Guía de Configuración e Implementación de Virtual Appliance de la Versión 7.2 del Software MSE

Contenido

Introducción

La versión 7.2 del software Cisco Mobility Services Engine (MSE) añade un dispositivo virtual y compatibilidad con VMware ESXi. Este documento proporciona pautas de configuración e instrumentación, así como consejos de Troubleshooting, para los usuarios que agreguen el dispositivo virtual MSE a una Cisco Unified WLAN y que ejecuten Servicios que reconocen el

contexto y/o Cisco Adaptive Wireless Intrusion Prevention System (wIPS). Además, este documento describe los requisitos del sistema para el dispositivo virtual MSE y proporciona pautas generales de implementación para el dispositivo virtual MSE. Este documento no proporciona detalles de configuración para el MSE y los componentes asociados. Esta información se proporciona en otros documentos; se proporcionan referencias.

Refiérase a la sección Información Relacionada para ver una lista de documentos sobre la configuración y el diseño de los Servicios de Movilidad con Identificación del Contexto. La configuración wIPS adaptativa tampoco se trata en este documento.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco 3300 Series Mobility Services Engine.

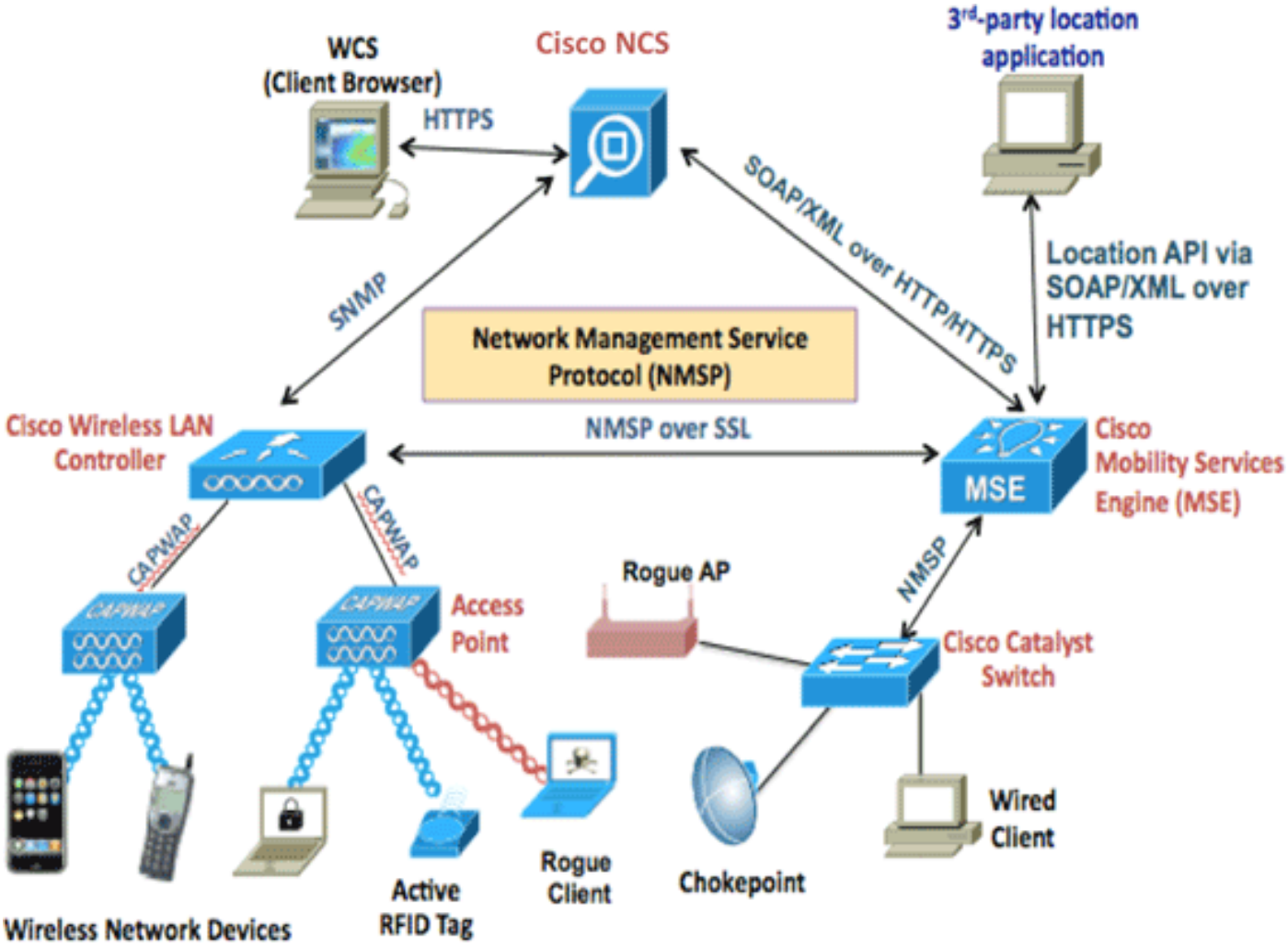
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Antecedentes

Esta imagen muestra la implementación típica de Cisco WLAN que incluye Cisco Mobility Services Engine (MSE). Esta implementación también incluye otro cliente de red por cable/inalámbrica, etiquetas RFID y un punto de acceso (AP) y cliente no autorizados. MSE proporciona visibilidad de estos elementos tanto para la ubicación como para wIPS. Antes de la versión 7.2 del software MSE, sólo los dispositivos físicos estaban limitados a MSE-3310 y MSE-3350/3355.



Requisitos del sistema

El appliance virtual versión 7.2 del software MSE es compatible y probado en VMware ESXi 4.1 y posterior. Estas configuraciones de servidor se han probado y se recomiendan como guía.

- Servidor de montaje en bastidor Cisco Unified Computing System (UCS) C200 M2¿Dos (2) Intel? ¿Xeon? CPU E5506 a 2,13 GHzRAM (según el nivel configurado)Unidades SAS con controladores RAID mejorados (mínimo de 500 GB+)
- Servidor de montaje en bastidor UCS C210 M2Dos (2) CPU Intel Xeon E5640 a 2,67 GHzRAM (según el nivel configurado)Unidades SAS con controladores RAID mejorados (mínimo de 500 GB+)
- Servidor de montaje en bastidor UCS C250 M2Dos (2) CPU Intel Xeon E5570 a 2,93 GHzRAM (según el nivel configurado)Unidades SAS con controladores RAID mejorados (mínimo de 500 GB+)
- Servidor de montaje en bastidor UCS C460 M2Dos (2) CPU Intel Xeon E7-4830 a 2,13 GHzRAM (según el nivel configurado)Unidades SAS con controladores RAID mejorados (mínimo de 500 GB+)

Nota: Utilice dos (2) procesadores de cuatro núcleos que sean al menos tan potentes como los mencionados anteriormente.

Software de gestión y licencia de VMware

El dispositivo virtual Cisco MSE Software Release 7.2 es compatible con ESX/ESXi 4.x y superiores.

Para administrar los hosts de ESXi y para configurar e implementar los appliances virtuales, Cisco recomienda instalar vCenter Server 4.x en una máquina con Windows XP o Windows 7 de 64 bits y obtener una licencia de vCenter Enterprise. Alternativamente, si sólo tiene un host ESXi, puede utilizar el cliente vSphere para administrarlo.

Necesidades de recursos

Los requisitos de recursos dependen de la licencia que desee implementar. Esta tabla enumera los diferentes niveles en los que puede configurar su dispositivo virtual:

MSE principal	Recursos		Licencia admitida (individualmente)	
Nivel de dispositivo virtual	Memoria total	CPU	Licencia CAS	Licencia de wIPS
Bajo	6 G	2	2000	2000
Estándar	11 G	8	18000	5000
Alto	20 G	16	50000	10000

Nota: Los límites sugeridos enumerados para las licencias CAS y wIPS son límites máximos admitidos cuando sólo se está ejecutando un servicio. Se aplican límites de coexistencia si desea ejecutar ambos servicios en el mismo dispositivo.

Configuración del Host ESXi

Complete estos pasos para configurar un dispositivo virtual MSE en un UCS o servidor similar:

1. Asegúrese de que su máquina tenga al menos 500 GB de espacio en disco duro y unidades SAS rápidas con controladores RAID mejorados. (Utilice un tamaño de bloque de al menos 4 MB cuando cree almacenes de datos para versiones anteriores a ESXi 5.0.)
2. Instale ESXi.Inserte el disco de instalación ESXi 4.1 o posterior y arranque desde la unidad.Si utiliza varias unidades, instale ESXi en la unidad configurada como la unidad de inicio. El nombre de usuario predeterminado es root y la contraseña está en blanco (sin contraseña).**Nota:** Si elige la unidad equivocada para la instalación, puede reformatear usando un CD de Fedora Live.
3. Configure la dirección IP.Elija los adaptadores de red que estén activados y activos. Es posible que tenga varios adaptadores de red si el host está conectado a varias redes. Puede establecer la misma dirección IP durante la configuración de CIMC; presione F8 durante el inicio para establecer la dirección IP. Además, cambie la contraseña predeterminada.

Una vez que se configura ESXi, puede utilizar una máquina con Windows XP o Windows 7, junto con la dirección IP y las credenciales de inicio de sesión configuradas anteriormente, para conectarse al host ESXi a través del cliente vSphere.

Consulte Licencia ESX 4.x, ESXi 4.x y vCenter Server 4.x para obtener información sobre la licencia del host ESXi.

Consulte estos artículos para obtener información sobre cómo configurar los almacenes de datos en ESXi:

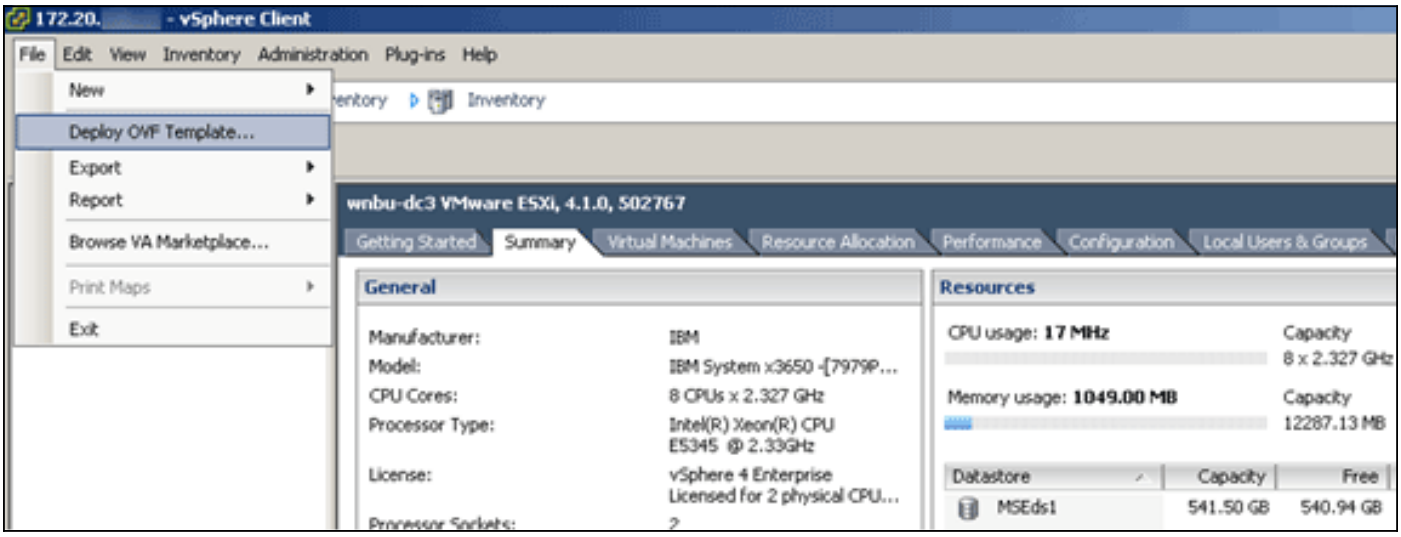
- Crear almacenes de datos VMFS
- Aumente los almacenes de datos VMFS

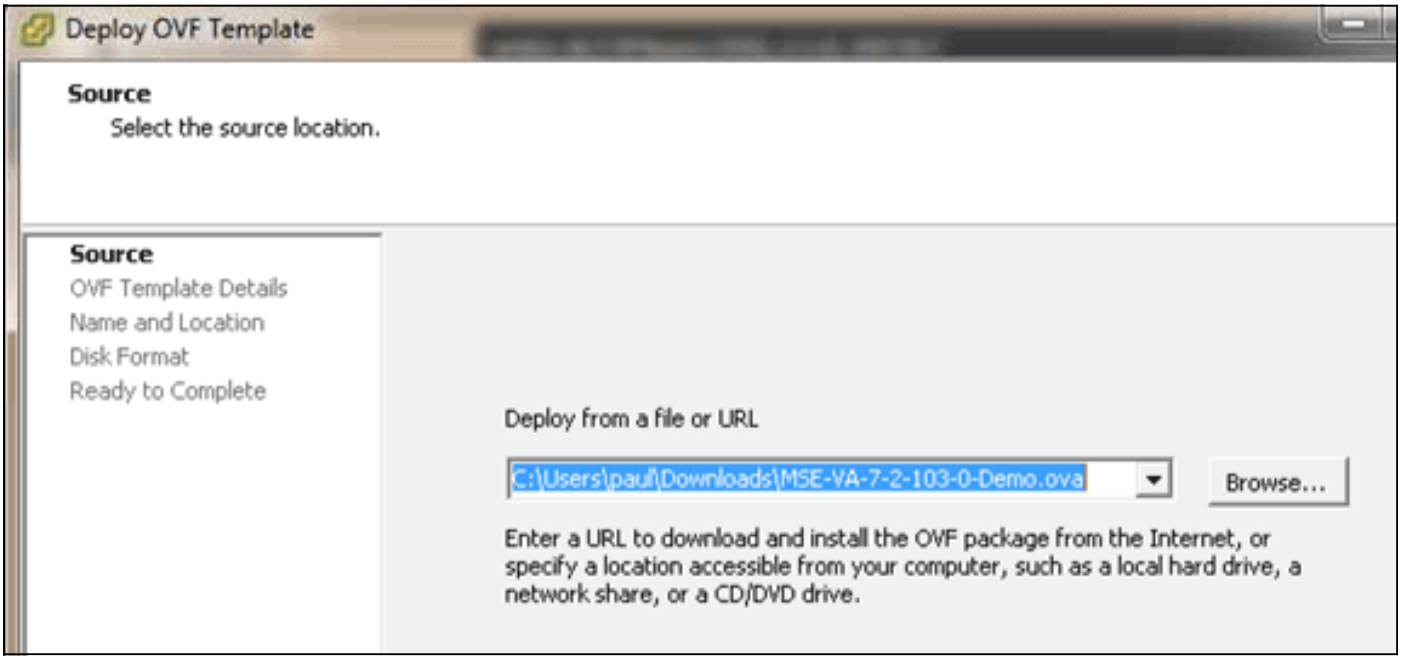
Advertencia: Utilice un tamaño de bloque de al menos 4 MB cuando cree almacenes de datos para ESXi 4.1.

