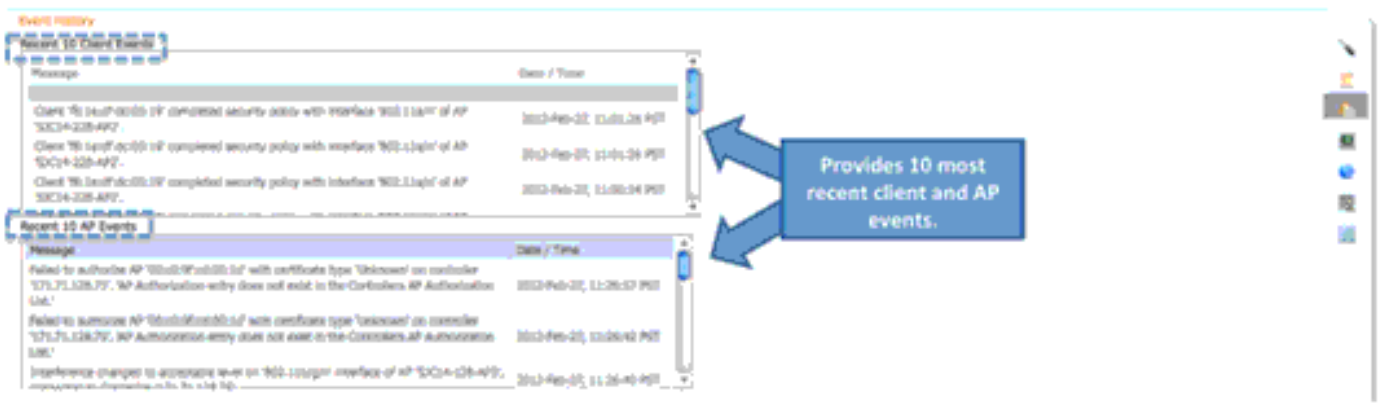

La ventana se visualiza para el cliente.



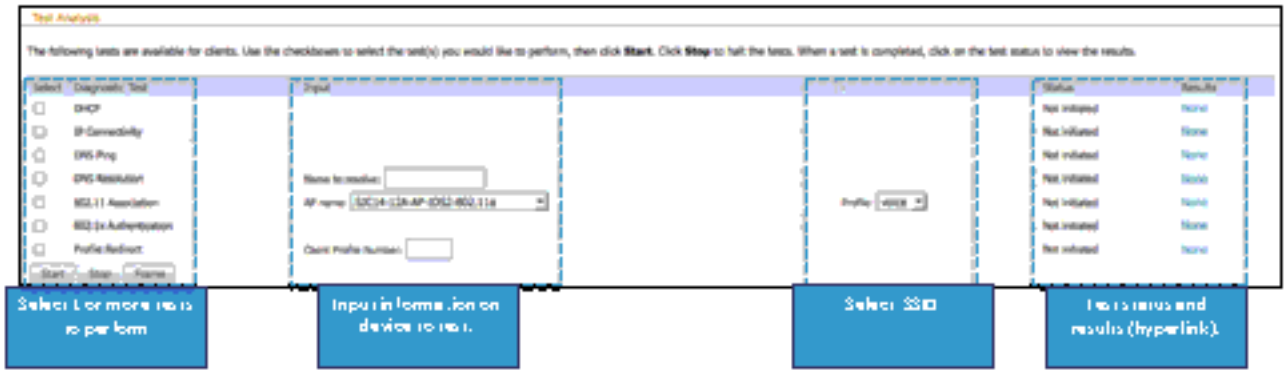

Los mensajes de registro se pueden extraer del regulador con el uso de la herramienta de análisis del registro.


Refiera al módulo de la aplicación de políticas (PEM) para más información sobre el estado PEM.

La herramienta del historial de eventos provee del usuario los mensajes del evento del cliente y del AP.



Pruebe la herramienta de análisis (los clientes CCXv5)



## Troubleshooting atado con alambre del cliente

NCS 1.0 proporciona a la administración integrada de atado con alambre y los dispositivos de red inalámbrica/los clientes. Una de las características importantes en NCS 1.0 es que vigila y que resuelve problemas para atado con alambre y los clientes de red inalámbrica. El SNMP se utiliza para descubrir a los clientes y para recoger los datos del cliente. ISE se sondea periódicamente para recoger las estadísticas del cliente y otros atributos para poblar los componentes y los informes relacionados del panel.

Si ISE se agrega a los sistemas y los dispositivos están autenticando a él, el cliente detalla las páginas muestra los detalles adicionales etiquetados como Seguridad.

Para navegar a la página del troubleshooting del cliente, haga clic en el icono del **troubleshooting** en el menú de las herramientas en la cima de la página.


Esto lleva al usuario a la página mostrada en la captura de pantalla. En este ejemplo, el dispositivo cliente tiene la Conectividad del link, pero autenticación fallada MAC.


En el Lado derecho de la pantalla es una barra de herramienta con estos items todo relacionados

a resolver problemas:

- Herramienta del troubleshooting del cliente
- Análisis del registro
- Historial de eventos
- Historial enterado del contexto

El historial de eventos proporciona a los mensajes relacionados con los eventos de la Conectividad para este cliente. En este ejemplo, el cliente no podido para autenticar con éxito. Se proporciona la fecha/la hora de ayudar al administrador de la red en resolver problemas a este cliente.

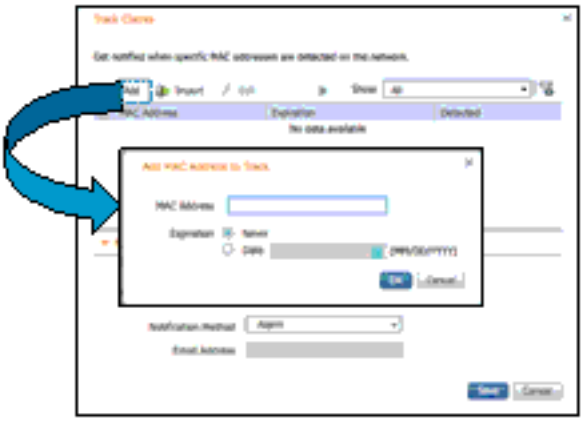

ISE proporciona a los expedientes de la autenticación a NCS vía el RESTO API. El administrador de la red puede elegir el período de tiempo para extraer los expedientes de la autenticación de ISE. En este ejemplo, el expediente de la autenticación indica que no encontraron al usuario en la base de datos ISE.


