

# Guide de configuration et de déploiement de l'appliance virtuelle MSE version 7.2

## Contenu

- [Introduction](#)
- [Conditions préalables](#)
- [Conditions requises](#)
- [Components Used](#)
- [Conventions](#)
- [Informations générales](#)
- [Configuration système nécessaire](#)
- [Logiciels de gestion et licences VMware](#)
- [Besoins en ressources](#)
- [Configuration de l'hôte ESXi](#)
- [Installation de l'appareil virtuel MSE](#)
- [Configuration des niveaux de l'appliance virtuelle MSE](#)
- [Configuration de l'appareil virtuel MSE](#)
- [Configuration du réseau](#)
- [Ajout d'espace disque dur](#)
- [Taille du bloc](#)
- [Outils VMware](#)
- [Mise à niveau de l'appareil virtuel](#)
- [Licence de l'appliance virtuelle](#)
- [Haute disponibilité sur l'appareil virtuel](#)
- [Configurer la haute disponibilité](#)
- [Activation du MSE secondaire](#)
- [Désactivation du MSE secondaire](#)
- [Appareil virtuel sur ESXi 5.0](#)
- [Procédure de console MSE](#)
- [Ajout de MSE VA à NCS](#)
- [Référence de ligne de commande](#)
- [Commandes WLC](#)
- [Commandes MSE](#)
- [Informations connexes](#)

## Introduction

La version 7.2 du logiciel Cisco Mobility Services Engine (MSE) ajoute une appliance virtuelle et la prise en charge de VMware ESXi. Ce document fournit des instructions de configuration et de déploiement, ainsi que des conseils de dépannage, pour les utilisateurs qui ajoutent le dispositif virtuel MSE à un WLAN Cisco Unified et qui exécute les services Context Aware ou le système de prévention d'intrusions pour le sans fil adaptatif Cisco (wIPS). En outre, ce document décrit la configuration système requise pour l'appliance virtuelle MSE et fournit des directives générales de

déploiement pour l'appliance virtuelle MSE. Ce document ne fournit pas de détails de configuration pour MSE et les composants associés. Ces informations figurent dans d'autres documents ; des références sont fournies.

Reportez-vous à la section [Informations connexes](#) pour obtenir la liste des documents relatifs à la configuration et à la conception des services de mobilité contextuelle. La configuration wIPS adaptative n'est pas non plus traitée dans ce document.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

Les informations de ce document sont basées sur le moteur de services de mobilité de la gamme Cisco 3300.

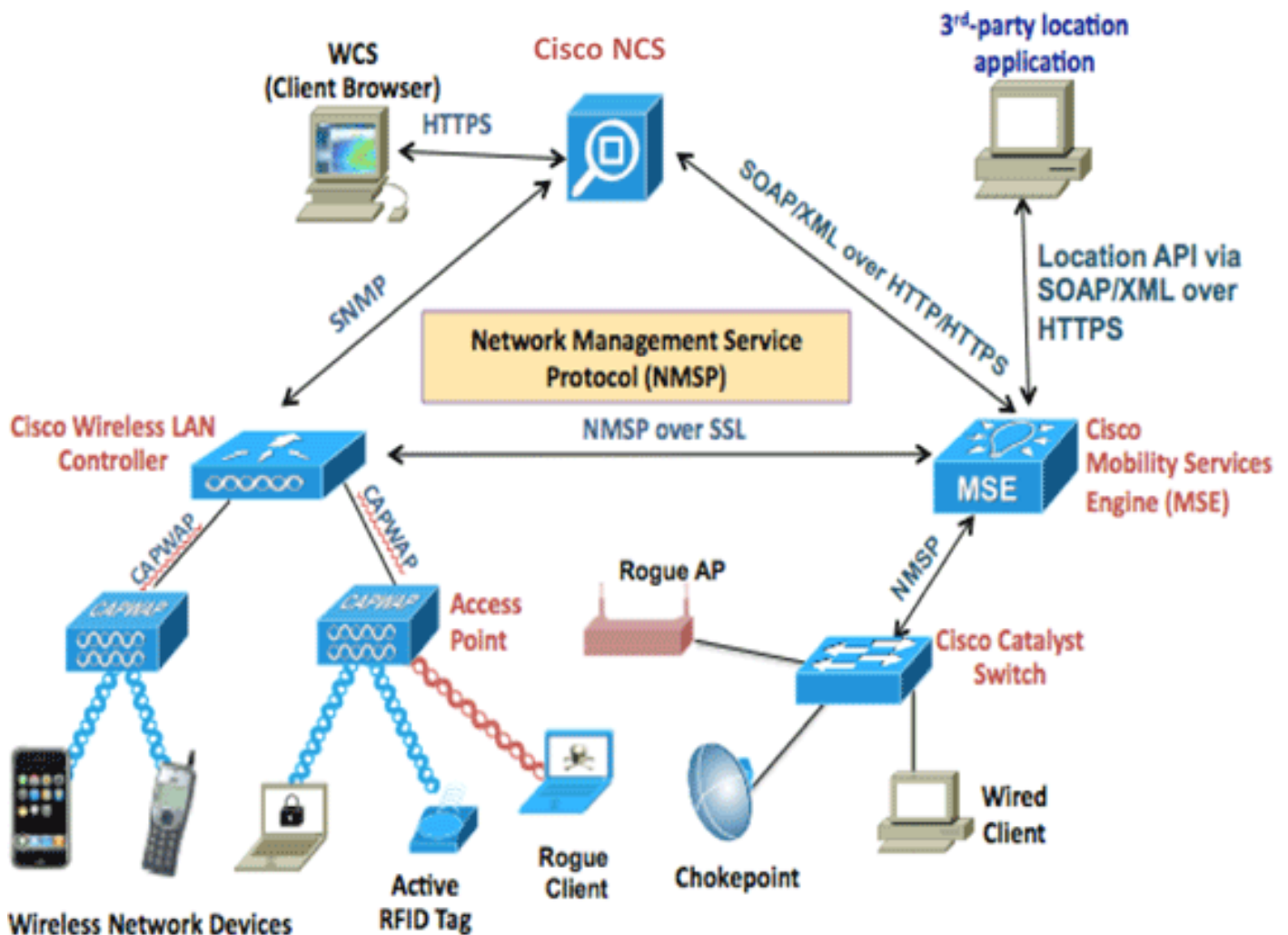
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Informations générales

Cette image montre le déploiement WLAN Cisco typique qui inclut Cisco Mobility Services Engine (MSE). Ce déploiement inclut également d'autres clients de réseau filaire/sans fil, des balises RFID et un point d'accès et client non autorisé. MSE fournit une visibilité sur ces éléments pour l'emplacement et wIPS. Avant la version 7.2 du logiciel MSE, seuls les appareils physiques étaient limités aux MSE-3310 et MSE-3350/3355.



## Configuration système nécessaire

MSE Software Release 7.2 Virtual Appliance est pris en charge et testé sur VMware ESXi 4.1 et versions ultérieures. Ces configurations de serveur ont été testées et sont recommandées à titre indicatif.

- Serveur rack Cisco Unified Computing System (UCS) C200 M2Deux (2) Intel<sup>®</sup> Xeon<sup>®</sup> CPU E5506 à 2,13 GHz RAM (selon le niveau configuré) Disques SAS avec contrôleurs RAID améliorés (500 Go minimum)
- Serveur rack UCS C210 M2Deux (2) processeurs Intel Xeon E5640 à 2,67 GHz RAM (selon le niveau configuré) Disques SAS avec contrôleurs RAID améliorés (500 Go minimum)
- Serveur rack UCS C250 M2Deux (2) processeurs Intel Xeon E5570 à 2,93 GHz RAM (selon le niveau configuré) Disques SAS avec contrôleurs RAID améliorés (500 Go minimum)
- Serveur rack UCS C460 M2Deux (2) processeurs Intel Xeon E7-4830 à 2,13 GHz RAM (selon le niveau configuré) Disques SAS avec contrôleurs RAID améliorés (500 Go minimum)

**Remarque :** utilisez deux (2) processeurs quatre coeurs au moins aussi puissants que ceux mentionnés ci-dessus.

## Logiciels de gestion et licences VMware

L'appliance virtuelle Cisco MSE version 7.2 prend en charge ESX/ESXi 4.x et versions ultérieures.

Afin de gérer les hôtes ESXi et de configurer et déployer les appliances virtuelles, Cisco vous recommande d'installer vCenter Server 4.x sur une machine Windows XP ou Windows 7 64 bits et d'obtenir une licence vCenter Enterprise. Vous pouvez également utiliser le client vSphere pour gérer un seul hôte ESXi.

## Besoins en ressources

Les besoins en ressources dépendent de la licence que vous souhaitez déployer. Ce tableau répertorie les différents niveaux auxquels vous pouvez configurer votre appliance virtuelle :

MSE principal	Ressources		Licence prise en charge (individuellement)	
Niveau d'appliance virtuelle	Mémoire totale	UC	Licence CAS	Licence wIPS
Faible	6 G	2	2000	2000
Standard	11 G	8	18000	5000
Élevé	20 G	16	50000	10 000

**Remarque :** Les limites suggérées pour les licences CAS et wIPS sont des limites maximales prises en charge lorsqu'un seul service est en cours d'exécution. Les limites de coexistence s'appliquent si vous voulez exécuter les deux services sur le même appareil.

## Configuration de l'hôte ESXi

Complétez ces étapes afin de configurer une appliance virtuelle MSE sur un serveur UCS ou similaire :

1. Assurez-vous que votre machine dispose d'au moins 500 Go d'espace disque et de disques SAS rapides avec contrôleurs RAID améliorés. (Utilisez une taille de bloc d'au moins 4 Mo lorsque vous créez des data stores pour les versions antérieures à ESXi 5.0.)
2. Installez ESXi. Insérez le disque d'installation ESXi 4.1 ou version ultérieure et démarrez à partir du lecteur. Si vous utilisez plusieurs lecteurs, installez ESXi dans le lecteur configuré comme lecteur de démarrage. Le nom d'utilisateur par défaut est root et le mot de passe est vide (pas de mot de passe). **Remarque :** Si vous choisissez le mauvais lecteur pour l'installation, vous pouvez reformater à l'aide d'un CD Fedora Live.
3. Configurez l'adresse IP. Choisissez les cartes réseau activées et actives. Vous pouvez avoir plusieurs cartes réseau si votre hôte est connecté à plusieurs réseaux. Vous pouvez définir la même adresse IP lors de la configuration de CIMC ; appuyez sur F8 au démarrage pour définir l'adresse IP. Modifiez également le mot de passe par défaut.

Une fois ESXi configuré, vous pouvez utiliser une machine Windows XP ou Windows 7, ainsi que l'adresse IP et les informations d'identification de connexion configurées ci-dessus, afin de vous connecter à l'hôte ESXi via le client vSphere.

Référez-vous à [Licensing ESX 4.x, ESXi 4.x et vCenter Server 4.x](#) pour plus d'informations sur la licence de l'hôte ESXi.

