MSE Software Release 7.2 Virtual Appliance - Konfigurations- und Bereitstellungsleitfaden

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen
Systemanforderungen
Management-Software und VMware-Lizenzierung
Ressourcenanforderungen
Einrichten des ESXi-Hosts
Installieren der MSE Virtual Appliance
Konfigurieren der MSE Virtual Appliance-Ebenen
Einrichten der MSE Virtual Appliance
Konfigurieren des Netzwerks
Hinzufügen von Festplattenspeicherplatz
Blockgröße
VMware-Tools
Aktualisieren der virtuellen Appliance
Lizenzierung der virtuellen Appliance
Hohe Verfügbarkeit auf der virtuellen Appliance
Konfiguration der Hochverfügbarkeit
Aktivieren der sekundären MSE
Deaktivieren der sekundären MSE
Virtuelle Appliance auf ESXi 5.0
MSE-Konsolenverfahren
Hinzufügen von MSE VA zum NCS
Befehlszeilenreferenz
WLC-Befehle
MSE-Befehle
Zugehörige Informationen

Einführung

Die Cisco Mobility Services Engine (MSE) Softwareversion 7.2 bietet eine virtuelle Appliance und Unterstützung für VMware ESXi. Dieses Dokument enthält Richtlinien für Konfiguration und Bereitstellung sowie Tipps zur Fehlerbehebung für Benutzer, die die virtuelle MSE-Appliance einem Cisco Unified WLAN hinzufügen und kontextsensitive Services und/oder das Cisco Adaptive Wireless Intrusion Prevention System (wIPS) ausführen. Darüber hinaus werden in diesem Dokument die Systemanforderungen für die virtuelle MSE-Appliance beschrieben und

allgemeine Bereitstellungsrichtlinien für die virtuelle MSE-Appliance beschrieben. Dieses Dokument enthält keine Konfigurationsdetails für die MSE und die zugehörigen Komponenten. Diese Informationen sind in anderen Dokumenten enthalten; werden Referenzen bereitgestellt.

Im Abschnitt Zugehörige Informationen finden Sie eine Liste von Dokumenten zur Konfiguration und zum Design von kontextsensitiven Mobilitätsdiensten. Die adaptive wIPS-Konfiguration wird in diesem Dokument ebenfalls nicht behandelt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Mobility Services Engine der Serie 3300.

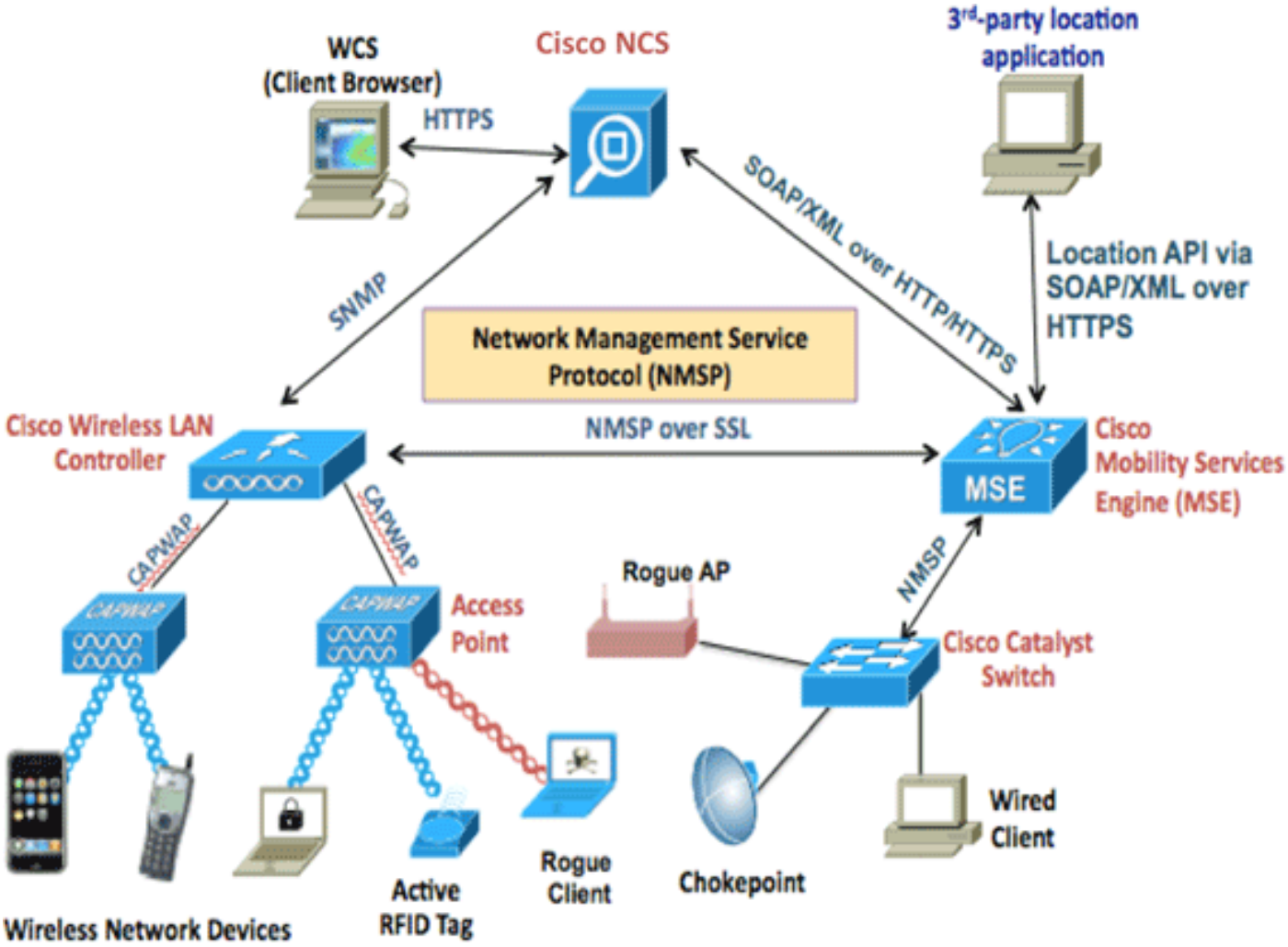
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Dieses Bild zeigt die typische Cisco WLAN-Bereitstellung, die die Cisco Mobility Services Engine (MSE) umfasst. Diese Bereitstellung umfasst auch andere kabelgebundene/Wireless-Netzwerkclients, RFID-Tags sowie einen nicht autorisierten Access Point (AP) und Client. MSE bietet Transparenz für diese Elemente, sowohl für den Standort als auch für wIPS. Vor MSE Software Release 7.2 waren nur physische Appliances auf MSE-3310 und MSE-3350/3355 beschränkt.



