

MSE軟體7.2版虛擬裝置配置和部署指南

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[系統要求](#)

[管理軟體和VMware許可](#)

[所需資源](#)

[設定ESXi主機](#)

[安裝MSE虛擬裝置](#)

[配置MSE虛擬裝置級別](#)

[設定MSE虛擬裝置](#)

[配置網路](#)

[新增硬碟空間](#)

[塊大小](#)

[VMware工具](#)

[升級虛擬裝置](#)

[許可虛擬裝置](#)

[虛擬裝置的高可用性](#)

[配置高可用性](#)

[啟用輔助MSE](#)

[停用輔助MSE](#)

[ESXi 5.0上的虛擬裝置](#)

[MSE控制檯過程](#)

[將MSE VA新增到NCS](#)

[命令列參考](#)

[WLC命令](#)

[MSE命令](#)

[相關資訊](#)

簡介

Cisco Mobility Services Engine(MSE)軟體7.2版新增了虛擬裝置並支援VMware ESXi。本文檔為將MSE虛擬裝置新增到Cisco Unified WLAN以及運行情景感知服務和/或Cisco Adaptive Wireless Intrusion Prevention System(wIPS)的使用者提供配置和部署指南以及故障排除提示。此外，本文檔還介紹了MSE虛擬裝置的系統要求，並提供了針對MSE虛擬裝置的常規部署指南。本文檔不提供MSE和相關元件的配置詳細資訊。其他檔案中提供了這方面的資料；提供參考資料。

請參閱[相關資訊](#)部分，獲取有關情景感知移動服務的配置和設計的文檔清單。自適應wIPS配置也不在本文檔中介紹。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco 3300系列行動化服務引擎。

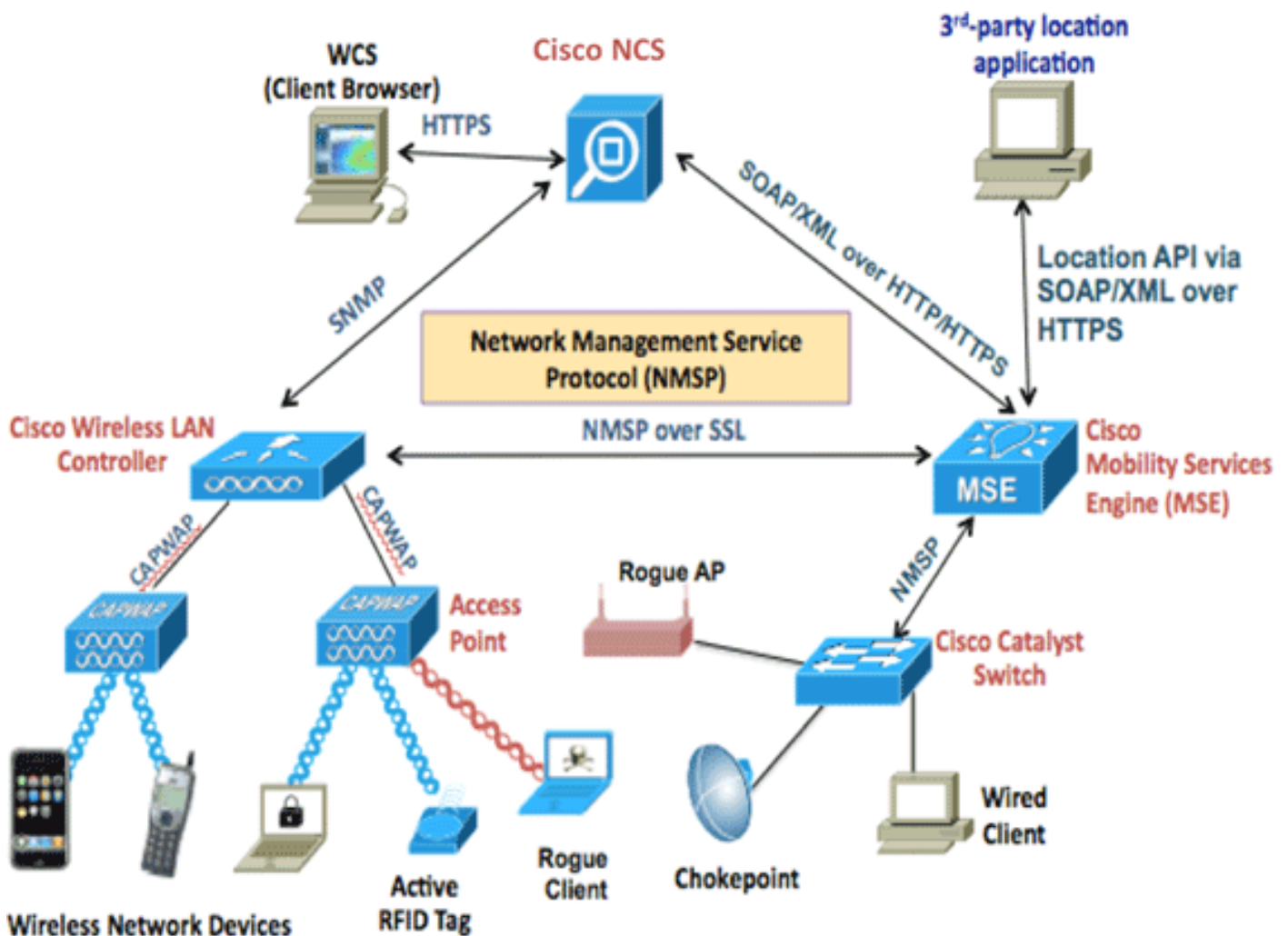
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

背景資訊

此圖顯示包括思科行動服務引擎(MSE)的典型思科WLAN部署。此部署還包括其他有線/無線網路客戶端、RFID標籤以及欺詐接入點(AP)和客戶端。MSE為位置和wIPS提供了對這些元素的可視性。在MSE軟體版本7.2之前，只有物理裝置限於MSE-3310和MSE-3350/3355。



系統要求

MSE軟體7.2版虛擬裝置在VMware ESXi 4.1及更高版本上受支援和測試。這些伺服器配置已經過測試，建議用作指南。

- 思科整合運算系統(UCS)C200 M2機架式伺服器兩(2)個英特爾®至強®CPU E5506 @ 2.13GHz RAM (根據配置的級別) 具有增強型RAID控制器的SAS驅動器 (至少500 GB+)
- UCS C210 M2機架式伺服器2個2 GHz英特爾至強CPU E5640 RAM (根據配置的級別) 具有增強型RAID控制器的SAS驅動器 (至少500 GB+)
- UCS C250 M2機架式伺服器2個2 GHz英特爾至強CPU E5570 RAM (根據配置的級別) 具有增強型RAID控制器的SAS驅動器 (至少500 GB+)
- UCS C460 M2機架式伺服器2個2 GHz英特爾至強CPU E7-4830 RAM (根據配置的級別) 具有增強型RAID控制器的SAS驅動器 (至少500 GB+)

附註： 使用兩(2)個至少與前述處理器一樣強大的四核處理器。

管理軟體和VMware許可

Cisco MSE軟體版本7.2虛擬裝置支援ESX/ESXi 4.x及更高版本。

為了管理ESXi主機以及配置和部署虛擬裝置，思科建議您在Windows XP或Windows 7 64位電腦上安裝vCenter Server 4.x並獲取vCenter Enterprise許可證。或者，如果您只有一個ESXi主機，則可以使用vSphere客戶端對其進行管理。

所需資源

資源要求取決於要部署的許可證。下表列出了可以配置虛擬裝置的不同級別：

主要MSE	資源		支援的許可證 (單獨)	
	虛擬裝置級別	總記憶體	CPU	CAS許可證
低	6G	2	2000	2000
標準	11G	8	18000	5000
高	20G	16	50000	10000

注意： 僅運行一個服務時，針對CAS和wIPS許可證列出的建議限制為最大支援限制。如果要在同一裝置上運行這兩種服務，則適用共存限制。

設定ESXi主機

完成以下步驟，以便在UCS或類似伺服器上設定MSE虛擬裝置：

1. 確保您的電腦具有至少500 GB+的硬碟空間和帶有增強型RAID控制器的快速SAS驅動器。
(為ESXi 5.0之前的版本建立資料儲存區時，應至少使用4 MB的塊大小。)
2. 安裝ESXi。插入ESXi 4.1或更高版本的安裝磁碟，然後從驅動器啟動。如果使用多個驅動器，請在配置為引導驅動器的驅動器中安裝ESXi。預設使用者名稱是root，密碼為空 (無密碼)。**註：** 如果您選擇了錯誤的驅動器進行安裝，則可以使用Fedora Live CD重新格式化。
3. 配置IP地址。選擇已啟用且處於活動狀態的網路介面卡。如果主機連線到多個網路，則您可能

擁有多個網路介面卡。您可以在CIMC設定期間設定相同的IP地址；在啟動過程中按F8鍵設定IP地址。另外，更改預設密碼。

設定ESXi後，您可以使用Windows XP或Windows 7電腦，以及上面配置的IP地址和登入憑據，以便通過vSphere客戶端連線到ESXi主機。

有關許可ESXi主機的資訊，請參閱[許可ESX 4.x、ESXi 4.x和vCenter Server 4.x](#)。

有關如何在ESXi上設定資料儲存區的資訊，請參閱以下文章：

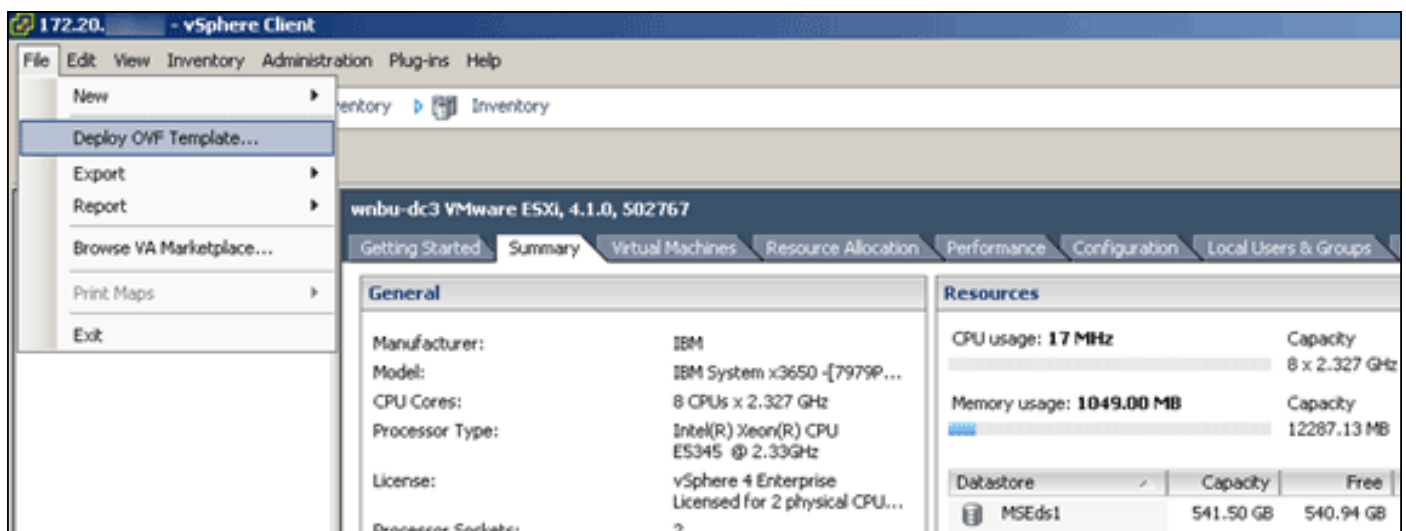
- [建立VMFS資料儲存區](#)
- [增加VMFS資料儲存區](#)