Instalación del dispositivo virtual MSE

El dispositivo virtual MSE se distribuye como una imagen Open Virtual Appliance (OVA) que se puede implementar en un host ESXi mediante el cliente vSphere. Hay dos versiones OVA disponibles: una versión es para una imagen de demostración, que sólo requiere 60 GB de espacio en disco, y la otra es una imagen de producción genérica.

La imagen de producción distribuible supone un mínimo de 500 GB y más de espacio en disco disponible en el almacenamiento de datos del host ESXi. El OVA se puede seleccionar e implementar a través del cliente vSphere. Elija **File > Deploy OVF Template** para implementar la plantilla.



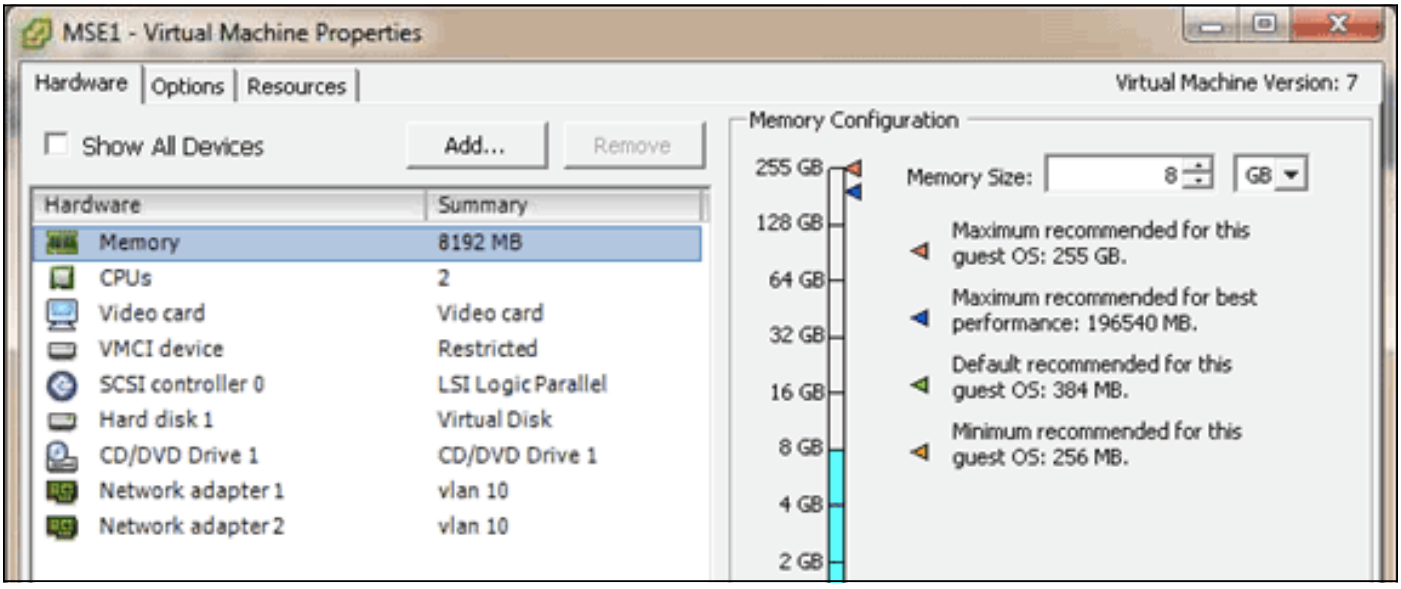


La imagen tarda unos minutos en implementarse en función de la velocidad de la red. Una vez implementada, puede editar la configuración de la máquina virtual (VM) para configurar el dispositivo; la máquina virtual debe apagarse cuando esté configurada.

Configuración de los Niveles de Dispositivos Virtuales MSE

En la tabla de esta sección se enumeran los niveles configurables en el dispositivo virtual y los requisitos de recursos correspondientes. Asigne núcleos dedicados al dispositivo y no a los núcleos virtuales con subprocesos múltiples, ya que afectará al rendimiento si asume que el host tiene más núcleos virtuales e implementa más dispositivos. Por ejemplo, en el UCS C200 mencionado anteriormente, hay ocho (8) núcleos físicos disponibles, pero dieciséis (16) núcleos virtuales con hipersubprocesamiento. No asuma que hay 16 núcleos disponibles; asigne sólo ocho (8) núcleos para garantizar que MSE funcione de forma fiable cuando esté estresado.

MSE principal	Recursos	Licencia admitida (individualmente)		MSE secundario admitido	
Nivel de dispositivo virtual	Memoria total	Licencia CAS	Licencia de wIPS	Dispositivo virtual	Caja física
Bajo	6 G	2000	2000	Bajo+	Not Supported
Estándar	11 G	18000	5000	Estándar+	
Alto	20 G	50000	10000	Alto+	



Configuración del Dispositivo Virtual MSE

Una vez que el dispositivo virtual se ha implementado y configurado, puede encenderlo. Cuando el dispositivo se enciende por primera vez, deberá introducir las credenciales de inicio de sesión predeterminadas: root/password.

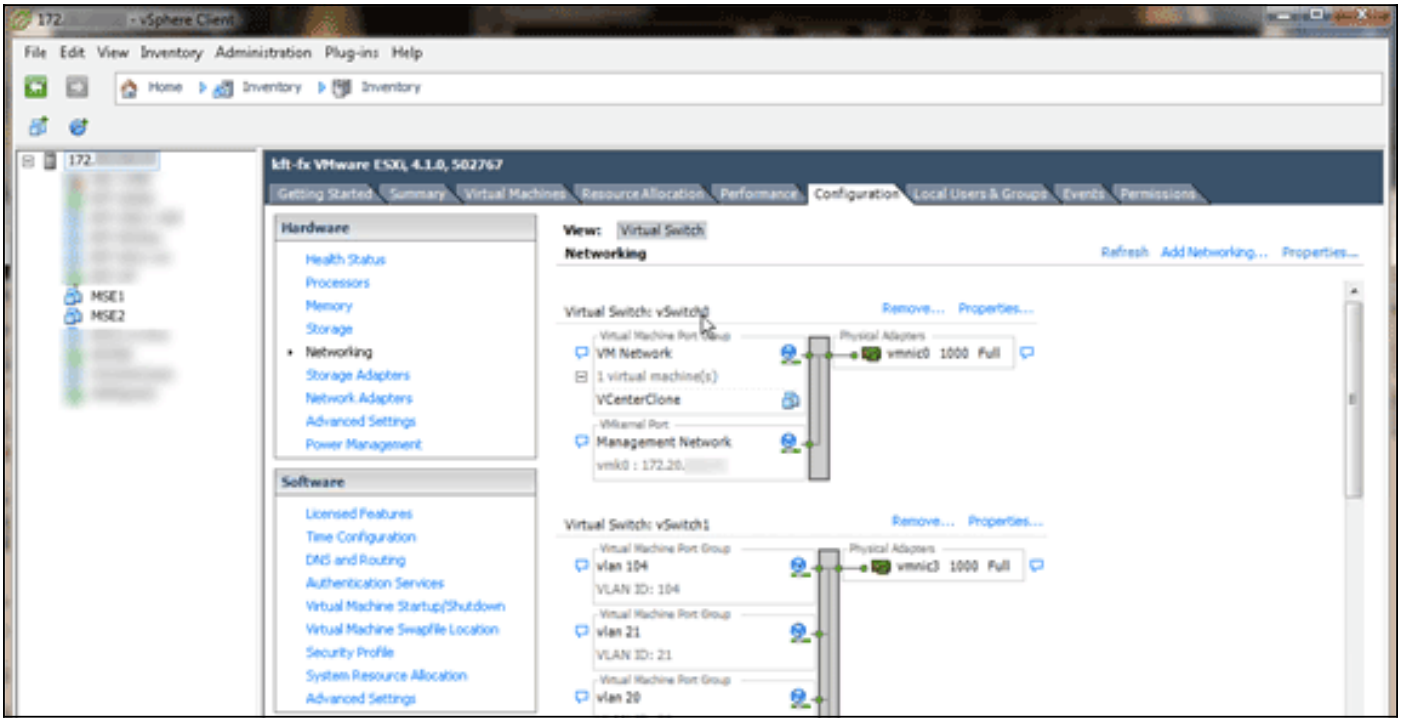
Cuando inicia sesión por primera vez, el dispositivo comienza la configuración del software MSE y también instala la base de datos Oracle. Se trata de un proceso único y lento que llevará al

menos 30-40 minutos. Una vez finalizada la instalación, se vuelve a mostrar el mensaje de inicio de sesión. Refiérase a la sección Configuración del Motor de Servicios de Movilidad de la *Guía de Inicio de Cisco 3355 Mobility Services Engine* para continuar configurando el dispositivo.

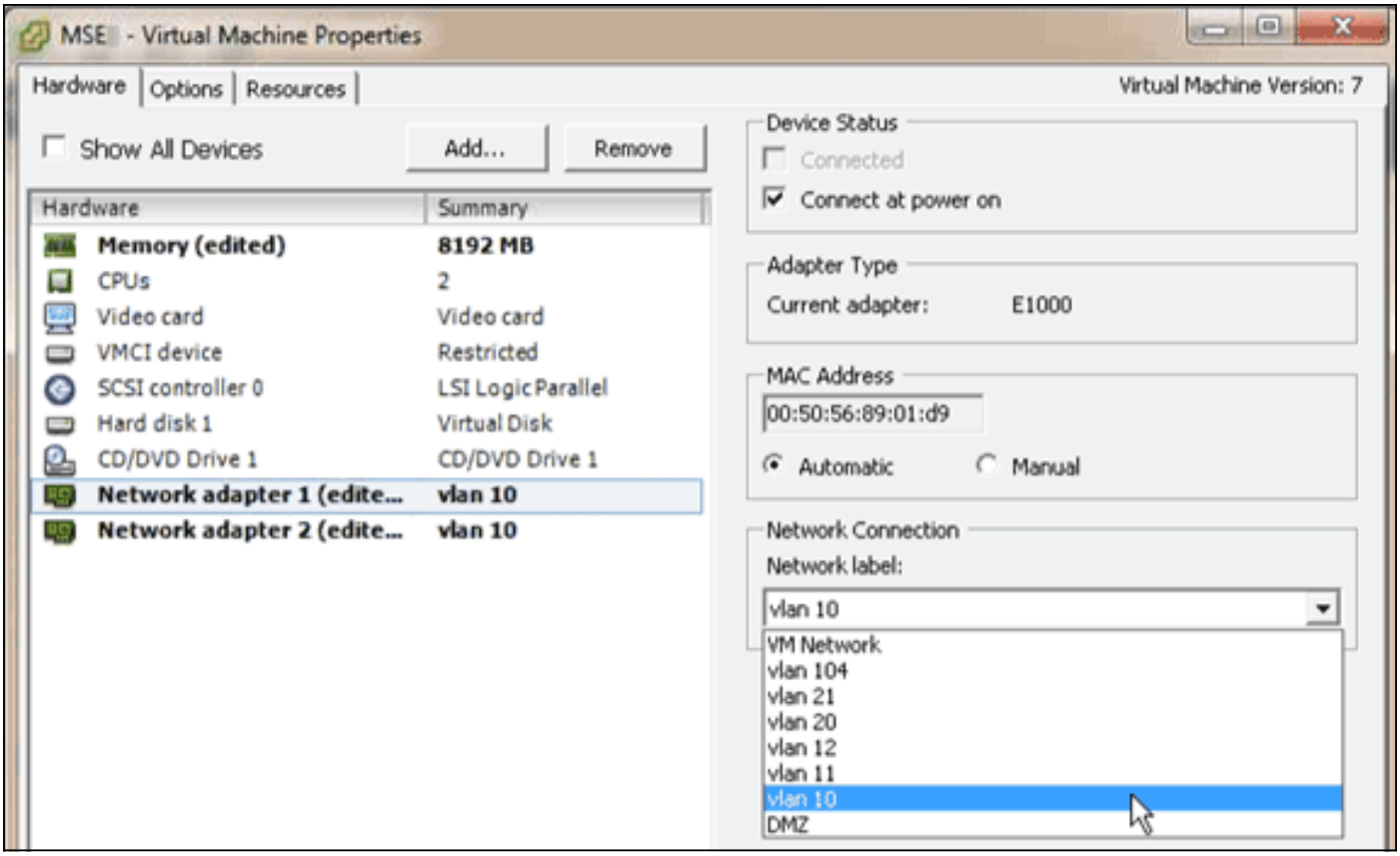
Configuración de la red

De forma predeterminada, las VM utilizan la configuración de red del host; por lo tanto, no es necesario configurar los adaptadores de VM en ESXi. Sin embargo, si tiene redes públicas y privadas conectadas al host y desea que las VM tengan acceso a ambas, puede configurar los adaptadores de VM en el cliente vShare.