# Características RF/Wireless

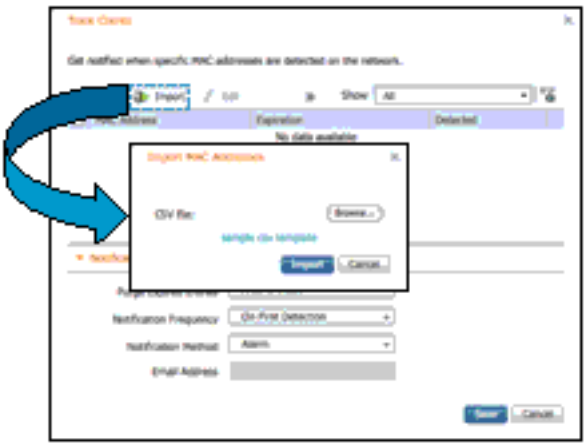
## Clientes de la pista

Esta característica permite que un administrador de la red siga a los clientes específicos y sea notificado cuando estos clientes conectan con la red. Esta característica se activa de la página del monitor > de los usuarios y de los clientes.


Para seguir al solo cliente, haga clic el **botón Add** y una sub-ventana aparece donde el usuario puede ingresar el MAC address del cliente junto con la expiración de seguimiento (nunca o fecha de extremo especificada).



Si el usuario quiere seguir a los clientes múltiples, la lista del cliente puede ser importada. La ventana resultante permite al usuario a la lista de importación de direcciones MAC del cliente con archivo CSV.



Una muestra archivo CSV puede ser descargada que proporciona al formato de datos.

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

## Configuraciones de la notificación

Hay tres opciones para las notificaciones:

1. Entradas expiradas purgadas — el usuario puede fijar la duración para mantener a los clientes seguidos la base de datos NCS. Los clientes pueden ser purgados:después de 1 semanadespués de 2 semanasdespués de 1 mesdespués de 2 mesesdespués de 6 mesesguardado indefinidamente
2. Frecuencia de la notificación — el usuario puede especificar cuando NCS envía la notificación del cliente seguido:en la primera detecciónen cada detección
3. Método de notificación — el usuario puede especificar para que el evento del cliente seguido genere la alarma o envíe el correo electrónico.

## Visualizar a los clientes seguidos

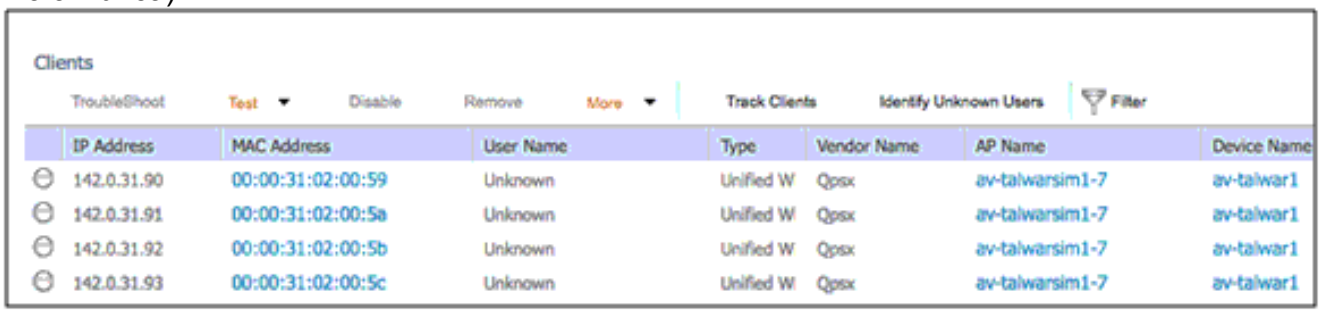
Después de que se haya ingresado la información de usuario seguida, la ventana seguida de los clientes permite que el usuario vea el estatus de los clientes seguidos existentes.


## Identificación del usuario desconocida

Autentican a no todos los usuarios/dispositivos vía el 802.1x (e.g impresoras). En este evento, la red administra tiene la opción para asignar un nombre al dispositivo.

Si un dispositivo cliente se autentica a la red vía la red auténtica, el WCS puede no tener información del nombre de usuario para ese cliente. En este decorado, los clientes pueden querer tener nombres del usuario asociados a los clientes, incluso si están utilizando la red auténtica.

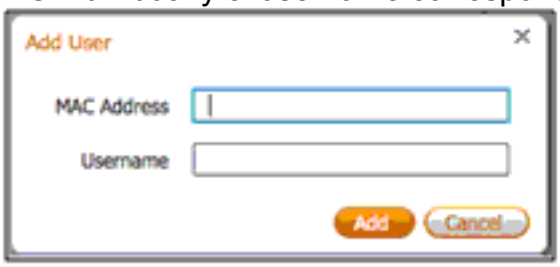
1. Elija el **monitor > a los clientes**.Visualizan a los clientes inalámbricos y atados con alambre. Según lo descrito previamente, una barra de herramientas está situada en la lista anterior de clientes que permite que el usuario invoque varias acciones:Troubleshootingpruebe (prueba del link, medida de radio, estadísticas CCXv5, parámetros de funcionamiento)neutralizaciónquite (desasocie al cliente de red inalámbrica)




2. Haga clic el icono de los **usuarios desconocidos de la identificación** en la barra de herramientas.


Esto resulta con una ventana emergente.

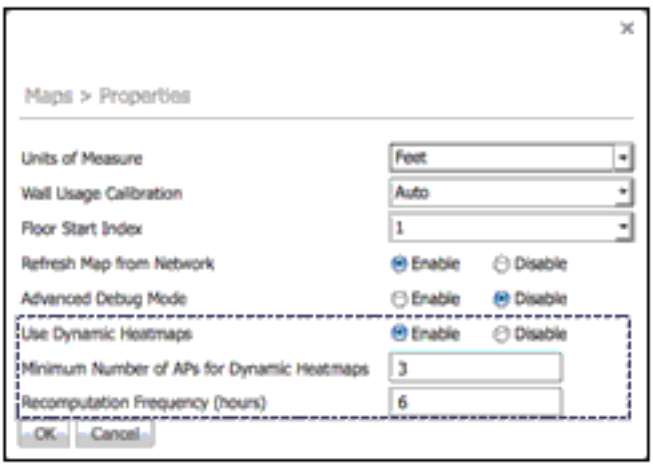
3. El tecleo **agrega** para ingresar a los detalles del cliente. 

