Guida alla configurazione e alla distribuzione dell'appliance virtuale di MSE release 7.2

Sommario

Introduzione

Il software Cisco Mobility Services Engine (MSE) versione 7.2 aggiunge l'appliance virtuale e il supporto per VMware ESXi. In questo documento vengono fornite linee guida per la configurazione e l'installazione, oltre a suggerimenti per la risoluzione dei problemi, per gli utenti che aggiungono l'appliance virtuale MSE a una WLAN unificata Cisco e che eseguono Servizi compatibili con il contesto e/o Cisco Adaptive Wireless Intrusion Prevention System (wIPS). In questo documento vengono inoltre descritti i requisiti di sistema per l'appliance virtuale MSE e

vengono fornite linee guida generali per la distribuzione dell'appliance. Questo documento non fornisce i dettagli di configurazione per MSE e i componenti associati. Queste informazioni sono fornite in altri documenti; vengono forniti riferimenti.

Fare riferimento alla sezione Informazioni correlate per un elenco di documenti sulla configurazione e la progettazione dei servizi di mobilità con riconoscimento del contesto. Nel presente documento, inoltre, non viene descritta la configurazione degli IPS adattivi.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco serie 3300 Mobility Services Engine.

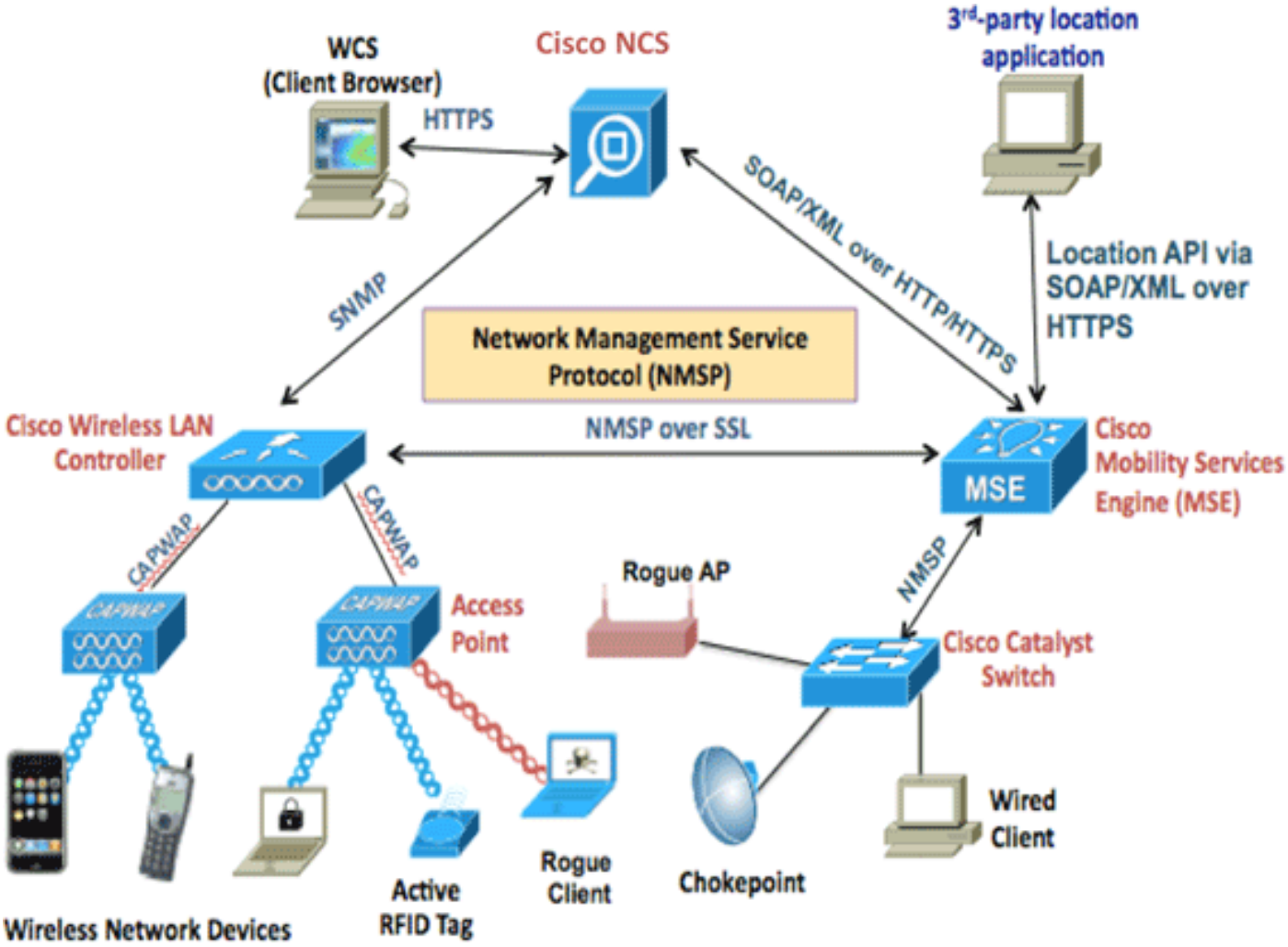
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Questa immagine mostra la tipica implementazione di Cisco WLAN che include Cisco Mobility Services Engine (MSE). L'installazione include anche altri client di rete cablati/wireless, tag RFID, punti di accesso non autorizzati e client. MSE fornisce visibilità a questi elementi sia per la posizione che per wIPS. Prima della versione 7.2 del software MSE, solo gli accessori fisici erano limitati a MSE-3310 e MSE-3350/3355.



Requisiti di sistema

Il software MSE release 7.2 Virtual Appliance è supportato e testato su VMware ESXi 4.1 e versioni successive. Queste configurazioni server sono state testate e sono consigliate come linee guida.

- Server rack Cisco Unified Computing System (UCS) C200 M2Due (2) processori Intel? Xeon? CPU E5506 a 2,13 GHzRAM (secondo il livello configurato)Unità SAS con controller RAID avanzati (almeno 500 GB+)
- Server rack UCS C210 M2Due (2) CPU Intel Xeon E5640 a 2,67 GHzRAM (secondo il livello configurato)Unità SAS con controller RAID avanzati (almeno 500 GB+)
- Server rack UCS C250 M2Due (2) CPU Intel Xeon E5570 a 2,93 GHzRAM (secondo il livello configurato)Unità SAS con controller RAID avanzati (almeno 500 GB+)
- Server rack UCS C460 M2Due (2) CPU Intel Xeon E7-4830 a 2,13 GHzRAM (secondo il livello configurato)Unità SAS con controller RAID avanzati (almeno 500 GB+)

Nota: Utilizza due (2) processori quad-core della stessa potenza di quelli sopra menzionati.

Software di gestione e licenze VMware

L'appliance virtuale Cisco MSE versione 7.2 supporta ESX/ESXi 4.x e versioni successive.

Per gestire gli host ESXi e configurare e installare le appliance virtuali, Cisco consiglia di installare

vCenter Server 4.x su un computer Windows XP o Windows 7 a 64 bit e di ottenere una licenza vCenter Enterprise. In alternativa, se si dispone di un solo host ESXi, è possibile utilizzare il client vSphere per gestirlo.

Fabbisogni di risorse

I requisiti delle risorse dipendono dalla licenza che si desidera distribuire. Nella tabella seguente vengono elencati i diversi livelli in base ai quali è possibile configurare il dispositivo virtuale:

MSE primario	Risorse		Licenza supportata (singolarmente)	
Livello Virtual Appliance	Memoria totale	CPU	Licenza CAS	Licenza wIPS
Bassa	6 G	2	2000	2000
Standard	11 G	8	18000	5000
Alta	20 G	16	50000	10000

Nota: i limiti consigliati elencati per le licenze CAS e wIPS sono limiti massimi supportati quando è in esecuzione un solo servizio. Se si desidera eseguire entrambi i servizi sullo stesso accessorio, è necessario rispettare i limiti di coesistenza.

Configurazione dell'host ESXi

Completare questa procedura per configurare un dispositivo virtuale MSE su un server UCS o simile:

1. Verificare che il computer disponga di almeno 500 GB di spazio su disco rigido e di unità SAS veloci con controller RAID avanzati. (utilizzare una dimensione di blocco di almeno 4 MB quando si creano archivi dati per versioni precedenti a ESXi 5.0).
2. Installare ESXi.Inserire il disco di installazione ESXi 4.1 o versione successiva e avviare il sistema dall'unità.Se si utilizzano più unità, installare ESXi nell'unità configurata come unità di avvio. Il nome utente predefinito è root e la password è vuota (nessuna password).**Nota:** se scegli l'unità sbagliata per l'installazione, puoi riformattarla usando un CD Fedora Live.
3. Configurare l'indirizzo IP.Scegliere le schede di rete abilitate e attive. Se l'host è connesso a più reti, potrebbero essere disponibili più schede di rete. È possibile impostare lo stesso indirizzo IP durante l'installazione di CIMC. premere F8 durante l'avvio per impostare l'indirizzo IP. Inoltre, modificare la password predefinita.

Una volta configurato ESXi, è possibile utilizzare un computer Windows XP o Windows 7, insieme all'indirizzo IP e alle credenziali di accesso configurate in precedenza, per connettersi all'host ESXi tramite il client vSphere.

Per informazioni sulla licenza dell'host ESXi, fare riferimento a Licensing ESX 4.x, ESXi 4.x e vCenter Server 4.x .

Per informazioni su come configurare gli archivi dati su ESXi, consultare i seguenti articoli:

- Creazione di archivi dati VMFS

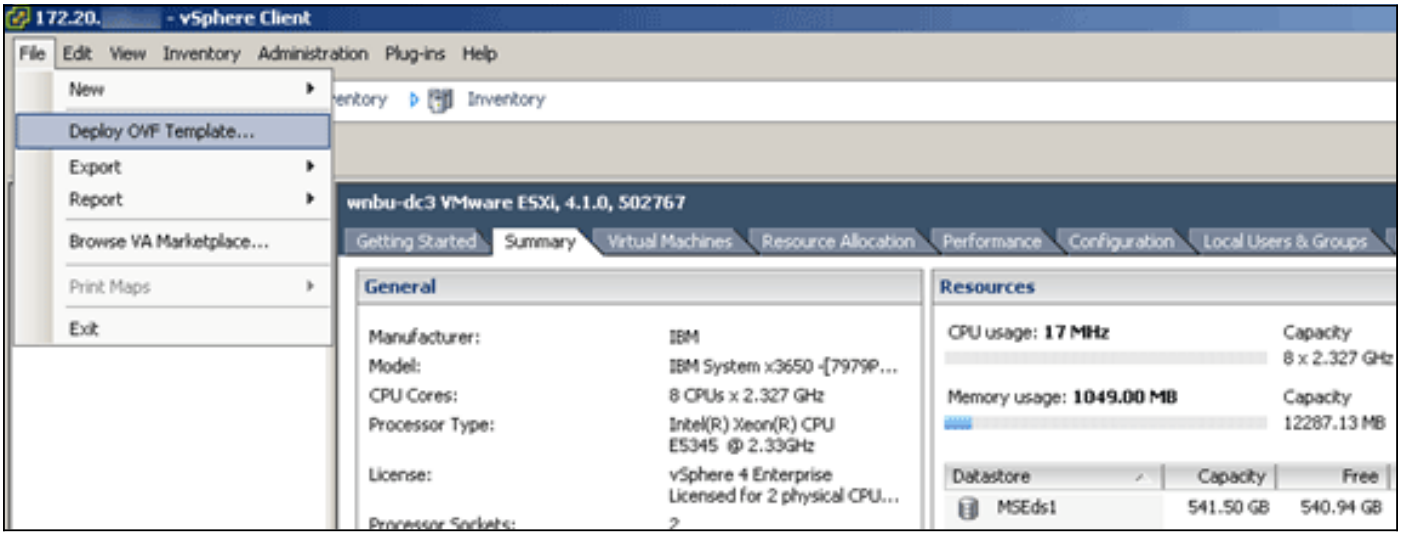
- Aumento degli archivi dati VMFS

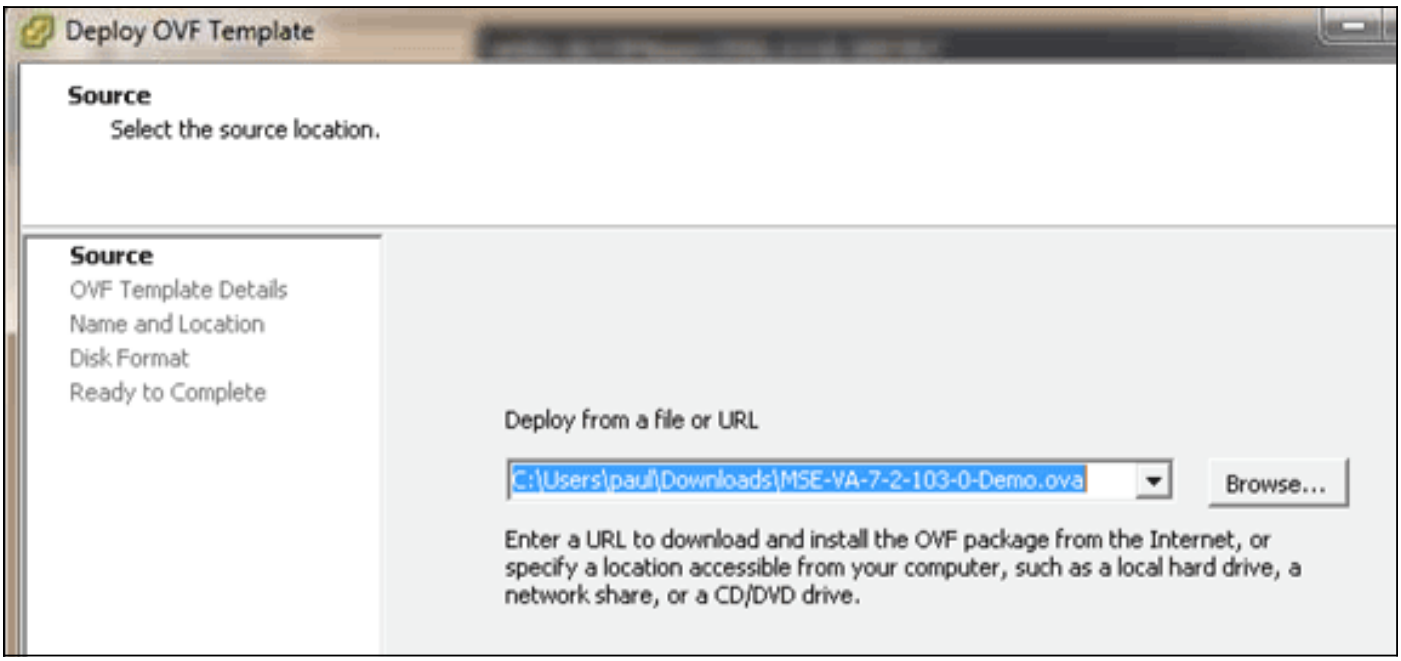
Avviso: Quando si creano gli archivi dati per ESXi 4.1, utilizzare una dimensione di blocco di almeno 4 MB.

Installazione di MSE Virtual Appliance

L'appliance virtuale MSE viene distribuita come immagine OVA (Open Virtual Appliance) che può essere distribuita su un host ESXi utilizzando il client vSphere. Sono disponibili due versioni OVA: una versione è per un'immagine demo, che richiede solo 60 GB di spazio su disco, mentre l'altra versione è un'immagine di produzione generica.

L'immagine di produzione distribuibile presuppone almeno 500 GB di spazio disponibile su disco nell'archivio dati dell'host ESXi. Gli OVA possono essere selezionati e distribuiti tramite il client vSphere. Per distribuire il modello, scegliete **File > Distribuisci modello OVF**.



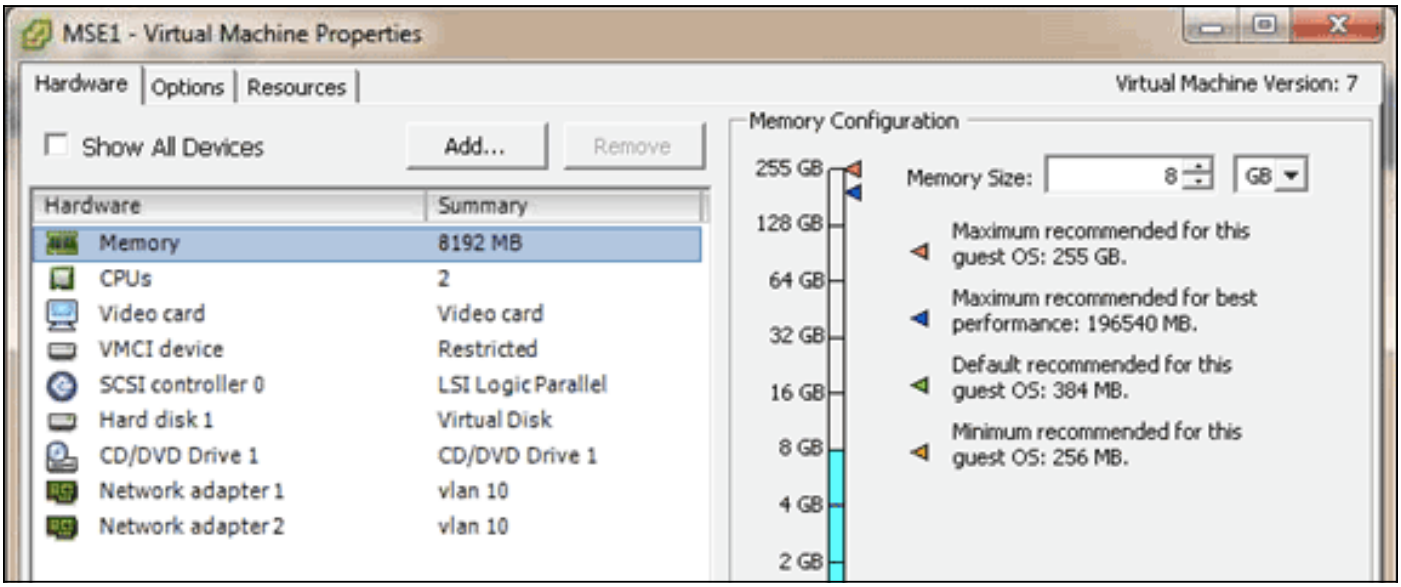


L'installazione dell'immagine richiede alcuni minuti a seconda della velocità della rete. Una volta installato, è possibile modificare la configurazione della macchina virtuale (VM) per configurare l'accessorio; la VM deve essere spenta quando configurata.

Configurazione dei livelli di MSE Virtual Appliance

Nella tabella riportata in questa sezione sono elencati i livelli configurabili nell'accessorio virtuale e i requisiti delle risorse corrispondenti. Assegnare core dedicati all'accessorio e non ai core virtuali iperthreaded, in quanto influisce sulle prestazioni se si presume che l'host abbia più core virtuali e si installano più accessori. Ad esempio, nell'UCS C200 menzionato in precedenza, sono disponibili otto (8) core fisici, ma sedici (16) core virtuali con hyper-threading. non presumere che siano disponibili sedici (16) core; allocare solo otto (8) core in modo da garantire prestazioni MSE affidabili in caso di stress.

MSE primario	**Risorse**	**Licenza supportata (singolarmente)**		**MSE secondario supportato**	
Livello Virtual Appliance	**Memoria totale**	**Licenza CAS**	**Licenza wIPS**	**Appliance virtuale**	**Scatola fisica**
Bassa	6 G	2000	2000	Basso+	Non supportato
Standard	11 G	18000	5000	Standard+	
Alta	20 G	50000	10000	Alta+	



Configurazione di MSE Virtual Appliance

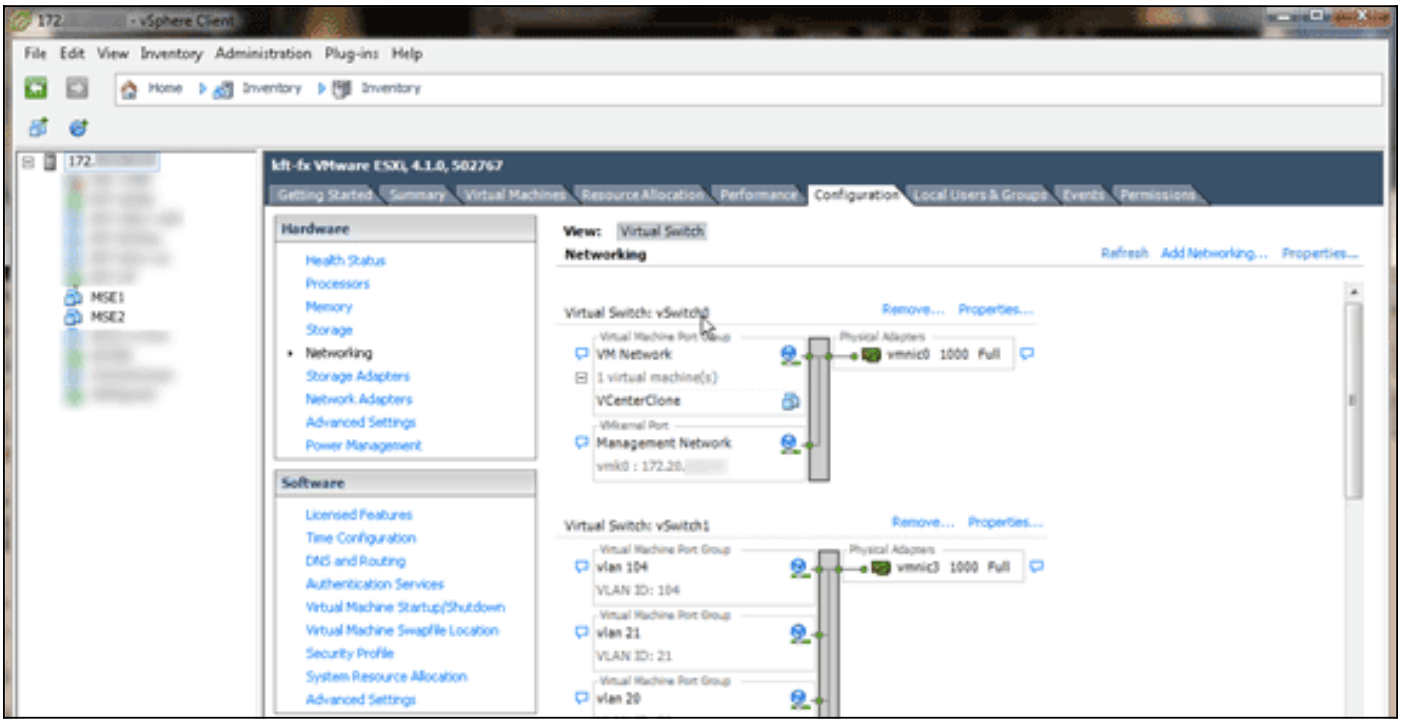
Una volta installato e configurato il dispositivo virtuale, è possibile accenderlo. Quando l'accessorio viene acceso per la prima volta, è necessario immettere le credenziali di accesso predefinite: root/password.

Al primo accesso, l'accessorio avvia la configurazione del software MSE e installa il database Oracle. Si tratta di un processo che richiede una sola volta e molto tempo, e che richiede almeno 30-40 minuti. Al termine dell'installazione, viene nuovamente visualizzata la richiesta di accesso. Per continuare a configurare l'accessorio, consultare la sezione Configurazione dei servizi di mobilità Engine della *Guida introduttiva a Cisco 3355 Mobility Services Engine*.