Reportez-vous aux articles suivants pour obtenir des informations sur la configuration de data

stores sur ESXi :

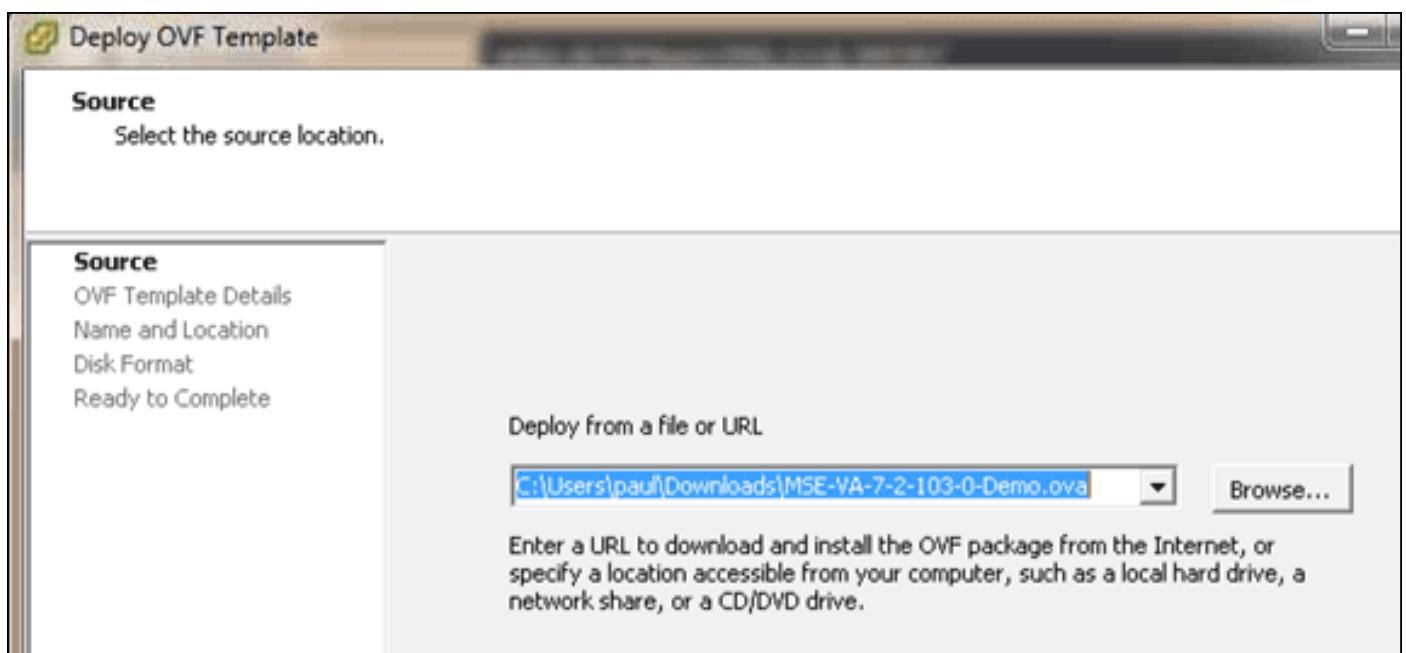
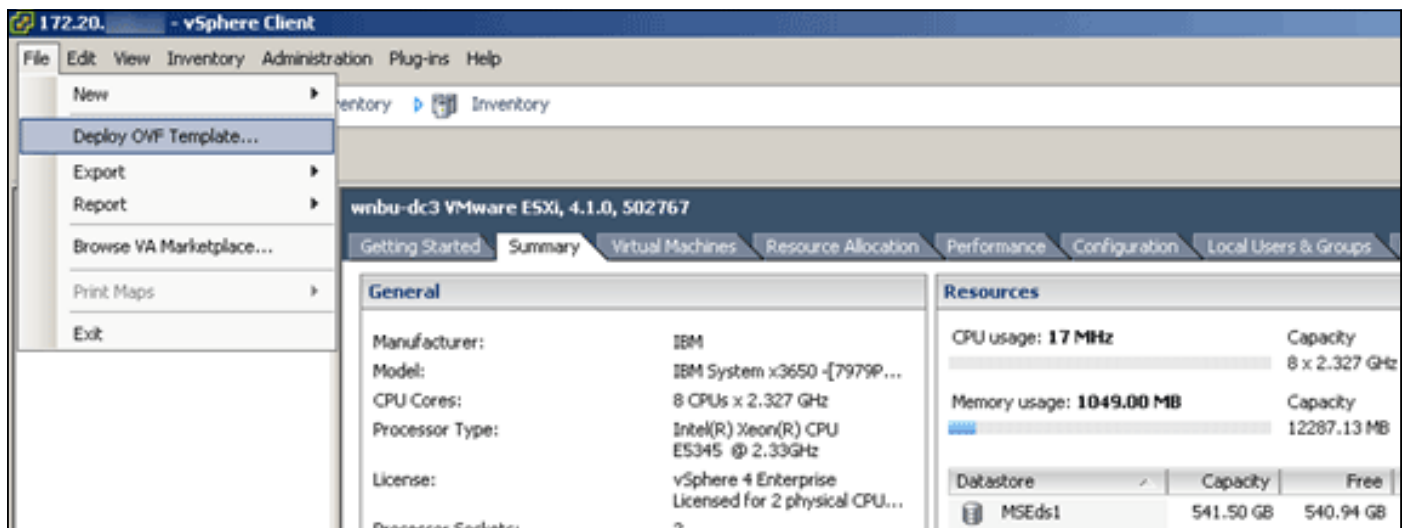
- [Créer des data stores VMFS](#)
- [Augmenter les data stores VMFS](#)

**Avertissement** : Utilisez une taille de bloc d'au moins 4 Mo lorsque vous créez des datastores pour ESXi 4.1.

## Installation de l'appareil virtuel MSE

L'appliance virtuelle MSE est distribuée sous la forme d'une image Open Virtual Appliance (OVA) qui peut être déployée sur un hôte ESXi à l'aide du client vSphere. Deux versions OVA sont disponibles : une version est destinée à une image de démonstration, qui ne nécessite que 60 Go d'espace disque, et l'autre version est une image de production générique.

L'image de production distribuable suppose un minimum de 500 Go et plus d'espace disque disponible sur le data store hôte ESXi. L'OVA peut être sélectionné et déployé via le client vSphere. Choisissez **Fichier > Déployer le modèle OVF** afin de déployer le modèle.



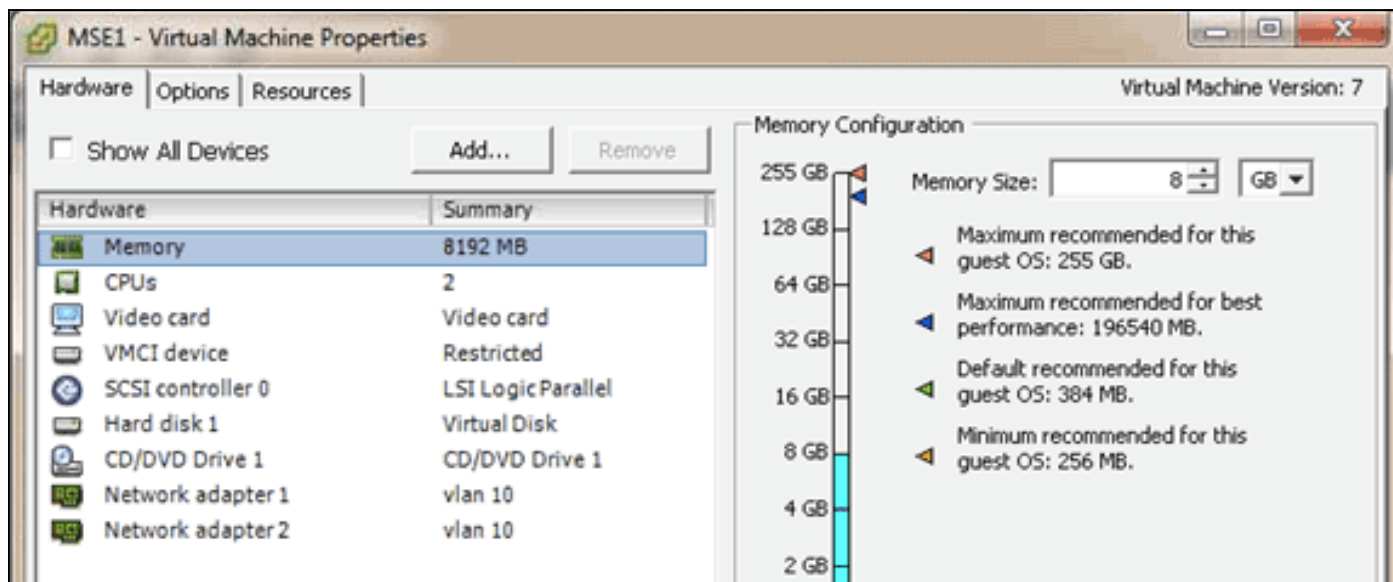
Le déploiement de l'image prend quelques minutes en fonction de la vitesse du réseau. Une fois

déployé, vous pouvez modifier la configuration de la machine virtuelle (VM) afin de configurer l'appliance ; la VM doit être mise hors tension lorsqu'elle est configurée.

## Configuration des niveaux de l'appliance virtuelle MSE

Le tableau de cette section répertorie les niveaux configurables sur l'appliance virtuelle et les ressources requises correspondantes. Allouer des cœurs dédiés à l'appliance et non aux cœurs virtuels hyperthread, car cela affectera les performances si vous supposez que l'hôte a plus de cœurs virtuels et que vous déployez plus d'appliances. Par exemple, dans l'UCS C200 mentionné ci-dessus, il y a huit (8) cœurs physiques disponibles, mais seize (16) cœurs virtuels avec hyperthreading. Ne supposez pas que seize (16) cœurs sont disponibles ; allouez seulement huit (8) cœurs afin de s'assurer que MSE fonctionne de manière fiable en cas de stress.

MSE principal	Ressources	Licence prise en charge (individuellement)		MSE secondaire pris en charge	
		Licence CAS	Licence wIPS	Appareil virtuel	Zone physique
Faible	6 G	2000	2000	Faible +	Non pris en charge
Standard	11 G	18000	5000	Standard+	
Élevé	20 G	50000	10 000	Élevé+	



## Configuration de l'appareil virtuel MSE

Une fois l'appliance virtuelle déployée et configurée, vous pouvez la mettre sous tension. Lorsque la solution matérielle-logicielle est mise sous tension pour la première fois, vous devez saisir les informations d'identification de connexion par défaut : root/password.