La dirección MAC individual y el username correspondiente pueden ser agregados. 

Una vez que han agregado a un cliente y una dirección MAC, el WCS utiliza esta tabla para las operaciones de búsqueda del cliente basadas en la dirección MAC que corresponde con.

## Correspondencias en tiempo real del calor

Una de las nuevas funciones en NCS 1.0, es la opción para visualizar las correspondencias en tiempo real del calor. Esto se activa como opción predeterminada. Elija el **monitor > las correspondencias > las propiedades** para navegar a las configuraciones.




## Vigilar el Switches del Cisco Catalyst usando NCS

La información atada con alambre del inventario es determinada por estos métodos:

- Descubrimiento atado con alambre del cliente vía el SNMP traps, la Consulta SNMP y los mensajes de Syslog del Switches
- ISE API en dirección del norte para la información adicional, tal como postura, profiler,

estadísticas, y así sucesivamente

NCS provee de la paridad de función WCS 7.x para la supervisión del cliente y de la información en todos los clientes (atados con alambre y Tecnología inalámbrica). Además, troubleshooting de los cruz-lanzamientos ISE NCS para los clientes atados con alambre. El nivel adicional de integración ISE está vía el cruz-lanzamiento de los informes ISE con los datos no contenidos en el WCS.

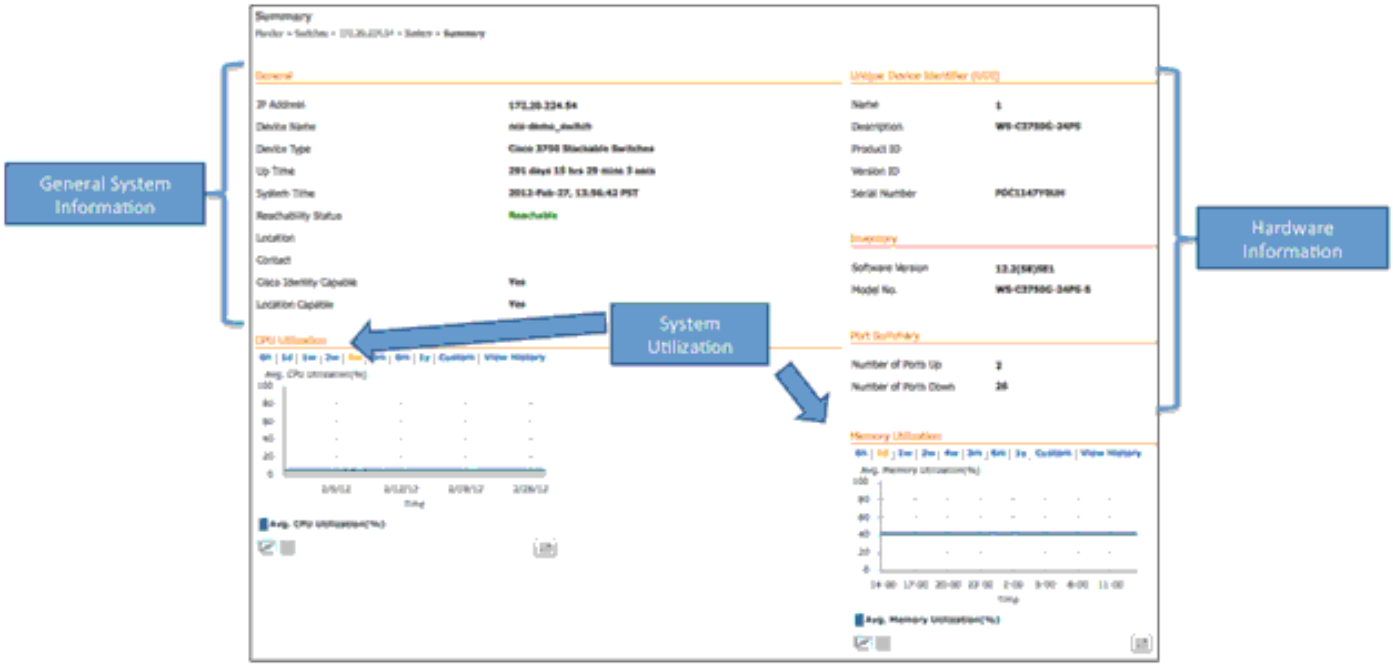
Esta información del conmutador se proporciona en NCS:

- Activos físicos, por ejemplo, chasis, módulos, puerto, y fuente de alimentación del MIB de la entidad
- Dispositivo/división/ficheros de destello
- Imagen instalada del software
- Interfaz de los Ethernetes
- Interfaz IP
- Interfaz del VLA N
- VLA N y VTP
- EtherChannel
- STP
- StackWise (utilizado solamente en los Cisco Catalyst 3750 Switch)

El monitor > el conmutador visualiza esta información del conmutador:

- Dirección IP
- Nombre del dispositivo: hostname según lo dado en la configuración IOS del conmutador
- Tipo de dispositivo: cambie el modelo
- Reachability: Conectividad SNMP
- Cuenta del cliente: número de clientes conectados directamente con el conmutador


La dirección IP visualizada es un enlace hipertexto, y hacerlo clic en toma al usuario **para configurar > conmutador de los Ethernetes > (dirección IP) >** pantalla **sumaria**.

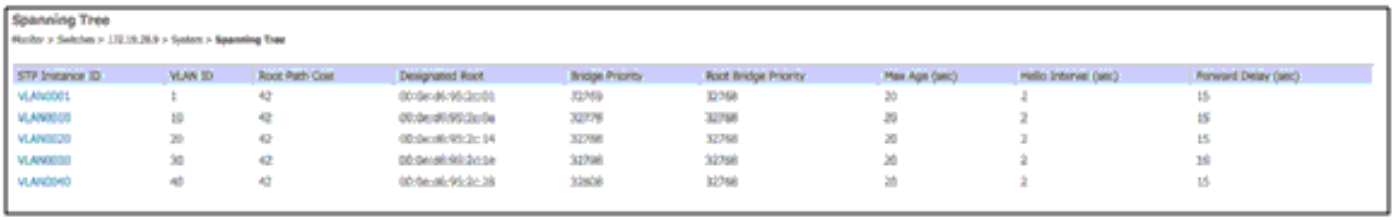



Descubren a los clientes atados con alambre vía el SNMP traps, la Consulta SNMP y los mensajes de Syslog del Switches.