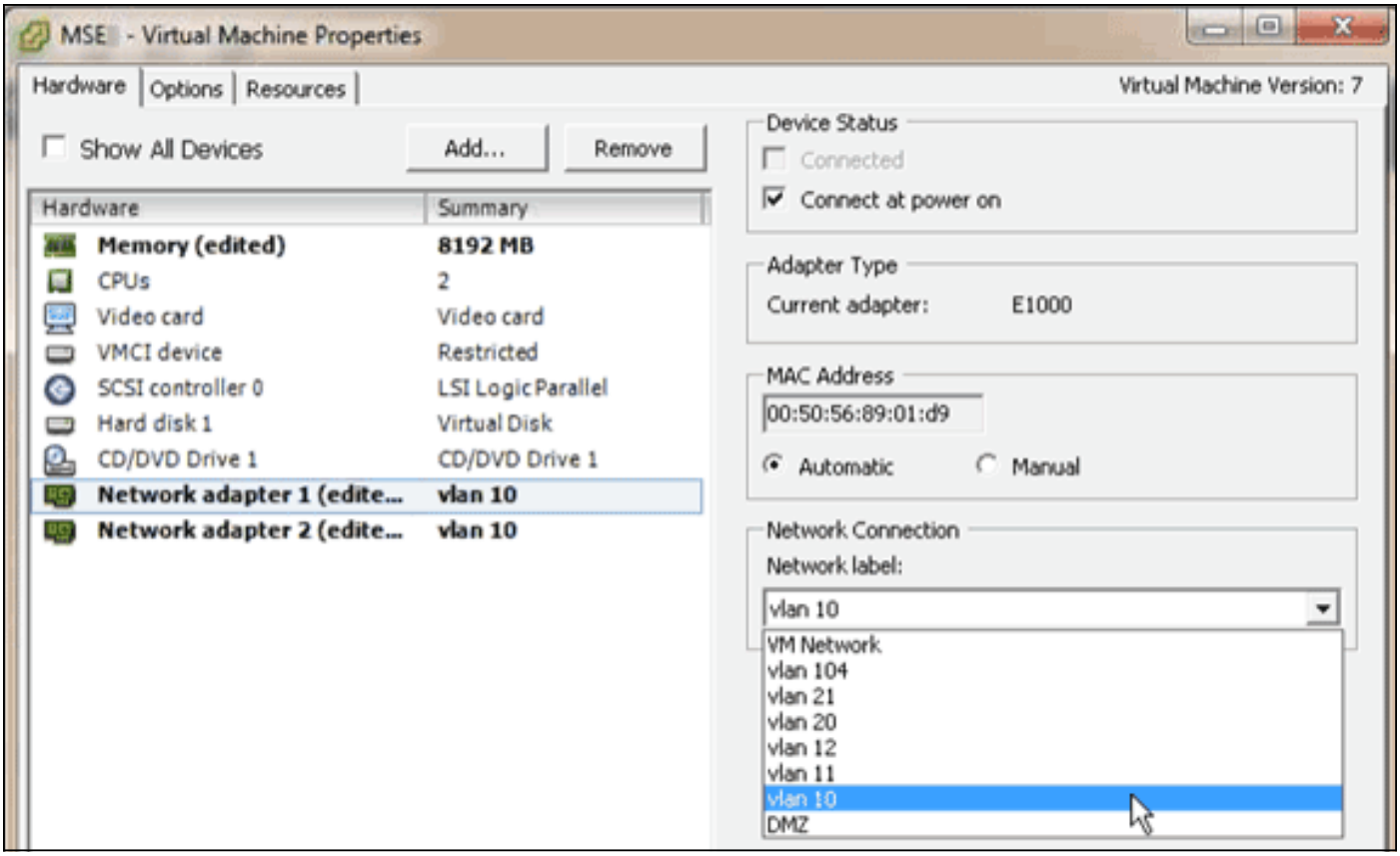
Configurazione della rete

Per impostazione predefinita, le VM utilizzano le impostazioni di rete dell'host; pertanto, non è necessario configurare le schede VM su ESXi. Tuttavia, se all'host sono connesse sia reti pubbliche che private e si desidera che le VM abbiano accesso a entrambe, è possibile configurare le schede di rete VM nel client vSphere.

Nel client vSphere, selezionare l'host, fare clic sulla scheda **Configurazione**, quindi fare clic su **Rete**. È possibile visualizzare le schede fisiche nelle proprietà del commutatore virtuale.



Per isolare le reti, creare switch separati con schede separate. Quindi, è possibile assegnare le schede VM a queste reti in base alle esigenze.



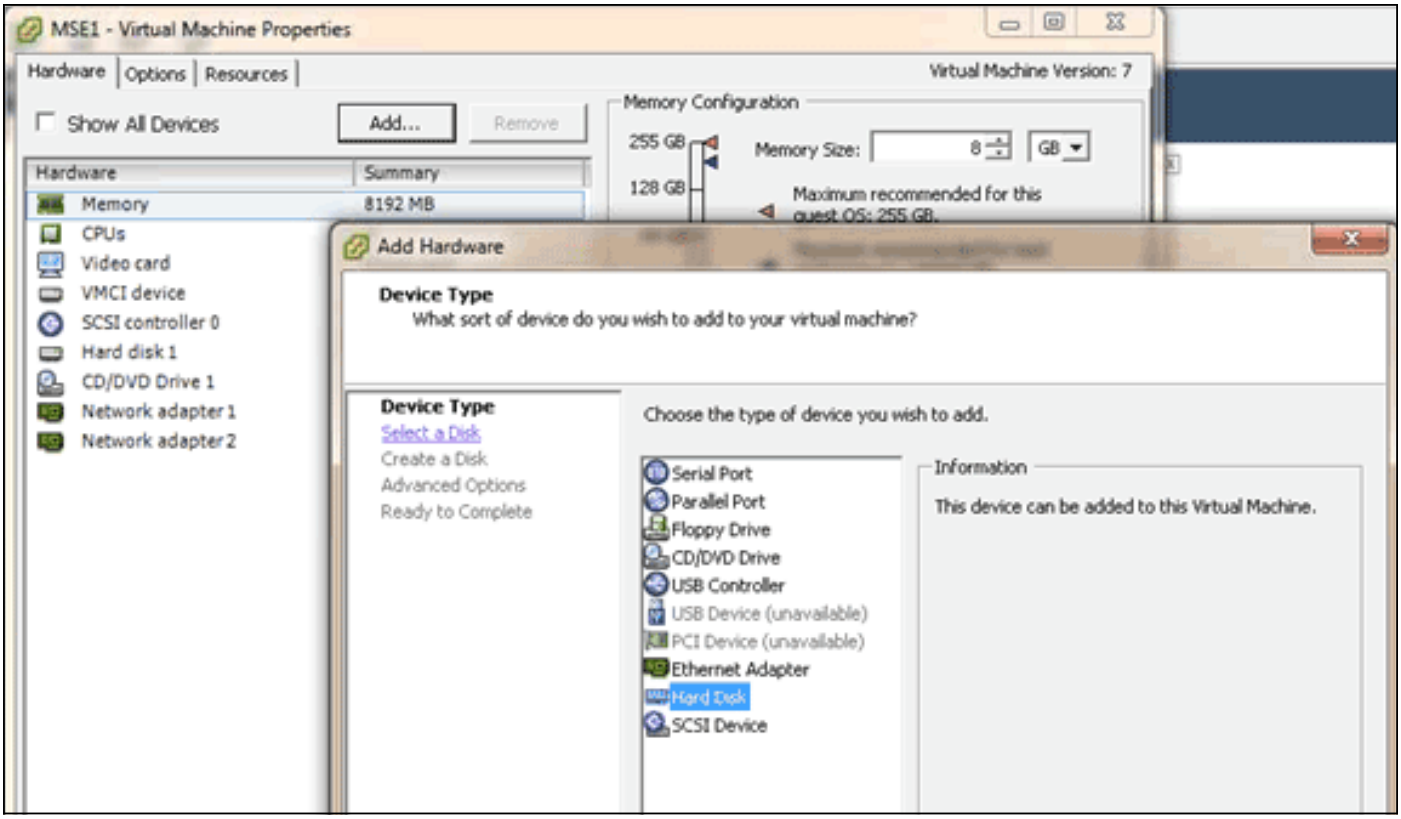
Aggiunta di spazio su disco rigido

Se necessario, aggiungere ulteriore capacità del disco alla VM ed espandere le partizioni.

Nota: lo script installDrive.sh (che si trova nella directory /opt/mse/framework/bin) rileva nuove unità e ripartisce le partizioni esistenti in modo da utilizzare ed estendere le nuove unità.

Prima di ripartizionare lo spazio su disco, verificare di eseguire il backup della macchina virtuale o almeno dei dati MSE.

Per aggiungere ulteriore spazio su disco alla macchina virtuale, arrestare la macchina virtuale, passare alle impostazioni della macchina virtuale e aggiungere il disco rigido aggiuntivo.

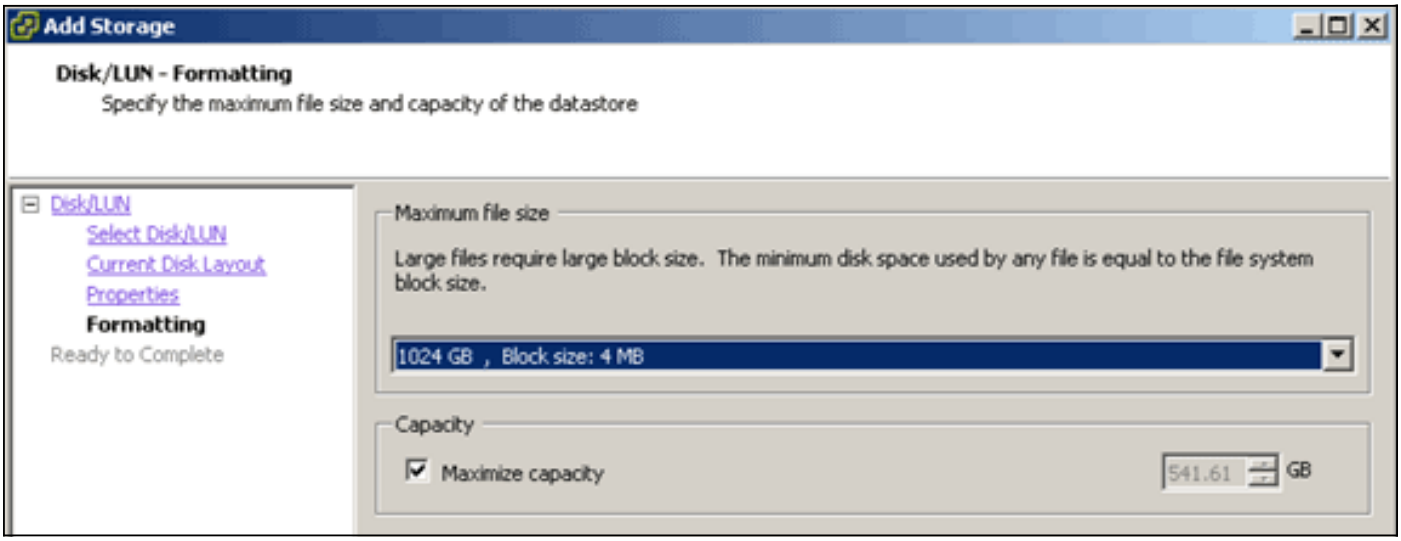


Una volta aggiunto il disco rigido, accendere la VM, accedere all'accessorio ed eseguire lo script installDrive.sh. Lo script deve montare e ripartizionare l'unità appena aggiunta. Se sono stati aggiunti più dischi rigidi, eseguire lo script una volta per ogni nuova unità.

Dimensione blocco

Per le versioni ESXi precedenti alla 5.0, Cisco consiglia di assegnare all'archivio dati sull'host una dimensione di blocco pari o superiore a 4 MB; in caso contrario, la distribuzione dell'OVA potrebbe non riuscire. Se la distribuzione non riesce, è possibile riconfigurare le dimensioni del blocco.

Per riconfigurare le dimensioni del blocco, selezionare ESX host Configuration > Storage > Delete the datastores, quindi aggiungere nuovamente lo storage ai nuovi datastore con una dimensione del blocco di almeno 4 MB.



Strumenti VMware

Se la VM genera il seguente errore, fare clic con il pulsante destro del mouse sulla VM nel client vSphere e scegliere **Guest > Install/Upgrade VMware Tools** per installare o aggiornare gli strumenti VMware:

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

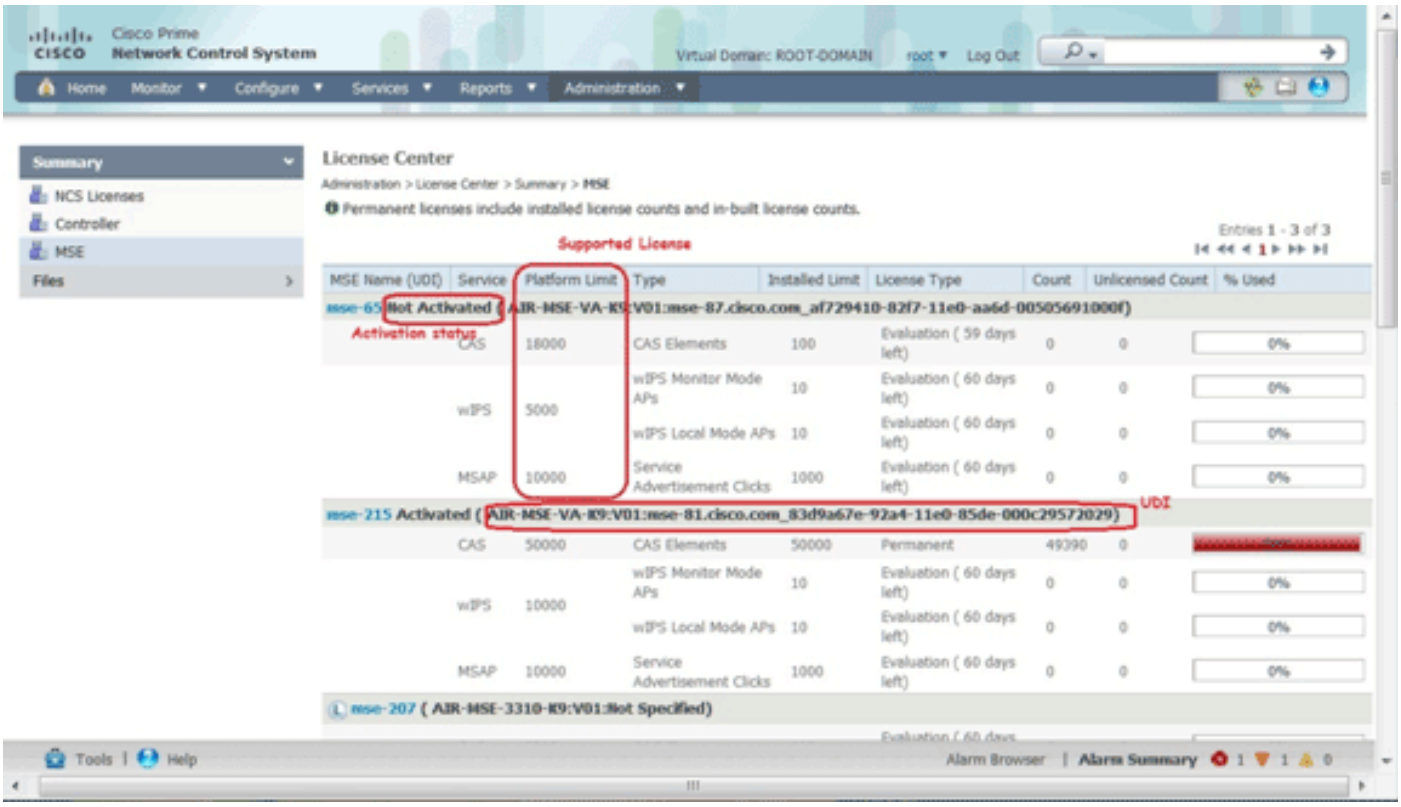
Aggiornamento dell'appliance virtuale

Una volta configurata, l'appliance virtuale deve essere trattata come una scatola MSE fisica. Non è necessario distribuire un nuovo OAV ogni volta che si desidera eseguire l'aggiornamento all'ultima versione di MSE; è possibile scaricare sull'accessorio l'immagine del programma di installazione appropriata e seguire le istruzioni per l'aggiornamento, come per un accessorio fisico.