警告： 為ESXi 4.1建立資料儲存區時，應至少使用4 MB的塊大小。

安裝MSE虛擬裝置

MSE虛擬裝置作為開放式虛擬裝置(OVA)映像進行分發，可以使用vSphere客戶端在ESXi主機上部署該映像。有兩種可用的OVA版本：一個版本用於僅需要60GB磁碟空間的演示映像，另一個版本是通用生產映像。

可分發的生產映像假定ESXi主機資料儲存區上的可用磁碟空間至少為500 GB及以上。可以通過vSphere客戶端選擇和部署OVA。選擇**File > Deploy OVF Template**以部署模板。

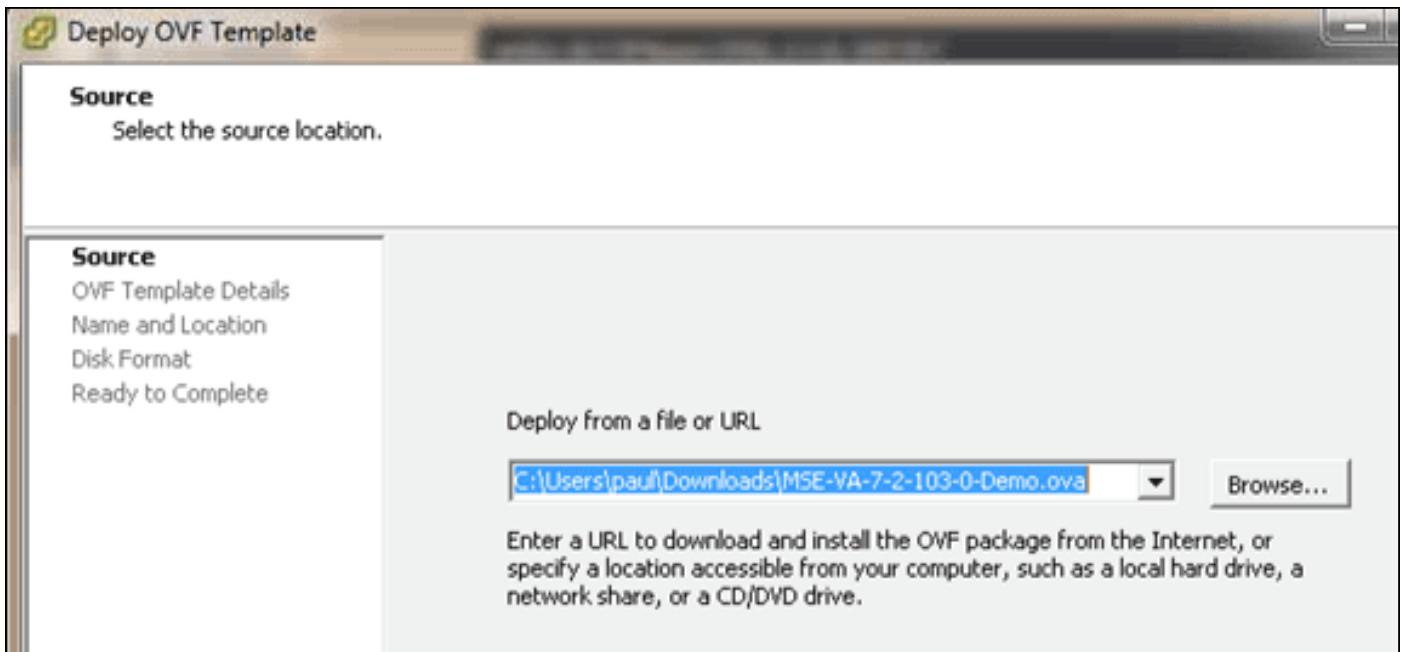


The screenshot shows the vSphere Client interface. The 'File' menu is open, highlighting 'Deploy OVF Template...'. The main window displays the summary page for a virtual machine named 'wnbu-dc3 VMware ESXi, 4.1.0, 502767'. The 'General' tab is selected, showing the following details:

General	
Manufacturer:	IBM
Model:	IBM System x3650 -[7979P...
CPU Cores:	8 CPUs x 2.327 GHz
Processor Type:	Intel(R) Xeon(R) CPU E5345 @ 2.33GHz
License:	vSphere 4 Enterprise Licensed for 2 physical CPU...
Processor Sockets:	2

The 'Resources' tab is also visible, showing the following resource usage and capacity:

Resources		
CPU usage: 17 MHz	Capacity	8 x 2.327 GHz
Memory usage: 1049.00 MB	Capacity	12287.13 MB
Datastore		
	Capacity	Free
MSEds1	541.50 GB	540.94 GB

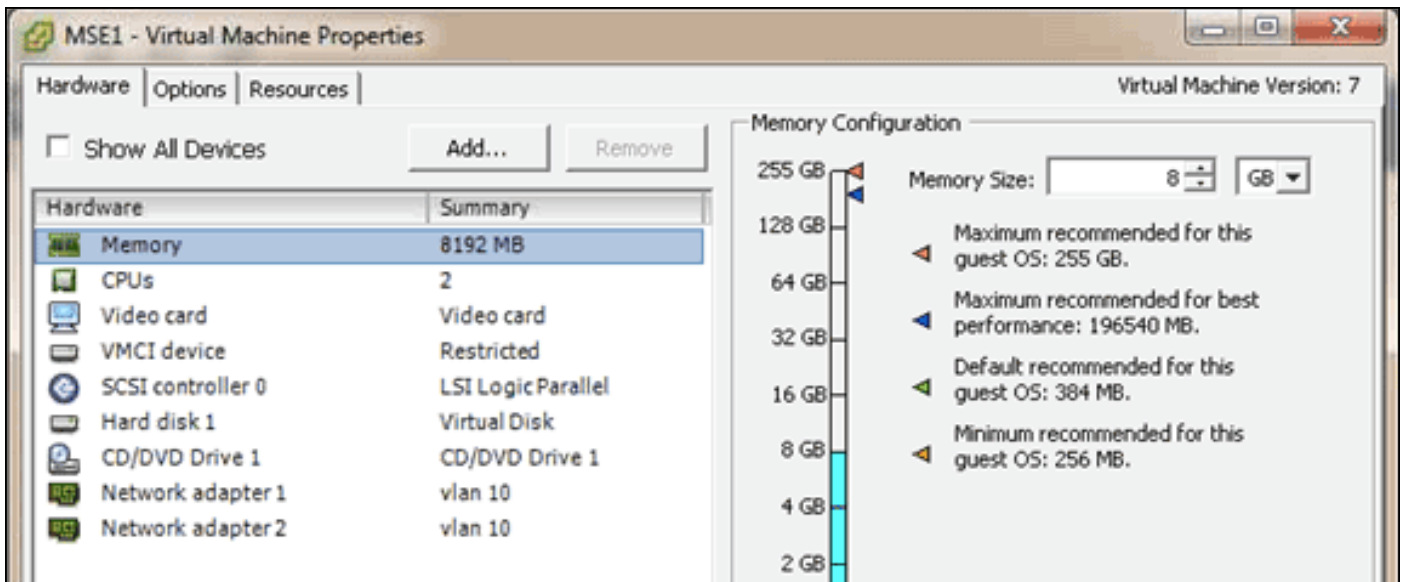


根據網路速度，部署映像需要幾分鐘時間。部署後，您可以編輯虛擬機器(VM)配置以配置裝置；配置時應關閉VM。

配置MSE虛擬裝置級別

本節中的表格列出了虛擬裝置上可配置的級別以及相應的資源要求。將專用核心分配給裝置，而不是超執行緒虛擬核心，因為如果您假定主機擁有更多虛擬核心，並且部署了更多裝置，則會影響效能。例如，在上面提到的UCS C200中，有八(8)個可用的物理核心，但是有十六(16)個採用超執行緒技術的虛擬核心。不要假設有十六(16)個核心可用；僅分配八(8)個核心，以確保MSE在受到壓力時可靠地運行。

主要MSE	資源	支援的許可證 (單獨)		支援的輔助 MSE	
		CAS許可證	wIPS許可證	虛擬裝置	物理盒
低	6G	2000	2000	低+	不支援
標準	11G	18000	5000	Standard+	
高	20G	50000	10000	高+	