Con NCS, el Switches del Cisco Catalyst se puede vigilar para esta información:

- Chasis: UDI, nombre modelo, uptime
- Utilización Memory/CPU
- Puertos/estatus de los interfaces
- Capa 2 (VLA N, VTP, atravesando - árbol)
- Entorno: estado de la fuente de alimentación y fans
- Memoria y ficheros en el sistema
- Clientes (atados con alambre)

## El atravesar - árbol

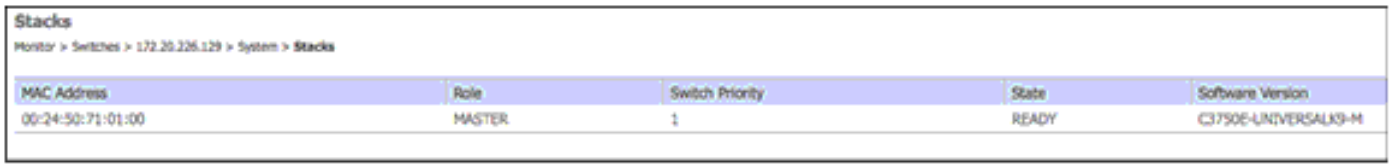



El atravesar - los detalles del árbol para cada instancia del árbol de expansión se proporcionan:

- Puerto STP
- Función del puerto
- prioridad de puerto
- Costo del trayecto
- Estado de puerto
- Tipo del puerto

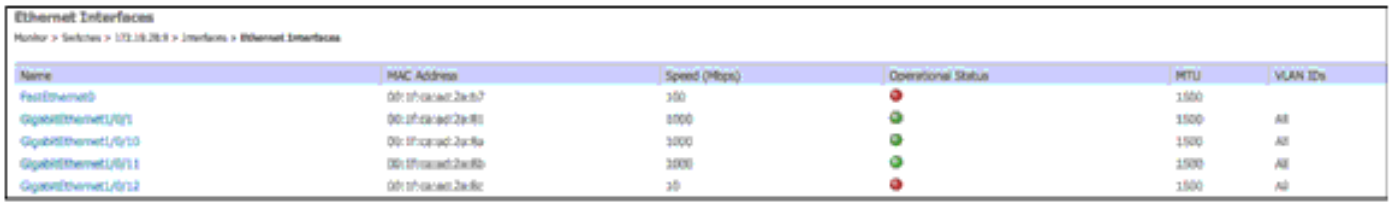

## Cisco StackWise

Para el Switches del Cisco Catalyst que utiliza la tecnología de StackWise, cada uno cambia el papel en la pila se proporciona incluyendo su papel en la pila, cambia la prioridad, el estado y la versión de software.

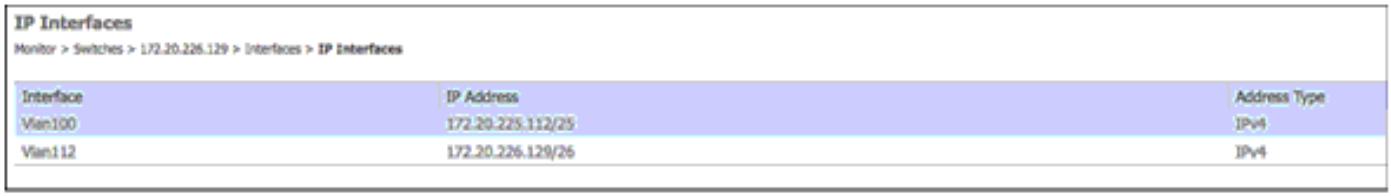



### Detalles del interfaz

La información de estatus en todos los interfaces de los Ethernetes se visualiza.

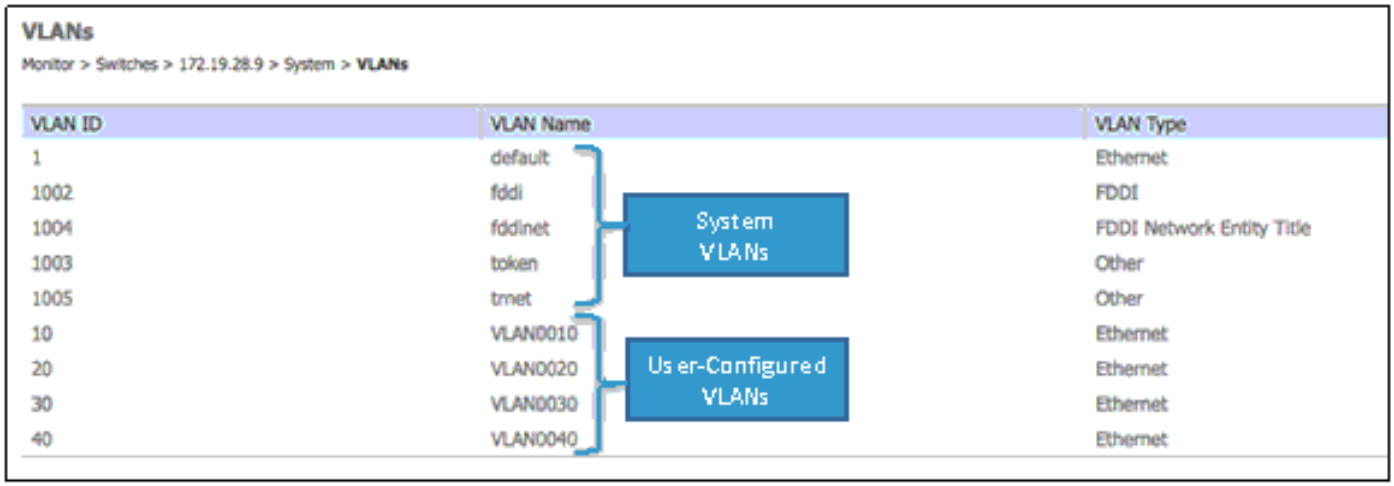



La información de la capa 3 también se proporciona (VLA N a la asignación de la subred IP).