Licenze per l'appliance virtuale

Una volta configurato, il dispositivo virtuale può essere utilizzato nella modalità di valutazione (predefinita 60 giorni) senza richiedere una licenza per l'accessorio. Tuttavia, se si prevede di implementare licenze permanenti o di utilizzare funzionalità quali High Availability (HA), è necessario attivare il dispositivo virtuale utilizzando una licenza di attivazione del dispositivo virtuale. È possibile ottenere l'UDI (Unique Device Identifier) dall'appliance virtuale (eseguire **show csludi** sull'appliance) o dalle proprietà generali di Cisco Prime Network Control System (NCS) MSE e utilizzare queste informazioni per acquistare la licenza di attivazione dell'appliance virtuale e le licenze di servizio permanenti.

Nell'immagine sono illustrate le modifiche recenti apportate all'interfaccia utente del centro licenze per l'appliance virtuale.



Per il dispositivo virtuale, un messaggio accanto al nome MSE indica chiaramente se è attivato o meno. Sono inoltre disponibili due colonne limite: Nella colonna Limite piattaforma è indicata la

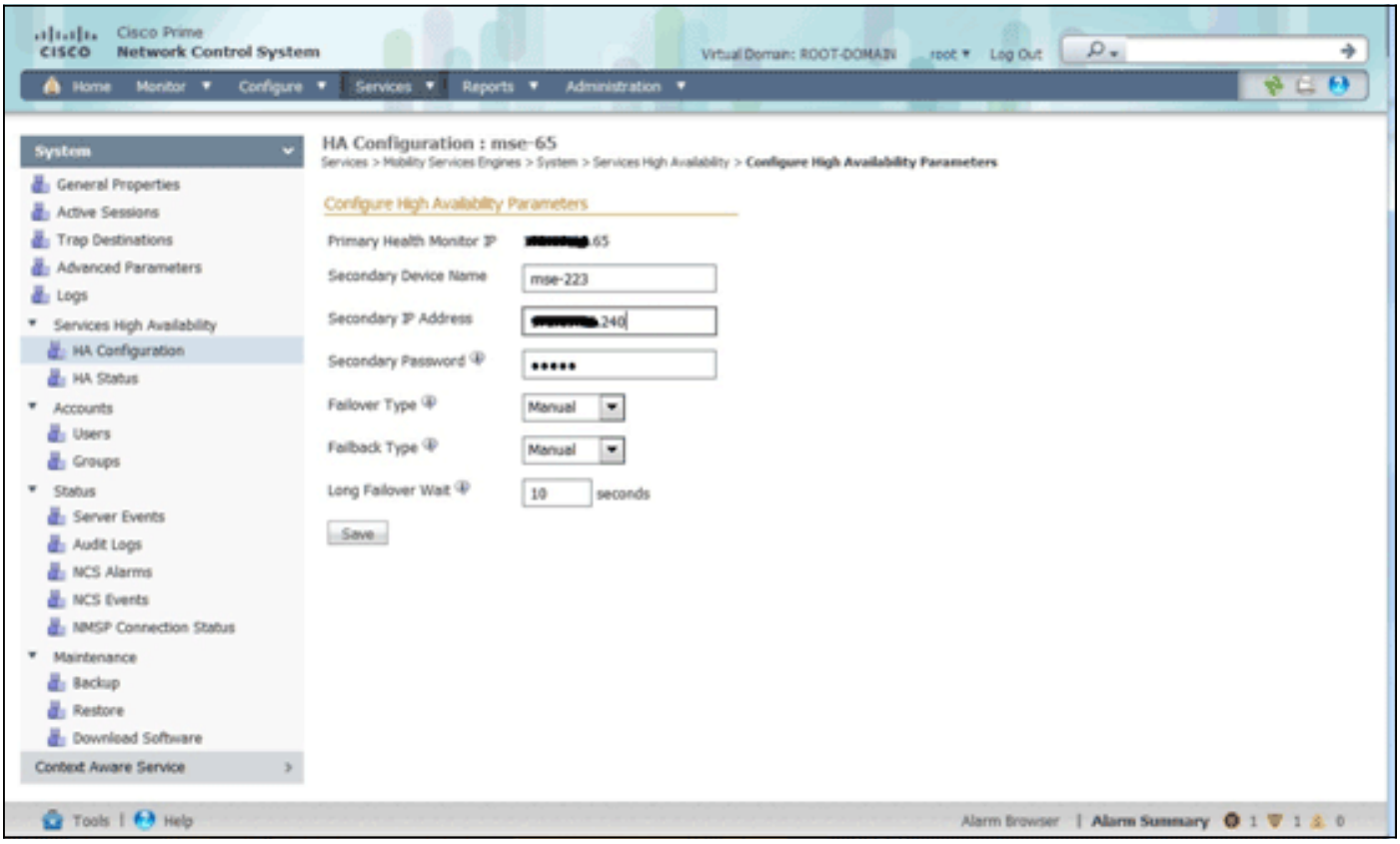
licenza massima supportata per il servizio su questo accessorio (in base all'allocazione delle risorse alla VM), mentre nella colonna Limite installato è indicata la licenza effettiva installata o disponibile tramite valutazione sull'accessorio.

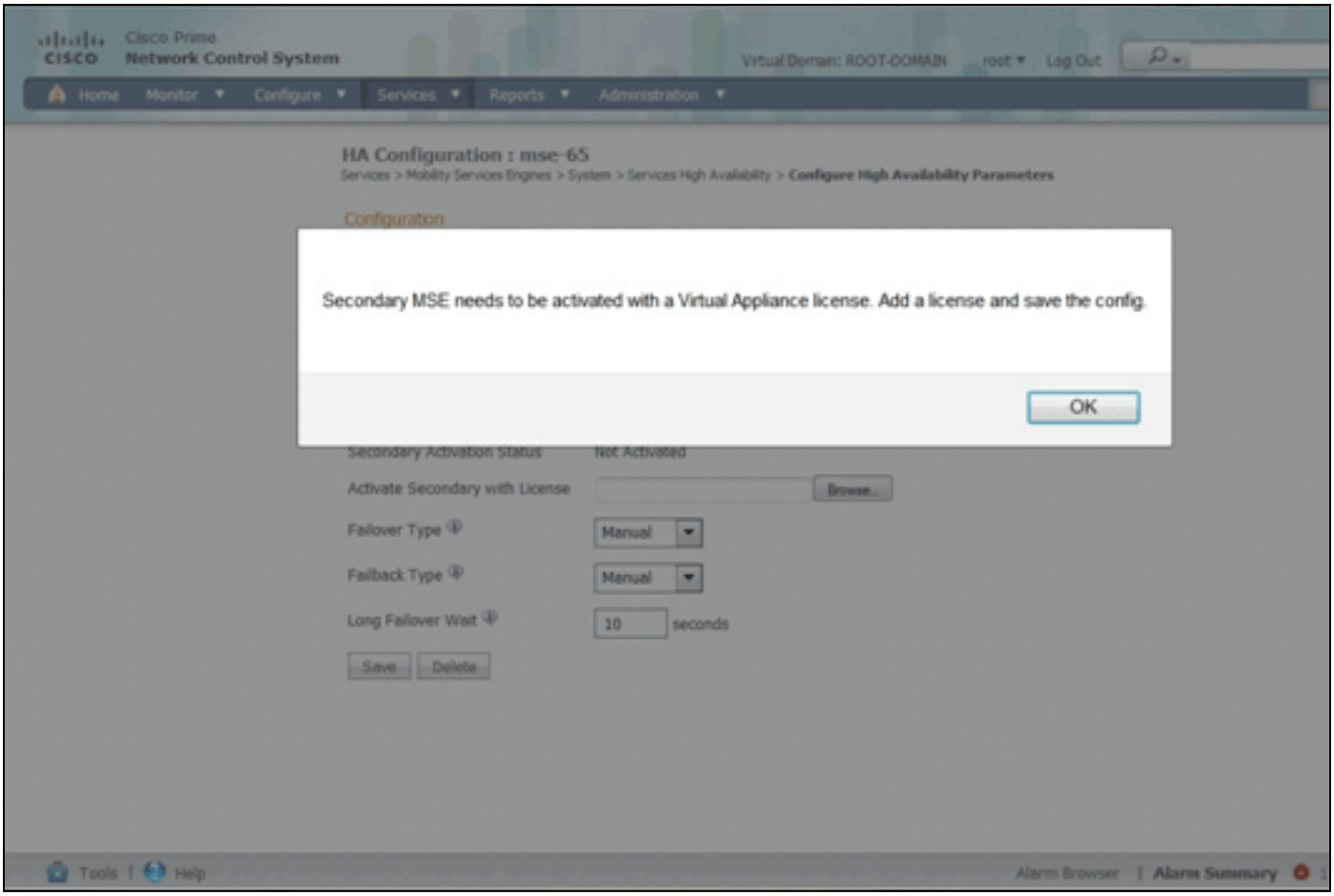
Alta disponibilità sull'appliance virtuale

Per poter utilizzare la funzione HA, è necessario attivare sia l'accessorio principale che quello secondario con una licenza di attivazione dell'accessorio virtuale.

Configura alta disponibilità

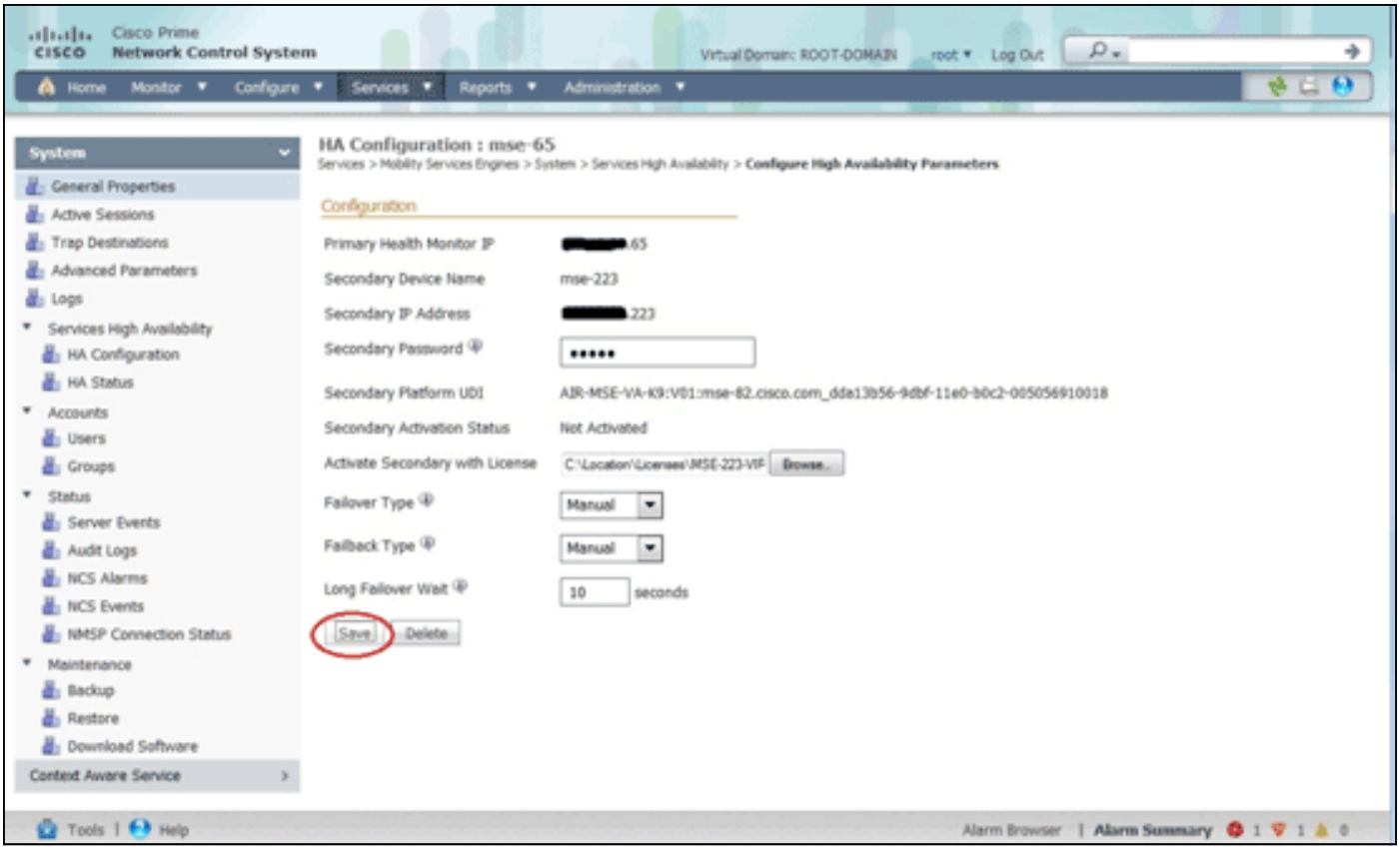
Èpossibile impostare la configurazione HA tramite il server MSE primario su NCS.