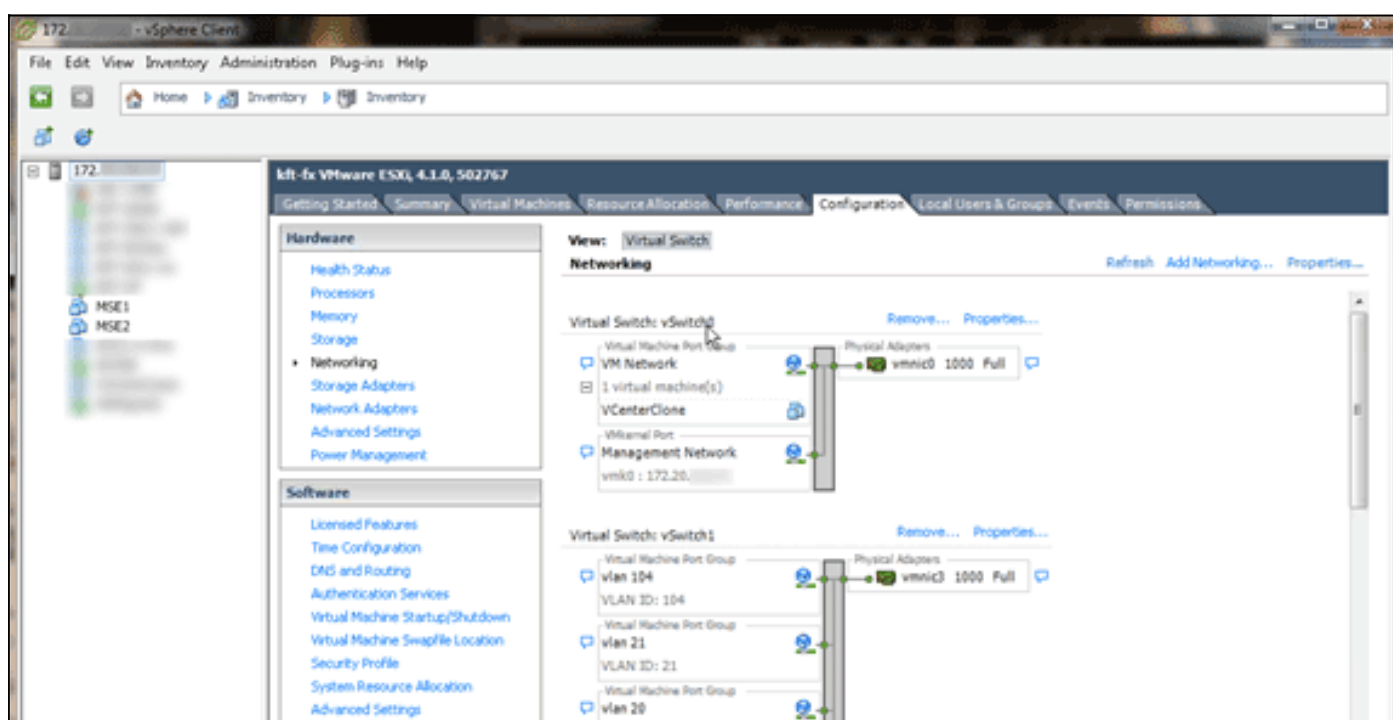
Lorsque vous vous connectez pour la première fois, l'appliance commence la configuration du logiciel MSE et installe également la base de données Oracle. Il s'agit d'un processus chronophage qui prendra au moins 30 à 40 minutes. Une fois l'installation terminée, l'invite de

connexion s'affiche à nouveau. Référez-vous à la section [Configuration du moteur de services de mobilité](#) du *Guide de démarrage du moteur de services de mobilité Cisco 3355* afin de continuer à configurer l'appareil.

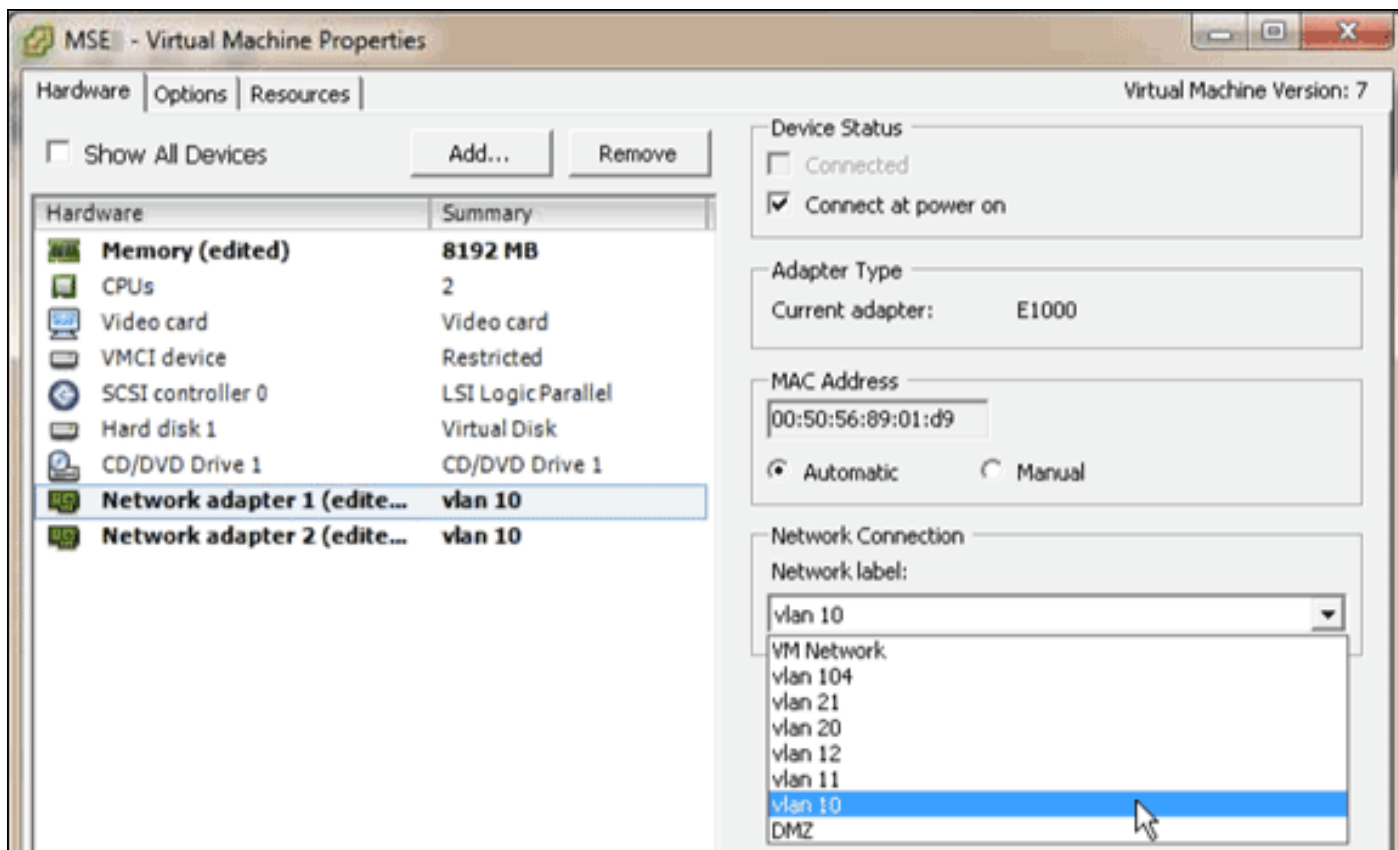
## Configuration du réseau

Par défaut, les machines virtuelles utilisent les paramètres du réseau hôte ; par conséquent, vous n'êtes pas tenu de configurer les adaptateurs de machine virtuelle sur ESXi. Cependant, si vous avez des réseaux publics et privés connectés à l'hôte et que vous souhaitez que les machines virtuelles aient accès aux deux, vous pouvez configurer les cartes d'ordinateurs virtuels dans le client vSphere.

Dans le client vSphere, sélectionnez l'hôte, cliquez sur l'onglet **Configuration**, puis sur **Mise en réseau**. Vous pouvez afficher les cartes physiques dans les propriétés du commutateur virtuel.



Créez des commutateurs séparés avec des adaptateurs séparés afin d'isoler les réseaux. Vous pouvez ensuite affecter les adaptateurs de machine virtuelle à ces réseaux, selon les besoins.



## Ajout d'espace disque dur

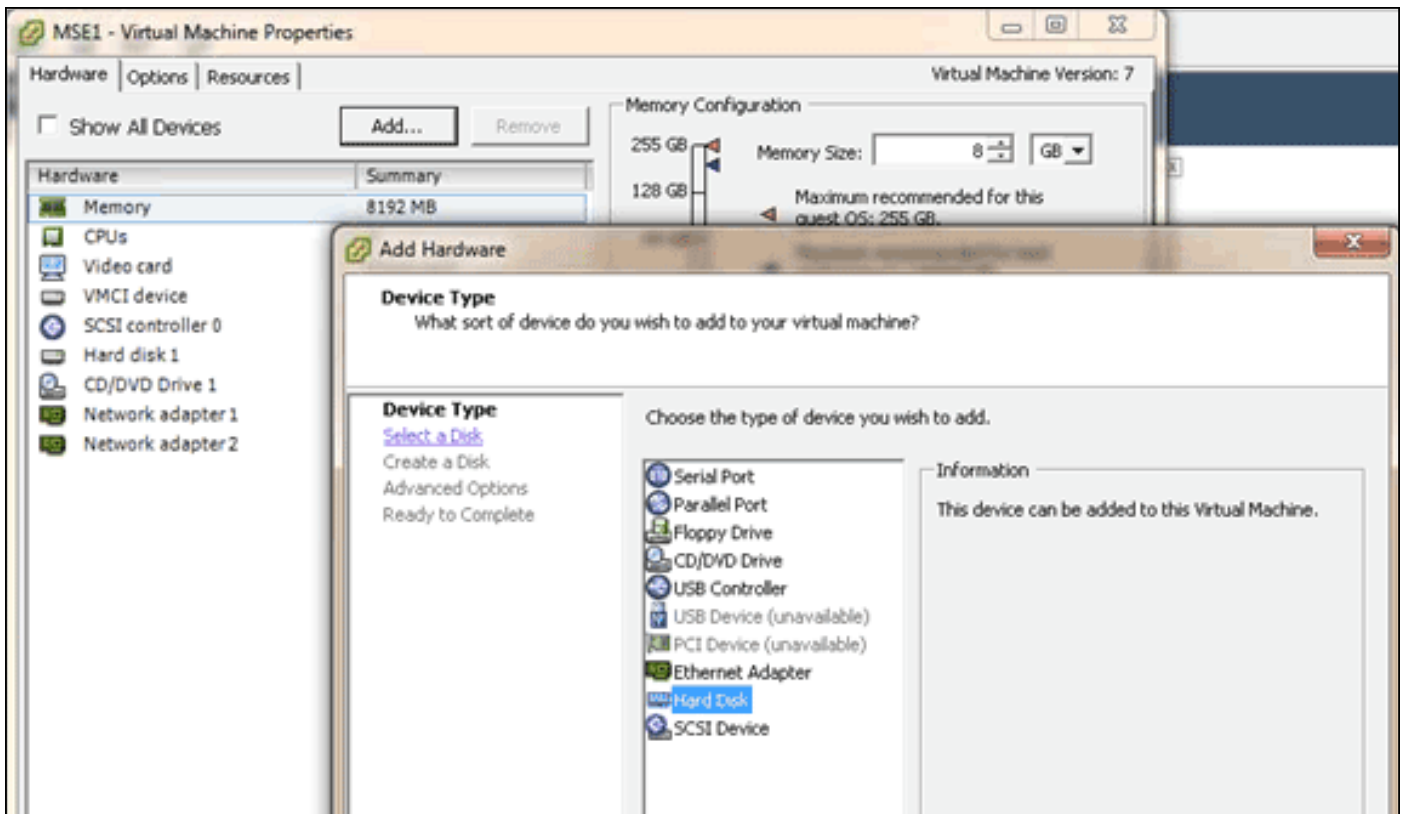
Si nécessaire, ajoutez une capacité de disque supplémentaire à la machine virtuelle et développez les partitions.

**Remarque** : le script `installDrive.sh` (situé dans le répertoire `/opt/mse/framework/bin`) détecte de nouveaux lecteurs et repartitionne les partitions existantes afin d'utiliser et d'étendre les nouveaux lecteurs.

Veillez à sauvegarder votre machine virtuelle (ou au moins les données MSE) avant de tenter de repartitionner l'espace disque.