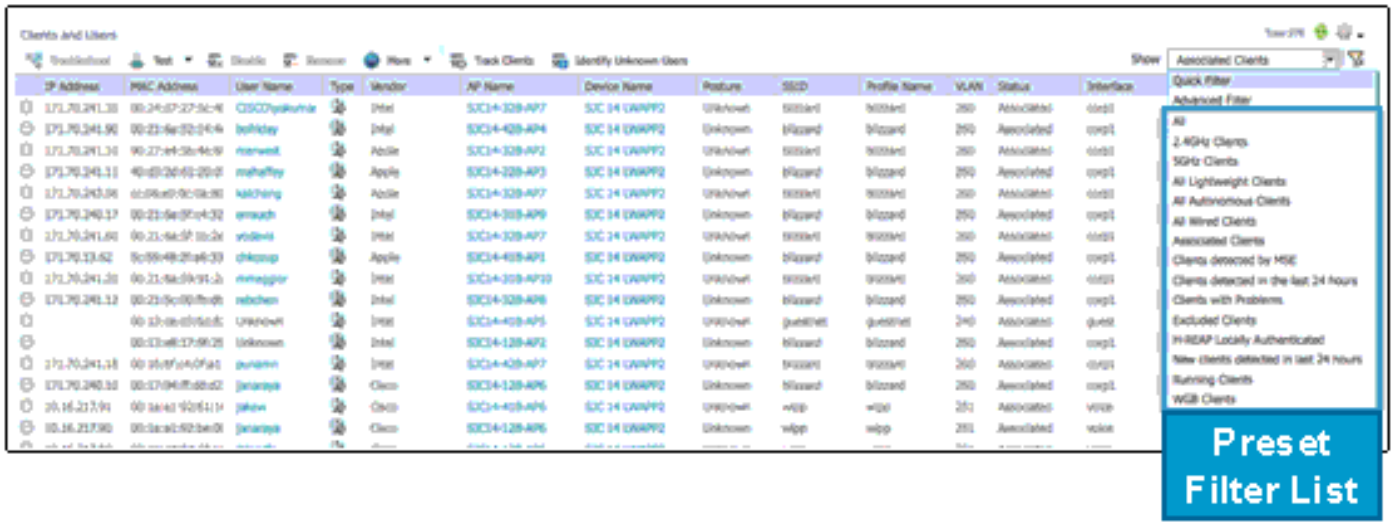



## Información del VLA N

Los detalles del VLA N están también disponibles de NCS. Se visualizan los VLA N del valor predeterminado del sistema y del usuario configurado. La identificación del VLA N, el nombre y el tipo se visualizan en un monopantella.




## Páginas de la lista del cliente




# Informes (Cruz-lanzamiento y escala)

NCS 1.0 proporciona a la administración integrada de atado con alambre y los dispositivos de red inalámbrica/los clientes. El SNMP se utiliza para recoger los datos del cliente. ISE se sondea periódicamente para recoger las estadísticas del cliente y otros atributos para poblar los informes relacionados.

Elija los **informes > la plataforma de lanzamiento de los informes**. Elija el informe para la creación/el arreglo para requisitos particulares.

## Nuevos informes

### Conexiones superiores N

Esto señala que las demostraciones rematan a los usuarios N en un período de tiempo dado basado en estas métricas:

- Intentos de conexión
- Tentativas pasajeras
- Intentos fallidos

Este informe contiene estas columnas:

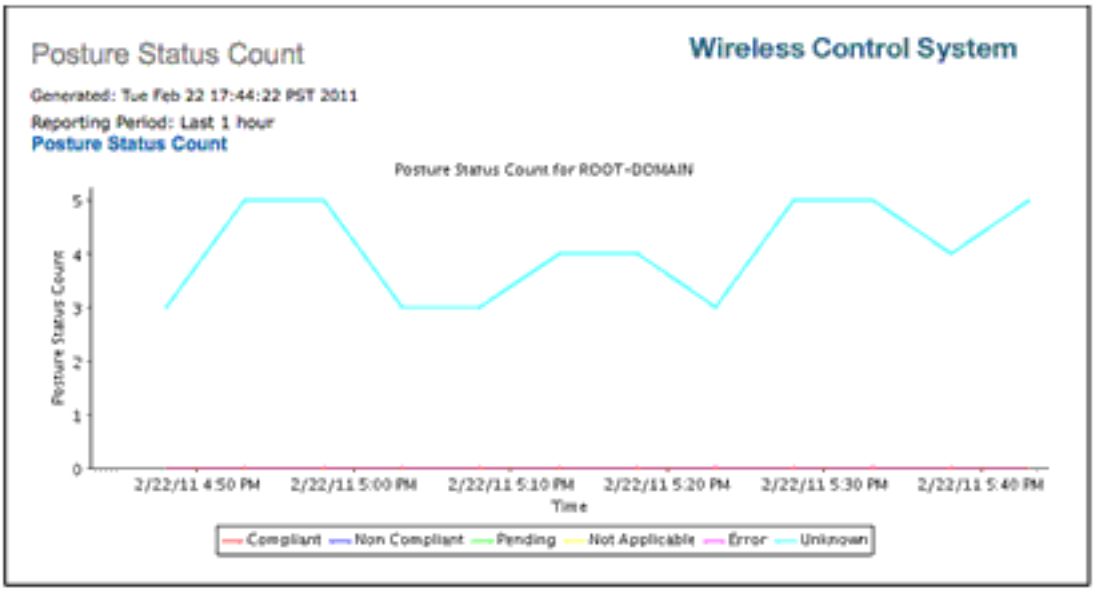
- Username
- Número de intentos de conexión totales
- Número de intentos de conexión pasajeros
- Número de tentativas de la falla de conexión

### Asociación AP

Este los informes enumera todos los detalles de la asociación AP para los clientes de red inalámbrica y son similares a los informes de la sesión de cliente.

### Cuenta del estatus de la postura

Este informe proporciona a una carta de la tendencia para mostrar el estatus de la postura del cliente en un cierto plazo. La carta es una carta de área; el área inferior es el número de clientes pasajeros el control de la postura y la área superior es el número de clientes que fallaron el control de la postura.