設定MSE虛擬裝置

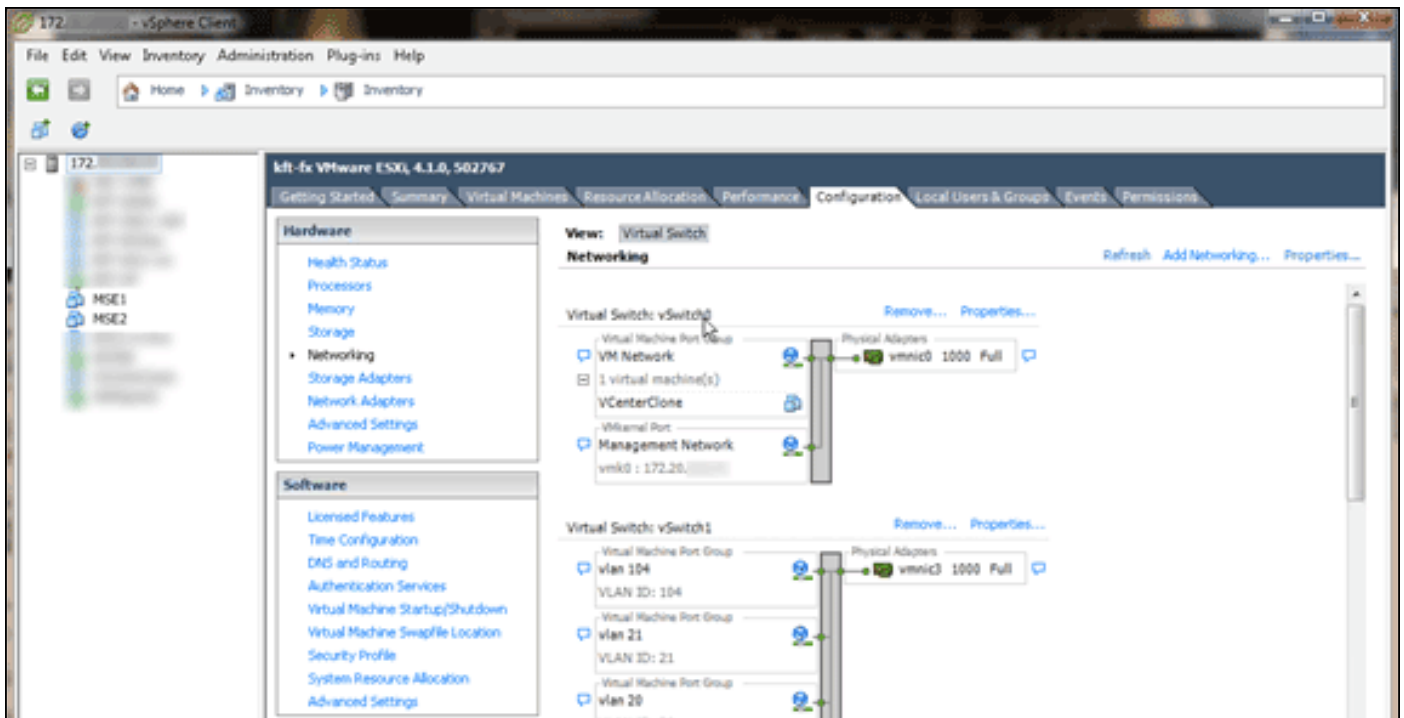
部署並配置虛擬裝置後，即可為其通電。當裝置首次通電時，您需要輸入預設登入憑證：
：root/password。

首次登入時，裝置將開始配置MSE軟體並安裝Oracle資料庫。這是一個一次性耗時的過程，至少需要30-40分鐘。安裝完成後，將再次顯示登入提示。請參閱 [Cisco 3355移動服務引擎入門指南](#) 的 [配置移動服務引擎](#) 部分，以繼續配置裝置。

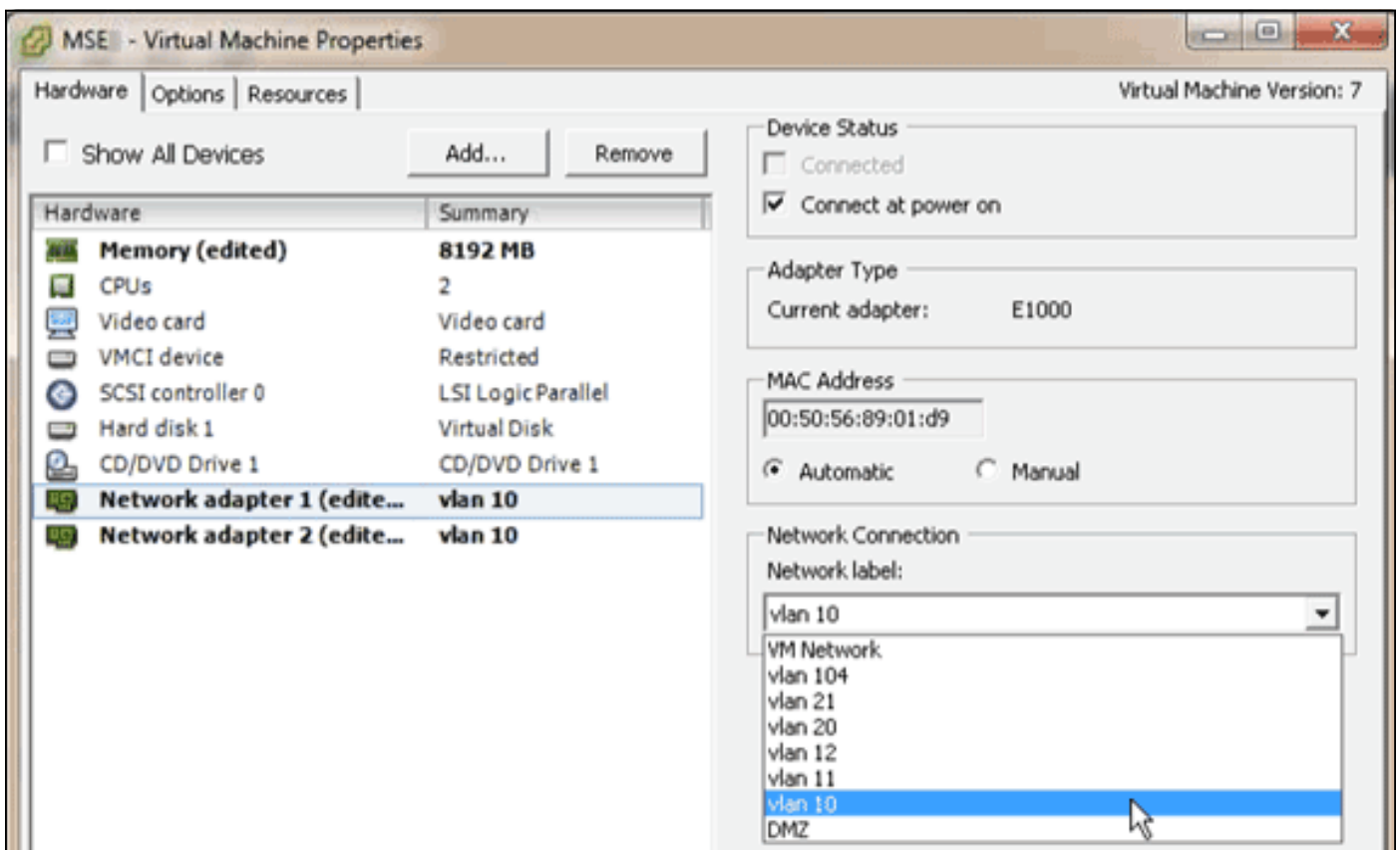
配置網路

預設情況下，VM使用主機網路設定；因此，不需要在ESXi上配置VM介面卡。但是，如果您將公共和專用網路都連線到主機，並且希望VM能夠同時訪問這兩個網路，則可以在SharePoint客戶端中配置VM介面卡。

在vSphere客戶端中，選擇主機，按一下**Configuration**頁籤，然後按一下**Networking**。您可以在虛擬交換機屬性中檢視物理介面卡。