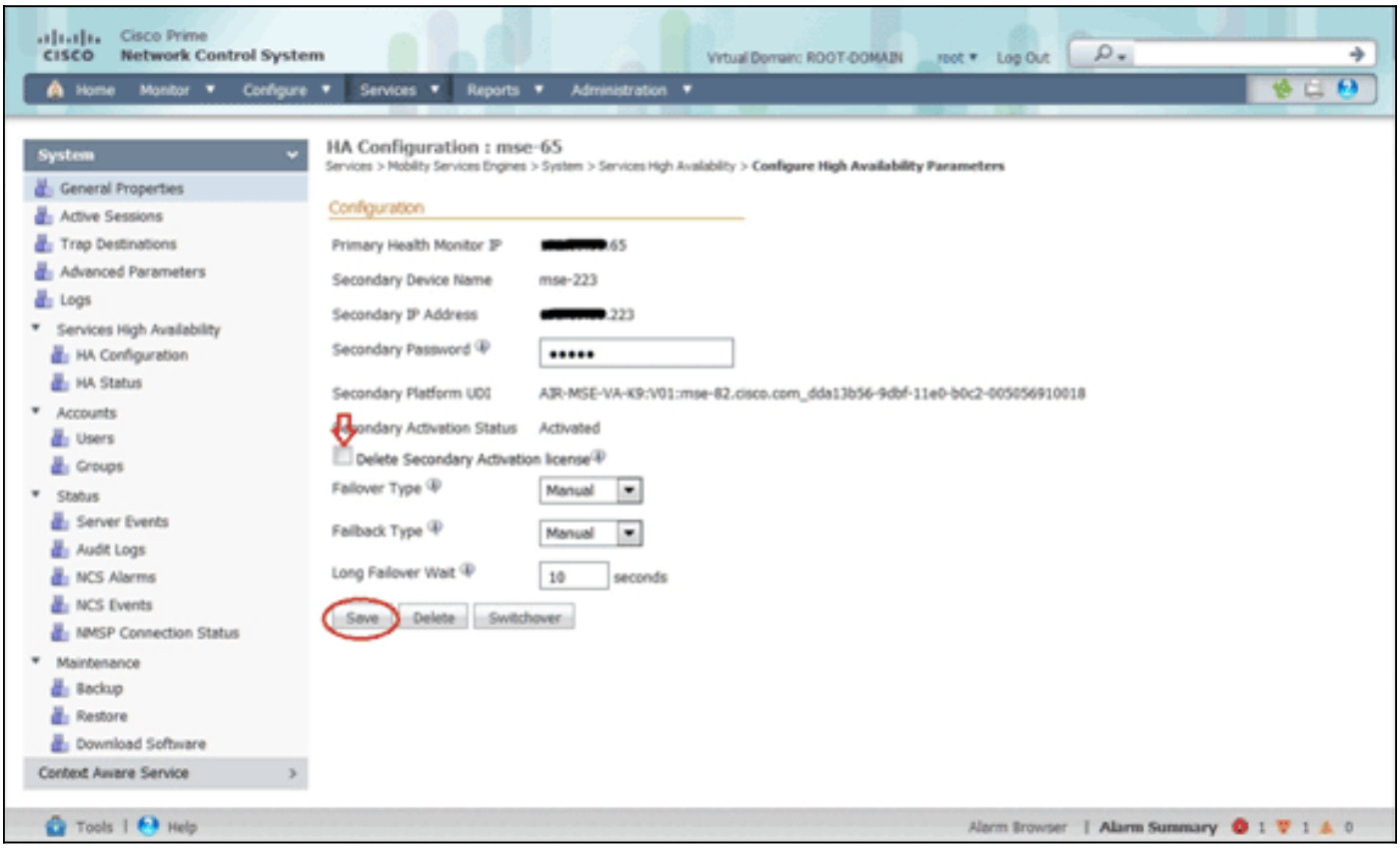
Attivazione di MSE secondario

L'accessorio secondario deve essere attivato. È possibile usare le informazioni UDI per richiedere una licenza di attivazione per il server MSE secondario. Nella pagina Configurazione HA, cercare la licenza e fare clic su **Salva**. L'opzione HA verrà impostata dopo l'attivazione corretta dell'MSE secondario.



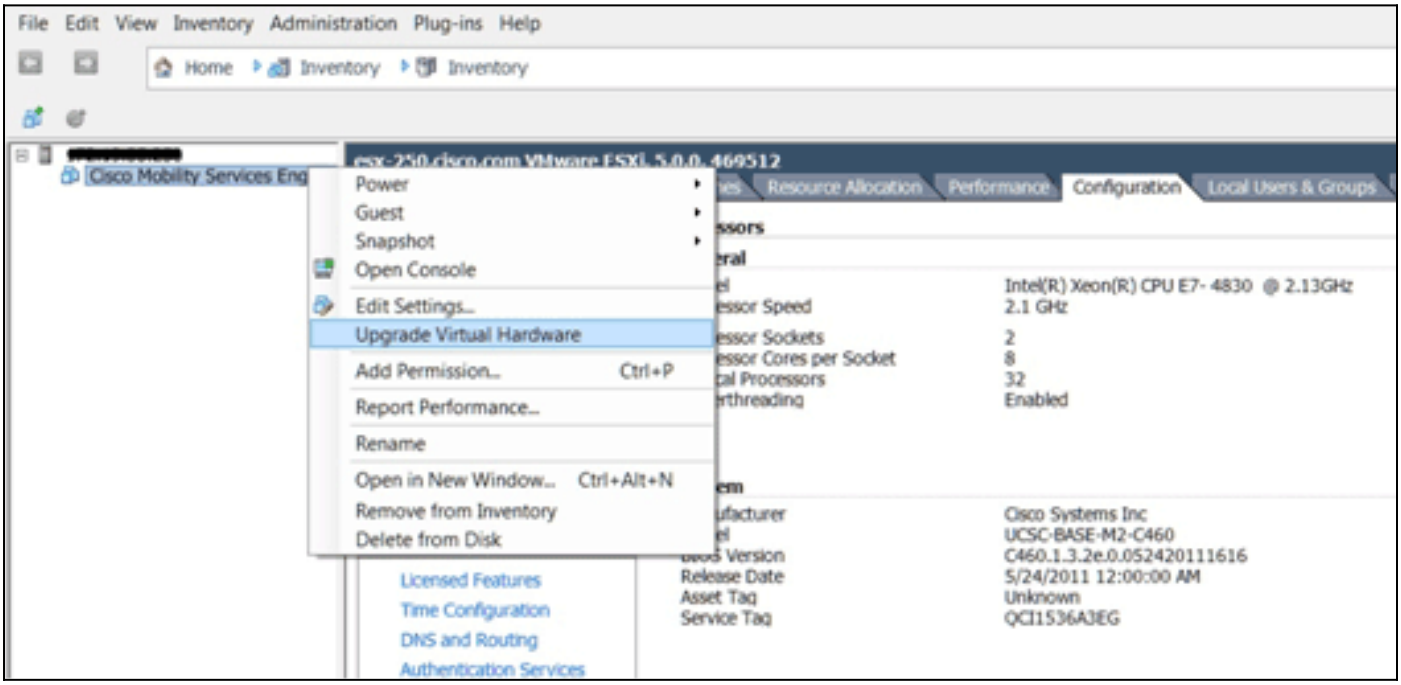
Disattivazione di MSE secondario

Se è necessario eliminare la licenza di attivazione dal server MSE secondario, è possibile fare clic sulla casella di controllo e scegliere **Salva** per disattivare il server MSE secondario.



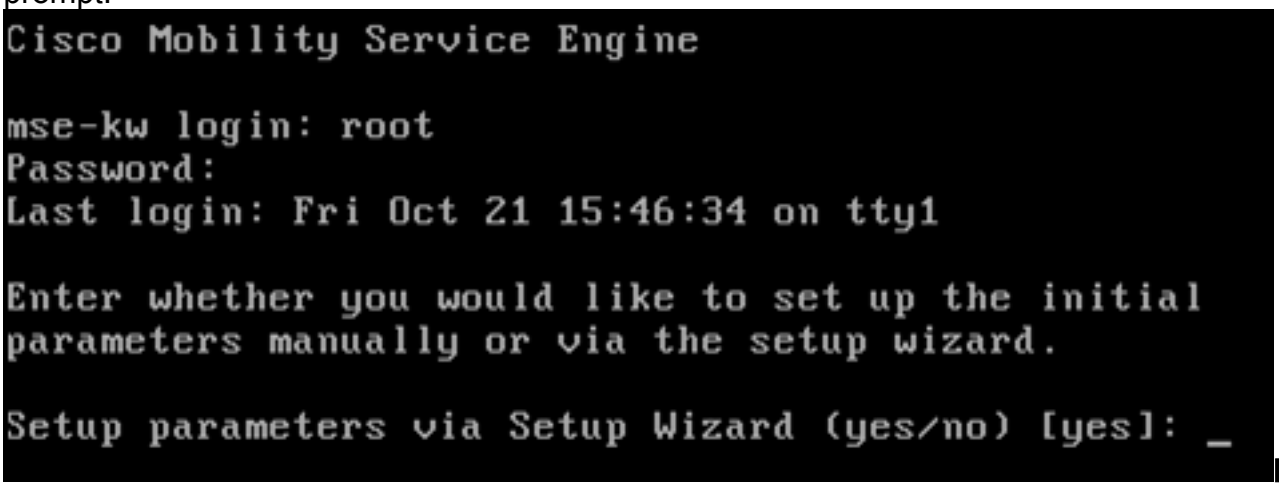
Appliance virtuale su ESXi 5.0

Su ESXi 5.0, la dimensione del blocco è fissa a 1 MB in quanto supporta installazioni VM di grandi dimensioni. Per poter assegnare più di otto (8) core all'appliance virtuale, è necessario aggiornare l'hardware virtuale. Per aggiornare l'hardware virtuale, selezionare MSE e scegliere **Aggiorna hardware virtuale**, come mostrato nell'immagine seguente:



Procedura console MSE

1. Accedere alla console con queste credenziali: root/password.Al primo avvio, MSE chiede all'amministratore di avviare lo script di installazione.
2. Immettere **yes** in questo prompt.



Not
a: se il programma di installazione di MSE non viene richiesto, immettere il comando seguente: /opt/mse/setup/setup.sh.

3. Configurare il nome 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. Configurare il nome di 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. Configurare il ruolo HA primario:

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

6. Configurare i parametri dell'interfaccia 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. Quando vengono richiesti i parametri dell'interfaccia eth1, digitare **Skip** per procedere al passaggio successivo, in quanto per il funzionamento non è necessaria una seconda scheda NIC.

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

Nota: l'indirizzo configurato deve fornire connettività IP ai WLC prospettici e al sistema di gestione WCS utilizzati con l'accessorio.

8. Immettere le informazioni sui server DNS. Per la corretta risoluzione del dominio è richiesto un solo server DNS. Immettere i server di backup per la resilienza.

```
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. Configurare il fuso orario. Cisco consiglia di utilizzare l'ora UTC (Coordinated Universal Time).Se il fuso orario predefinito di New York non è applicabile al proprio ambiente, sfogliare i menu di posizione per selezionare il fuso orario corretto.