## Alarmas/eventos

Las alarmas y los eventos proporcionan a una sola opinión de la página de las alarmas y de los eventos para atado con alambre y Tecnología inalámbrica. Visualizan el resumen y al navegador persistentes de la alarma en el abajo a la derecha de la pantalla sin importar en qué pantalla está el usuario. NCS 1.0 proporciona a las opiniones genéricas de la alarma incluyendo estas páginas:

- Páginas de la lista de la alarma
- Páginas del detalle de la alarma
- Páginas de la Lista de eventos
- Páginas del detalle del evento
- Búsqueda de la alarma por la categoría y la categoría sub
- Ventana del resumen de la alarma
- Panel de la alarma

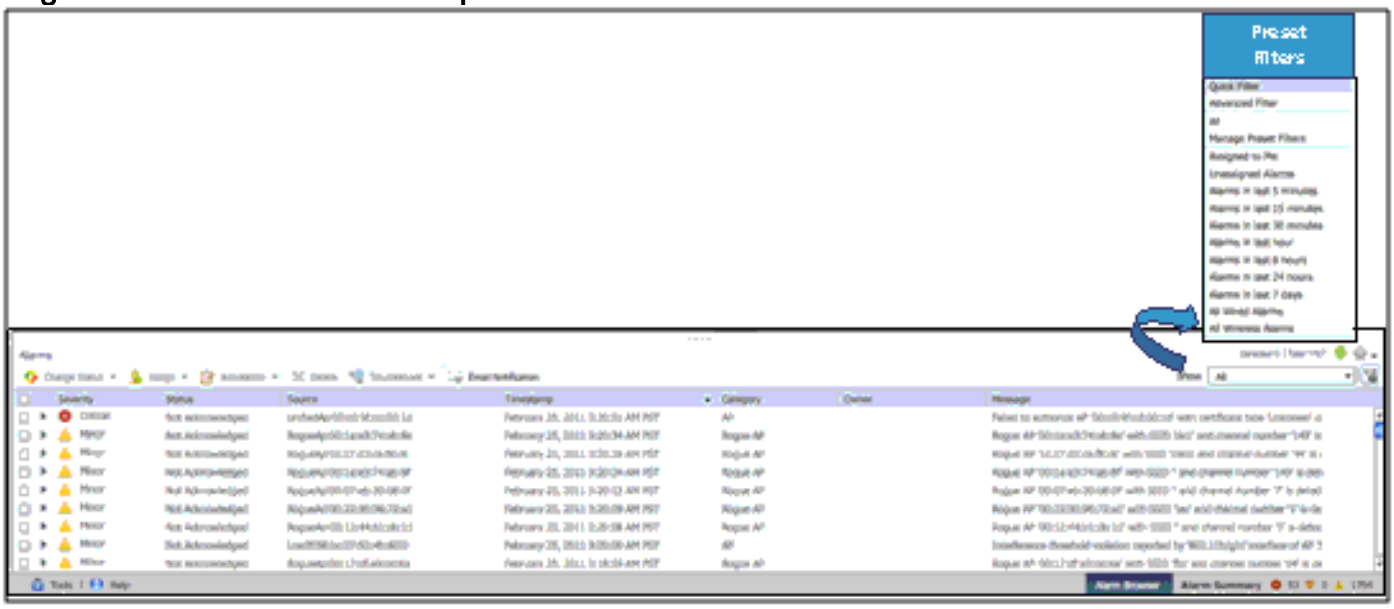
- Acciones de la alarma (reconozca, borre, asigne, unassign, cancelación, etc.)
- Notificación de alarma (correo electrónico, desvío)
- Navegaciones de la página de la alarma (y a las distintas vistas)
- El panel de la descripción de la alarma - drilldown a la lista filtrada
- Página existente del troubleshooting del lanzamiento WCS de la página de la alarma

Las columnas se pueden personalizar por ejemplo visualizado, ocultado, y haber reordenado. Las acciones se pueden adquirir una o más alarmas simultáneamente.

## Filtro rápido

Esta característica permite que un usuario filtre en una o más columnas basadas en la cadena de texto ingresada en el filtro clasifiado en la cima de cada columna. Proporciona a una vista filtrada opcional de las alarmas para las alarmas atadas con alambre y inalámbricas.

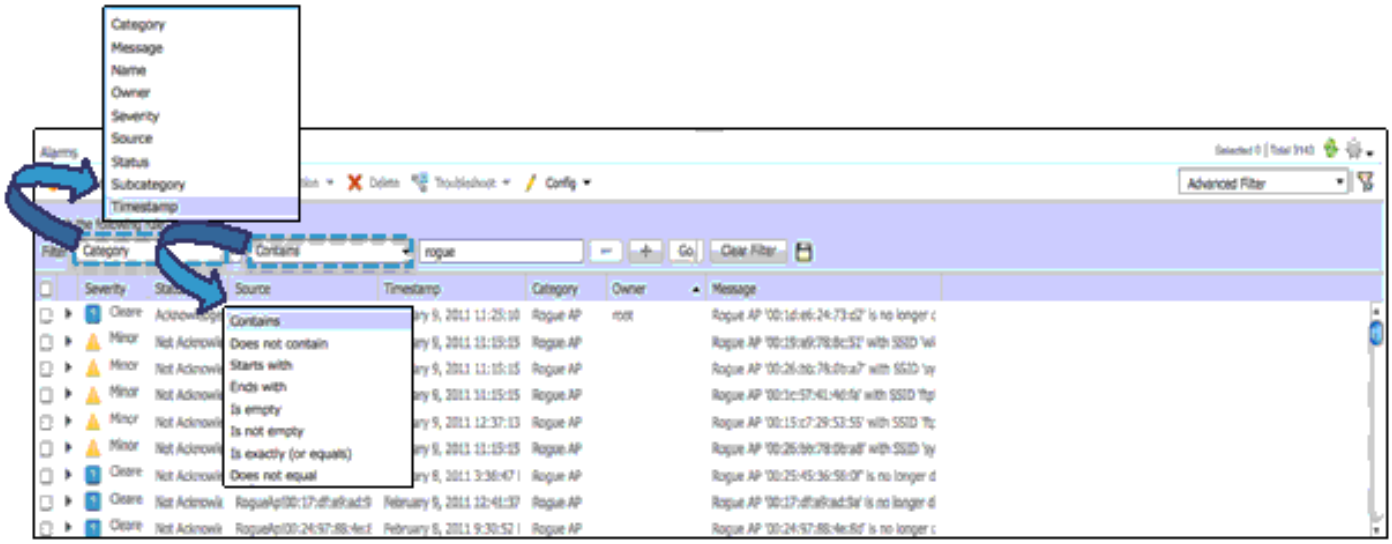
**Página de las alarmas – Filtro rápido**