使用單獨的介面卡建立單獨的交換機，以隔離網路。然後，您可以根據需要將VM介面卡分配給這些網路。



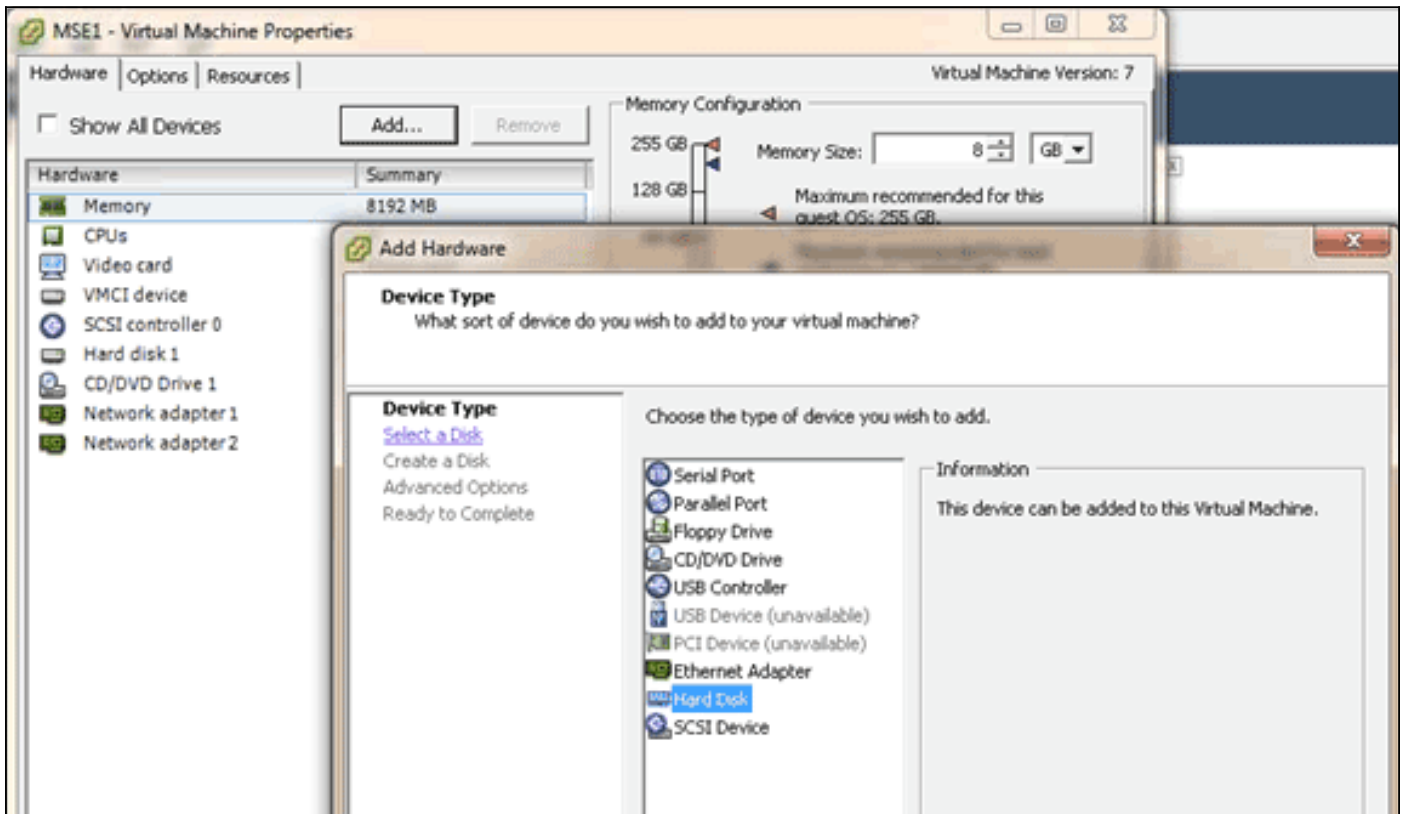
新增硬碟空間

如果需要，請向VM新增額外的磁碟容量並擴展分割槽。

注意：installDrive.sh指令碼（位於/opt/mse/framework/bin目錄中）檢測新驅動器並重新分割槽現有分割槽，以便使用和擴展新驅動器。

嘗試重新分割槽磁碟空間之前，請確保備份VM（或至少備份MSE資料）。

若要向虛擬機器新增更多磁碟空間，請關閉虛擬機器，轉到VM設定並新增其他硬碟。

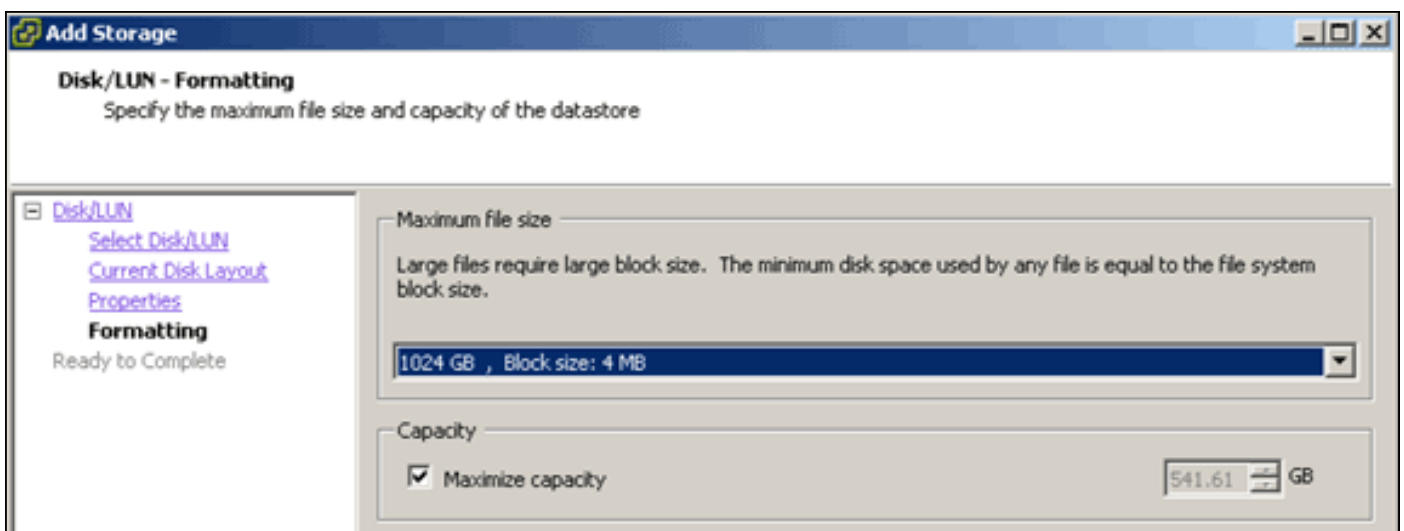


新增硬碟後，開啟VM的電源，登入裝置並運行installDrive.sh指令碼。指令碼應裝載並重新分割槽新增的驅動器。如果新增了多個硬碟，請為每個新硬碟運行一次指令碼。

塊大小

對於5.0之前的ESXi版本，思科建議主機上的資料儲存區具有4 MB或更大的塊大小；否則，OVA的部署可能會失敗。如果部署失敗，您可以重新配置塊大小。

要重新配置資料塊大小，請轉到ESX主機配置>儲存>刪除資料儲存區，然後再次將儲存區新增到塊大小至少為4MB的新資料儲存區。



如果VM引發以下錯誤，請在vSphere客戶端中按一下右鍵VM，然後選擇**Guest > Install/Upgrade VMware Tools**以安裝或升級VMware工具：

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

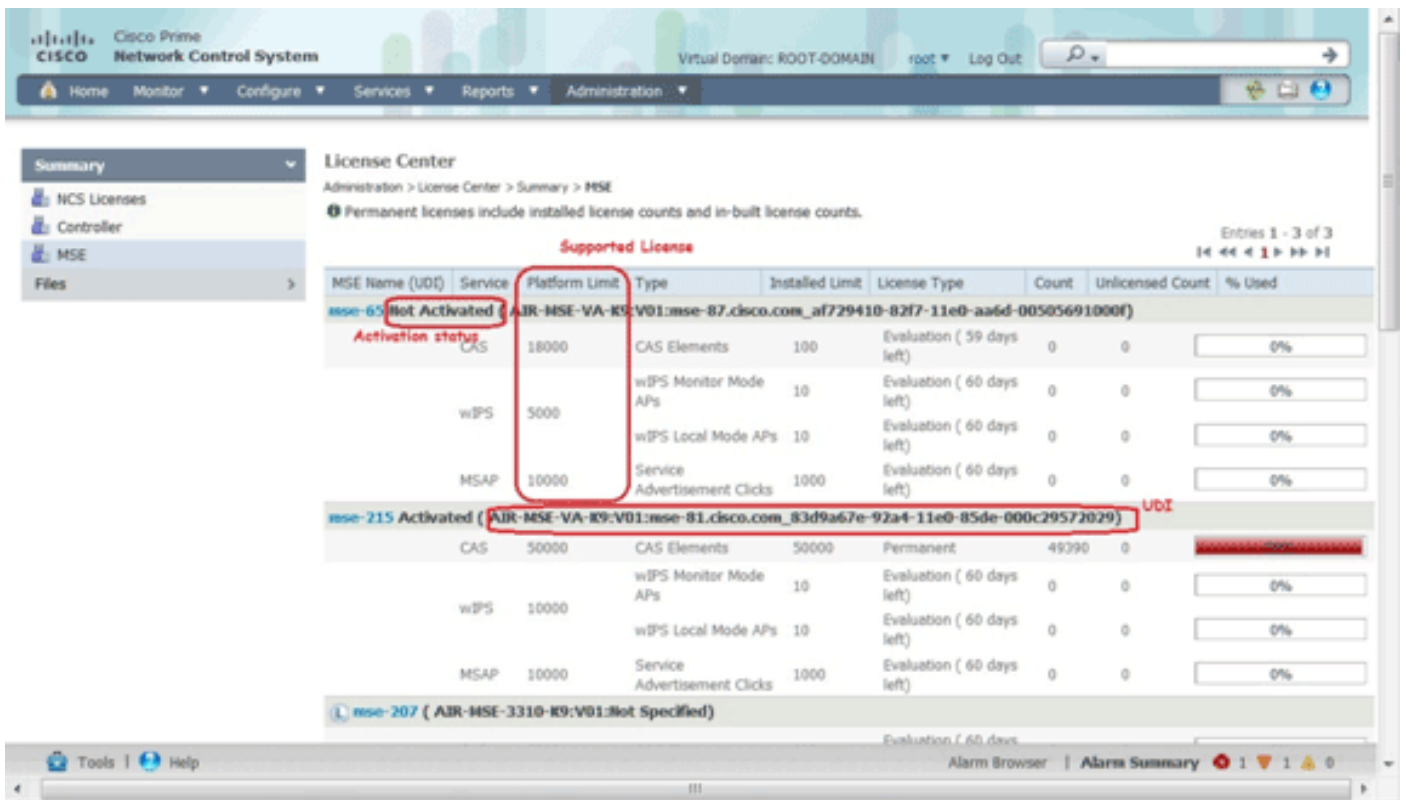
升級虛擬裝置

配置虛擬裝置後，應將其視為物理MSE盒。您無需在每次要升級到最新的MSE版本時都部署新的OVA;您可以將相應的安裝程式映像下載到裝置中，然後按照物理裝置的升級步驟進行升級。

許可虛擬裝置

配置虛擬裝置後，可以在評估模式（預設60天）下使用虛擬裝置，而無需授權裝置。但是，如果您計畫部署永久許可證或使用高可用性(HA)等功能，則必須使用虛擬裝置啟用許可證啟用虛擬裝置。您可以從虛擬裝置(在裝置上運行**show csludi**)或從Cisco Prime網路控制系統(NCS)MSE常規屬性獲取唯一裝置識別符號(UDI)，並使用此資訊購買虛擬裝置啟用許可證和永久服務許可證。