Afin d'ajouter de l'espace disque à votre machine virtuelle, arrêtez la machine virtuelle, accédez aux paramètres de la machine virtuelle et ajoutez le disque dur supplémentaire.



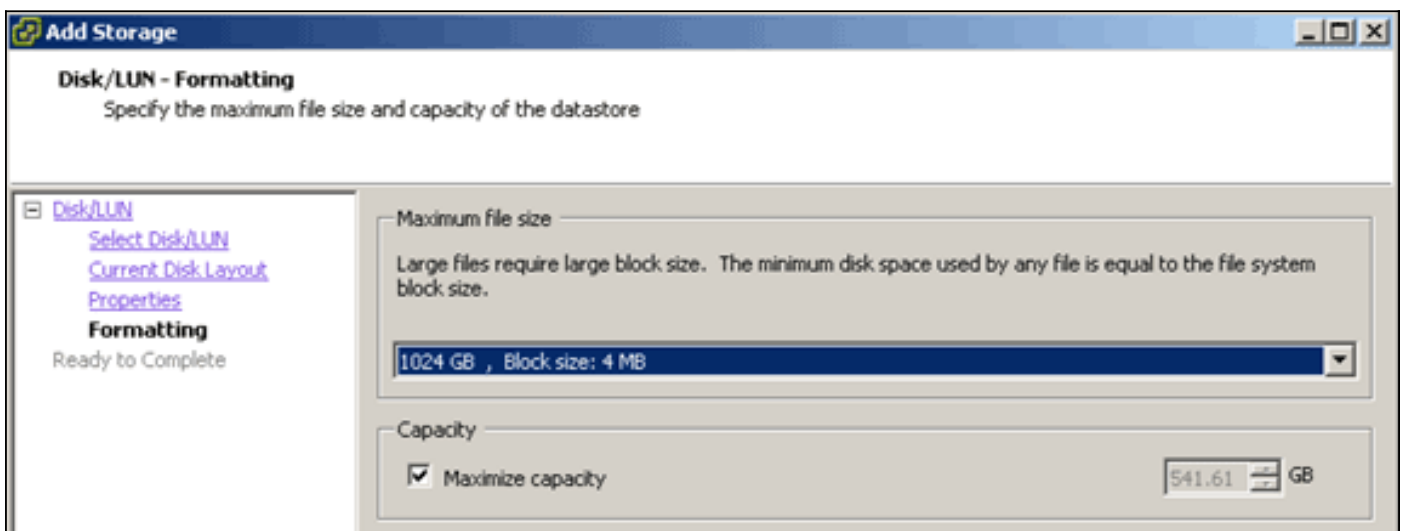


Une fois le disque dur ajouté, mettez la machine virtuelle sous tension, connectez-vous à l'appliance et exécutez le script `installDrive.sh`. Le script doit monter et repartitionner le lecteur nouvellement ajouté. Si vous avez ajouté plusieurs disques durs, exécutez le script une fois pour chaque nouveau disque.

## Taille du bloc

Pour les versions d'ESXi antérieures à la version 5.0, Cisco recommande que le data store sur l'hôte ait une taille de bloc de 4 Mo ou plus ; sinon, le déploiement de l'OVA pourrait échouer. Si le déploiement échoue, vous pouvez reconfigurer la taille du bloc.

Afin de reconfigurer la taille de bloc, accédez à Configuration > Stockage > Hôte ESX > Supprimer les datastores, et ajoutez de nouveau le stockage aux nouveaux datastores avec une taille de bloc d'au moins 4 Mo.



## Outils VMware

Si la machine virtuelle émet l'erreur suivante, cliquez avec le bouton droit sur la machine virtuelle dans le client vSphere, puis sélectionnez **Invité > Installer/Mettre à niveau les outils VMware** afin d'installer ou de mettre à niveau les outils VMware :

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

## Mise à niveau de l'appareil virtuel

Une fois que vous avez configuré l'appareil virtuelle, elle doit être traitée comme une boîte MSE physique. Vous n'avez pas besoin de déployer un nouvel OVA à chaque mise à niveau vers la dernière version de MSE ; vous pouvez télécharger l'image du programme d'installation appropriée sur l'appareil et suivre les étapes de mise à niveau comme avec une appliance physique.

## Licence de l'appareil virtuelle

Une fois que vous avez configuré l'appareil virtuelle, elle peut être utilisée en mode évaluation (par défaut, 60 jours) sans licence pour l'appareil. Cependant, vous devez activer l'appareil virtuelle à l'aide d'une licence d'activation d'appareil virtuelle si vous prévoyez de déployer des licences permanentes ou d'utiliser des fonctionnalités telles que la haute disponibilité (HA). Vous pouvez obtenir l'UDI (Unique Device Identifier) à partir de l'appareil virtuelle (exécutez **show csludi** sur l'appareil) ou des propriétés générales MSE de Cisco Prime Network Control System (NCS) et utiliser ces informations pour acheter la licence d'activation de l'appareil virtuelle et les licences de service permanent.

Cette image montre les modifications récentes apportées à l'interface du Centre de licences pour l'appareil virtuelle.

The screenshot displays the Cisco Prime Network Control System License Center interface. The main content area shows a table of supported licenses for MSE appliances. The table has columns for MSE Name (UDI), Service, Platform Limit, Type, Installed Limit, License Type, Count, Unlicensed Count, and % Used. Two licenses are highlighted with red boxes: 'mse-65' (Not Activated) and 'mse-215' (Activated). The 'mse-65' license is for a platform with a limit of 18000 CAS Elements, 5000 wIPS, and 10000 MSAP. The 'mse-215' license is for a platform with a limit of 50000 CAS Elements, 10000 wIPS, and 10000 MSAP. The UDI for the 'mse-215' license is highlighted in red.

MSE Name (UDI)	Service	Platform Limit	Type	Installed Limit	License Type	Count	Unlicensed Count	% Used
<b>mse-65</b> (Not Activated) (AJR-MSE-VA-R9:V01:mse-87.cisco.com_af729410-82f7-11e0-aa6d-00505691000f)	CAS	18000	CAS Elements	100	Evaluation ( 59 days left)	0	0	0%
	wIPS	5000	wIPS Monitor Mode APs	10	Evaluation ( 60 days left)	0	0	0%
			wIPS Local Mode APs	10	Evaluation ( 60 days left)	0	0	0%
	MSAP	10000	Service Advertisement Clicks	1000	Evaluation ( 60 days left)	0	0	0%
<b>mse-215</b> (Activated) (AJR-MSE-VA-R9:V01:mse-81.cisco.com_83d9a67e-92a4-11e0-85de-000c29572029)	CAS	50000	CAS Elements	50000	Permanent	49390	0	98%
	wIPS	10000	wIPS Monitor Mode APs	10	Evaluation ( 60 days left)	0	0	0%
			wIPS Local Mode APs	10	Evaluation ( 60 days left)	0	0	0%
	MSAP	10000	Service Advertisement Clicks	1000	Evaluation ( 60 days left)	0	0	0%

Pour l'appareil virtuelle, un message en regard du nom MSE indique clairement si elle est

activée ou non. En outre, il existe deux colonnes de limite : la colonne Plate-forme limitée répertorie la licence maximale prise en charge pour ce service sur cet appareil (en fonction de l'allocation des ressources à la machine virtuelle), et la colonne Plate-forme installée répertorie la licence réelle installée ou disponible via l'évaluation sur l'appareil.

## Haute disponibilité sur l'appareil virtuel

Pour utiliser la fonctionnalité HA, les appliances principale et secondaire doivent être activées avec une licence d'activation d'appliance virtuelle.

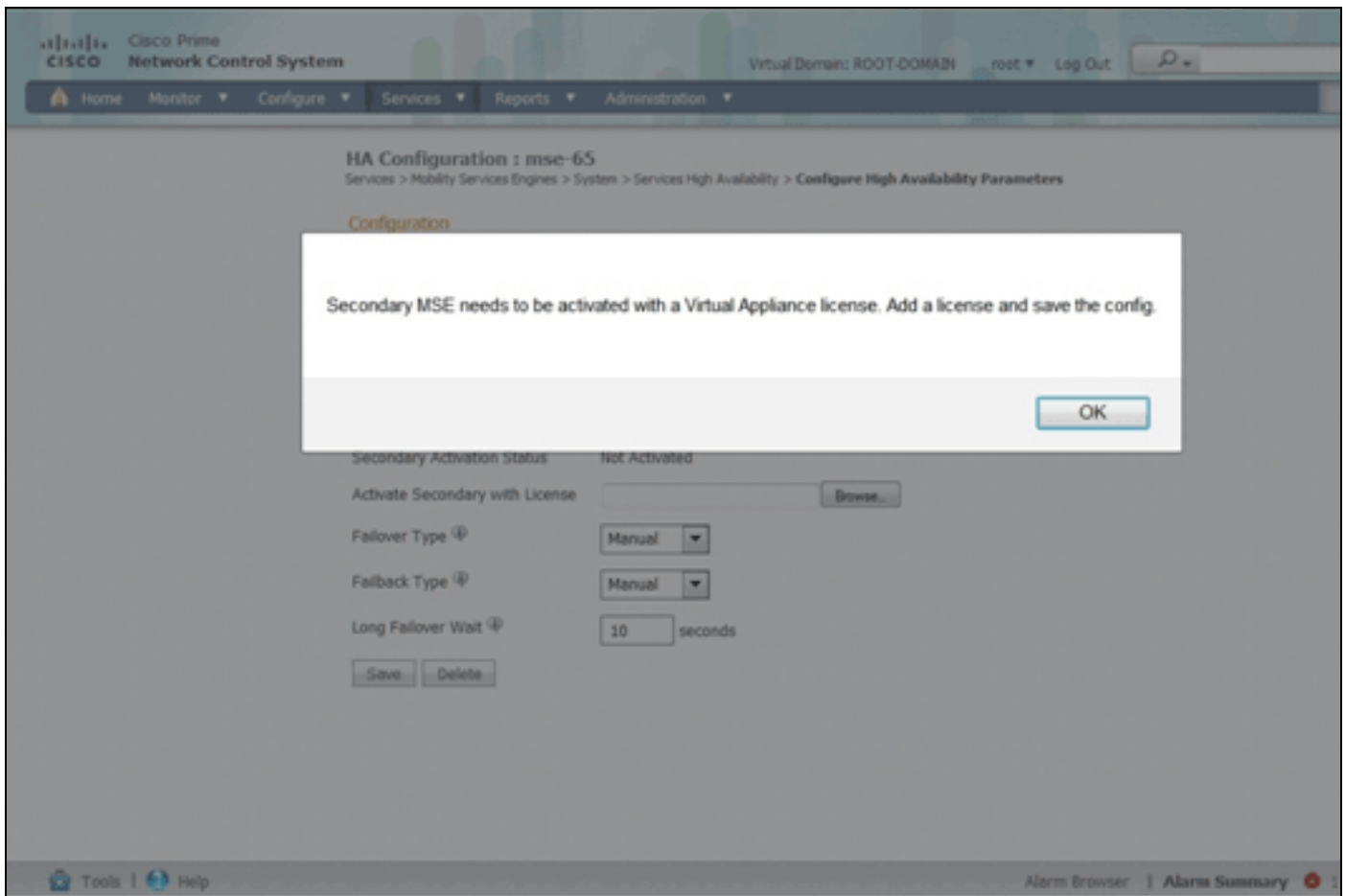
### Configurer la haute disponibilité

Vous pouvez configurer la configuration HA via le MSE principal sur le NCS.