## Filtro avanzado

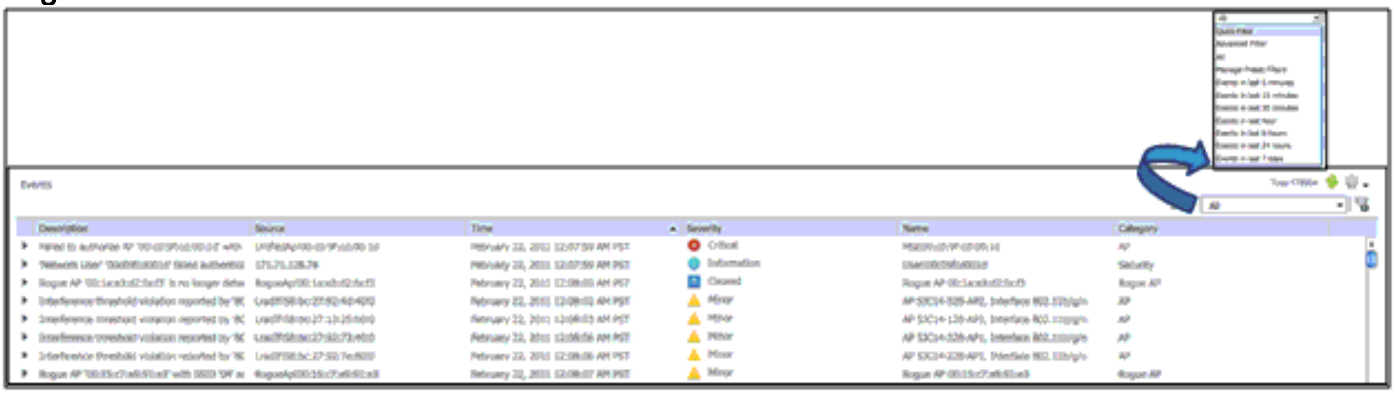
El filtro avanzado proporciona incluso a la mayor capacidad de la búsqueda. Proporciona a la capacidad de buscar en los campos específicos con las diversas condiciones, por ejemplo contiene, no contiene, comienza con, y termina con. Este diagrama muestra las diversas opciones de filtro. Además, el filtro avanzado permite la jerarquización de la condición y (Y/O) de las condiciones boleanas que se especificarán.

**Página de las alarmas – Filtro avanzado**

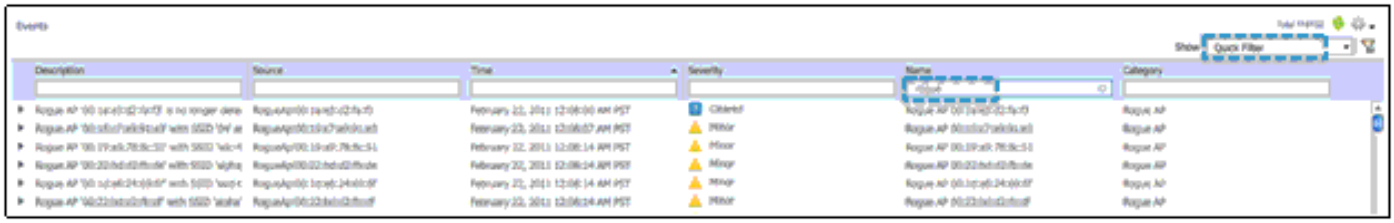



Semejantemente, los eventos se pueden visualizar y filtro encendido fácilmente. También ha preestablecido, aprisa y los filtros avanzados. Estos filtros funcionan de la misma manera que estos el mismo filtro en las alarmas.