此影象顯示了虛擬裝置的許可證中心UI的最新更改。



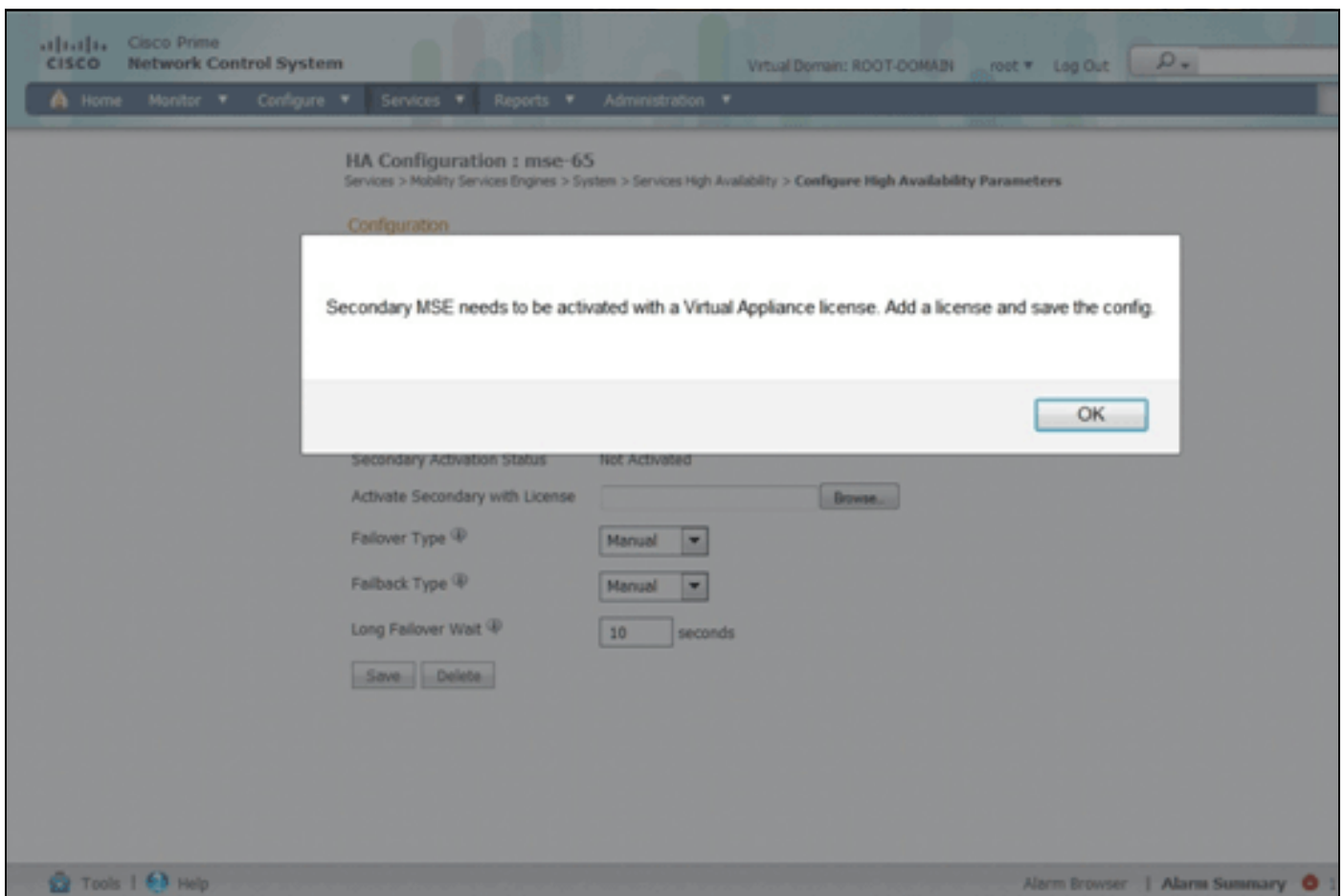
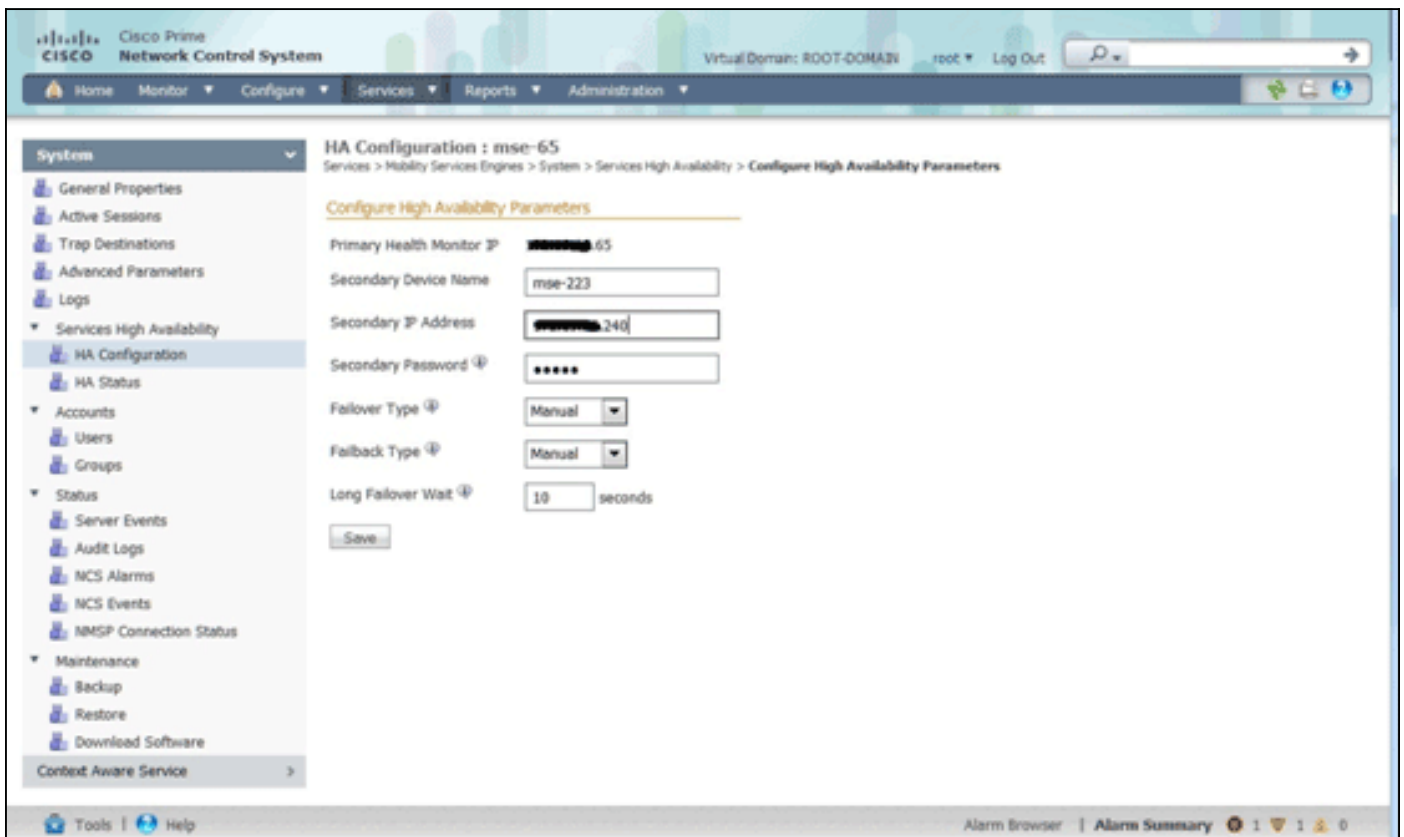
對於虛擬裝置，MSE名稱旁邊的消息清楚地指示其是否已啟用。此外，還有兩個限制列：「平台限制」列列出此裝置上該服務支援的最大許可證（具體取決於分配給VM的資源），「安裝限制」列列出實際安裝的許可證或通過裝置評估提供的許可證。