```
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. Quando viene richiesto di configurare il giorno e l'ora del riavvio futuri, digitare **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. Configurare il server syslog remoto, se applicabile.

```
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. Configurare il protocollo NTP (Network Time Protocol) o l'ora di sistema.L'NTP è opzionale, ma assicura che il sistema mantenga un'ora di sistema accurata. Se si sceglie di abilitare NTP, l'ora di sistema verrà configurata dai server NTP selezionati. In caso contrario, verrà richiesto di immettere la data e l'ora correnti.

```
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. Quando viene richiesto di configurare il banner di accesso, digitare

Skip.

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

14. Abilitare l'accesso alla directory principale della console locale.Questo parametro viene utilizzato per abilitare/disabilitare l'accesso alla console locale al sistema. È necessario abilitare l'accesso alla directory principale della console locale per consentire la risoluzione dei problemi locale. Il valore predefinito è
    Skip.

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

15. Abilitare l'accesso radice Secure Shell (SSH).Questo parametro viene utilizzato per abilitare/disabilitare l'accesso della console remota al sistema. Per poter eseguire la risoluzione remota dei problemi, è necessario abilitare l'accesso radice SSH. È tuttavia possibile che i criteri di protezione aziendali richiedano la disabilitazione di questa opzione.

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

16. Configurare la modalità utente singolo e la complessità della password.Questi parametri di configurazione non sono obbligatori; il valore predefinito è
    Skip.

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

17. Modificare la password di root.Questa operazione è fondamentale per garantire la sicurezza del sistema. Assicurarsi di selezionare una password complessa costituita da lettere e numeri senza parole del dizionario. La lunghezza minima della password è di otto (8) caratteri. Le credenziali predefinite sono
    root/password.

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

18. Configurare i parametri relativi all'accesso e alla
    password:

```
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. Configurare una password di avvio (Grub). (Facoltativo)Questo parametro di configurazione non è obbligatorio. Il valore predefinito è
    Skip.

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

20. Configurare il nome utente di comunicazione
    NCS.

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

21. Accettare la modifica apportata alla

configurazione.

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

Nell'immagine è illustrato un esempio della schermata di completamento:

```
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. Eseguire il comando **getserverinfo** per verificare la configurazione.