The screenshot shows the Cisco Prime Network Control System (NCS) interface. The top navigation bar includes Home, Monitor, Configure, Services, Reports, and Administration. The main content area is titled "HA Configuration : mse-65" and shows the configuration for High Availability (HA) parameters. The configuration fields are as follows:

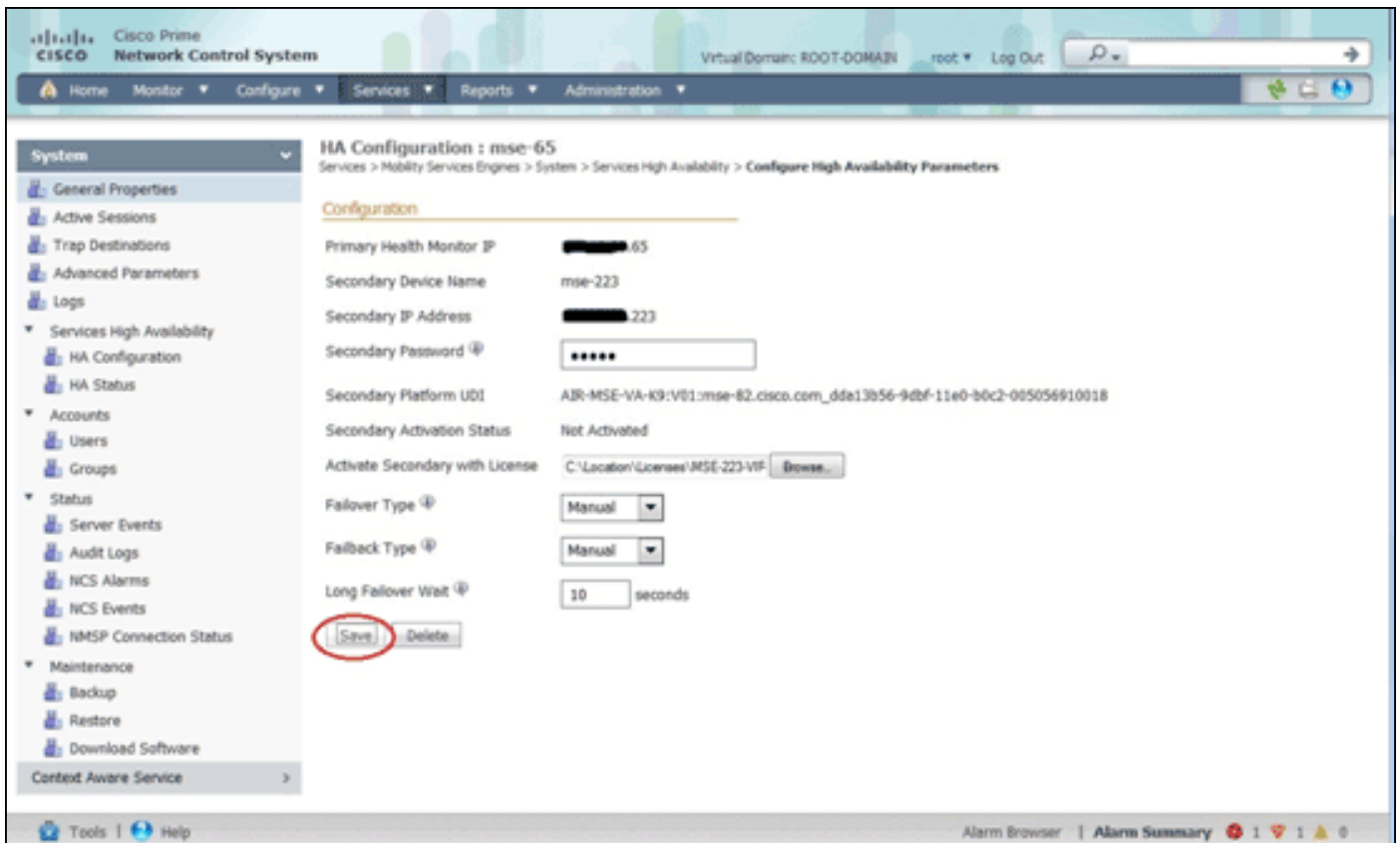
- Primary Health Monitor: mse-65
- Secondary Device Name: mse-223
- Secondary IP Address: 10.10.10.240
- Secondary Password: \*\*\*\*\*
- Failover Type: Manual
- Failback Type: Manual
- Long Failover Wait: 10 seconds

A "Save" button is located below the configuration fields. The left sidebar shows the navigation menu with "HA Configuration" selected under "Services High Availability". The bottom status bar shows "Alarm Browser | Alarm Summary" with 1 alarm and 0 notifications.



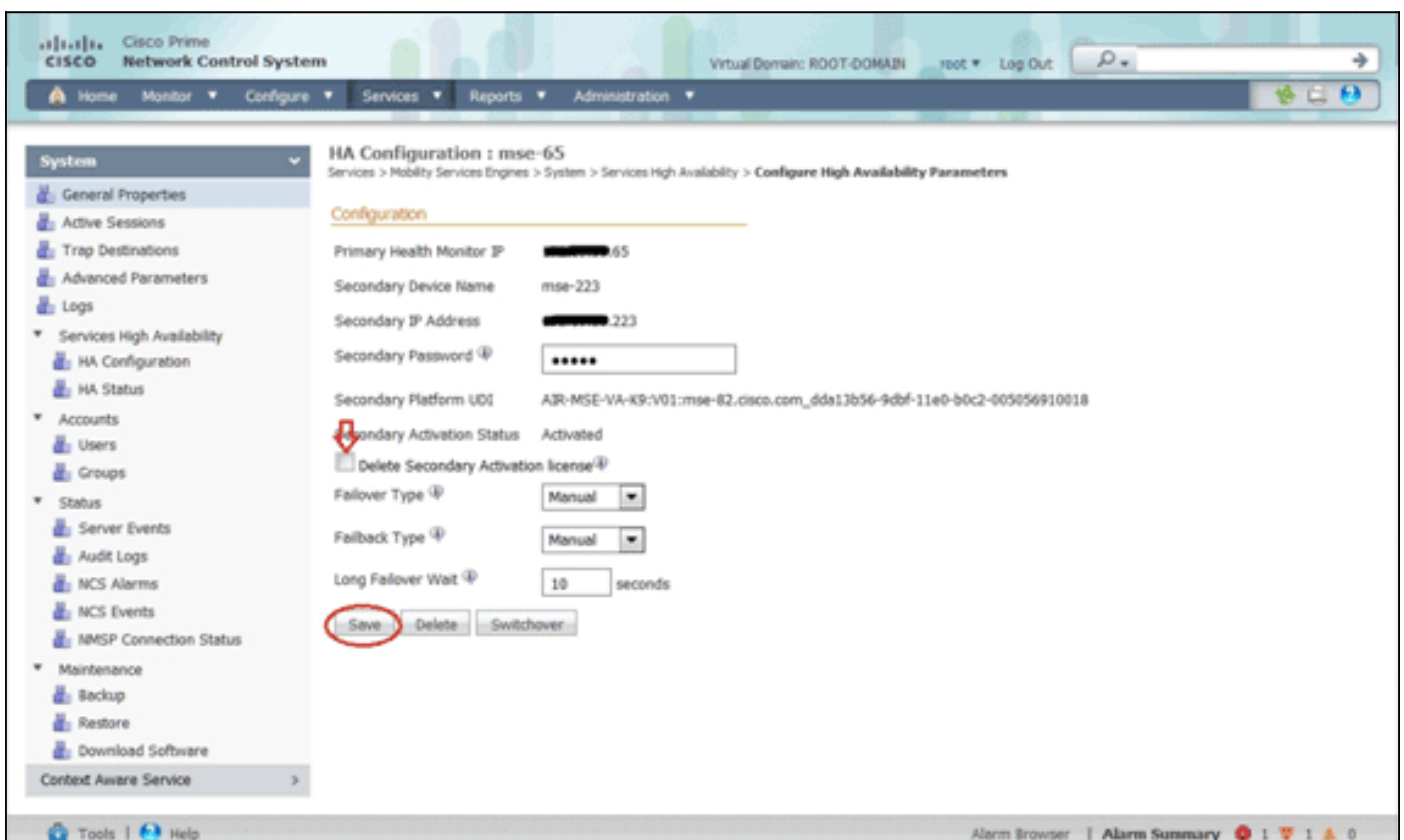
## Activation du MSE secondaire

Le périphérique secondaire doit être activé. Vous pouvez utiliser les informations UDI afin de demander une licence d'activation pour le MSE secondaire. Sur la page Configuration HA, recherchez la licence, puis cliquez sur **Enregistrer**. La HA sera configurée une fois que le MSE secondaire sera activé.



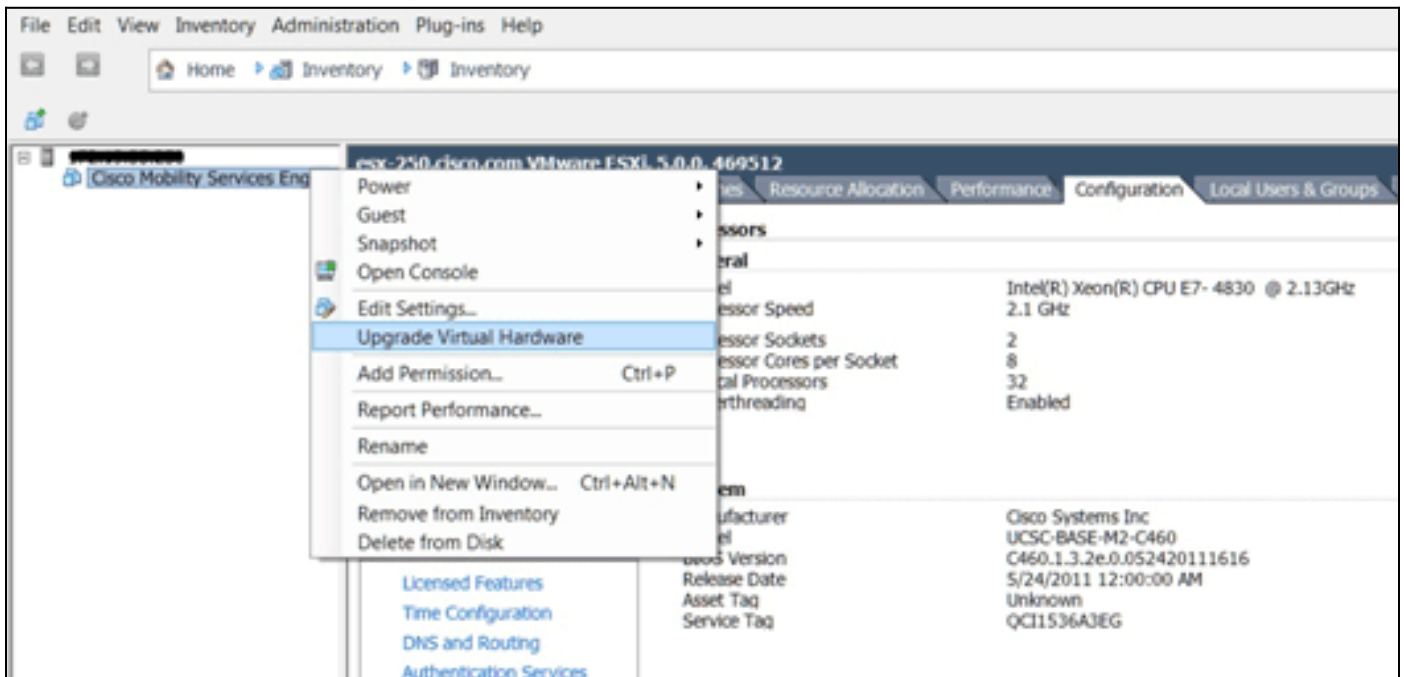
## Désactivation du MSE secondaire

Si vous devez supprimer la licence d'activation du MSE secondaire, vous pouvez cocher la case et cliquer sur **Enregistrer** afin de désactiver le MSE secondaire.