En vSphere Client, seleccione el host, haga clic en la ficha **Configuration** y, a continuación, haga clic en **Networking**. Puede ver los adaptadores físicos en las propiedades del switch virtual.



Cree switches independientes con adaptadores independientes para aislar las redes. A continuación, puede asignar los adaptadores VM a estas redes según sea necesario.



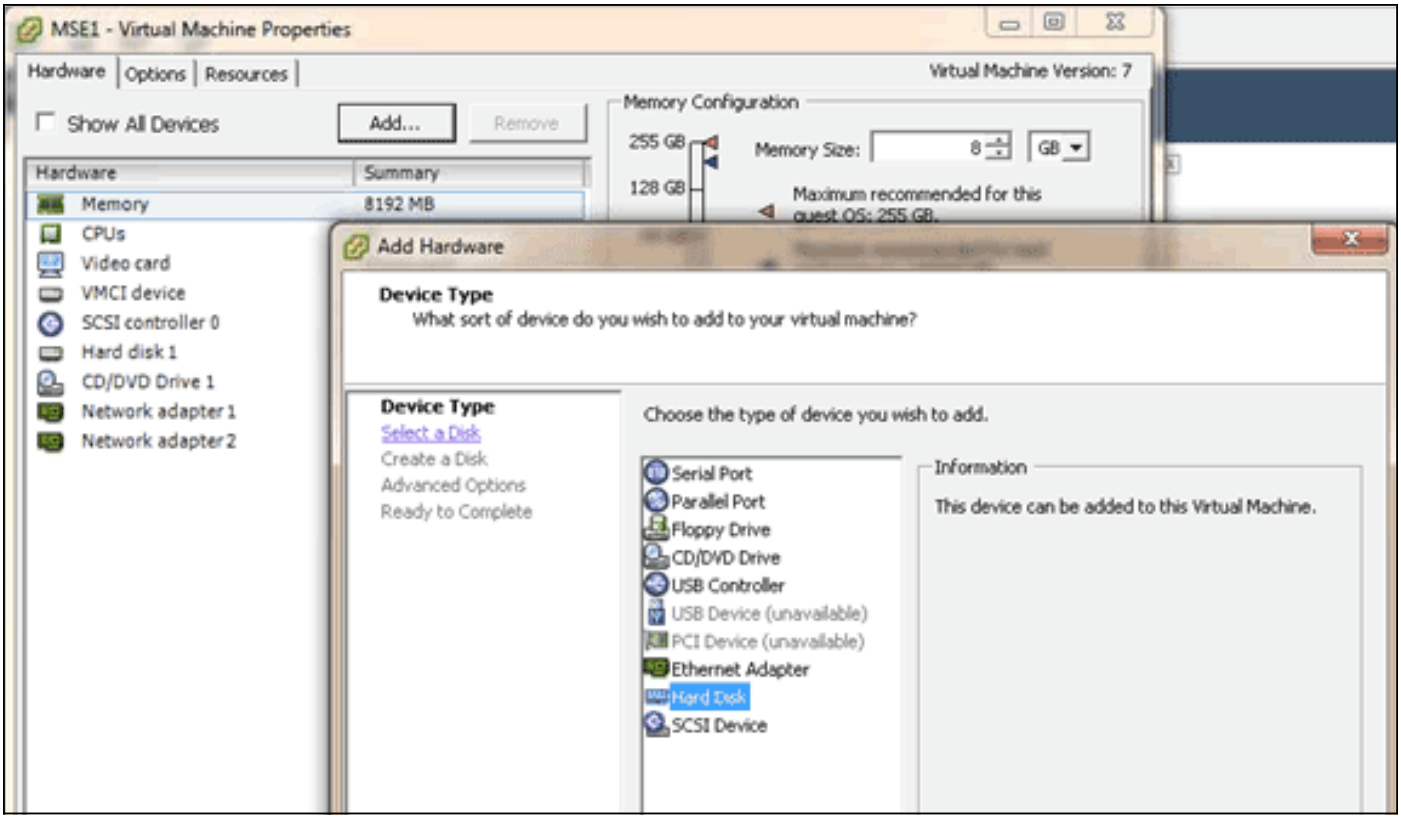
Adición de espacio de disco duro

Si es necesario, agregue capacidad de disco adicional a la máquina virtual y expanda las particiones.

Nota: El script installDrive.sh (ubicado en el directorio /opt/mse/framework/bin) detecta nuevas unidades y redivide las particiones existentes para utilizar y extender las nuevas unidades.

Asegúrese de realizar una copia de seguridad de la máquina virtual (o al menos de los datos de MSE) antes de intentar reparticionar el espacio en disco.

Para agregar más espacio en disco a la máquina virtual, apague la máquina virtual, vaya a la configuración de la máquina virtual y agregue el disco duro adicional.

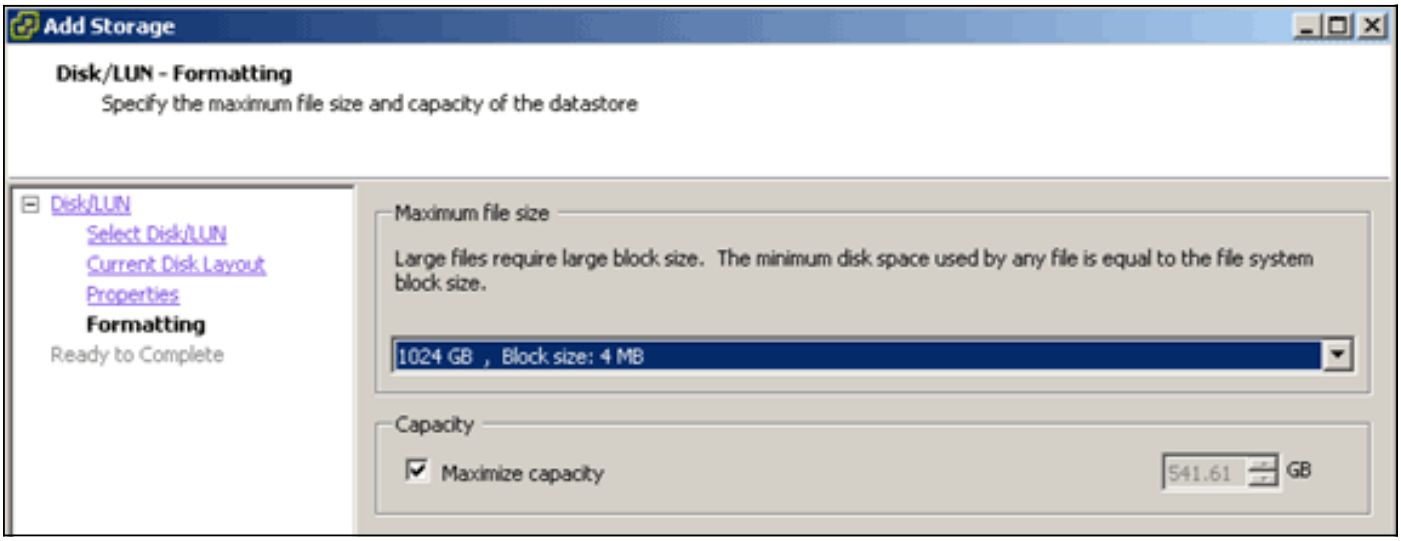


Una vez agregado el disco duro, encienda la máquina virtual, inicie sesión en el dispositivo y ejecute el script installDrive.sh. El script debe montar y reparticionar la unidad recién agregada. Si ha agregado varios discos duros, ejecute el script una vez para cada unidad nueva.

Tamaño del bloque

Para las versiones de ESXi anteriores a la 5.0, Cisco recomienda que el almacén de datos del host tenga un tamaño de bloque de 4 MB o más; de lo contrario, el despliegue del OVA podría fallar. Si la implementación falla, puede reconfigurar el tamaño del bloque.

Para reconfigurar el tamaño del bloque, vaya a ESX host Configuration > Storage > Delete the datastores, y agregue el almacenamiento nuevamente a los nuevos datastores con un tamaño de bloque de al menos 4MB.



Herramientas de VMware

Si la VM produce el siguiente error, haga clic con el botón derecho del ratón en la VM en el vSphere Client y elija **Guest > Install/Upgrade VMware Tools** para instalar o actualizar las herramientas de VMware:

```
Guest OS cannot be shutdown because Vmware tools is not installed or running.
```

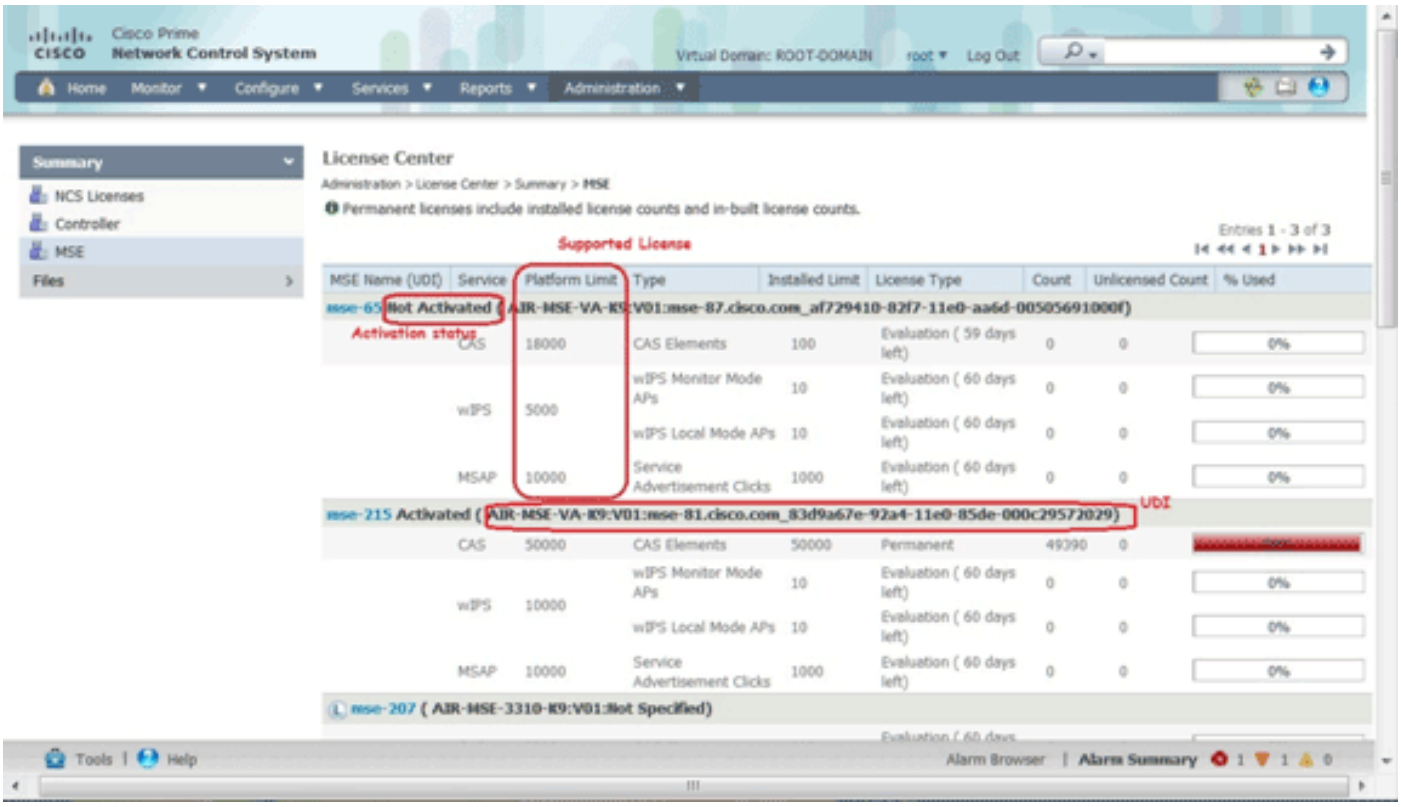
Actualización del dispositivo virtual

Una vez que haya configurado el dispositivo virtual, debe tratarse como un cuadro MSE físico. No necesita implementar un nuevo OVA cada vez que desee actualizar a la última versión de MSE; puede descargar la imagen de instalador adecuada en el dispositivo y seguir los pasos para la actualización como lo haría con un dispositivo físico.

Licencia del dispositivo virtual

Una vez configurado el dispositivo virtual, se puede utilizar en el modo de evaluación (60 días por defecto) sin necesidad de conceder licencias al dispositivo. Sin embargo, debe activar el dispositivo virtual mediante una licencia de activación de dispositivo virtual si piensa implementar licencias permanentes o utilizar funciones como High Availability (HA). Puede obtener el identificador de dispositivo único (UDI) del dispositivo virtual (ejecute **show csludi** en el dispositivo) o de las propiedades generales de Cisco Prime Network Control System (NCS) MSE y utilizar esta información para comprar la licencia de activación de dispositivo virtual y las licencias de servicio permanentes.

Esta imagen muestra los cambios recientes en la interfaz de usuario del centro de licencias para el dispositivo virtual.