虛擬裝置的高可用性

為了使用HA功能，必須使用虛擬裝置啟用許可證啟用主裝置和輔助裝置。

配置高可用性

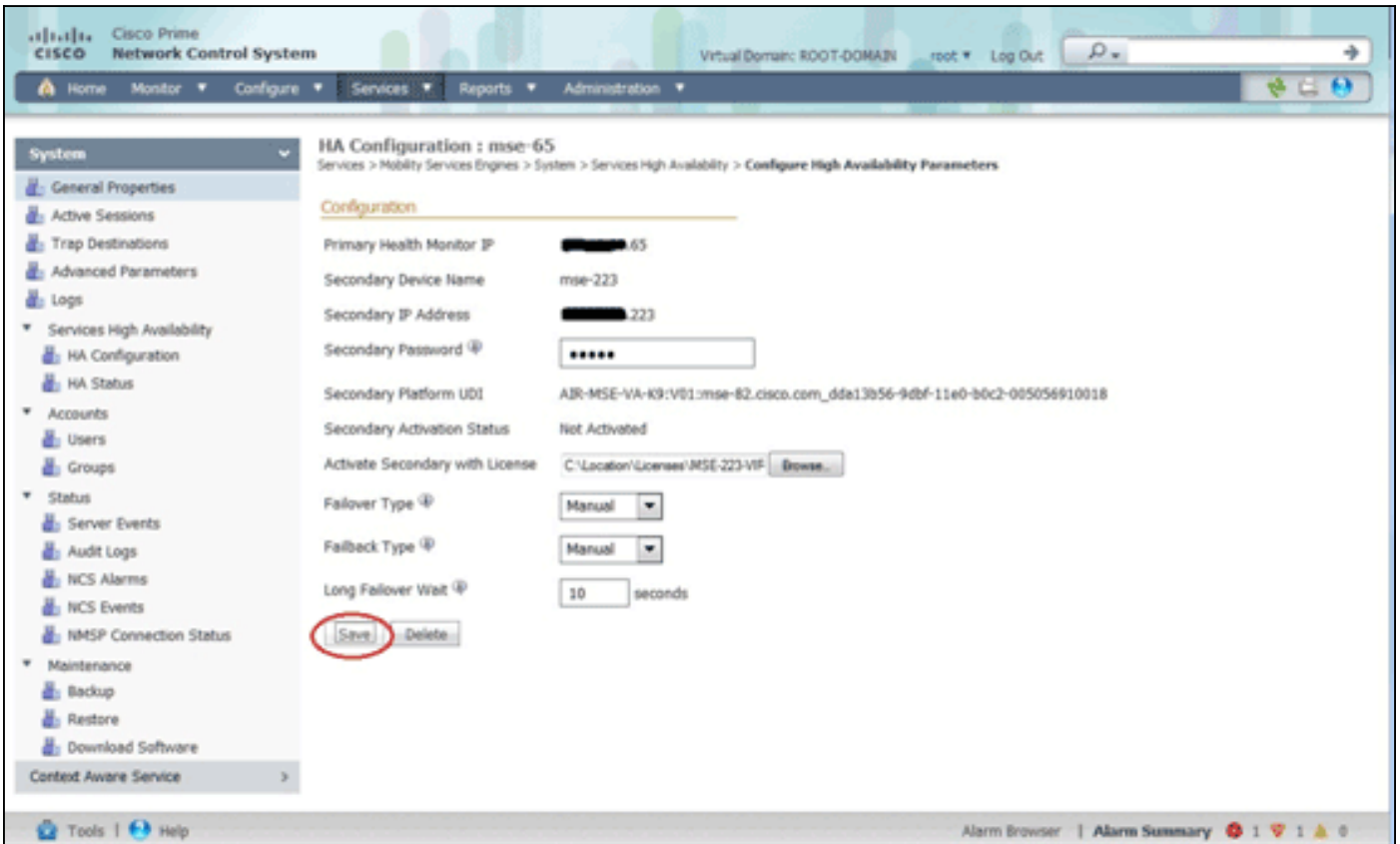
可以通過NCS上的主MSE設定HA配置。



啟用輔助MSE

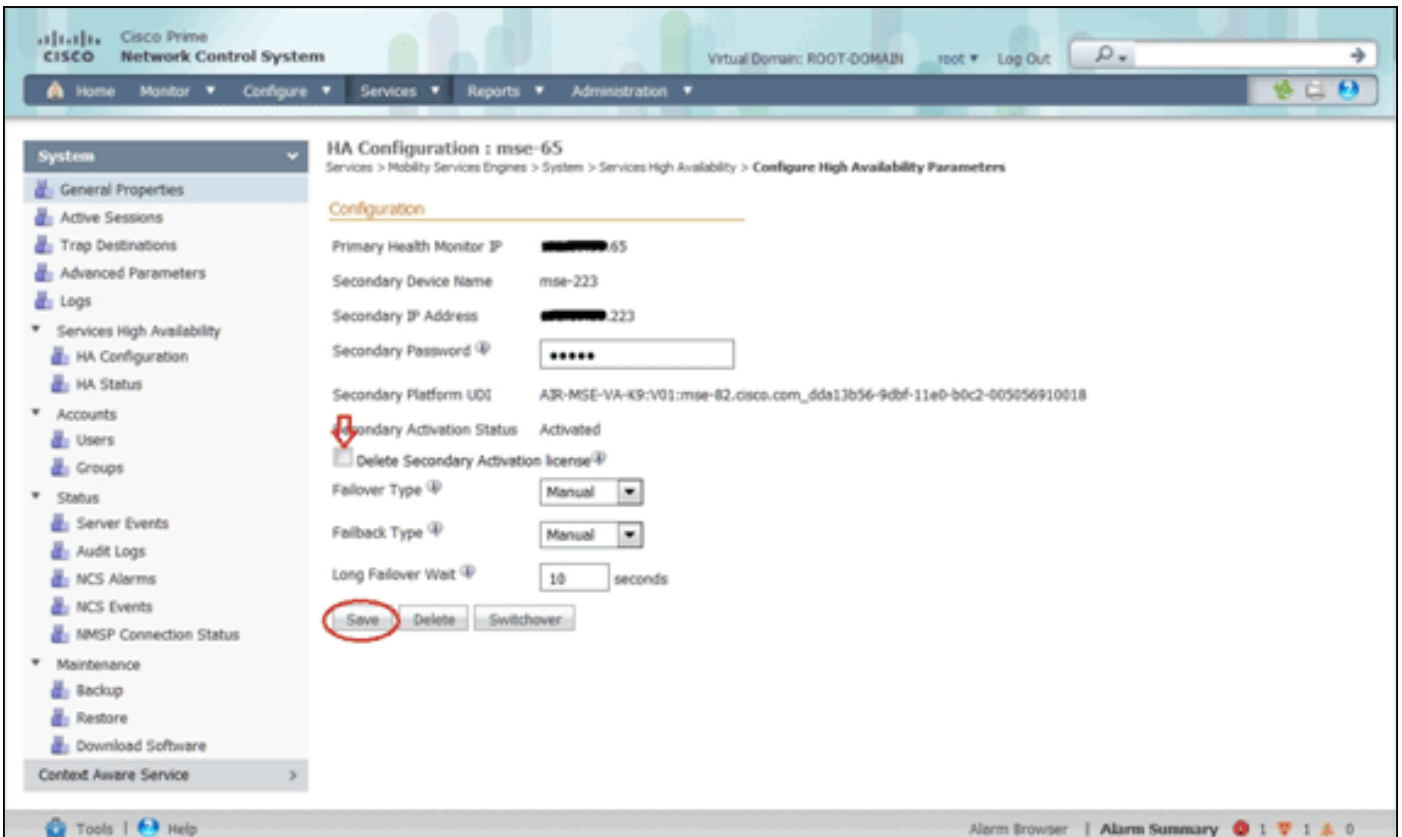
必須啟用輔助裝置。您可以使用UDI資訊請求輔助MSE的啟用許可證。在HA Configuration頁面上

，瀏覽許可證並按一下**Save**。成功啟用輔助MSE後，將設定HA。



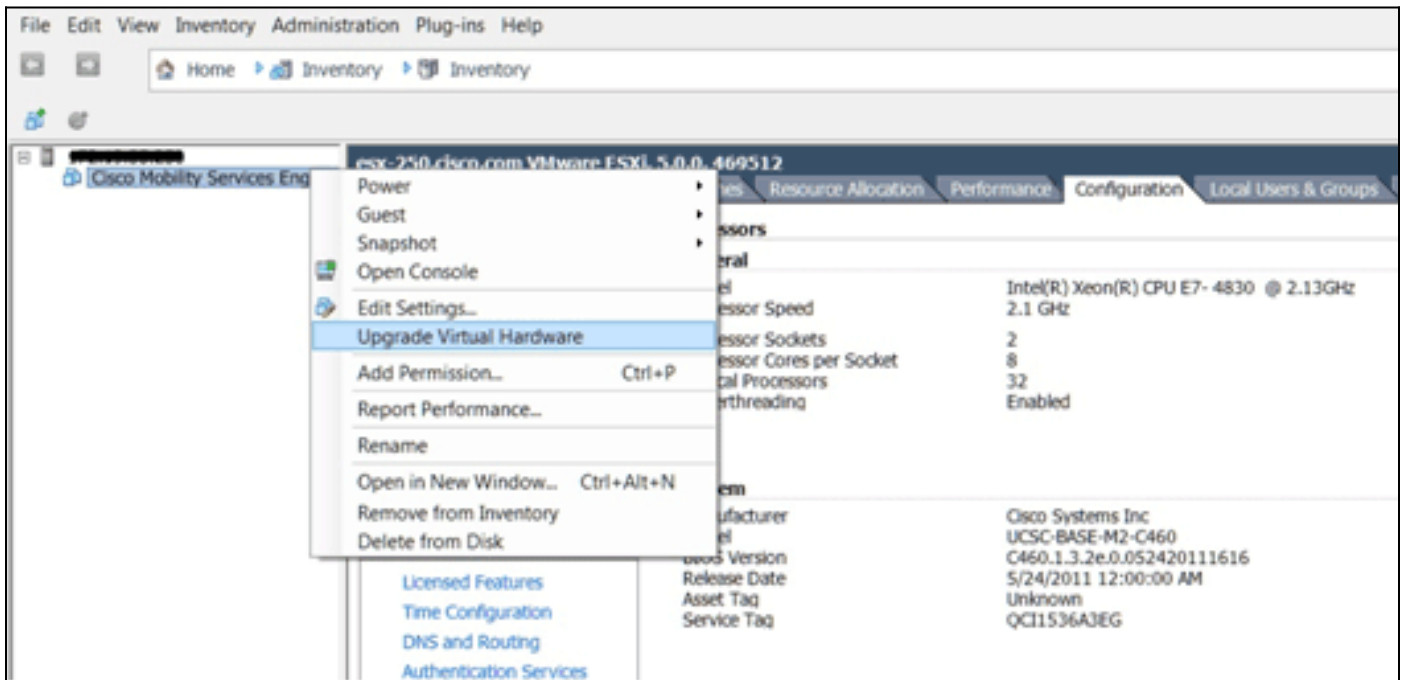
停用輔助MSE

如果需要從輔助MSE刪除啟用許可證，可以按一下覈取方塊，然後按一下**Save**以停用輔助MSE。



ESXi 5.0上的虛擬裝置

在ESXi 5.0上，塊大小固定為1 MB，因為它支援大型虛擬機器部署。為了能夠向虛擬裝置分配八(8)個以上的核心，您必須升級虛擬硬體。若要升級虛擬硬體，請選擇MSE，然後選擇**Upgrade Virtual Hardware**，如下圖所示：



MSE控制檯過程

1. 使用以下憑證登入主控台：root/password。初始啟動時，MSE提示管理員啟動安裝指令碼。
2. 在此提示中輸入yes。

```
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]: _
```

注

意：如果MSE沒有提示進行設定，請輸入以下命令：/opt/mse/setup/setup.sh。

3. 配置主機名
：

```
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. 配置DNS域名

:

```
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. 配置主HA角色

:

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

6. 配置乙太網介面引數

:

```
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. 當系統提示輸入eth1介面引數時，鍵入Skip以繼續執行下一步，因為操作不需要第二個NIC。

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

注意：所配置的地址必須提供IP連線，以連線至此裝置使用的透視WLC和WCS管理系統。

8. 輸入DNS伺服器資訊。只有一個DNS伺服器才能成功解析域，請輸入備份伺服器以實現恢復能力。

```
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. 配置時區。思科建議您使用UTC (協調世界時)。如果紐約的預設時區不適用於您的環境，請瀏覽位置選單以選擇正確的時區。

```
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. 當系統提示配置將來的重新啟動日期和時間，請鍵入Skip。

```
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. 配置遠端系統日誌伺服器 (如果適用)。

```
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. 配置網路時間協定(NTP)或系統時間。NTP是可選的，但可確保您的系統保持準確的系統時間。如果選擇啟用NTP，系統時間將從您選擇的NTP伺服器進行配置。否則，系統將提示您輸入當前日期和時間。

```
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. 當系統提示配置登入標語時，鍵入Skip。

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

14. 啟用本地控制檯根登入。此引數用於啟用/禁用對系統的本地控制檯訪問。應啟用本地控制檯根登入，以便進行本地故障排除。預設值為Skip。

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

15. 啟用安全殼層(SSH)根目錄登入。此引數用於啟用/禁用對系統的遠端控制檯訪問。應啟用SSH根登入，以便進行遠端故障排除。但是，公司安全策略可能要求禁用此選項。

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

16. 配置單使用者模式和口令強度。這些配置引數不是必需的；預設值為Skip。

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

17. 更改根密碼。此步驟對於確保系統安全至關重要。請務必選擇由字母和數字組成的強密碼，且密碼沒有詞典文字。最小密碼長度為8(8)個字元。預設憑據為root/password。

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

18. 配置登入和密碼相關引數

:

```
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. 配置引導密碼(Grub)密碼。(選用)不需要此配置引數。預設值為Skip。

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

20. 配置NCS通訊使用者名稱。

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

21. 接受對配置的更改。

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

此圖顯示完成螢幕的示例

:

```
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 successfullu. Starting framework and services .....
```

22. 執行getserverinfo命令以驗證設定。

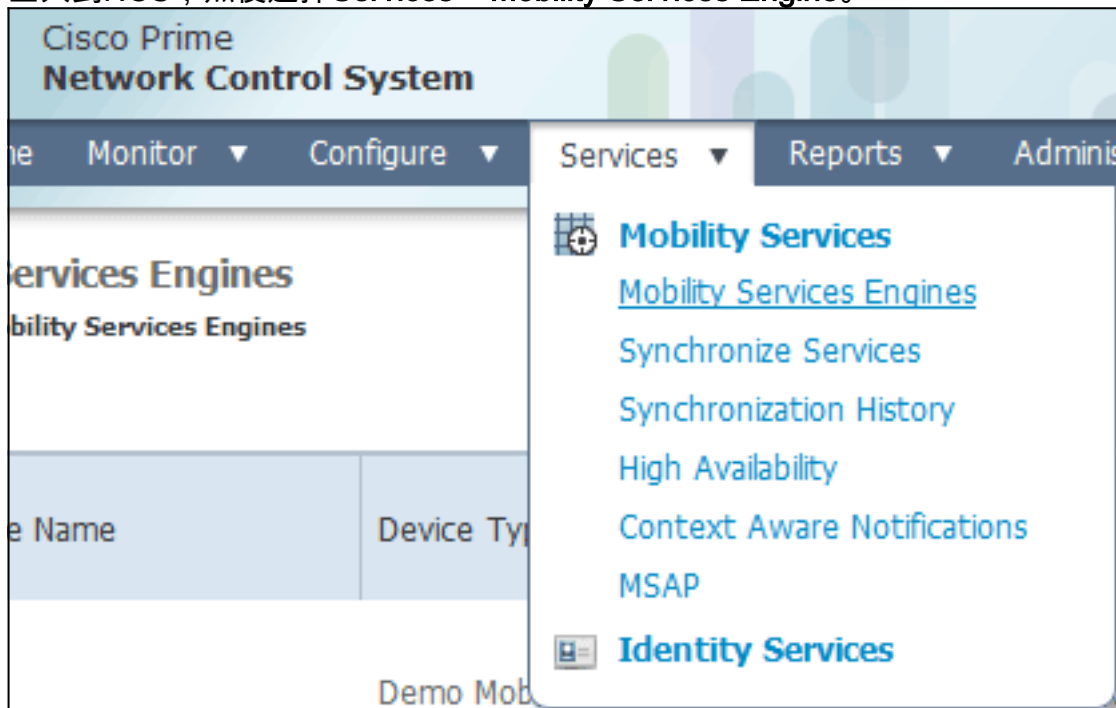
```
Active Wired Clients: 0
Active Elements(Wireless Clients, Rogue APs, Rogue Clients,
Clients, Tags) Limit: 115
Active Sessions: 1
Wireless Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogue APs Not Tracked due to the limiting: 0
Rogue Clients Not Tracked due to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