## Appareil virtuel sur ESXi 5.0

Sur l'ESXi 5.0, la taille du bloc est fixée à 1 Mo car elle prend en charge les déploiements de machines virtuelles volumineux. Pour pouvoir affecter plus de huit (8) cœurs à l'appliance virtuelle, vous devez mettre à niveau le matériel virtuel. Afin de mettre à niveau le matériel virtuel, sélectionnez le MSE et choisissez **Mettre à niveau le matériel virtuel** comme indiqué dans cette image :



## Procédure de console MSE

1. Connectez-vous à la console avec les informations d'identification suivantes :  
root/password. Au démarrage initial, le MSE invite l'administrateur à lancer le script de configuration.
2. Entrez **yes** à cette invite.

```
Cisco Mobility Service Engine

mse-kw login: root
Password:
Last login: Fri Oct 21 15:46:34 on tty1

Enter whether you would like to set up the initial
parameters manually or via the setup wizard.

Setup parameters via Setup Wizard (yes/no) [yes]: _
```

Re

**marque** : si le MSE n'invite pas la configuration, entrez la commande suivante :  
/opt/mse/setup/setup.sh.

3. Configurez le nom d'hôte  
:

```
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. Configurez le nom de domaine 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. Configurez le rôle HA principal

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

6. Configurez les paramètres d'interface 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. Lorsque vous êtes invité à entrer les paramètres d'interface eth1, tapez **Skip** afin de passer à l'étape suivante car une deuxième carte réseau n'est pas requise pour l'opération.

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

**Remarque :** L'adresse configurée doit fournir une connectivité IP aux WLC de perspective et au système de gestion WCS utilisé avec cet appareil.

8. Entrez les informations du ou des serveurs DNS. Un seul serveur DNS est requis pour une résolution de domaine réussie. Entrez les serveurs de sauvegarde pour la résilience.

```
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. Configurez le fuseau horaire. Cisco vous recommande d'utiliser UTC (temps universel coordonné). Si le fuseau horaire par défaut de New York ne s'applique pas à votre environnement, naviguez dans les menus d'emplacement afin de sélectionner le fuseau horaire approprié.

```
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. Lorsque vous êtes invité à configurer le jour et l'heure du prochain redémarrage, tapez **Ignorer**.

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

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

11. Configurez le serveur syslog distant, le cas échéant.

```
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)se default [Skip]:
```

12. Configurez le protocole NTP (Network Time Protocol) ou l'heure système. Le protocole NTP est facultatif, mais il garantit que votre système conserve une heure système précise. Si vous choisissez d'activer NTP, l'heure système sera configurée à partir des serveurs NTP que vous sélectionnez. Sinon, vous serez invité à saisir la date et l'heure actuelles.

```
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. Lorsque vous êtes invité à configurer la bannière de connexion, tapez

Skip.

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

14. Activez la connexion racine de la console locale. Ce paramètre est utilisé pour activer/désactiver l'accès de la console locale au système. La connexion de la racine de la console locale doit être activée afin que le dépannage local puisse se produire. La valeur par défaut est

Ignorer.

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

15. Activez la connexion racine Secure Shell (SSH). Ce paramètre est utilisé pour activer/désactiver l'accès à distance à la console du système. La connexion de la racine SSH doit être activée afin que le dépannage à distance puisse se produire. Cependant, les stratégies de sécurité de l'entreprise peuvent exiger que cette option soit désactivée.

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

16. Configurez le mode utilisateur unique et la puissance du mot de passe. Ces paramètres de configuration ne sont pas obligatoires ; la valeur par défaut est

Ignorer.

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

17. Modifiez le mot de passe racine. Cette étape est essentielle pour garantir la sécurité du système. Veillez à choisir un mot de passe fort composé de lettres et de chiffres sans mot de dictionnaire. La longueur minimale du mot de passe est de huit (8) caractères. Les informations d'identification par défaut sont

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

18. Configurez les paramètres de connexion et de mot de passe

:

```
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. Configurez un mot de passe de démarrage (Grub). (Facultatif) Ce paramètre de configuration n'est pas requis. La valeur par défaut est

Ignorer.

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

20. Configurez le nom d'utilisateur de communication

NCS.

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

21. Acceptez la modification apportée à la configuration.

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

Cette image présente un exemple de l'écran de fin :

```
Stopping MSE Platform
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. Exécutez la commande `getserverinfo` afin de vérifier la configuration.