Para el dispositivo virtual, un mensaje junto al nombre MSE indica claramente si está activado o no. Además, hay dos columnas de límite: la columna Límite de plataforma enumera la licencia

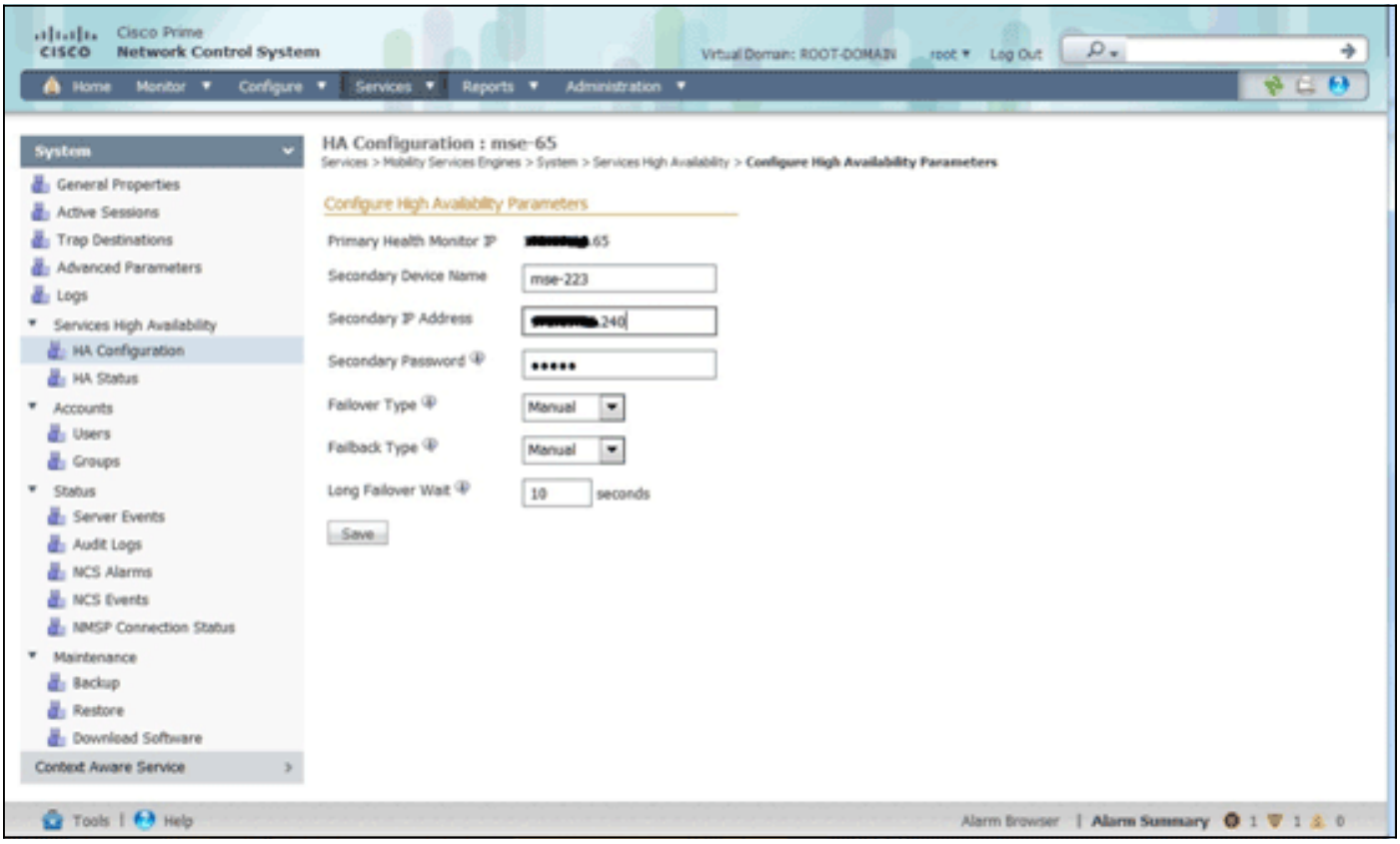
máxima admitida para ese servicio en este dispositivo (dependiendo de la asignación de recursos a la VM), y la columna Límite instalado muestra la licencia real instalada o disponible a través de la evaluación en el dispositivo.

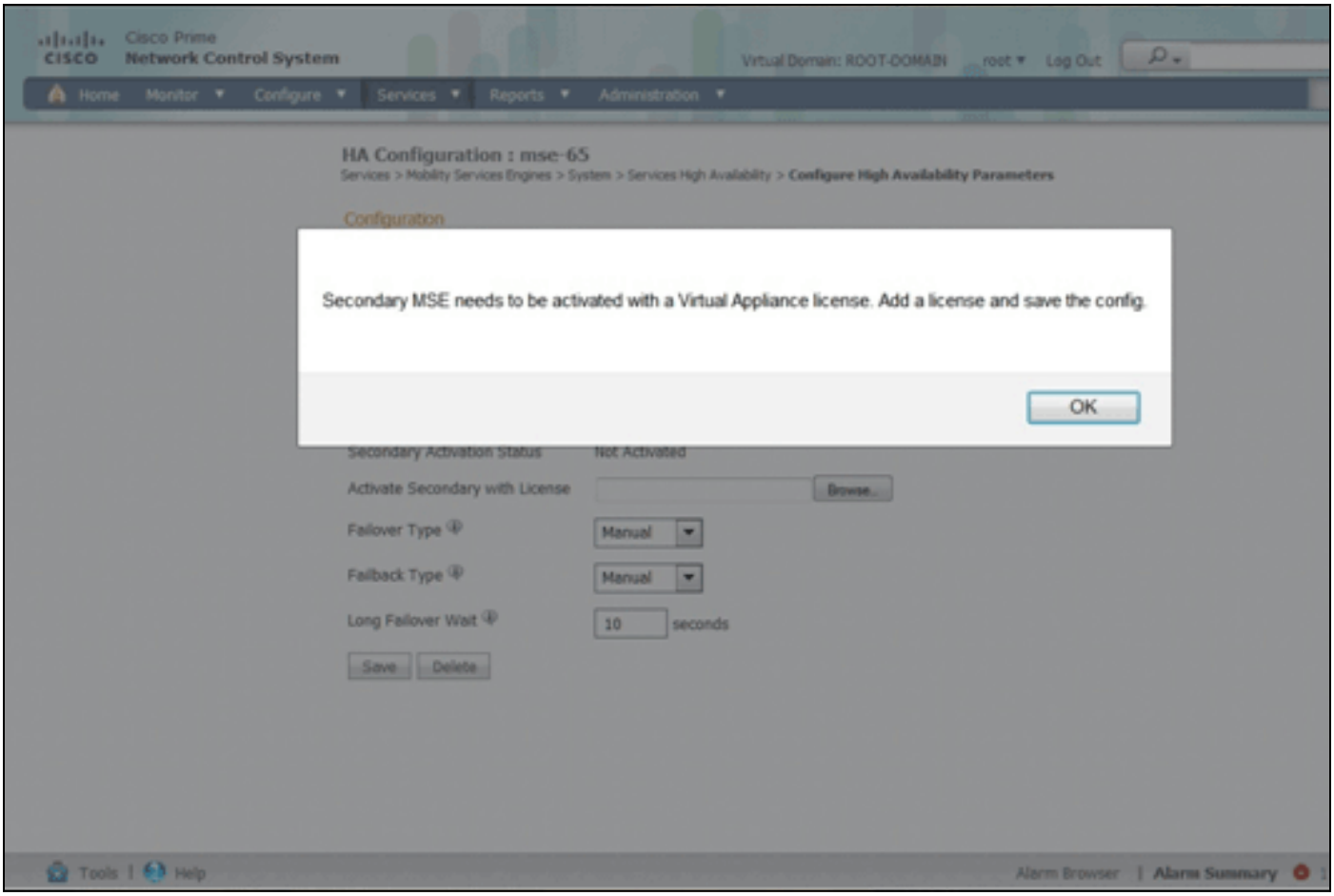
Alta disponibilidad en el dispositivo virtual

Para utilizar la función HA, los appliances primarios y secundarios deben activarse con una licencia de activación de dispositivo virtual.

Configuración de alta disponibilidad

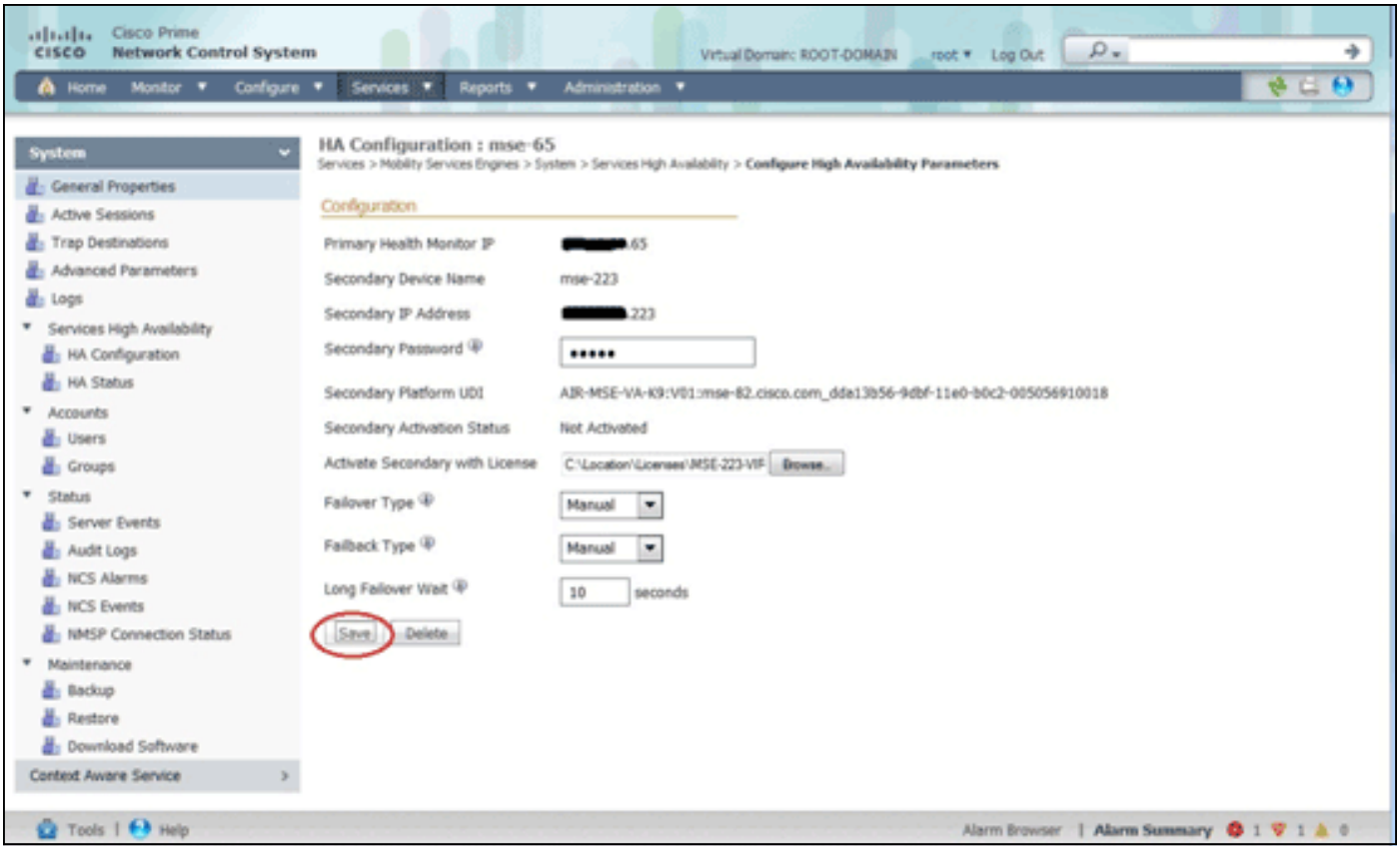
Puede configurar la configuración HA a través del MSE primario en el NCS.





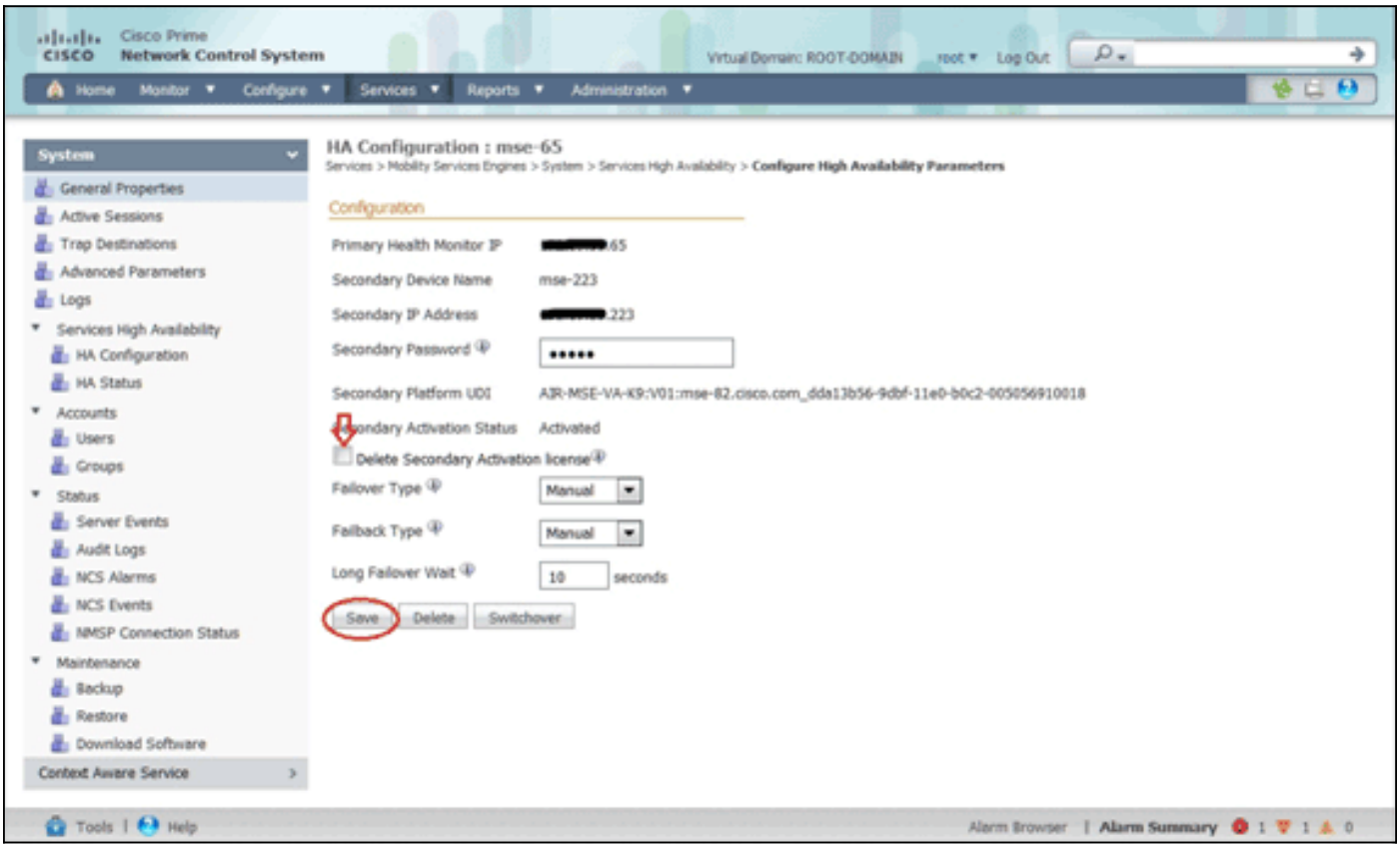
Activación del MSE secundario

Se debe activar el dispositivo secundario. Puede utilizar la información de UDI para solicitar una licencia de activación para el MSE secundario. En la página de configuración de HA, busque la licencia y haga clic en **Guardar**. HA se configurará una vez que el MSE secundario se haya activado correctamente.