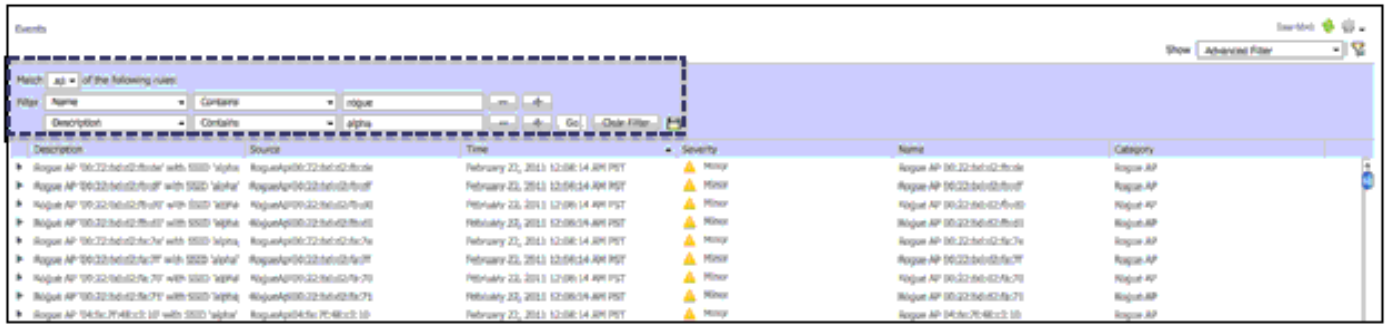
### Página de los eventos



### Página del evento - Filtro rápido

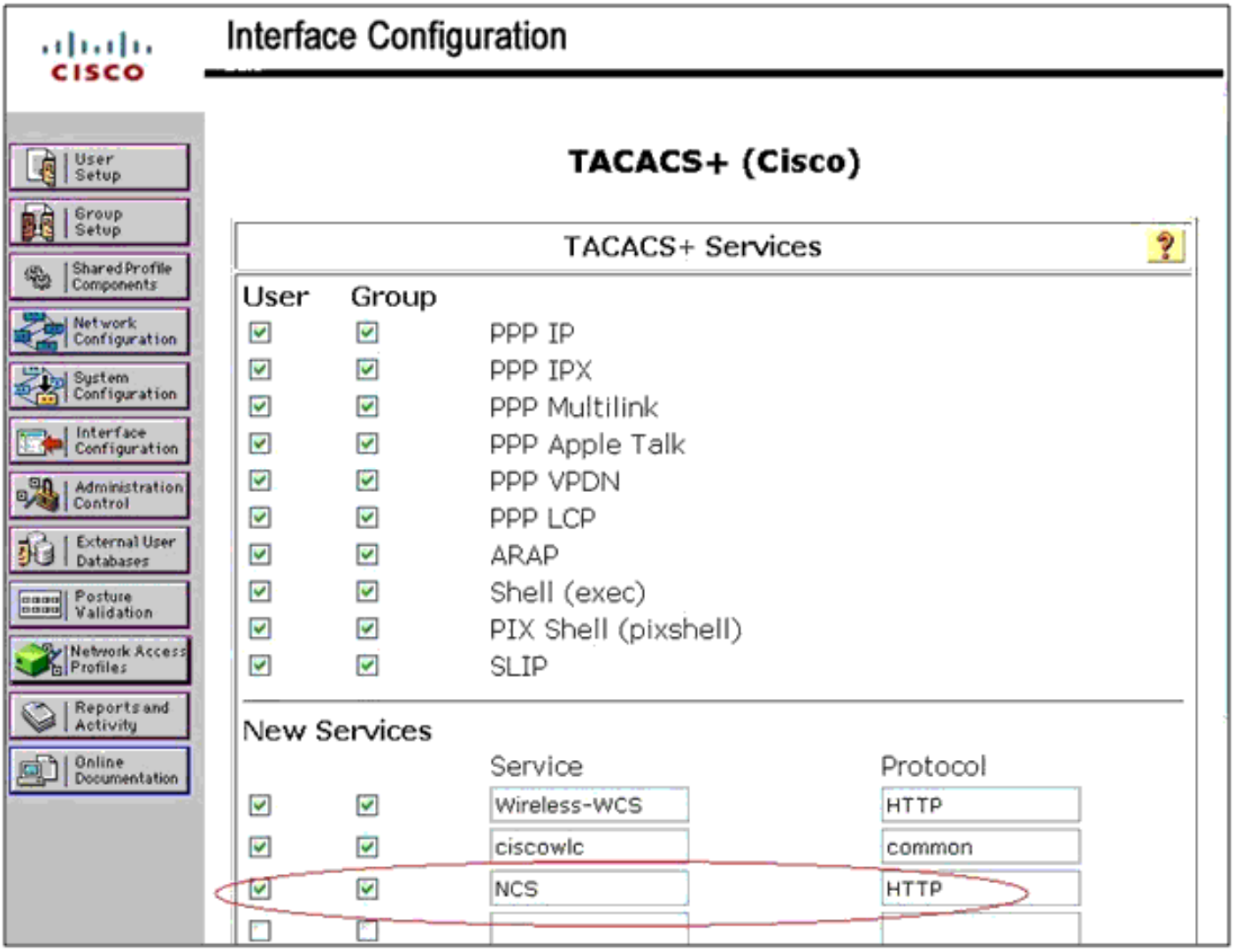


### Página del evento - Filtro avanzado



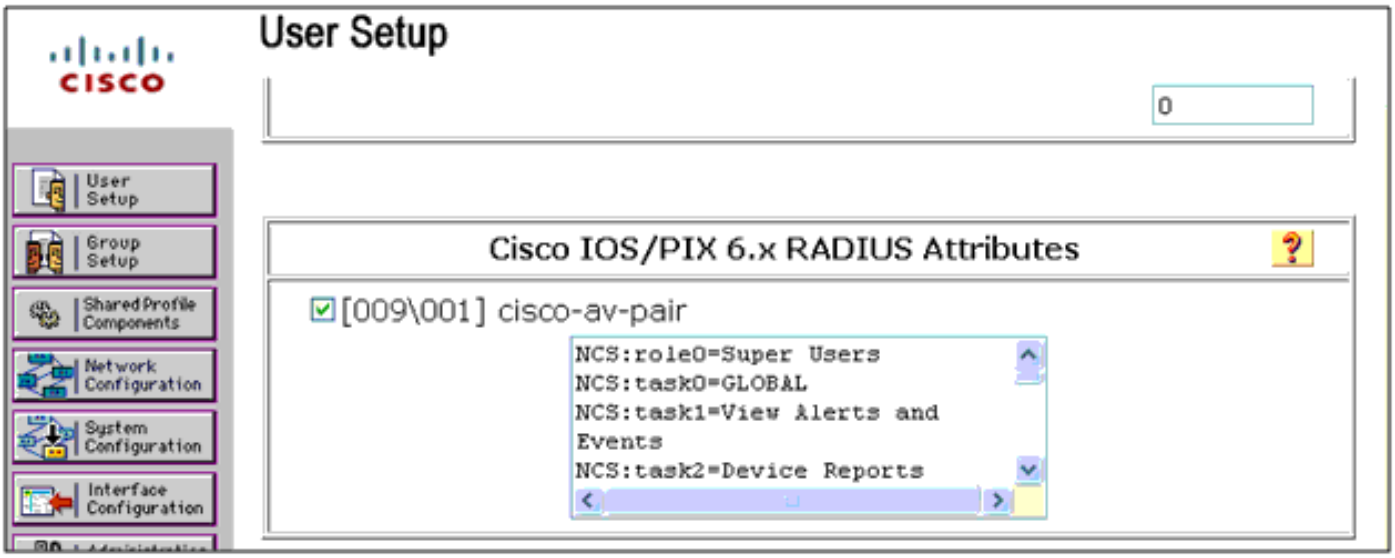
## Autenticación de usuario AAA vía el TACACS+/RADIUS usando ACS 4.2

Para que a los usuarios TACACS+ autentiquen con éxito en NCS, requieren algunos cambios en ACS 4.2. Un nuevo servicio NCS HTTP necesita ser agregado en la página de la configuración de la interfaz para TACACS+ (Cisco IOS).




El conjunto entero de los atributos personalizados de la lista de tareas TACACS+ del grupo de usuarios NCS necesita ser copiado en la área de texto de los atributos personalizados NCS HTTP tal y como se muestra en de la captura de pantalla para un usuario AAA. Lo mismo se considera bueno para el grupo de usuarios.


Para la autenticación de usuario de RADIUS, usted necesita copiar los nuevos atributos personalizados del radio de la lista de tareas del grupo de usuarios NCS en la sección de los atributos de RADIUS de Cisco IOS/PIX 6.x para el usuario/el grupo de usuarios.




De NCS, agregue la nueva Entrada de servidor TACACS+/Radius en la **administración >AAA > los servidores/radio TACACS+**. Fije el modo AAA en **configuraciones de modo de la administración >AAA >AAA a TACACS+/al radio** por consiguiente. Re-clave como usuario AAA.

## Información Relacionada

- Soporte técnico y documentación - Cisco Systems