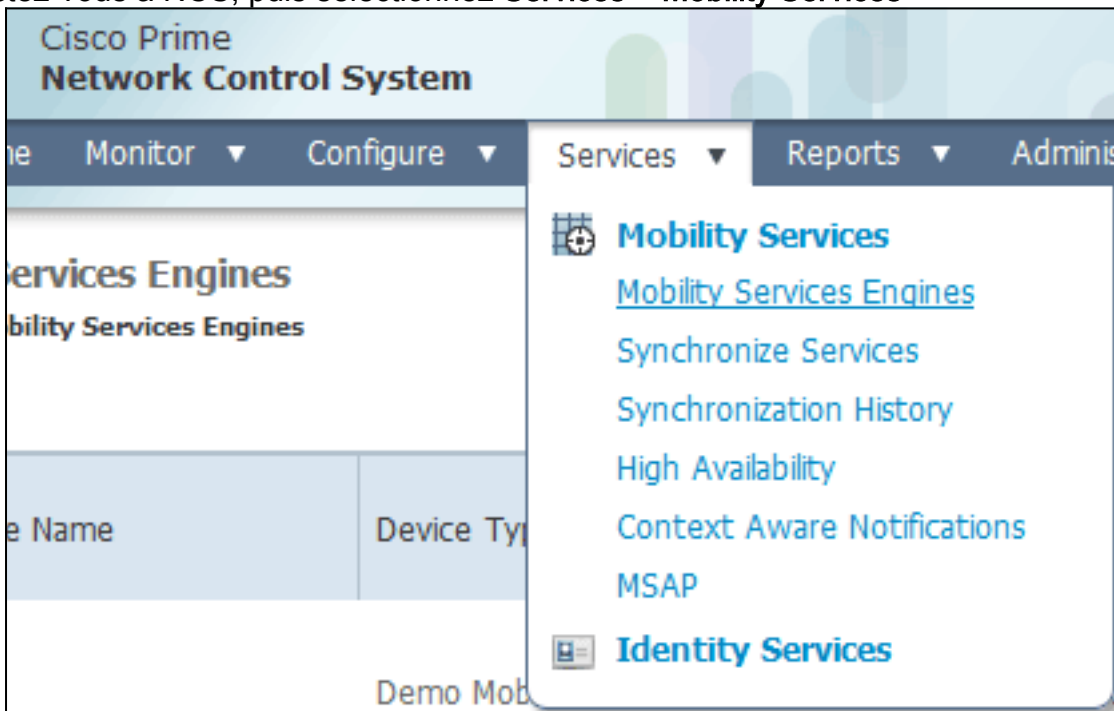
```
Active Wired Clients: 0
Active Elements(Wireless Clients, Rogue APs, Rogue Clients,
lients, Tags) Limit: 115
Active Sessions: 1
Wireless Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogue APs Not Tracked due to the limiting: 0
Rogue Clients Not Tracked due to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

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

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

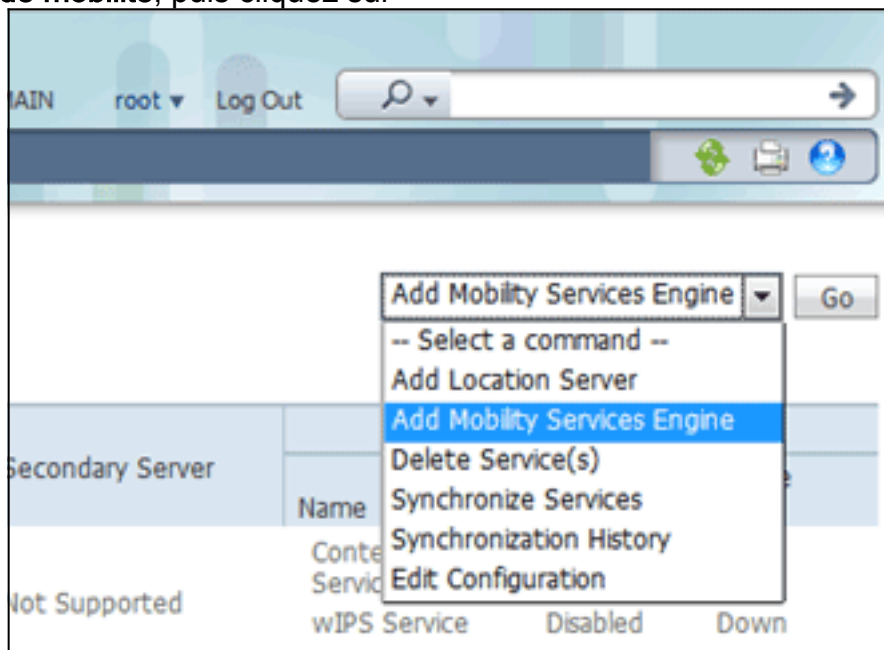
Ajout de MSE VA à NCS

1. Connectez-vous à NCS, puis sélectionnez **Services > Mobility Services**



Engine.

2. Dans la liste déroulante située sur le côté droit de la page, sélectionnez **Ajouter un moteur de services de mobilité**, puis cliquez sur



Exécuter.

3. Entrez un nom de périphérique unique pour le MSE, l'adresse IP précédemment configurée lors de la configuration du MSE, un nom de contact pour le support. et le nom d'utilisateur et le mot de passe NCS configurés lors de la configuration de MSE. Ne modifiez pas le nom d'utilisateur par défaut d'*admin*. Vous pouvez le laisser par défaut.

Cisco NCS - MSE Configuration Wizard

Cisco Prime Network Control System

root Log Out

**Add HSE Configuration**

Licensing

Select Service

Tracking

Assign Maps

**Add Mobility Services Engine**

Device Name:

IP Address:

Contact Name:

Username:

Password:

HTTP:  Enable

Delete synchronized service assignments  (network designs, controllers, wired switches and event definitions)

Selecting **Delete synchronized service assignments** permanently removes all service assignments from the MSE. Existing location history data is retained, however you must use manual service assignments to do any future location calculations.

Starting version 7.2.x of the MSE, Virtual IP (VIP) address support has been added for High Availability. If you wish to use High Availability and have configured a VIP, add the MSE using the VIP and not the health monitor IP.

Next

4. Cliquez sur **Next** (Suivant).
5. Cliquez sur **Licence**, puis vérifiez la licence. Lors de l'installation, la licence de démonstration par défaut est suffisante pour les tests. Vous pouvez ajouter d'autres licences achetées ou supprimer des licences sur la page Licences.

Cisco NCS - License Center - 10.10.10

Cisco Prime Network Control System

root Log Out

**MSE License Summary**

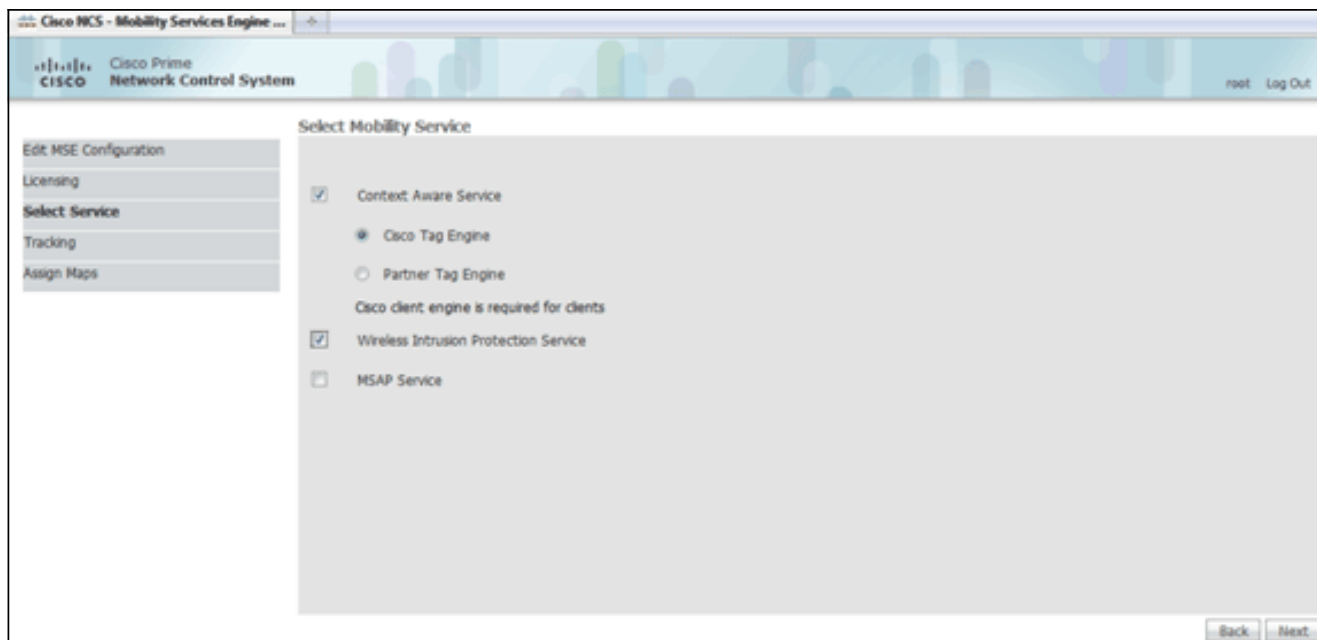
Permanent licenses include installed license counts and in-built license counts.

MSE Name (UDI)	Service	Platform Limit	Type	Installed Limit	License Type	Count	Unlicensed Count	% Used
mse2 Not Activated ( AIR-MSE-VA-K9:V01:mse-kw.corp.rf-demo.com_539b9f18-e86b-11e0-90b7-000c29556bb7)								
	CAS	2100	CAS Elements	100	Evaluation ( 60 days left)	0	0	0%
	wPS	2000	wPS Monitor Mode APs	10	Evaluation ( 60 days left)	0	0	0%
			wPS Local Mode APs	10	Evaluation ( 60 days left)	0	0	0%
	MSAP	0	Service Advertisement Clks	100	Evaluation ( 60 days left)	0	0	0%

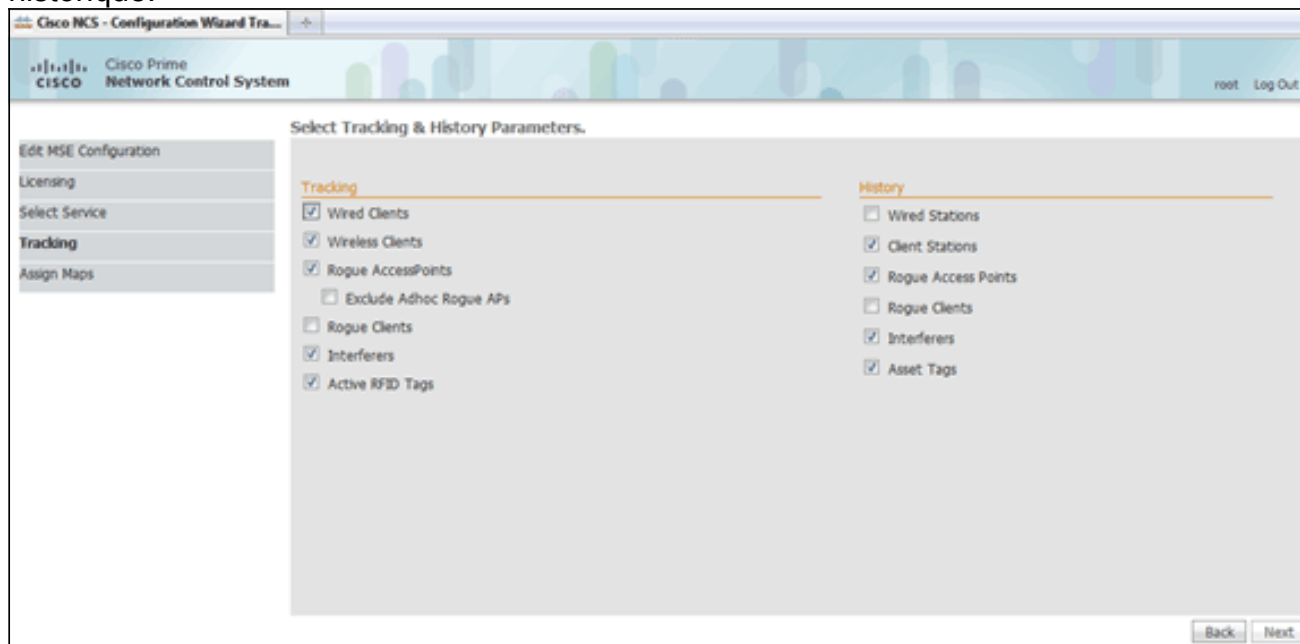
Add License Remove License

Back Next

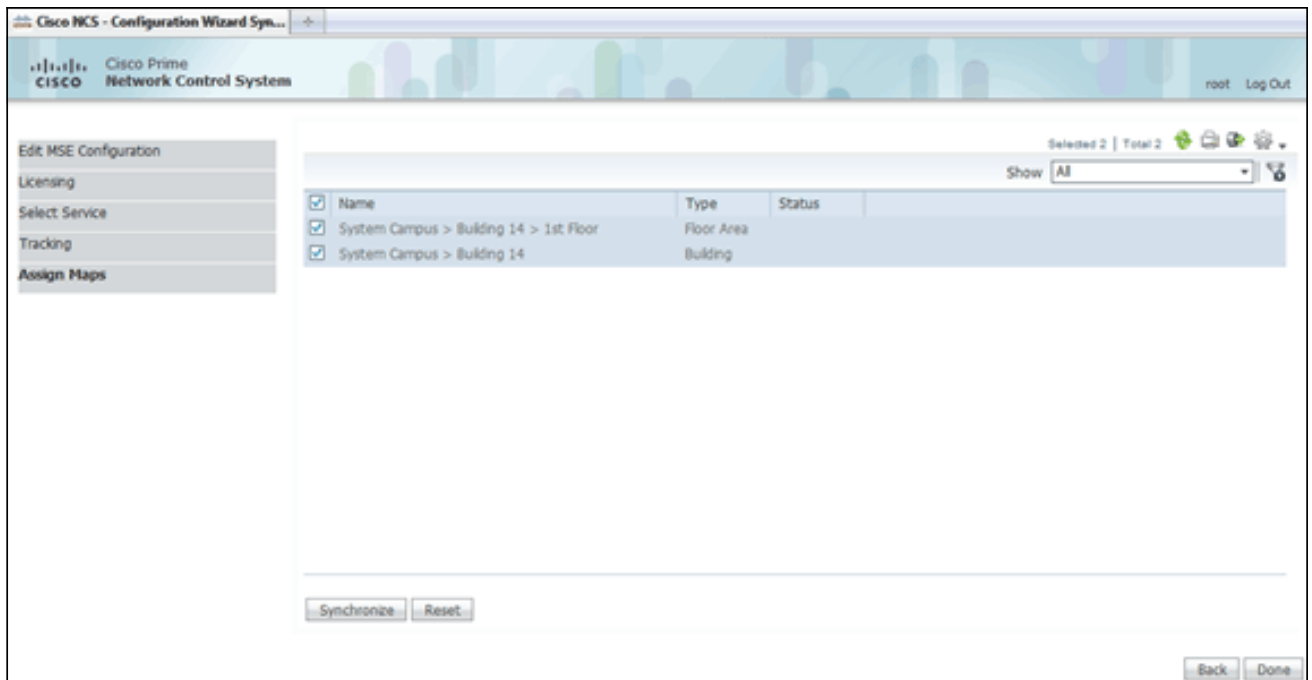
6. Cliquez sur **Next** (Suivant).



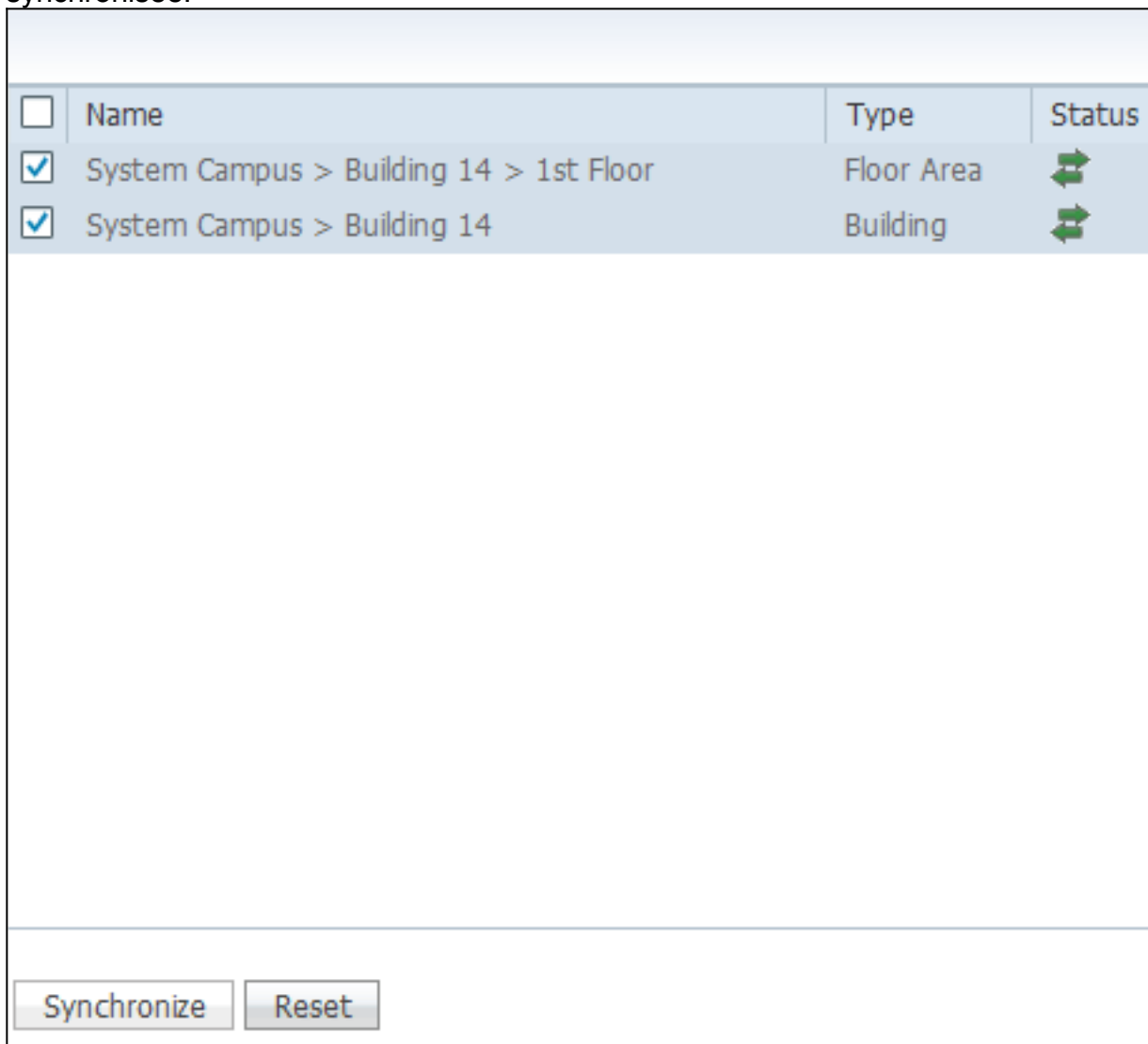
7. Sur la page Sélectionner le service de mobilité, cliquez sur le bouton radio **Cisco Tag Engine** (disponible depuis 7.0MR) (pour la prise en charge des balises RFID et client) ou cliquez sur le bouton radio **Partner Tag Engine** (pour Aeroscout, etc.).
8. Activez la case à cocher **Wireless Intrusion Protection Service** afin de tester la fonctionnalité de sécurité WIPS des fonctions Monitor Mode et Enhanced Local Mode.
9. Cliquez sur **Next** (Suivant).
10. Cochez les cases correspondant aux éléments à activer pour le suivi et aux paramètres d'historique de ces éléments à mettre à disposition pour le rapport historique.



11. Cliquez sur **Next** (Suivant).

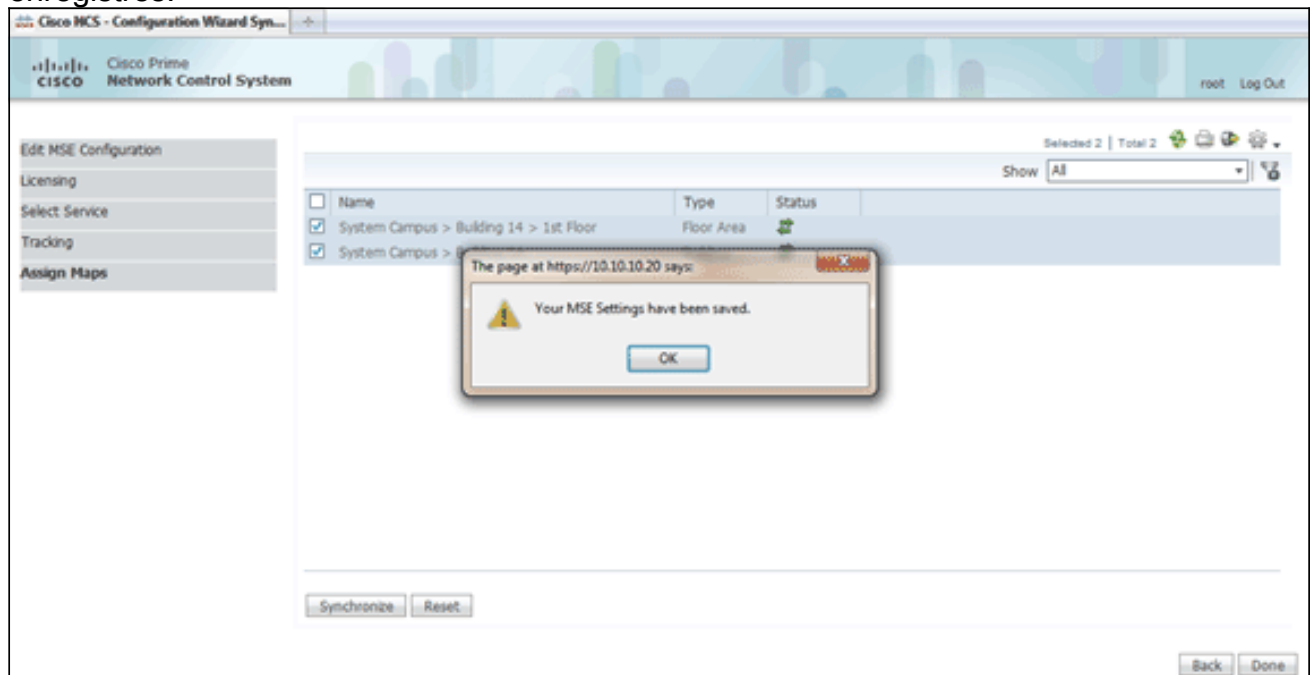


12. Cochez les cases correspondant au bâtiment et au sol existants, puis cliquez sur **Synchroniser**. Une fois synchronisée, la colonne Status se met à jour pour indiquer que la conception initiale du réseau a été synchronisée.

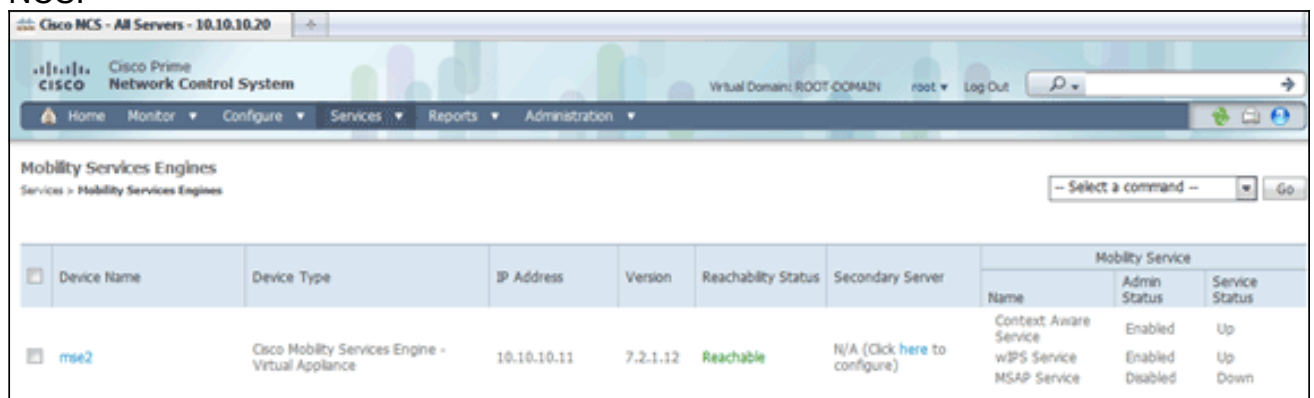


13. Lorsque la synchronisation est terminée, cliquez sur **Terminé**. Une boîte de dialogue s'affiche pour indiquer que les paramètres MSE ont été

enregistrés.



14. Confirmez la configuration sur la page MSE principale de NCS.



Assurez-vous de synchroniser les autres conceptions réseau, les contrôleurs, les commutateurs filaires et les groupes d'événements, selon les disponibilités. **Remarque :** Le service Cisco Context-Aware dépend fortement d'une horloge synchronisée entre le WLC, NCS et MSE. Si ces trois systèmes ne sont pas dirigés vers le même serveur NTP et configurés avec les mêmes paramètres de fuseau horaire, le service Context-Aware ne fonctionnera pas correctement. Avant d'essayer une procédure de dépannage, assurez-vous que l'horloge système est identique sur tous les composants du système Context-Aware.

15. Vérifiez la communication entre MSE et le contrôleur pour les services sélectionnés. Vérifiez que le MSE communique avec chacun des contrôleurs pour le service choisi uniquement ; L'état NMSP (Network Mobility Service Protocol) doit être *actif*. Cette image fournit un exemple de quand le hachage de clé n'est pas ajouté au WLC.

Cisco Prime Network Control System root Log

---

**Controller: 10.10.10.5 & MSE: mse2**

❗ Please refer to the Troubleshooting guide for additional troubleshooting steps.

**NMSP Troubleshooting Checklist**

Controller reachable from NCS	✓
Controller reachable from MSE	✓
Controller time after MSE time	✓
MSE KeyHash present on the Controller	✓
Controller Keyhash matches with the MSE	✗

**Suggested Action**  
Please check if the Mobility Service Status background task is enabled or manually run the task. If after 10 min the Nmosp connection still shows as Inactive, please synchronize and unsynchronize the controller. NMSP Status may also be Inactive, if the SNMP Community string of the controller is set to Read-Only Access mode.

**Additional Information**  
HashKey mismatch between Controller 10.10.10.5 and MSE: mse2

Sur la console WLC, utilisez la commande **show auth-list**. L'exemple suivant montre à partir de la console WLC qu'aucun serveur d'emplacement n'est 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
```