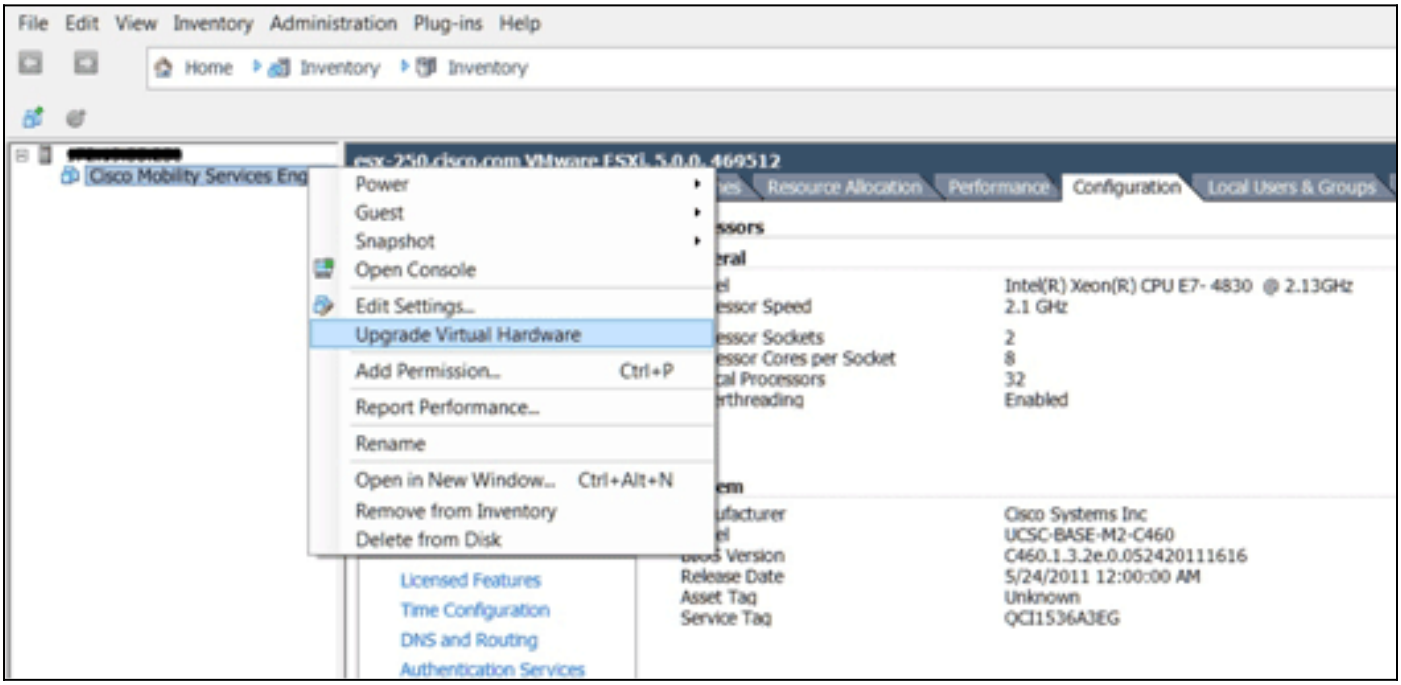
Desactivación del MSE secundario

En caso de que necesite eliminar la licencia de activación del MSE secundario, puede hacer clic en la casilla de verificación y hacer clic en **Guardar** para desactivar el MSE secundario.



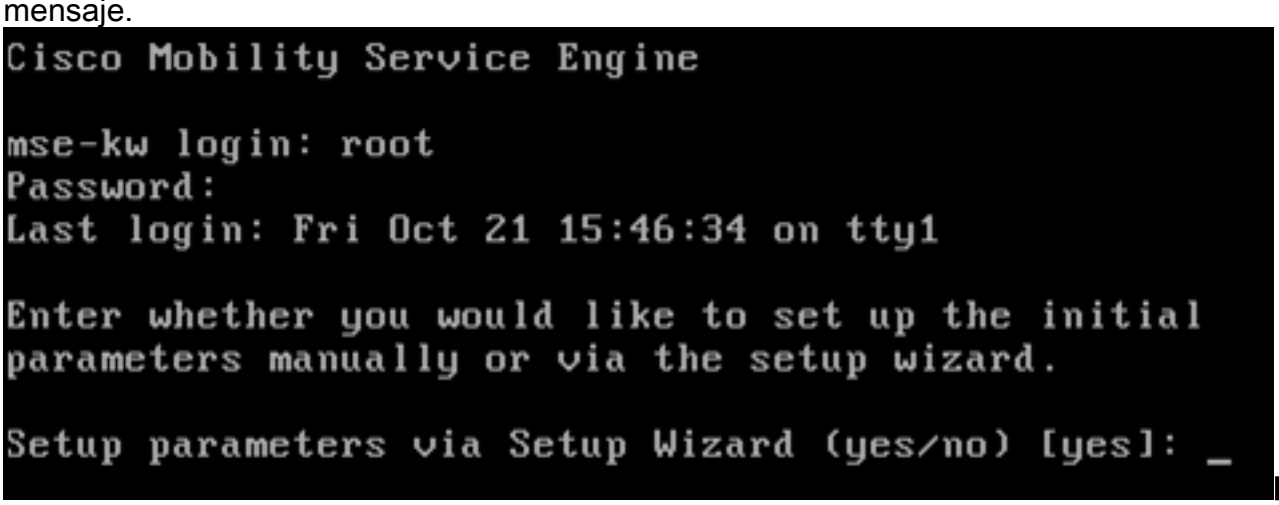
Dispositivo virtual en ESXi 5.0

En ESXi 5.0, el tamaño del bloque se fija en 1 MB, ya que admite implementaciones de VM de gran tamaño. Para poder asignar más de ocho (8) núcleos al dispositivo virtual, debe actualizar el hardware virtual. Para actualizar el hardware virtual, seleccione el MSE y elija **Upgrade Virtual Hardware** como se muestra en esta imagen:



Procedimiento de consola MSE

1. Inicie sesión en la consola con estas credenciales: root/password.Cuando se inicia el inicio inicial, el MSE solicita al administrador que inicie el script de configuración.
2. Ingrese **yes** a este mensaje.



Not
a: Si el MSE no solicita la configuración, ingrese el siguiente comando: /opt/mse/setup/setup.sh.

3. Configure el nombre de host:

```
Please enter the requested information.  At any prompt,
enter ^ to go back to the previous prompt. You may exit at
any time by typing <Ctrl+C>.

You will be prompted to choose whether you wish to configure a
parameter, skip it, or reset it to its initial default value.
Skipping a parameter will leave it unchanged from its current
value.

Changes made will only be applied to the system once all the
information is entered and verified.

------------------------------------------------------------



Current hostname=[mse-kw]
Configure hostname?  (Y)es/(S)kip/(U)se default [Skip]: y

The host name should be a unique name that can identify
the device on the network. The hostname should start with
a letter, end with a letter or number, and contain only
letters, numbers, and dashes.

Enter a host name [mse-kw]: _
```

4. Configure el nombre de dominio DNS:

```
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a domain name for the network domain to which this device
belongs.  The domain name should start with a letter, and it should
end with a valid domain name suffix such as ".com".  It must contain
only letters, numbers, dashes, and dots.

Enter a domain name [corp.rf-demo.com]: _
```

5. Configure el rol principal de HA:

```
Current role=[Primary]
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]: _
```

6. Configure los parámetros de la interfaz Ethernet:

```
Current IP address=[10.10.10.11]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[10.10.10.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

7. Cuando se le pida que introduzca los parámetros de la interfaz eth1, escriba **Skip** para continuar con el siguiente paso, ya que no se requiere una segunda NIC para el funcionamiento.

```
The second ethernet interface is currently disabled for this machine.
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

Nota: La dirección configurada debe proporcionar conectividad IP a la perspectiva WLCs y WCS Management System utilizados con este dispositivo.

8. Introduzca la información de los servidores DNS. Sólo se necesita un servidor DNS para la resolución correcta del dominio, ingrese los servidores de respaldo para la resistencia.

```
Domain Name Service (DNS) Setup
DNS is currently enabled.
Current DNS server 1=[10.10.10.10]
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

9. Configure la zona horaria. Cisco recomienda utilizar UTC (tiempo universal coordinado).Si la zona horaria predeterminada de Nueva York no se aplica a su entorno, navegue por los menús de ubicación para seleccionar la zona horaria correcta.

```
Current timezone=[America/New_York]
Configure timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
```

10. Cuando se le pida que configure el día y la hora de reinicio futuro, escriba **Skip**.

```
Enter whether you would like to specify the
day and time when you want the MSE to be restarted. If you don't specif
y, then
Saturday 1 AM will be taken as default.

Configure future restart day and time ? (Y)es/(S)kip [Skip]: _
```

11. Configure el servidor syslog remoto si corresponde.

```
Configure Remote Syslog Server to publish/MSE logs MSE logs.

A Remote Syslog Server has not been configured for this machine.
Configure Remote Syslog Server Configuration parameters? (Y)es/(S)kip/(U)s
ult [Skip]:
```

12. Configure el protocolo de tiempo de red (NTP) o la hora del sistema.NTP es opcional, pero garantiza que el sistema mantenga una hora precisa. Si elige habilitar NTP, la hora del sistema se configurará desde los servidores NTP que seleccione. De lo contrario, se le solicitará que introduzca la fecha y hora actuales.

```
Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select.  Otherwise,
you will be prompted to enter the current date and time.

NTP is currently enabled.
Current NTP server 1=[10.10.10.10]
Current NTP server 2=[none]
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: _
```

13. Cuando se le solicite configurar el banner de inicio de sesión, escriba

Skip.

```
Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [Skip]:
```

14. Habilite el inicio de sesión de la raíz de la consola local.Este parámetro se utiliza para habilitar/inhabilitar el acceso de la consola local al sistema. El inicio de sesión de la raíz de la consola local debe estar habilitado para que pueda ocurrir la resolución de problemas local. El valor predeterminado es
Omitir.

```
System console is not restricted.
Configure system console restrictions? (Y)es/(S)kip/(U)se default [Skip]:
```

15. Habilitar inicio de sesión raíz de Secure Shell (SSH).Este parámetro se utiliza para habilitar/inhabilitar el acceso remoto a la consola en el sistema. El inicio de sesión de la raíz SSH debe estar habilitado para que pueda ocurrir la resolución de problemas remota. Sin embargo, las políticas de seguridad corporativas pueden requerir que se deshabilite esta opción.

```
SSH root access is currently enabled.
Configure ssh access for root (Y)es/(S)kip/(U)se default [Skip]: _
```

16. Configure el modo de usuario único y la seguridad de la contraseña.Estos parámetros de configuración no son obligatorios; el valor predeterminado es
Omitir.

```
Single user mode password check is currently disabled.
Configure single user mode password check (Y)es/(S)kip/(U)se default [Skip]:
```

17. Cambie la contraseña raíz.Este paso es fundamental para garantizar la seguridad del sistema. Asegúrese de elegir una contraseña segura que consta de letras y números sin palabras de diccionario. La longitud mínima de la contraseña es de ocho (8) caracteres. Las credenciales predeterminadas son
root/password.

```
Configure root password? (Y)es/(S)kip/(U)se default [Skip]: _
```

18. Configure los parámetros relacionados con el login y la
contraseña:

```
Login and password strength related parameter setup
Maximum number of days a password may be used : 99999
Minimum number of days allowed between password changes : 0
Minimum acceptable password length : disabled
Login delay after failed login : 5
Checking for strong passwords is currently enabled.
Configure login/password related parameters? (Y)es/(S)kip/(U)se default
```

19. Configure una contraseña de inicio (Grub). (Opcional)Este parámetro de configuración no es necesario. El valor predeterminado es
Omitir.

```
GRUB password is not currently configured.
Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Skip]:
```

20. Configure el nombre de usuario de la comunicación
NCS.

```
Configure NCS communication username? (Y)es/(S)kip/(U)se default [Skip]:
```

21. Acepte el cambio en la

configuración.