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

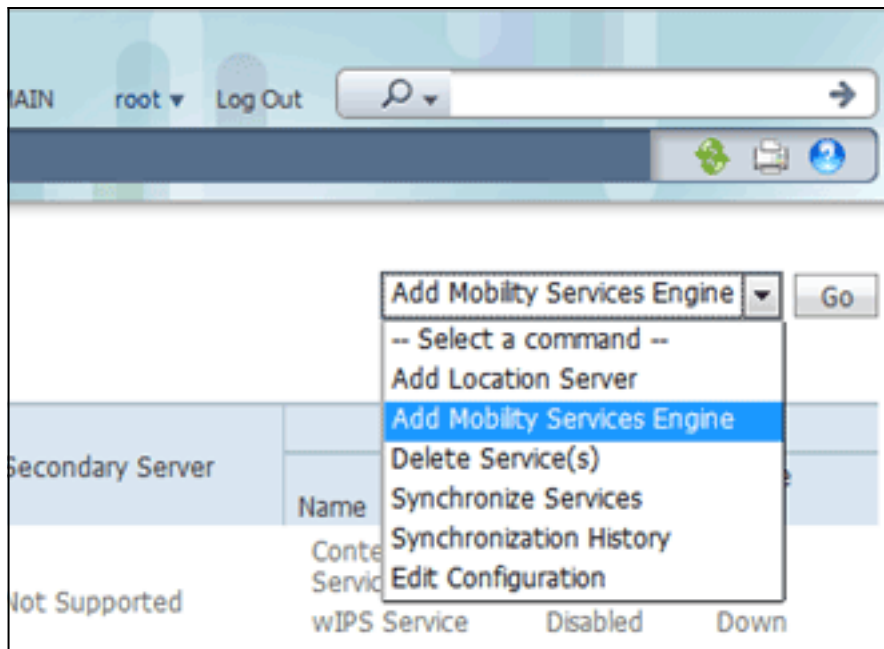
Subservice Name: Aeroscout Tag Engine
Admin Status: Disabled
Operation Status: Down
```

將MSE VA新增到NCS

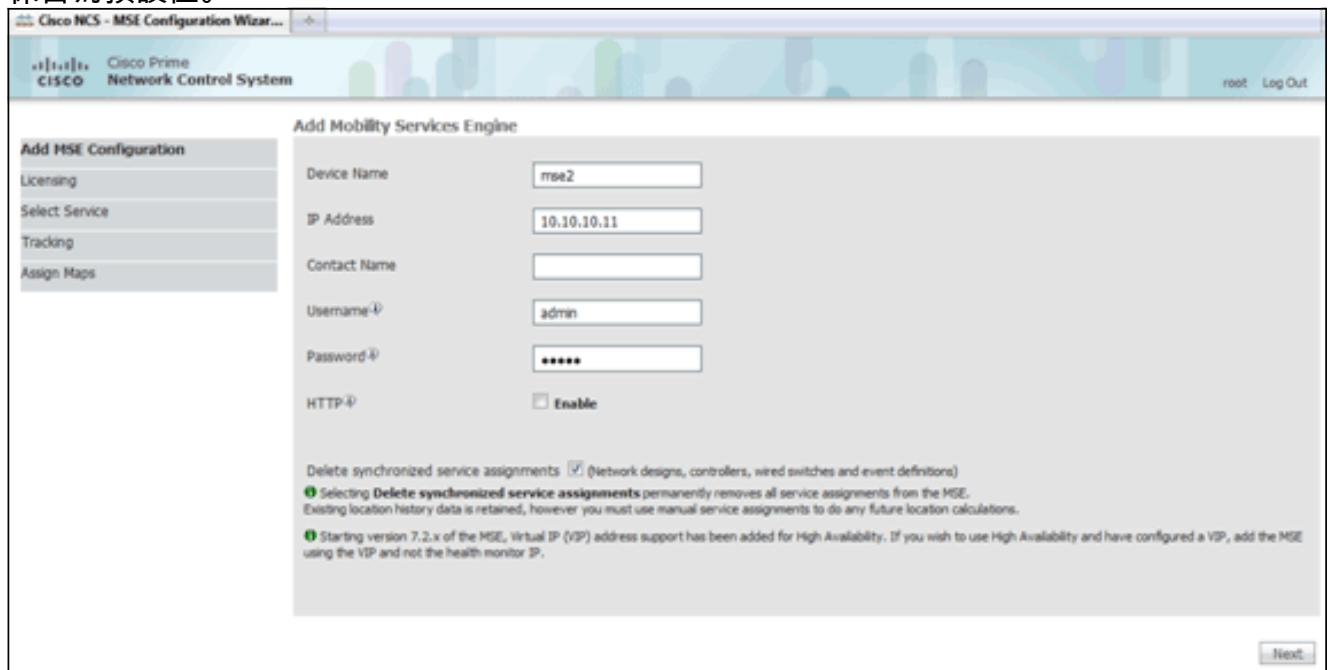
1. 登入到NCS，然後選擇Services > Mobility Services Engine。



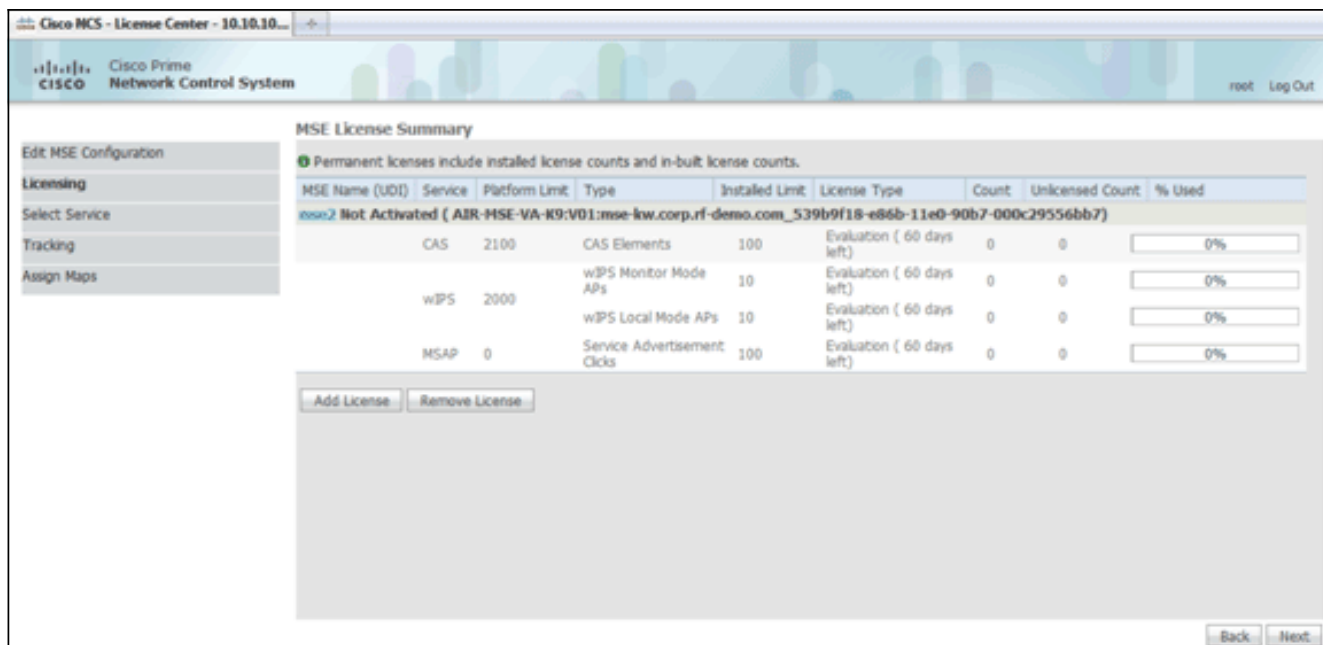
2. 在頁面右側的下拉選單中，選擇Add Mobility Services Engine，然後按一下Go。



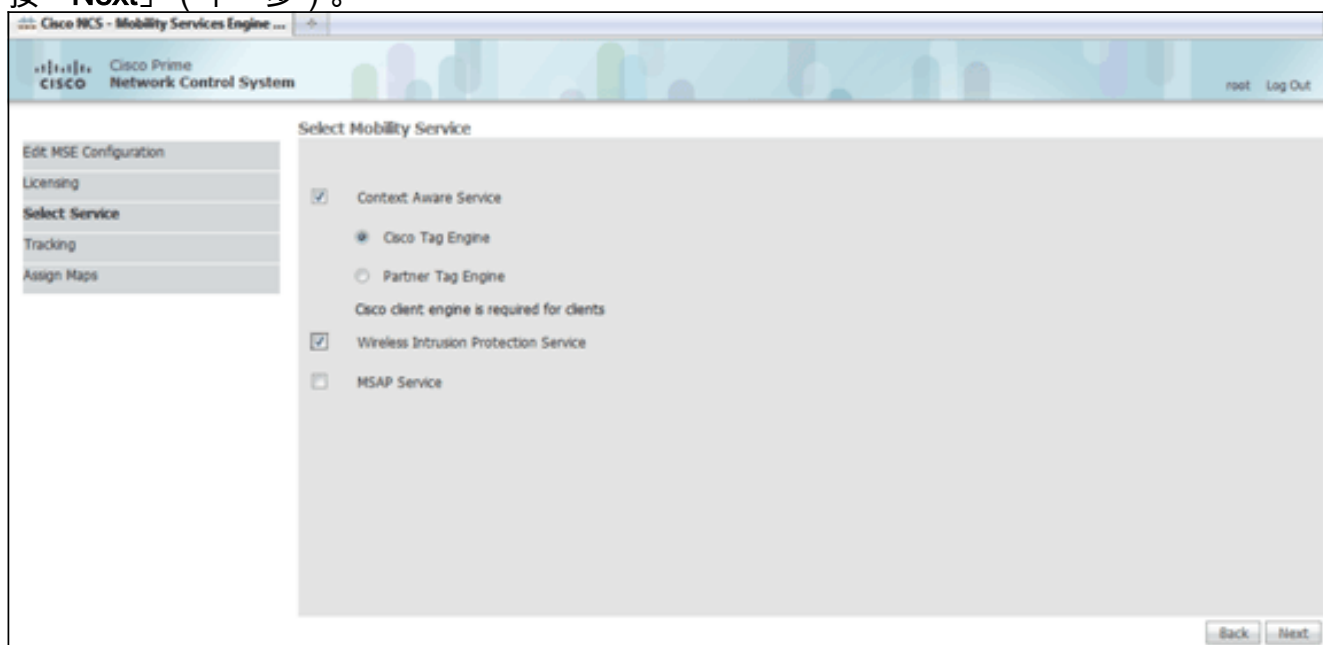
3. 輸入MSE的唯一裝置名稱、之前在MSE設定期間配置的IP地址、支援聯絡人的姓名。以及MSE設定期間配置的NCS使用者名稱和密碼。請勿將使用者名稱從預設值`admin`變更。您可以保留為預設值。



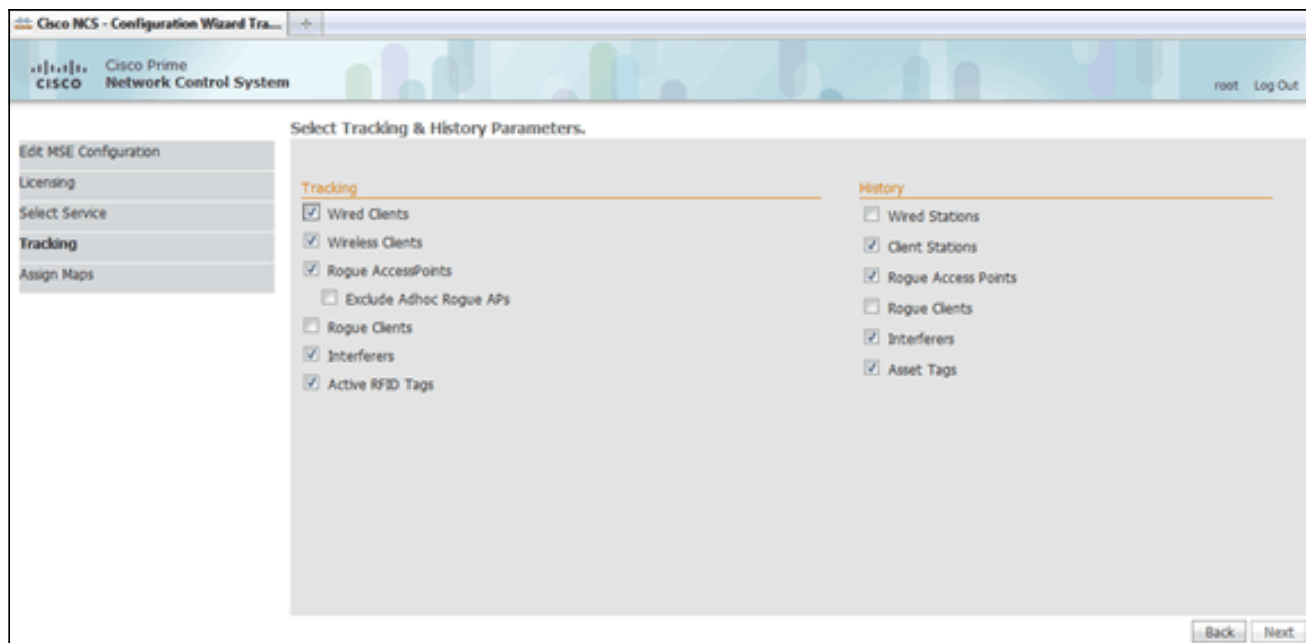
4. 按「Next」（下一步）。
5. 按一下**Licensing**，然後驗證許可。安裝時，預設演示許可證足以進行測試。您可以在「許可」頁面上新增更多購買的許可證或刪除許可證。



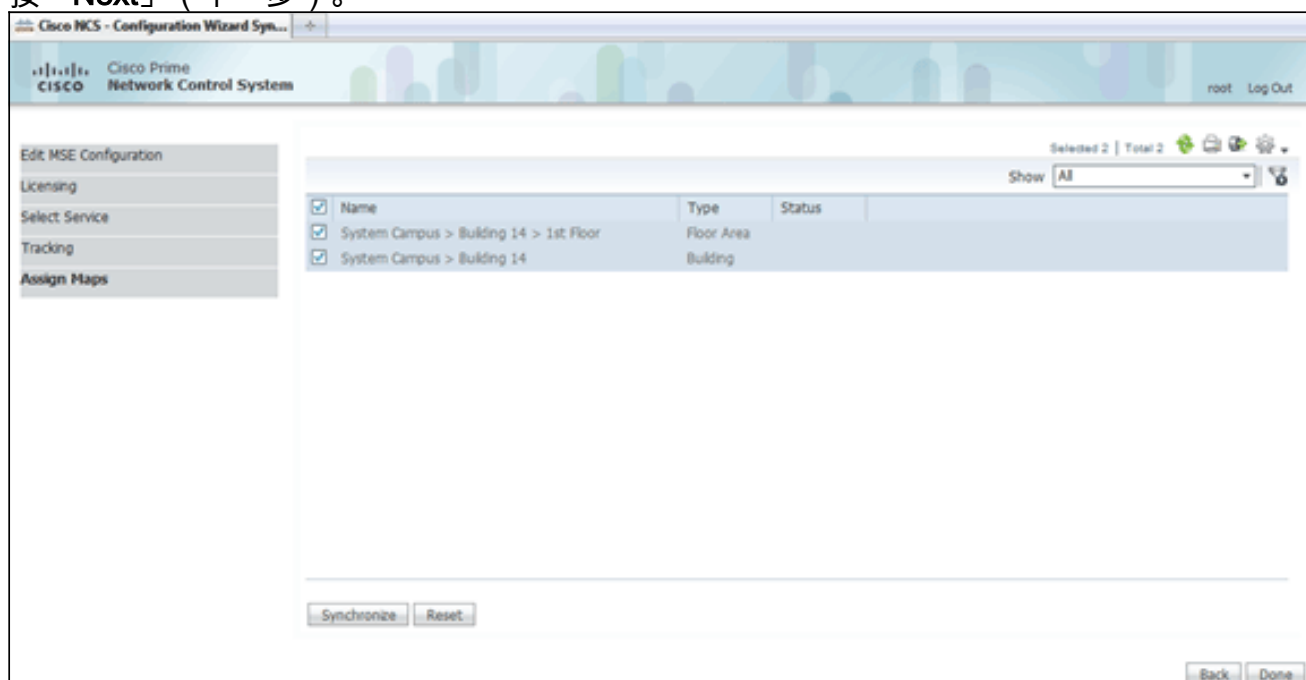
6. 按「Next」（下一步）。



7. 在「選擇移動服務」頁面上，按一下**Cisco Tag Engine**（自7.0MR以來可用）單選按鈕（用於客戶端和RFID標籤支援），或按一下**Partner Tag Engine**單選按鈕（用於Aeroscout等）。
8. 按一下**Wireless Intrusion Protection Service**覈取方塊以測試監控模式和增強本地模式功能的WIPS安全功能。
9. 按「Next」（下一步）。
10. 選中要啟用跟蹤的元素以及那些可用於歷史報告的元素的歷史引數的覈取方塊。



11. 按「Next」（下一步）。



12. 選中現有建築和樓層的覈取方塊，然後按一下**Synchronize**。同步後，Status列將更新以顯示初始網路設計已同步。

<input type="checkbox"/>	Name	Type	Status
<input checked="" type="checkbox"/>	System Campus > Building 14 > 1st Floor	Floor Area	
<input checked="" type="checkbox"/>	System Campus > Building 14	Building	

Synchronize Reset

13. 同步完成後，按一下**完成**。此時將出現一個對話方塊，說明已儲存MSE設定。

The screenshot shows the Cisco Prime Network Control System interface. A dialog box is displayed in the center with the following text:

The page at https://10.10.10.20 says:
 Your MSE Settings have been saved.
 OK

The background interface shows a table with the following data:

<input type="checkbox"/>	Name	Type	Status
<input checked="" type="checkbox"/>	System Campus > Building 14 > 1st Floor	Floor Area	
<input checked="" type="checkbox"/>	System Campus >		

Buttons at the bottom of the interface include Synchronize, Reset, Back, and Done.

14. 在NCS的MSE首頁上確認配置。

Cisco Prime Network Control System

Virtual Domain: ROOT-OCMAN root Log Out