fin d'ajouter manuellement le MSE et d'établir une connexion NMSP au WLC, complétez ces étapes : Sur la console MSE, exécutez la commande **cmdshell**, puis la commande **show server-auth-info**. Cet exemple montre l'adresse MAC et le hachage de clé à utiliser pour l'ajout au

```
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.

Exécutez la commande **config auth-list add ssc <mac address> <MSE keyhash>**, puis exécutez la commande **show auth-list**. Cet exemple montre que le MSE a été ajouté au WLC (manuellement).

```
(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
```

Sur le NCS, vérifiez que la connexion NMSP affiche



Actif.

Groups	IP Address	Target Type	Version	NMSP Status	Echo Request Count	Echo Response
Status	10.10.10.5	Controller	7.2.1.51	Inactive	0	0
Server Events	10.10.10.25	Controller	7.0.116.0	Active	2	2
Audit Logs						
NCS Alarms						
NCS Events						
NMSP Connection Status						

## Référence de ligne de commande

### Commandes 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 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
```

## Commandes MSE

Exécutez cette commande afin de déterminer l'état des services MSE :

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

Exécutez cette commande afin de démarrer le moteur contextuel pour le suivi client :

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

Exécutez cette commande afin de déterminer l'état du moteur contextuel pour le suivi client :

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

Exécutez cette commande afin d'arrêter le moteur contextuel pour le suivi client :

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

Exécutez cette commande afin d'effectuer des diagnostics :

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

**Remarque** : La commande **rundiag** peut également être utilisée pour afficher les informations UDI MSE requises pour obtenir le fichier de licence du moteur contextuel pour les clients.

## Informations connexes

- [Guide de configuration MSE \(appliance virtuelle et physique\)](#)
- [Configuration de la haute disponibilité MSE](#)
- [Guide de déploiement de Cisco WIPS](#)
- [Commande de produits](#)
- [Support et documentation techniques - Cisco Systems](#)