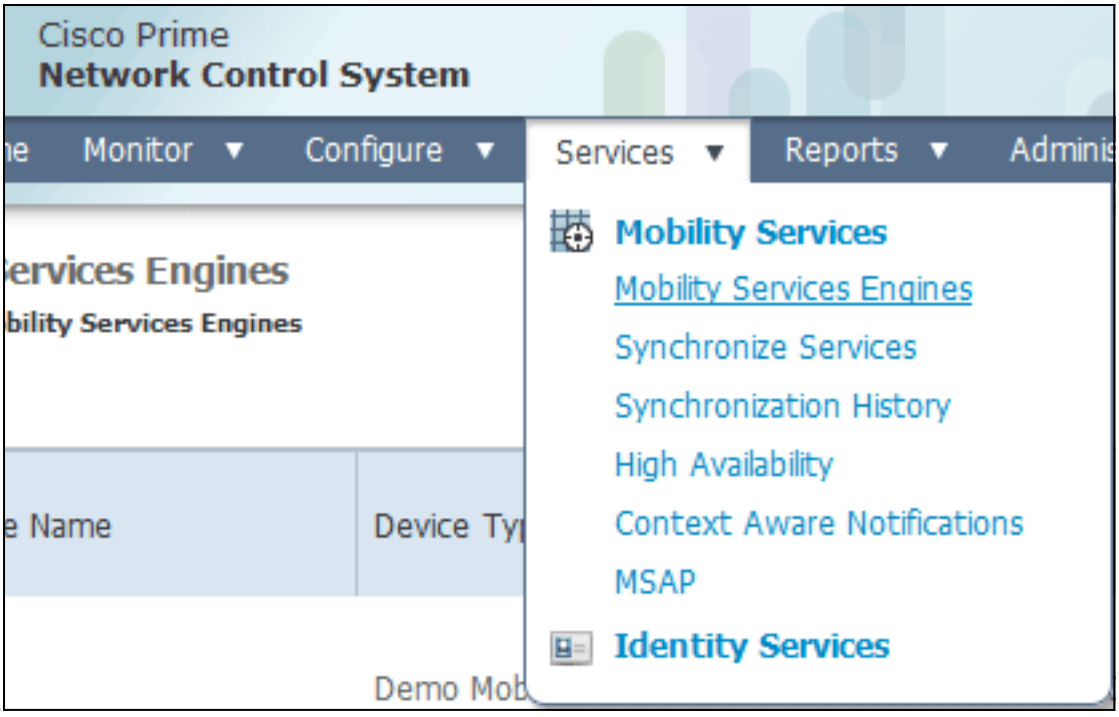
```
Active Wired Clients: 0
Active Elements(Wireless Clients, Rogue APs, Rogue Clients,
lients, Tags) Limit: 115
Active Sessions: 1
Wireless Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogue APs Not Tracked due to the limiting: 0
Rogue Clients Not Tracked due to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

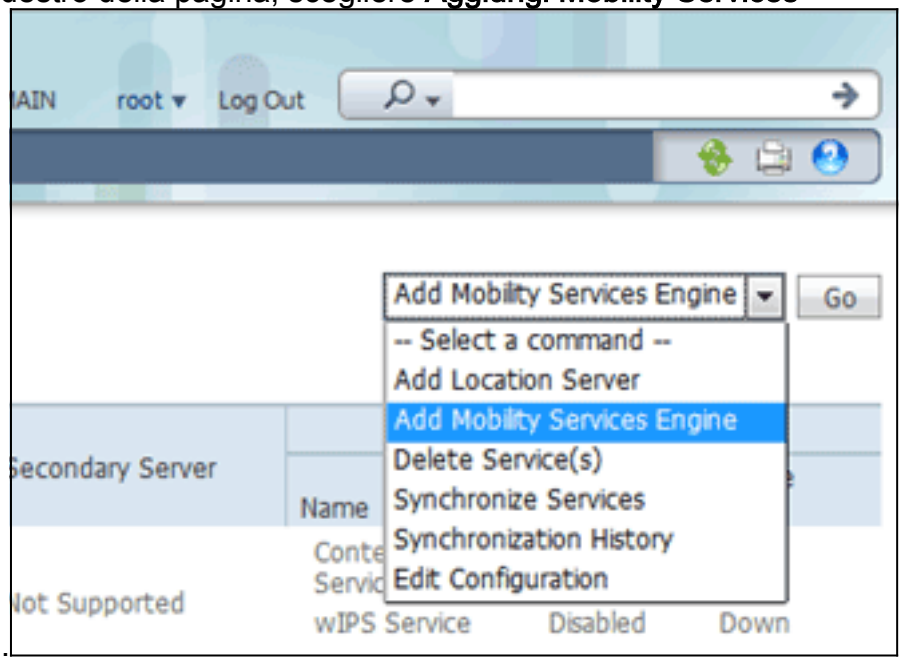
Aggiunta di MSE VA a NCS

1. Accedere alla NCS e scegliere **Servizi > Mobility Services**

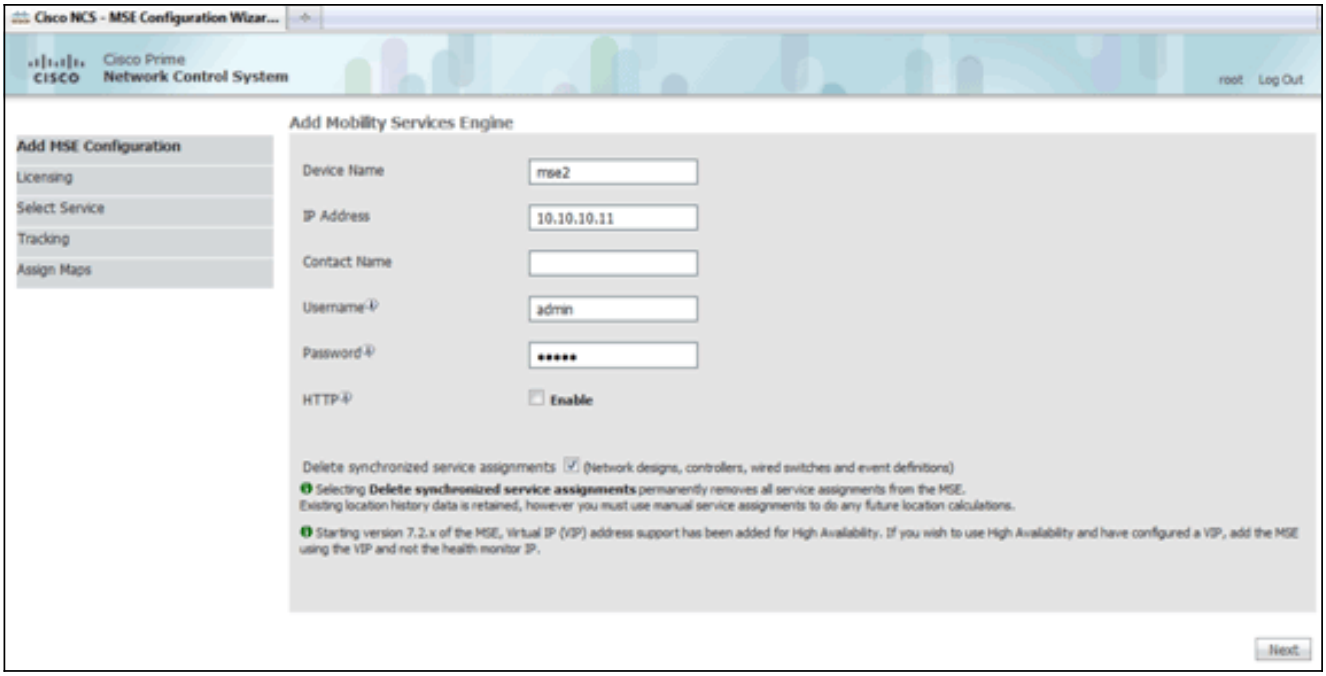


Engine.

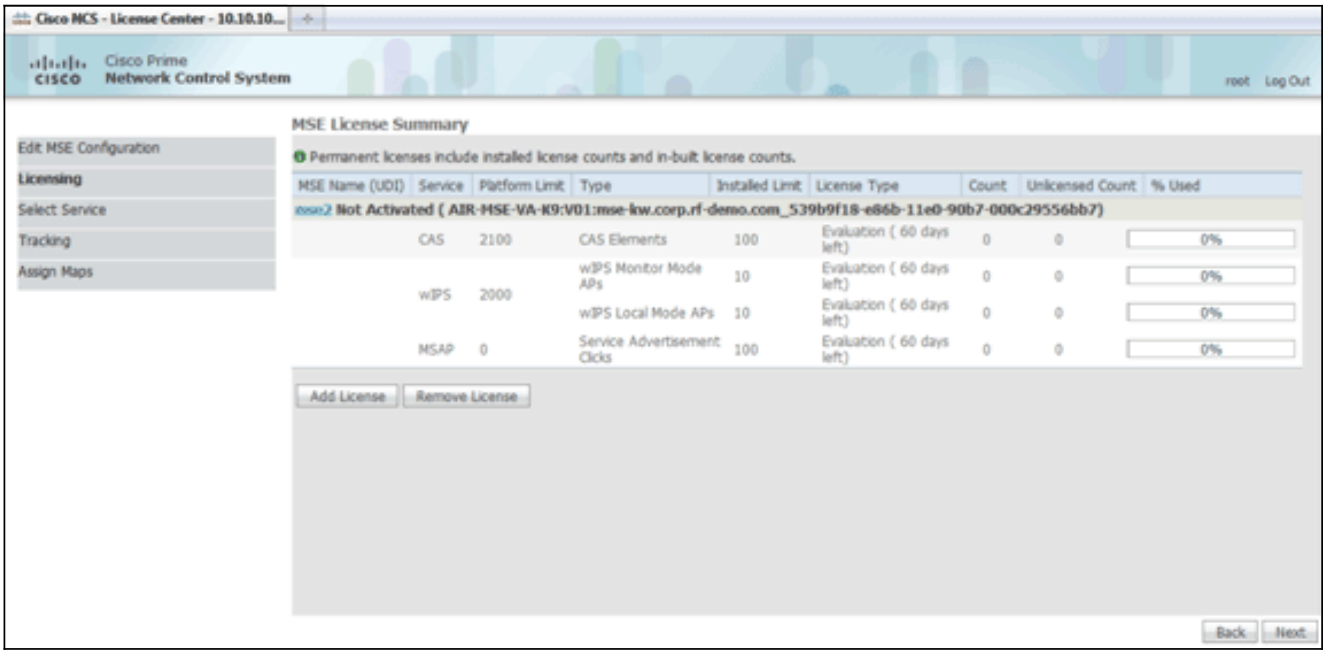
2. Dall'elenco a discesa sul lato destro della pagina, scegliere **Aggiungi Mobility Services Engine**, quindi fare clic su **Vai**.



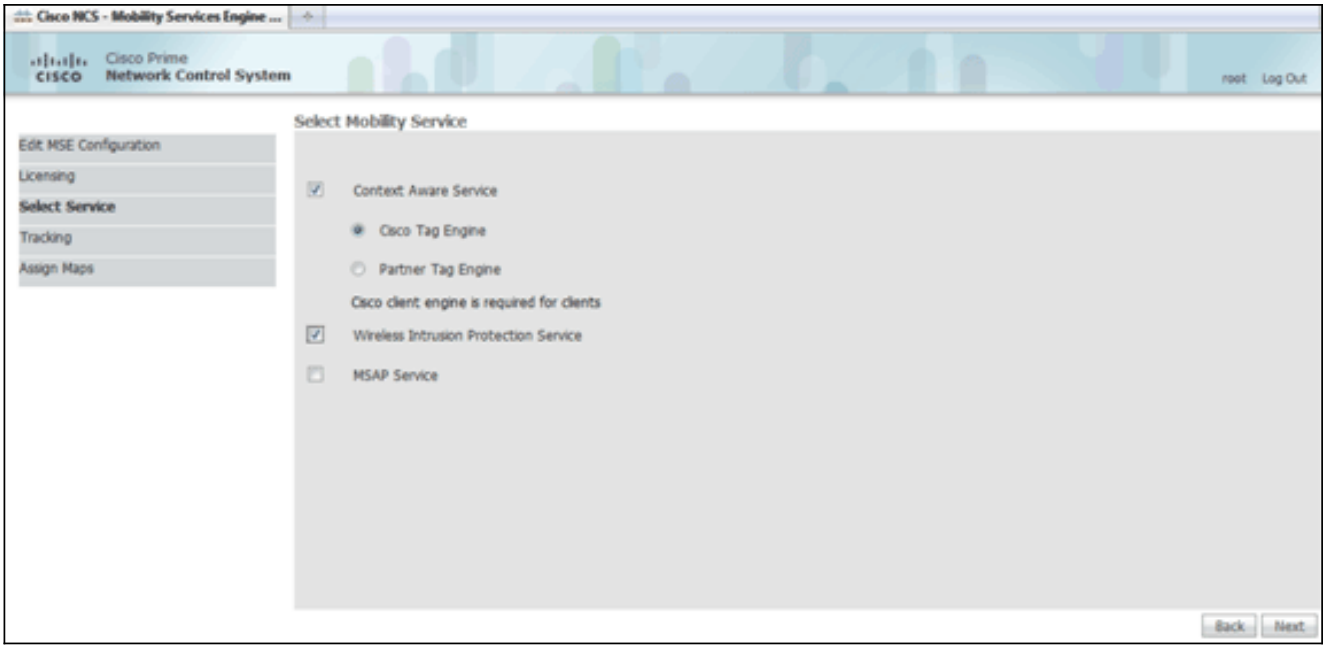
3. Immettere un nome di dispositivo univoco per MSE, l'indirizzo IP precedentemente configurato durante l'installazione di MSE, un nome di contatto per il supporto. e il nome utente e la password NCS configurati durante la configurazione di MSE.Non modificare il nome utente predefinito di *admin*. È possibile mantenere l'impostazione predefinita.



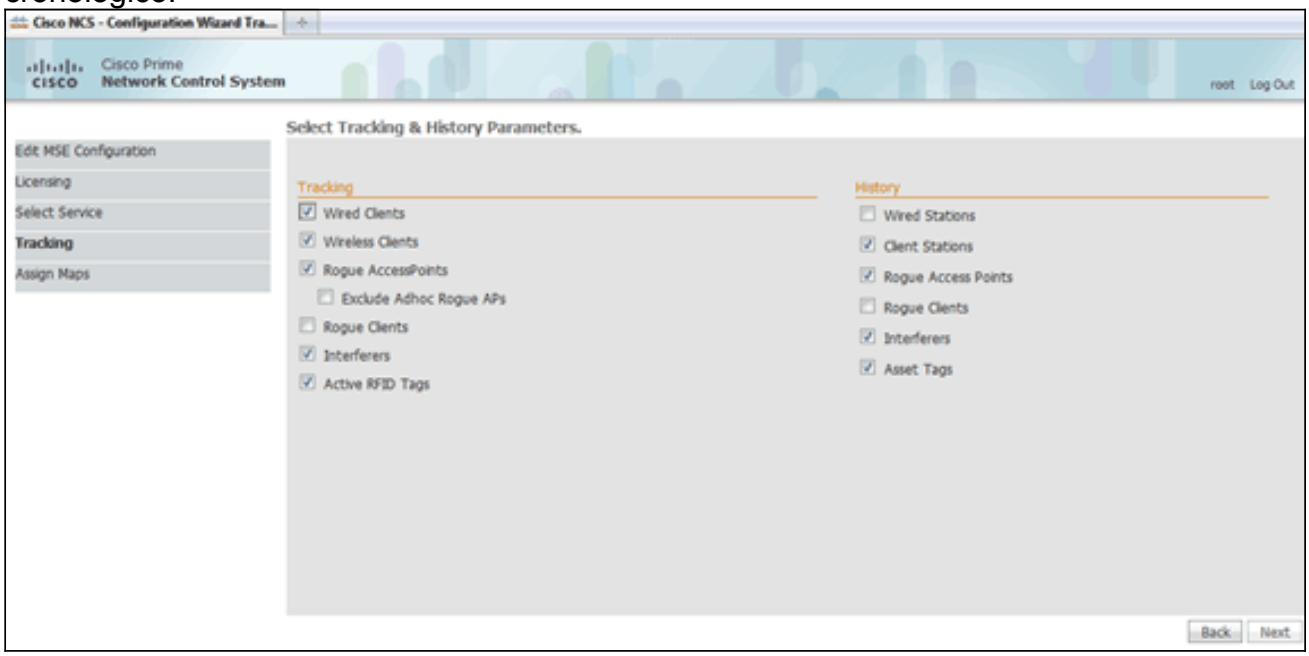
4. Fare clic su **Next** (Avanti).
5. Fare clic su **Licenze** e verificare le licenze. Al momento dell'installazione, la licenza demo predefinita è sufficiente per il test. È possibile aggiungere altre licenze acquistate o rimuovere licenze nella pagina
   Licenze.



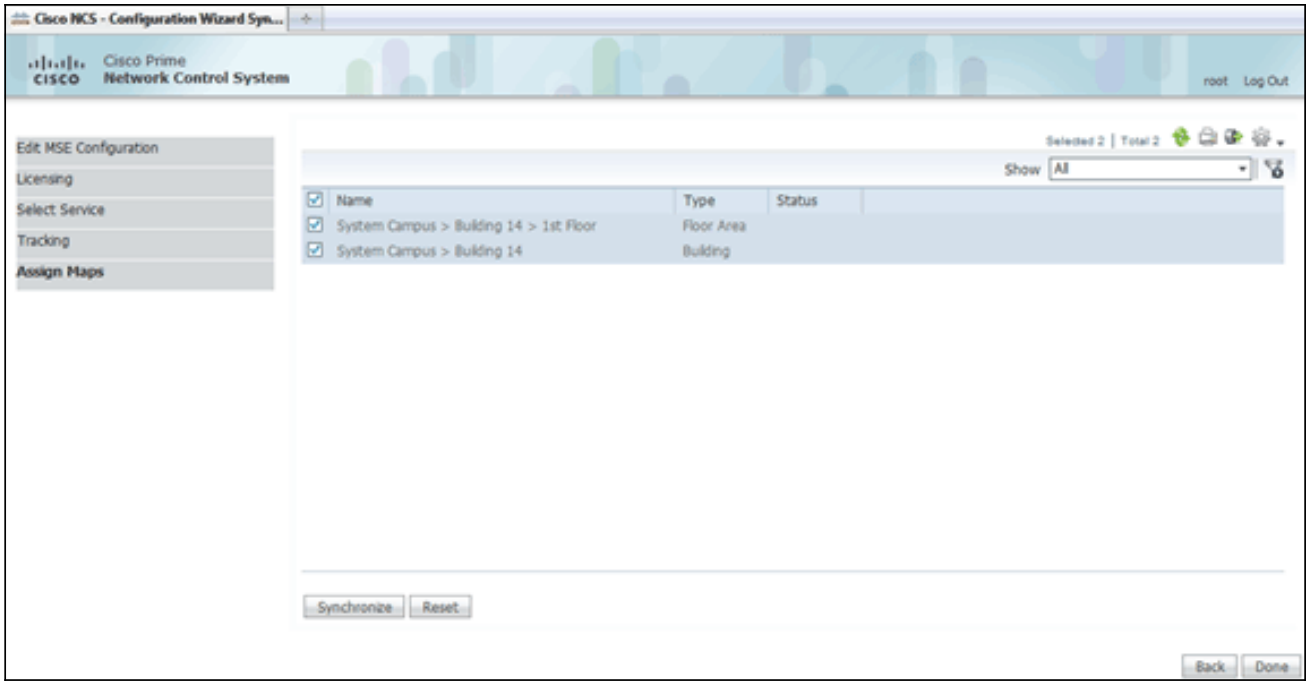
6. Fare clic su **Next**
   (Avanti).



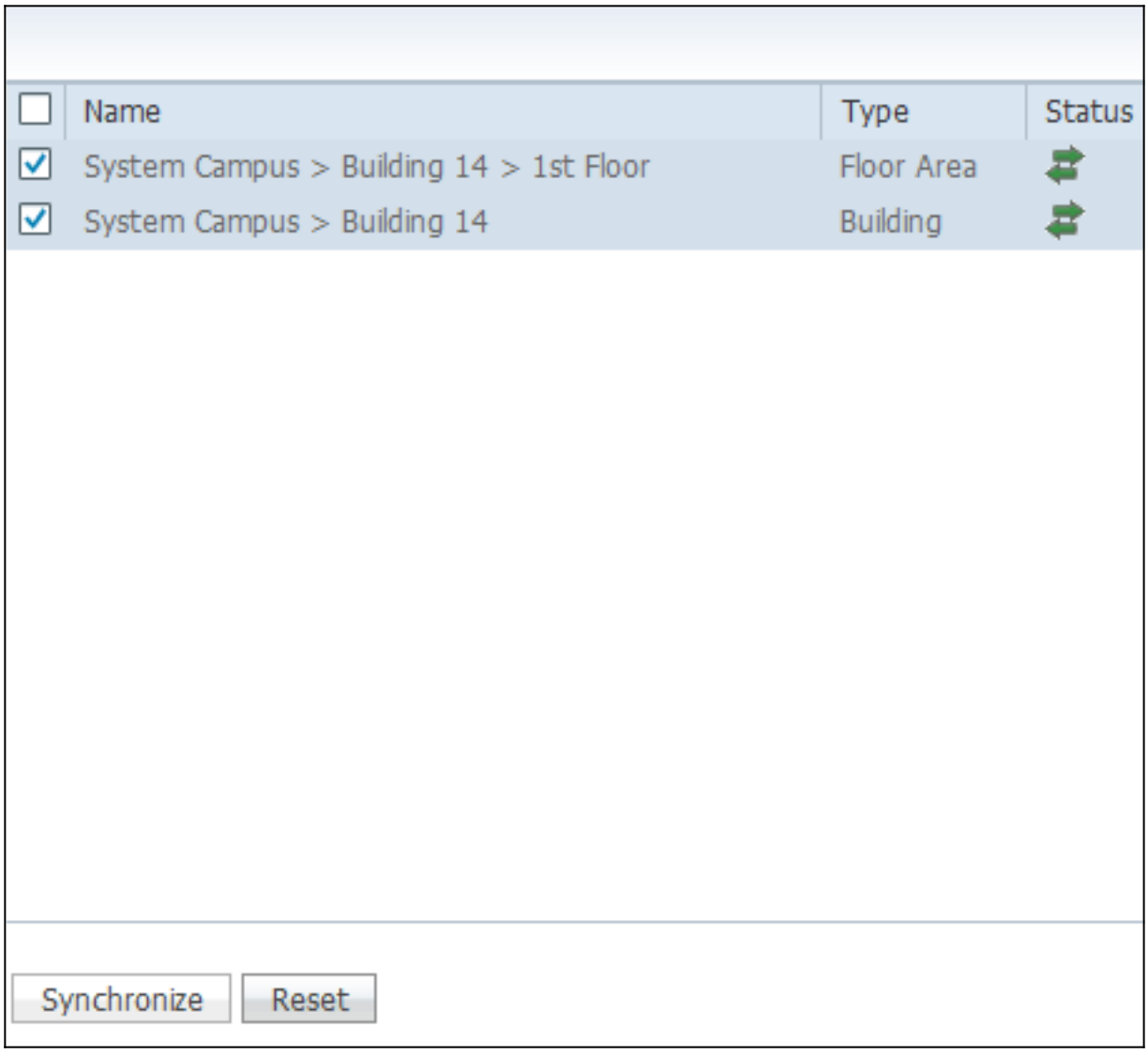
7. Nella pagina Select Mobility Service, fare clic sul pulsante di opzione **Cisco Tag Engine** (disponibile dalla versione 7.0MR) (per il supporto di tag client e RFID) oppure fare clic sul pulsante di opzione **Partner Tag Engine** (per Aeroscout, ecc.).
8. Per eseguire il test della funzionalità di protezione wIPS delle funzionalità Monitor Mode e Enhanced Local Mode, selezionare la casella di controllo **Servizio protezione intrusioni wireless**.
9. Fare clic su **Next** (Avanti).
10. Selezionare le caselle di controllo relative agli elementi da abilitare per il rilevamento e ai parametri della cronologia per tali elementi da rendere disponibili per il reporting cronologico.



11. Fare clic su **Next** (Avanti).

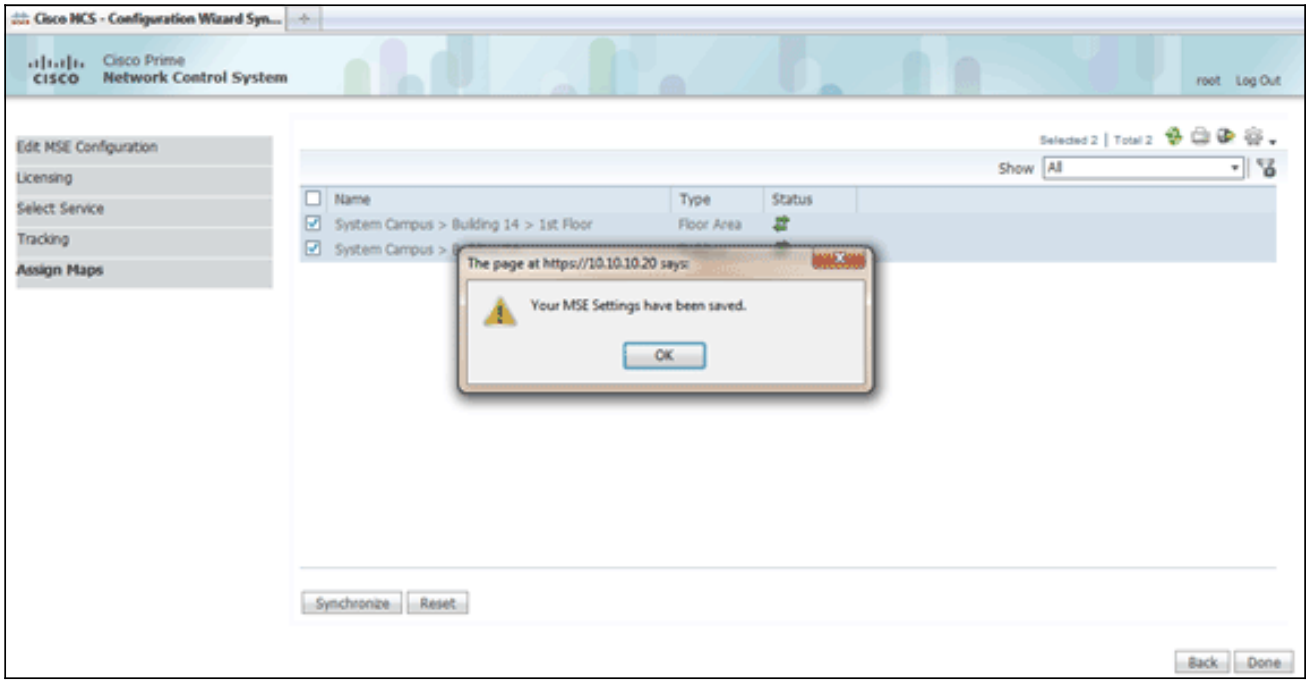


12. Selezionare le caselle di controllo relative all'edificio e al piano esistenti e fare clic su **Sincronizza**.Una volta eseguita la sincronizzazione, la colonna Stato viene aggiornata per indicare che la progettazione iniziale della rete è stata sincronizzata.

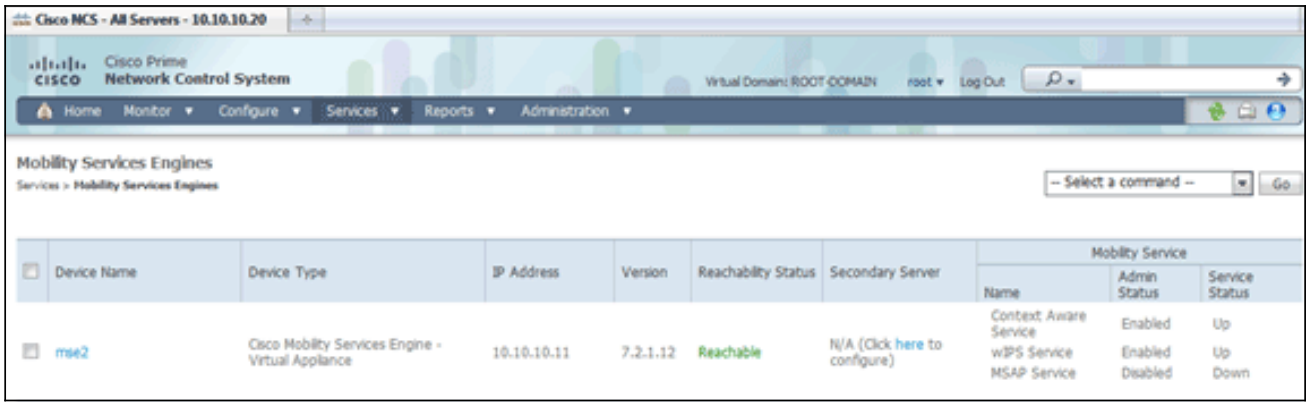


13. Al termine della sincronizzazione, fare clic su **Fine**.Viene visualizzata una finestra di dialogo che indica che le impostazioni MSE sono state

salvate.

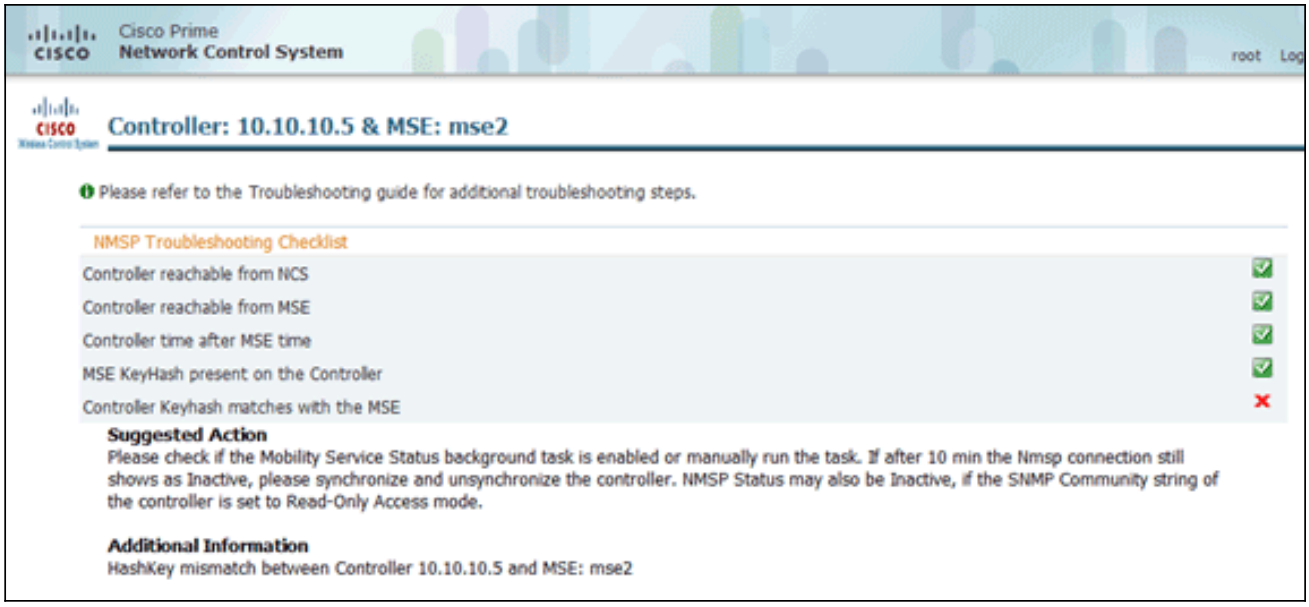


14. Confermare la configurazione nella pagina MSE principale di NCS.



Assicurarsi di sincronizzare il resto dei progetti di rete, dei controller, degli switch cablati e dei gruppi di eventi, se disponibili.**Nota:** il servizio sensibile al contesto di Cisco dipende fortemente da un orologio sincronizzato tra WLC, NCS e MSE. Se tutti e tre questi sistemi non sono indirizzati allo stesso server NTP e configurati con le stesse impostazioni di fuso orario, il servizio sensibile al contesto non funzionerà correttamente. Prima di tentare una procedura di risoluzione dei problemi, verificare che l'orologio di sistema sia lo stesso su tutti i componenti del sistema sensibile al contesto.

15. Controllare la comunicazione tra MSE e controller per i servizi scelti.verificare che l'MSE comunichi con ciascuno dei controller solo per il servizio scelto; Lo stato del protocollo NMSP (Network Mobility Service Protocol) deve essere *attivo*.Questa immagine fornisce un esempio di quando il keyhash non viene aggiunto al WLC.



Sulla console WLC, usare il comando **show auth-list**.L'esempio seguente mostra dalla console WLC che non è disponibile alcun server di posizione:

```
(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
```

Per aggiungere manualmente l'MSE e stabilire una connessione NMSP al WLC, attenersi alla seguente procedura:Sulla console MSE eseguire il comando **cmdshell** e quindi il comando **show server-auth-info**.Nell'esempio vengono mostrati l'indirizzo MAC e il keyhash da usare per l'aggiunta al WLC.

```
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
```

Eseguire il comando **config auth-list add ssc <*indirizzo mac*> <*keyhash MSE*>**, quindi eseguire il comando **show auth-list**.Nell'esempio viene mostrato come l'MSE sia stato aggiunto al WLC (manualmente).

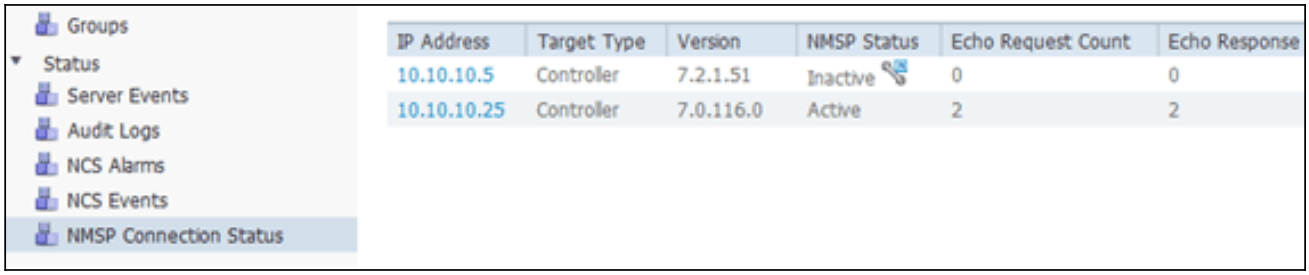
```
(Cisco Controller) config>auth-list add ssc 00:0c:29:55:6b:b7 1469187db14ac53ac6108e56b04d48015bdd70d7

(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
```

Sulla NCS, verificare che la connessione NMSP sia *Attiva*.



Informazioni di riferimento per la riga di comando

Comandi 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
```

Comandi MSE

Per determinare lo stato dei servizi MSE, eseguire questo comando:

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

Eseguire questo comando per avviare il motore sensibile al contesto per il rilevamento dei client:

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

Eseguire questo comando per determinare lo stato del motore sensibile al contesto per il monitoraggio dei client:

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

Eseguire questo comando per arrestare il motore sensibile al contesto per il rilevamento dei client:

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

Per eseguire la diagnostica, eseguire questo comando:

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

Nota: il comando **rundiag** può essere utilizzato anche per visualizzare le informazioni UDI MSE necessarie per ottenere il file della licenza per il motore sensibile al contesto per i client.

Informazioni correlate

- Guida alla configurazione di MSE (dispositivo virtuale e fisico)
- Configurazione alta disponibilità MSE
- Guida alla distribuzione di Cisco WIPS
- Ordinazione prodotti
- Documentazione e supporto tecnico – Cisco Systems