Home Monitor Configure Services Reports Administration

Mobility Services Engines

Services > Mobility Services Engines

Device Name	Device Type	IP Address	Version	Reachability Status	Secondary Server	Mobility Service		
						Name	Admin Status	Service Status
<input checked="" type="checkbox"/> mse2	Cisco Mobility Services Engine - Virtual Appliance	10.10.10.11	7.2.1.12	Reachable	N/A (Click here to configure)	Context Aware Service	Enabled	Up
						wPS Service	Enabled	Up
						MSAP Service	Disabled	Down

確保同步其餘的網路設計、控制器、有線交換機和事件組（如果可用）。**注意：**Cisco環境感知服務高度依賴於WLC、NCS和MSE之間的同步時鐘。如果這三個系統均未指向同一NTP伺服器並使用相同的時區設定進行配置，則情景感知服務將無法正常運行。在嘗試任何故障排除步驟之前，請確保情景感知系統所有元件的系統時鐘相同。

- 檢查所選服務的MSE和控制器通訊。確認MSE僅與所選服務的每個控制器進行通訊；網路移動服務協定(NMSP)狀態必須為活動。此映像提供未將keyhash新增到WLC的範例。

Cisco Prime Network Control System

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

在WLC主控台上，使用show auth-list指令。以下示例從WLC控制檯顯示沒有可用的位置伺服器

```
(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
```

若要手動新增MSE並建立到WLC的NMSP連線，請完成以下步驟：在MSE控制檯上，運行cmdshell命令，然後運行show server-auth-info命令。此範例顯示用於新增到WLC的MAC位址和金鑰雜湊。

```

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

```

運行

config auth-list add ssc <mac address> <MSE keyhash>命令，然後運行show auth-list。此範例顯示MSE已新增到WLC (手動)。

```
(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

```

在NCS上，確認NMSP連線顯示Active。

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						

命令列參考

WLC命令

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

MSE命令

運行此命令可確定MSE服務的狀態：

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

運行此命令可啟動用於客戶端跟蹤的情景感知引擎：

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

運行此命令以確定用於客戶端跟蹤的情景感知引擎的狀態：

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

運行此命令可停止用於客戶端跟蹤的情景感知引擎：

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

運行此命令可執行診斷：

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

注意：rundiag命令還可用於檢視獲取客戶端環境感知引擎的許可證檔案所需的MSE UDI資訊。

相關資訊

- [MSE配置指南（虛擬和物理裝置）](#)
- [MSE高可用性配置](#)

- [Cisco WIPS部署指南](#)
- [產品訂購](#)
- [技術支援與文件 - Cisco Systems](#)