```
Configuration Changed
Is the above information correct (yes, no, or ^): _
```

Esta imagen muestra un ejemplo de la pantalla de finalización:

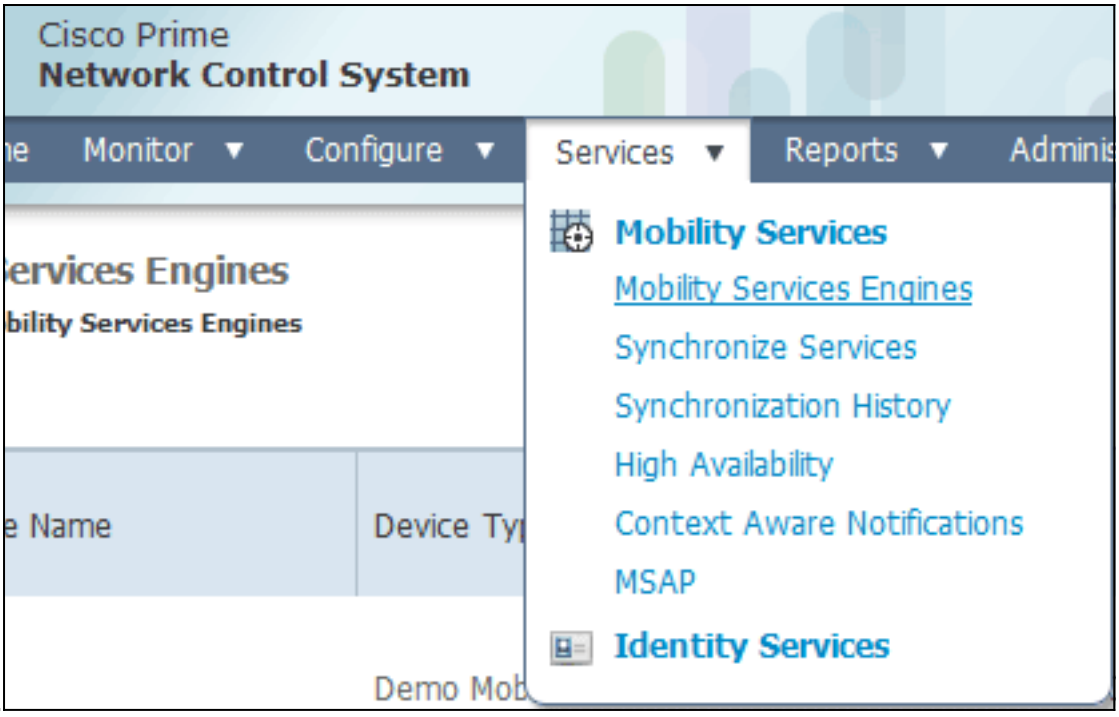
```
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: nat filter                [  OK  ]
Unloading iptables modules: Removing netfilter NETLINK layer.
                                                           [  OK  ]
ip_tables: (C) 2000-2006 Netfilter Core Team
Netfilter messages via NETLINK v0.30.
ip_conntrack version 2.4 (8192 buckets, 65536 max) - 304 bytes per conntrack

Starting MSE Platform

Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules: Removing netfilter NETLINK layer.
                                                           [  OK  ]
  syslogd: unknown facility name "LOCAL*"
ip_tables: (C) 2000-2006 Netfilter Core Team
Netfilter messages via NETLINK v0.30.
ip_conntrack version 2.4 (8192 buckets, 65536 max) - 304 bytes per conntrack
Starting Health Monitor, Waiting to check the status.
Health Monitor successfully started
Starting Admin process...
Started Admin process.
Starting database ...
Database started successfully. Starting framework and services .......
```

22. Ejecute el comando **getserverinfo** para verificar la configuración.

```
Active Wired Clients: 0
Active Elements(Wireless Clients, Rogue APs, Rogue Clients,
lients, Tags) Limit: 115
Active Sessions: 1
Wireless Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogue APs Not Tracked due to the limiting: 0
Rogue Clients Not Tracked due to the limiting: 0
Interferers Not Tracked due to the limiting: 0
Wired Clients Not Tracked due to the limiting: 0
Total Elements(Wireless Clients, Rogue APs, Rogue Clients,
ients) Not Tracked due to the limiting: 0

-------------------------
Context Aware Sub Services
-------------------------

Subservice Name: Aeroscout Tag Engine
Admin Status: Disabled
Operation Status: Down
```

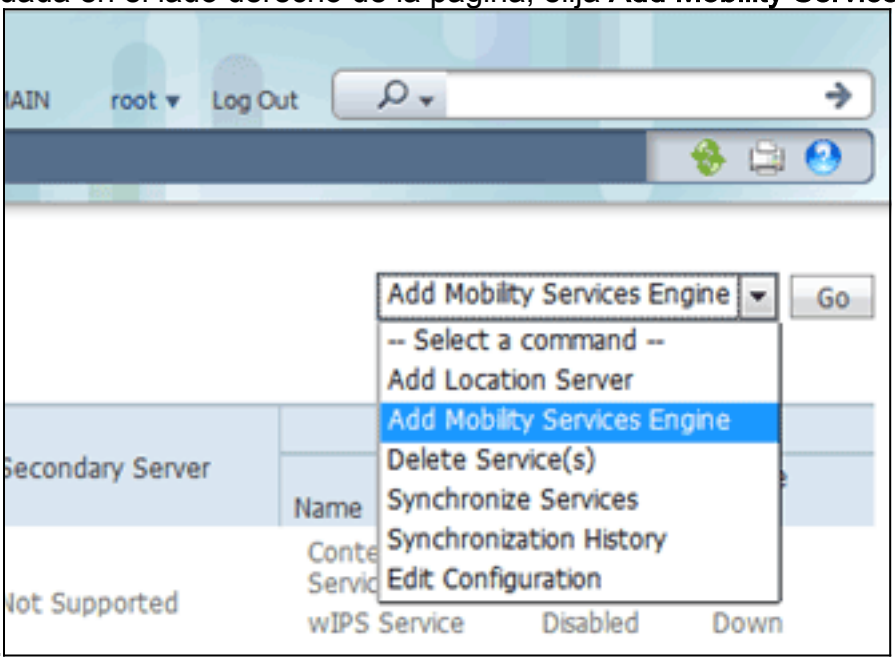
Adición de MSE VA a NCS

1. Inicie sesión en NCS y elija **Services > Mobility Services**

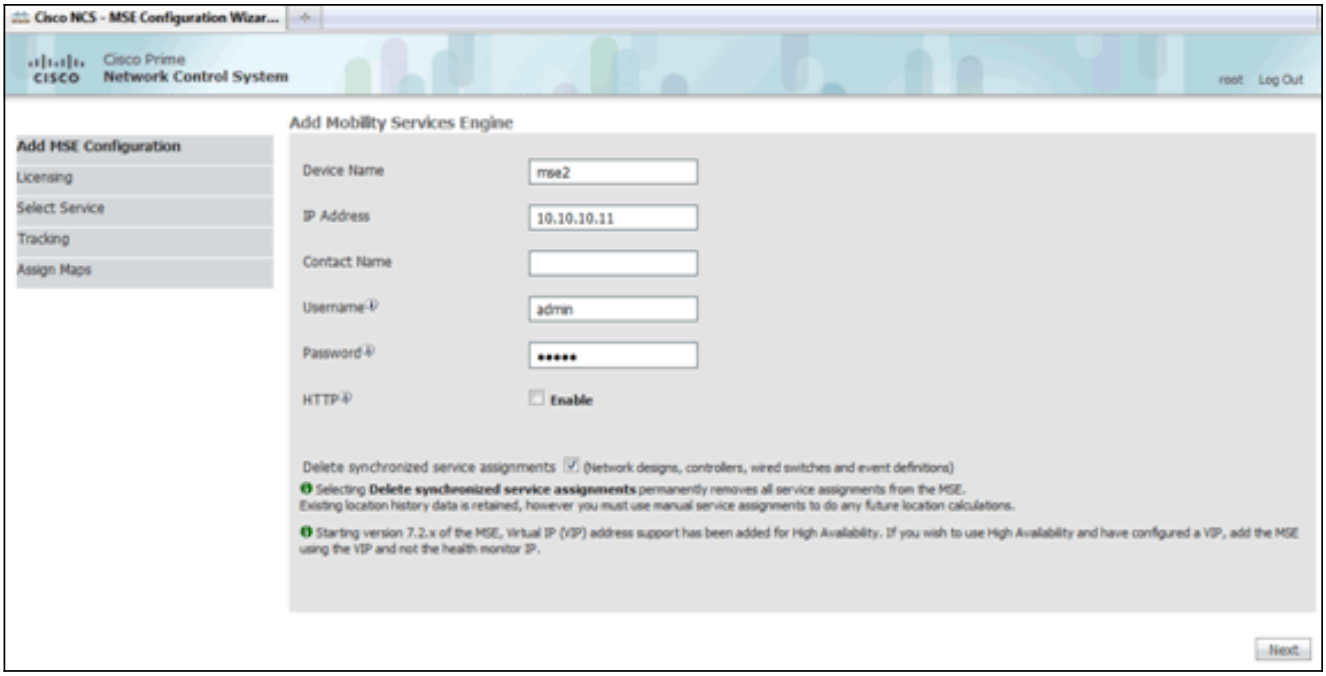


Engines.

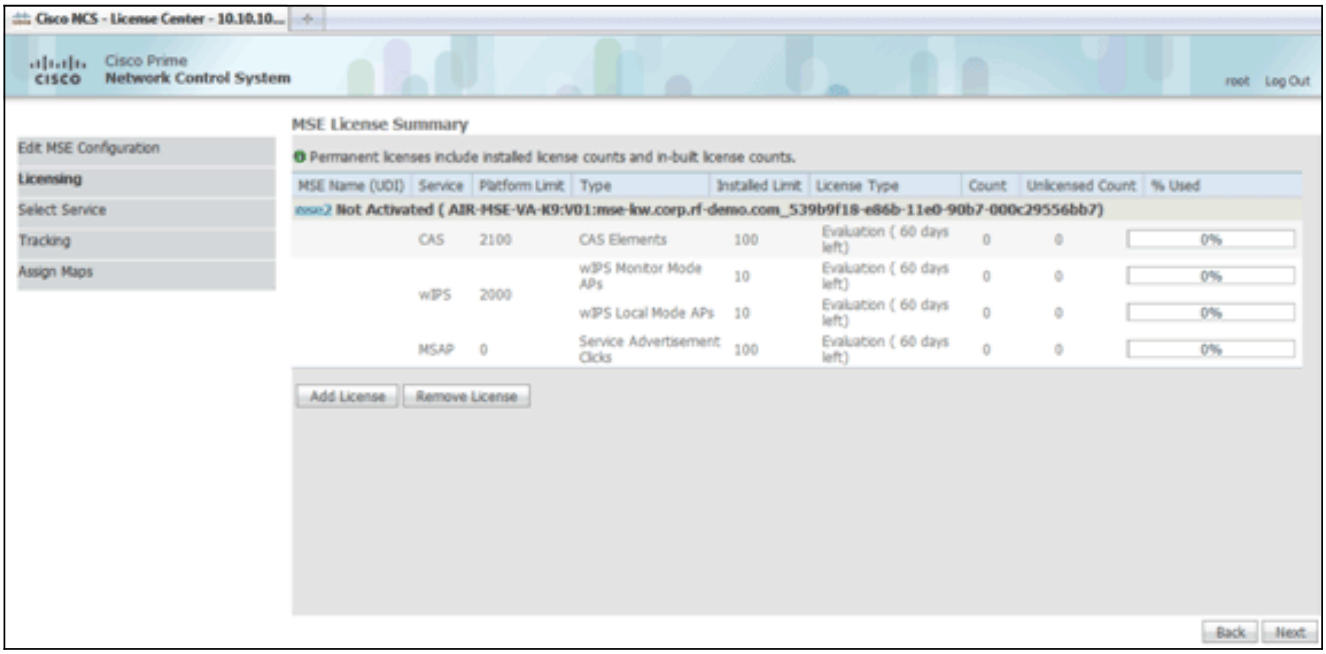
2. En la lista desplegable situada en el lado derecho de la página, elija **Add Mobility Services Engine** y haga clic en **Go**.



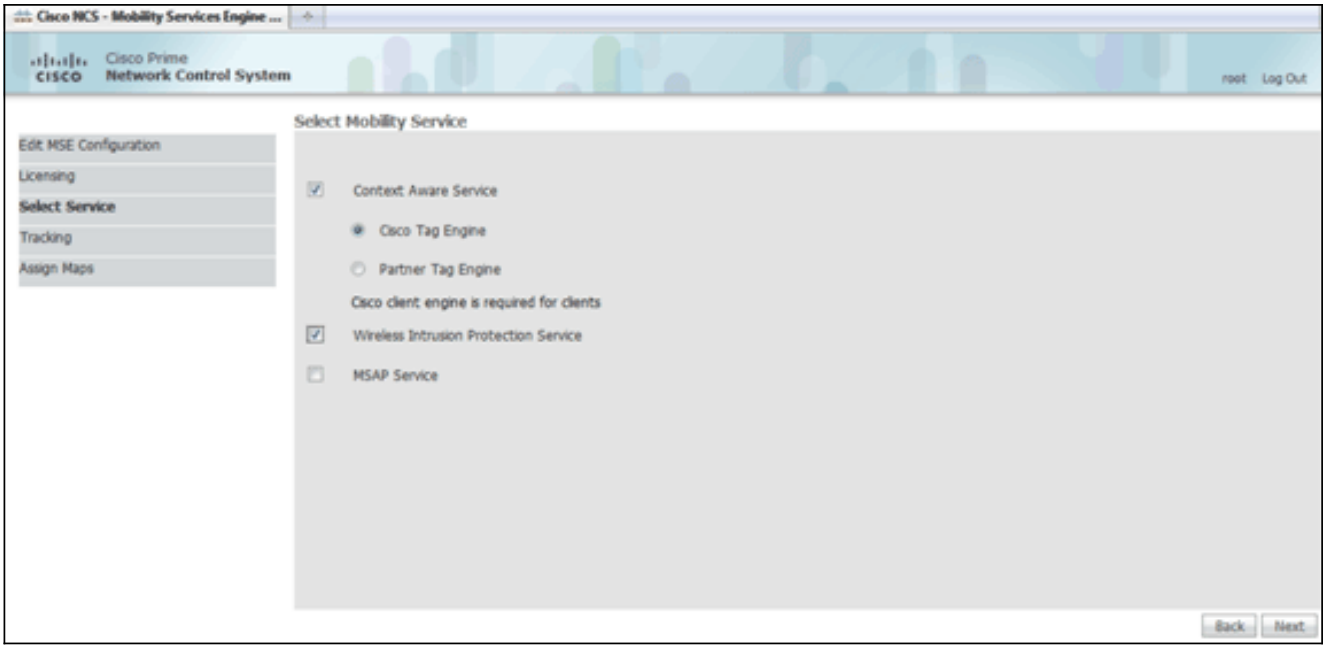
3. Introduzca un nombre de dispositivo único para el MSE, la dirección IP configurada anteriormente durante la configuración de MSE, un nombre de contacto para soporte. y el nombre de usuario y la contraseña de NCS configurados durante la configuración de MSE.No cambie el nombre de usuario del valor predeterminado de *admin*. Puede salir como valor
predeterminado.



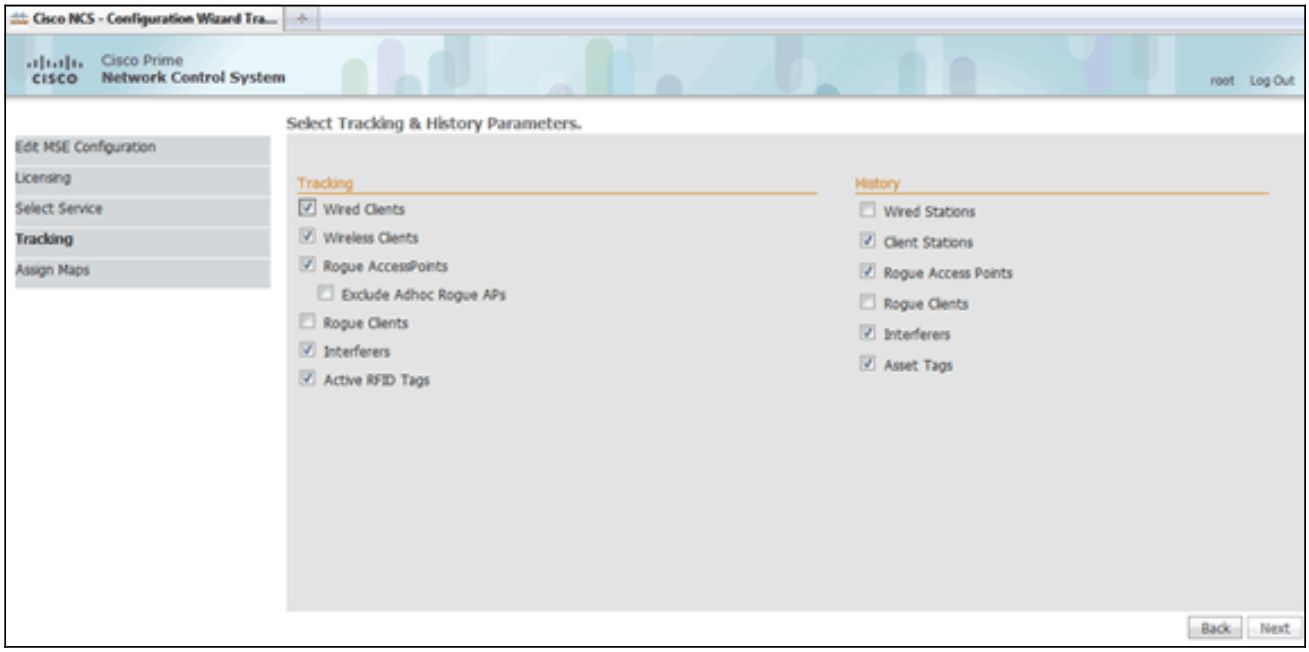
4. Haga clic en Next (Siguiente).
5. Haga clic en **Licencias** y verifique la licencia. En la instalación, la licencia de demostración predeterminada es suficiente para realizar pruebas. Puede agregar más licencias adquiridas o quitarlas en la página Licencias.



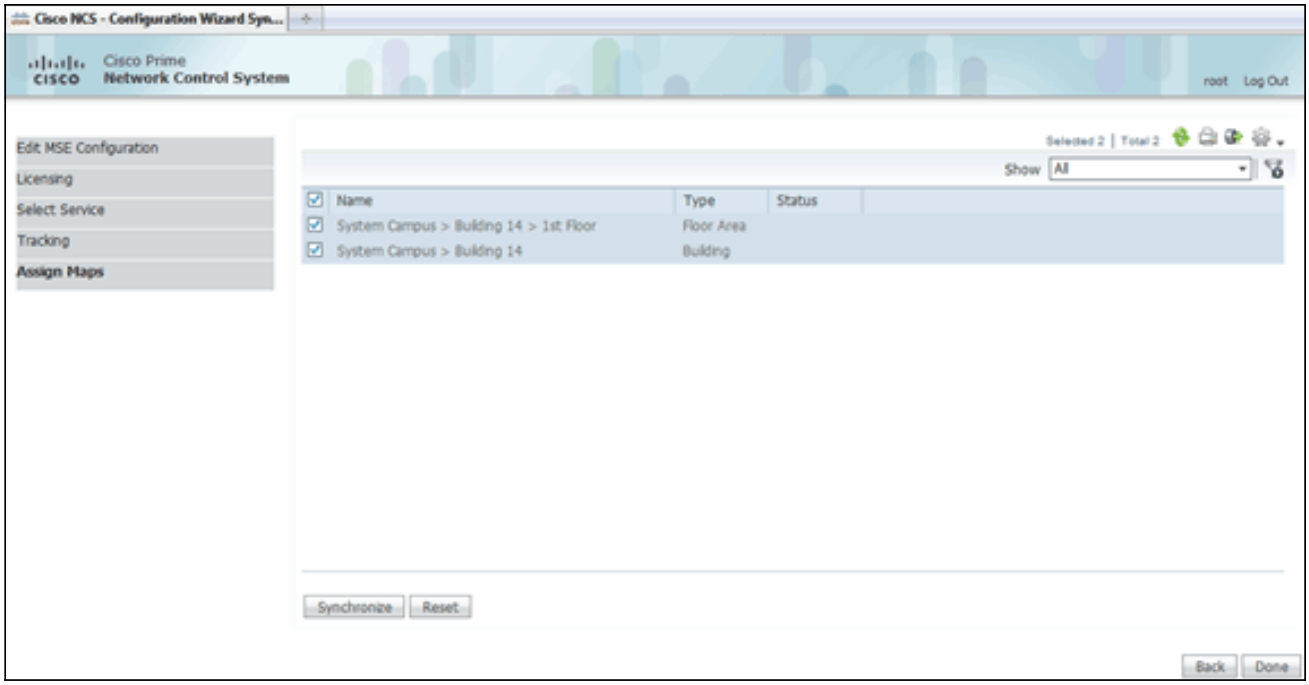
6. Haga clic en Next (Siguiente).



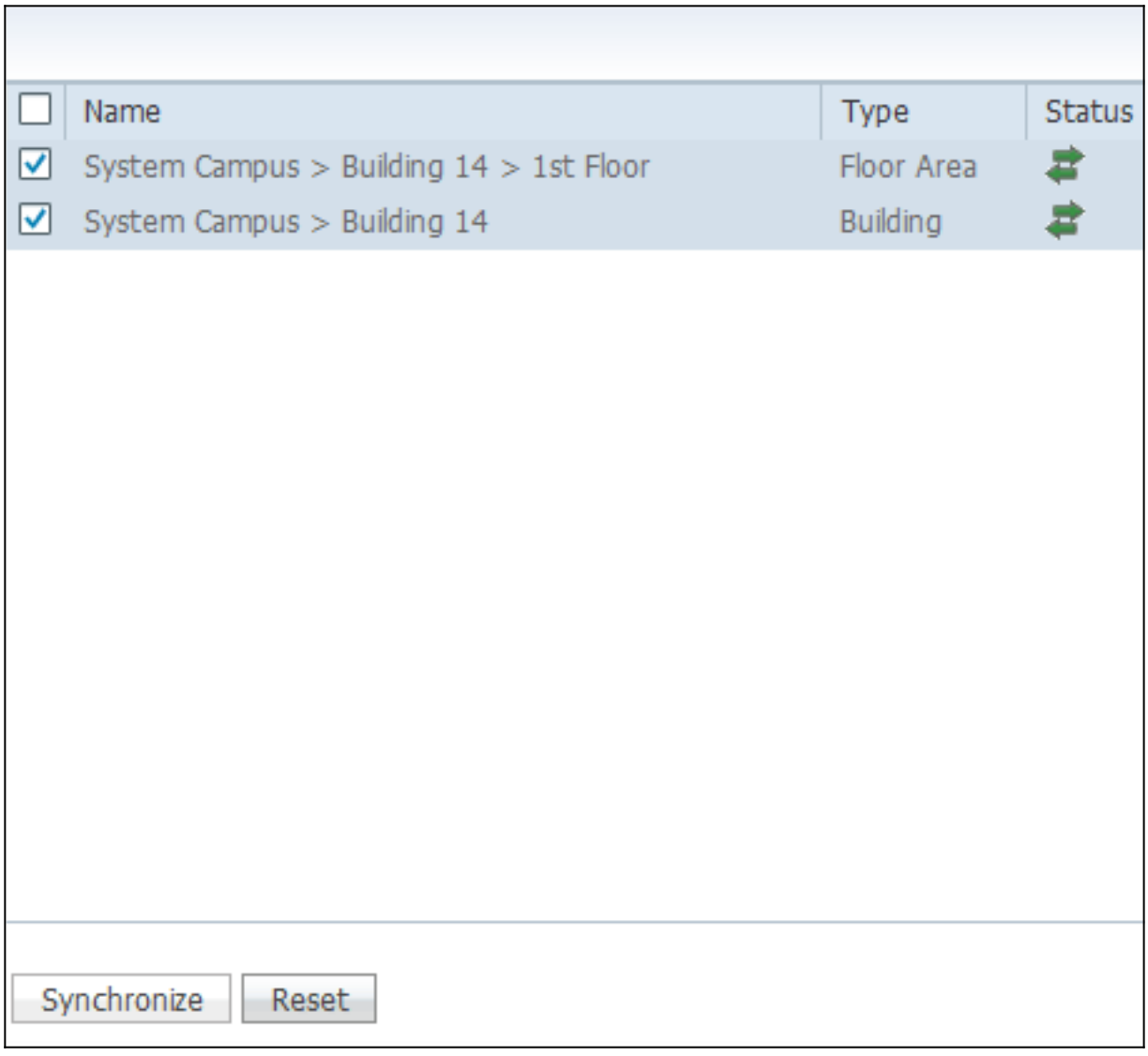
7. En la página Seleccionar servicio de movilidad, haga clic en el botón de opción **Cisco Tag Engine** (disponible desde 7.0MR) (para el soporte de etiquetas RFID y cliente) o haga clic en el botón de opción **Partner Tag Engine** (para Aeroscout, etc.).
8. Haga clic en la casilla de verificación **Wireless Intrusion Protection Service** para probar la función de seguridad wIPS de las funciones Modo Monitor y Modo local mejorado.
9. Haga clic en Next (Siguiente).
10. Active las casillas de verificación de los elementos que se van a habilitar para el seguimiento y de los parámetros del historial de dichos elementos que se van a habilitar para los informes históricos.



11. Haga clic en Next (Siguiente).

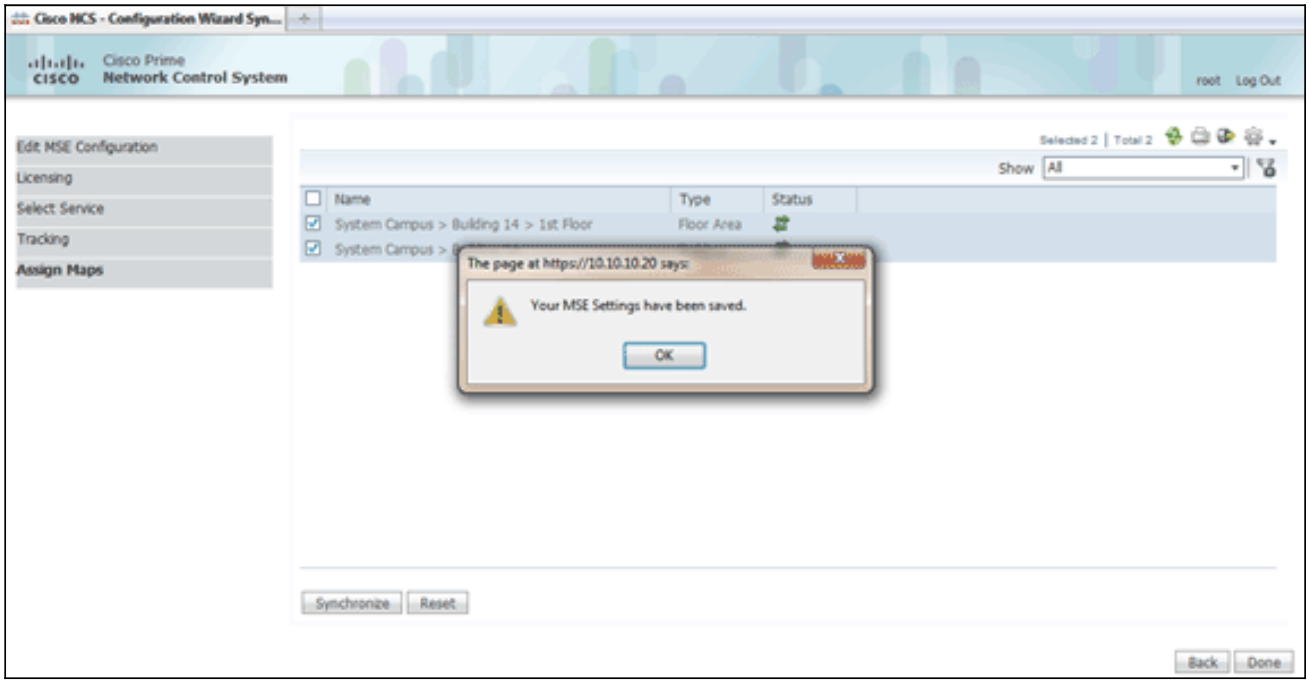


12. Marque las casillas de verificación del edificio y el piso existentes y haga clic en **Sincronizar**.Una vez sincronizada, la columna Estado se actualiza para mostrar que el diseño de red inicial se ha sincronizado.

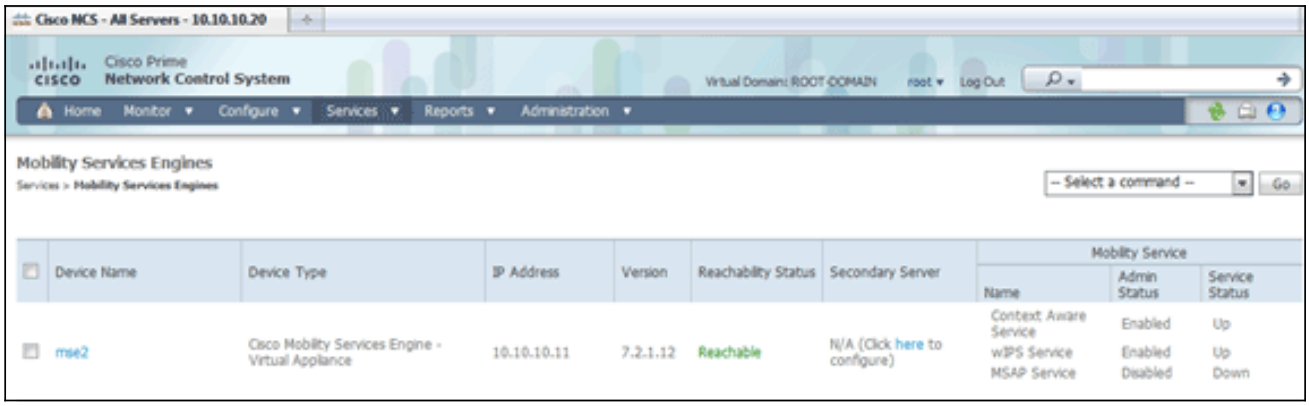


13. Cuando se complete la sincronización, haga clic en **Finalizado**.Aparece un cuadro de diálogo que indica que se ha guardado la configuración de

MSE.

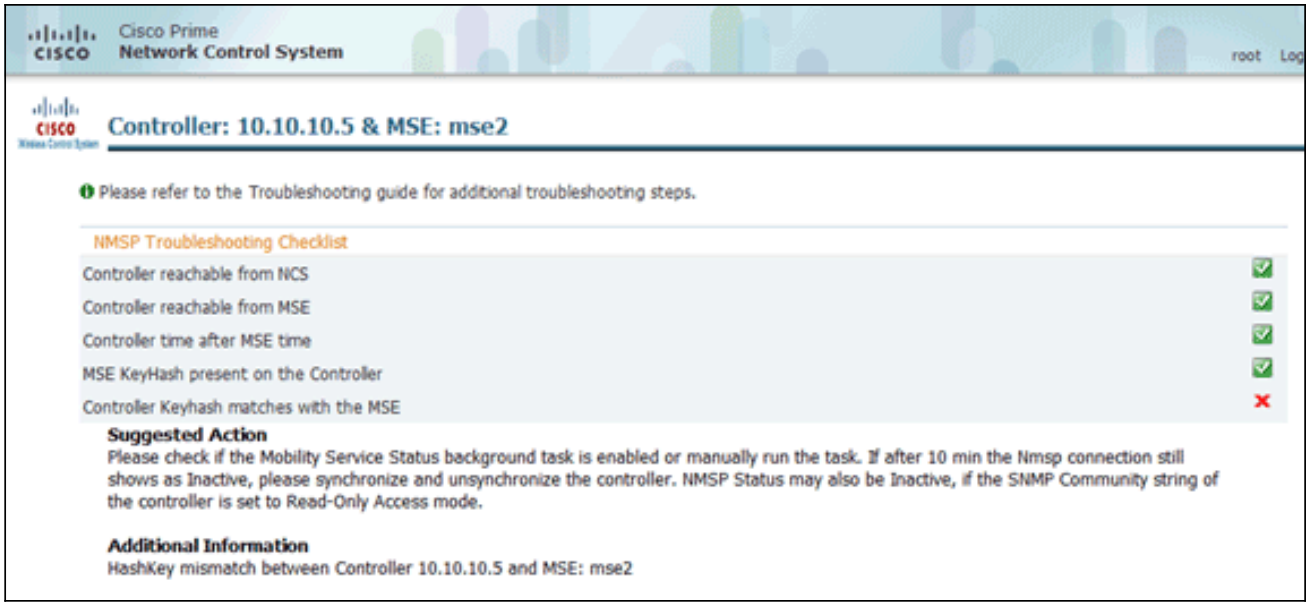


14. Confirme la configuración en la página principal de MSE de NCS.



Asegúrese de sincronizar el resto de diseños de red, controladores, switches por cable y grupos de eventos según esté disponible.**Nota:** El servicio Cisco Context-Aware depende en gran medida de un reloj sincronizado entre el WLC, NCS y MSE. Si estos tres sistemas no apuntan al mismo servidor NTP y se configuran con la misma configuración de zona horaria, el servicio sensible al contexto no funcionará correctamente. Antes de intentar cualquier procedimiento de resolución de problemas, asegúrese de que el reloj del sistema es el mismo en todos los componentes del sistema sensible al contexto.

15. Verifique MSE y la comunicación del controlador para los servicios seleccionados.Verifique que el MSE se comunica con cada uno de los controladores sólo para el servicio seleccionado; El estado del protocolo de servicio de movilidad de red (NMSP) debe estar *activo*.Esta imagen proporciona un ejemplo de cuándo el hash de llave no se agrega al WLC.



En la consola WLC, use el comando **show auth-list**.El siguiente ejemplo muestra desde la consola WLC que no hay servidor de ubicación
disponible:

```
(Cisco Controller) >show auth-list

Authorize MIC APs against AAA ..................... disabled
Authorize LSC APs against Auth-List ............... disabled
APs Allowed to Join
  AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate.................. no
  AP with Locally Significant Certificate........ no
```

P
ara agregar manualmente el MSE y establecer una conexión NMSP al WLC, complete estos pasos:En la consola MSE, ejecute el comando **cmdshell** y, a continuación, el comando **show server-auth-info**.Este ejemplo muestra la dirección MAC y el hash de clave que se utilizará para agregar al

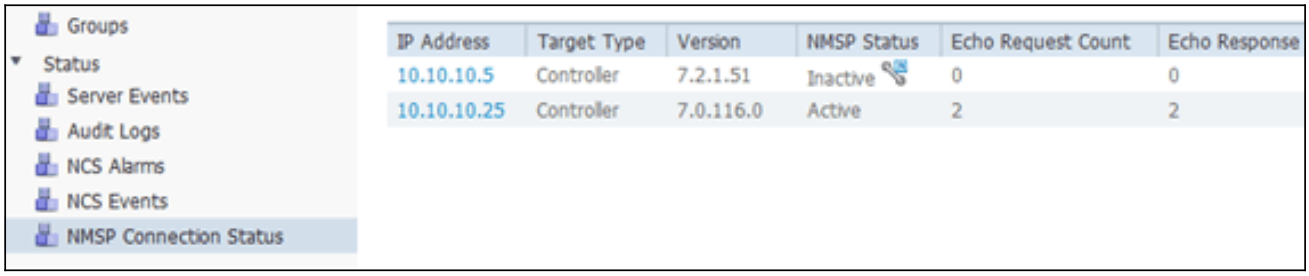
```
cmd> show server-auth-info
invoke command: com.aes.server.cli.CmdGetServerAuthInfo
----------------
Server Auth Info
----------------
MAC Address: 00:0c:29:55:6b:b7
Key Hash: 1469187db14ac53ac6108e56b04d48015bdd70d7
Certificate Type: SSC
```

WLC.
Ejecute el comando **config auth-list add ssc <*mac address*> <*MSE keyhash*>** , y luego ejecute el comando **show auth-list**.Este ejemplo muestra que el MSE fue agregado al WLC (manualmente).

```
(Cisco Controller) config>auth-list add ssc 00:0c:29:55:6b:b7 1469187db14ac53ac6108e56b04d48015bdd70d7

(Cisco Controller) config>exit
(Cisco Controller) >show auth-list

Authorize MIC APs against AAA ..................... disabled
Authorize LSC APs against Auth-List ............... disabled
APs Allowed to Join
  AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate.................. no
  AP with Locally Significant Certificate........ no

Mac Addr                Cert Type    Key Hash
----------------------  ----------   ----------------------------------------
00:0c:29:55:6b:b7       SSC          1469187db14ac53ac6108e56b04d48015bdd70d7
```

En NCS, confirme que la conexión NMSP muestra

Activo.



Referencia de la línea de comandos

Comandos WLC

```
config location expiry ?
client         Timeout for clients
calibrating-client Timeout for calibrating clients
tags           Timeout for RFID tags
rogue-aps      Timeout for Rogue APs
```

```
show location ap-detect ?
all            Display all (client/rfid/rogue-ap/rogue-client) information
client         Display client information
rfid           Display rfid information
rogue-ap       Display rogue-ap information
rogue-client   Display rogue-client information
(Cisco Controller) >show location ap-detect client
```

```
show client summary
Number of Clients.............................. 7
MAC Address       AP Name           Status        WLAN/Guest-Lan Auth Protocol Port Wired
----------------- ----------------- ------------- -------------- ---- -------- ---- -----
00:0e:9b:a4:7b:7d AP6               Probing       N/A            No   802.11b  1    No
00:40:96:ad:51:0c AP6               Probing       N/A            No   802.11b  1    No
(Cisco Controller) >show location summary
 Location Summary
 Algorithm used:                 Average
 Client
        RSSI expiry timeout:     5 sec
        Half life:               0 sec
        Notify Threshold:        0 db
 Calibrating Client
        RSSI expiry timeout:     5 sec
        Half life:               0 sec
 Rogue AP
        RSSI expiry timeout:     5 sec
        Half life:               0 sec
        Notify Threshold:        0 db
 RFID Tag
        RSSI expiry timeout:     5 sec
        Half life:               0 sec
        Notify Threshold:        0 db
```

```
show rfid config
```

```
RFID Tag data Collection..................... Enabled
RFID  timeout................................ 1200 seconds
RFID mobility................................ Oui:00:14:7e : Vendor:pango  State:Disabled
```

show rfid detail

```
RFID address.....................................00:0c:cc:7b:77:3b
Vendor.......................................... Aerosct
Last Heard...................................... 7 seconds ago
Packets Received................................ 40121
Bytes Received.................................. 2567744
Detected Polling Interval....................... 30 seconds
Cisco Type.....................................

Content Header
=================
CCX Tag Version................................. 1
Tx Power........................................ 18 dBm
Channel......................................... 11
Reg Class....................................... 6
Burst Length.................................... 1

CCX Payload
===========
Last Sequence Control........................... 0
Payload length.................................. 29
Payload Data Hex Dump
00 02 00 33 02 07 42 00 00 00 00 00 00 03 05 01
41 bc 80 00 04 07 00 0c cc 00 00 00 00 d

Nearby AP Statistics:

      demo-AP1260(slot 0, chan 11) 6 seconds .... -48 dBm
```

show location plm

```
Location Path Loss Configuration
Calibration Client : Enabled   , Radio: Uniband
Normal Clients : Disabled      , Burst Interval: 60

(Cisco Controller) >config location ?
plm            Configure Path Loss Measurement (CCX S60) messages
algorithm      Configures the algorithm used to average RSSI  and SNR values
notify-threshold Configure the LOCP notification threshold for RSSI measurements
rssi-half-life Configures half life when averaging two RSSI readings
expiry         Configure the timeout for RSSI values
```

config location expiry client ?

```
<seconds>      A value between 5 and 3600 seconds
```

config location rssi-half-life client ?

```
<seconds>      Time in seconds (0,1,2,5,10,20,30,60,90,120,180,300 sec)
```

show nmsp subscription summary

```
Mobility Services Subscribed:
Server IP               Services
---------               --------
172.19.32.122           RSSI, Info, Statistics, IDS
```

Comandos MSE

Ejecute este comando para determinar el estado de los servicios MSE:

```
[root@MSE ~]# getserverinfo
```

Ejecute este comando para iniciar el motor contextual para el seguimiento del cliente:

```
[root@MSE ~]# /etc/init.d/msed start
```

Ejecute este comando para determinar el estado del motor sensible al contexto para el seguimiento del cliente:

```
[root@MSE ~]# /etc/init.d/msed status
```

Ejecute este comando para detener el motor sensible al contexto para el seguimiento del cliente:

```
[root@MSE ~]# /etc/init.d/msed stop
```

Ejecute este comando para realizar diagnósticos:

```
[root@MSE ~]# rundiag
```

Nota: El comando **rundiag** también se puede utilizar para ver la información de UDI de MSE que se requiere para obtener el archivo de licencia para el motor contextual para los clientes.

Información Relacionada

- Guía de configuración de MSE (dispositivo virtual y físico)
- Configuración de alta disponibilidad de MSE
- Guía de implementación de Cisco WIPS
- Pedidos de productos
- Soporte Técnico y Documentación - Cisco Systems