Systemanforderungen

Die virtuelle MSE Software Release 7.2 wird auf VMware ESXi 4.1 und höher unterstützt und getestet. Diese Serverkonfigurationen wurden getestet und werden als Richtlinie empfohlen.

- Cisco Unified Computing System (UCS) C200 M2 Rackmount-ServerZwei (2) Intel? Xeon? CPU E5506 bei 2,13 GHzRAM (je nach konfigurierter Stufe)SAS-Laufwerke mit erweiterten RAID-Controllern (mindestens 500 GB+)
- UCS C210 M2 Rackmount-ServerZwei (2) Intel Xeon CPU E5640 mit 2,67 GHzRAM (je nach konfigurierter Stufe)SAS-Laufwerke mit erweiterten RAID-Controllern (mindestens 500 GB+)
- UCS C250 M2 Rackmount-ServerZwei (2) Intel Xeon CPU E5570 mit 2,93 GHzRAM (je nach konfigurierter Stufe)SAS-Laufwerke mit erweiterten RAID-Controllern (mindestens 500 GB+)
- UCS C460 M2 Rackmount-ServerZwei (2) Intel Xeon CPU E7-4830 mit 2,13 GHzRAM (je nach konfigurierter Stufe)SAS-Laufwerke mit erweiterten RAID-Controllern (mindestens 500 GB+)

Hinweis: Verwenden Sie zwei (2) Quadcore-Prozessoren, die mindestens so leistungsstark sind wie die oben genannten.

Management-Software und VMware-Lizenzierung

Die virtuelle Cisco MSE Software Release 7.2 unterstützt ESX/ESXi 4.x und höher.

Um ESXi-Hosts zu verwalten und die virtuellen Appliances zu konfigurieren und bereitzustellen, empfiehlt Cisco, vCenter Server 4.x auf einem 64-Bit-Computer unter Windows XP oder Windows 7 zu installieren und eine vCenter Enterprise-Lizenz zu erwerben. Wenn Sie nur einen ESXi-Host haben, können Sie auch den vSphere-Client verwenden, um diesen zu verwalten.

Ressourcenanforderungen

Die Ressourcenanforderungen hängen von der Lizenz ab, die Sie bereitstellen möchten. In dieser Tabelle sind die verschiedenen Ebenen aufgelistet, auf denen Sie Ihre virtuelle Appliance konfigurieren können:

Primäre MSE	Ressourcen		Unterstützte Lizenz (einzeln)	
Virtuelle Appliance-Ebene	Gesamter Speicher	CPU	CAS-Lizenz	wIPS-Lizenz
Niedrig	6 G	2	2000	2000
Standard	11 G	8	18.000	5000
Hoch	20 G	16	50000	10.000

Hinweis: Die empfohlenen Grenzwerte für die CAS- und wIPS-Lizenzen sind bei Ausführung von nur einem Service die maximal unterstützten Grenzwerte. Wenn Sie beide Dienste auf derselben Appliance ausführen möchten, gelten Co-Existenzbeschränkungen.

Einrichten des ESXi-Hosts

Gehen Sie wie folgt vor, um eine virtuelle MSE-Appliance auf einem UCS oder einem ähnlichen Server einzurichten:

1. Stellen Sie sicher, dass Ihr System über mindestens 500 GB Festplattenspeicher und schnelle SAS-Laufwerke mit erweiterten RAID-Controllern verfügt. (Verwenden Sie eine Blockgröße von mindestens 4 MB, wenn Sie Datenspeicher für Versionen vor ESXi 5.0 erstellen.)
2. Installieren Sie ESXi.Legen Sie den ESXi 4.1 oder höher-Installationsdatenträger ein, und starten Sie das Laufwerk.Wenn Sie mehrere Laufwerke verwenden, installieren Sie ESXi in dem Laufwerk, das als Boot-Laufwerk konfiguriert ist. Der Standard-Benutzername ist root, und das Kennwort ist leer (kein Kennwort).**Hinweis:** Wenn Sie das falsche Laufwerk für die Installation wählen, können Sie die Formatierung mit einer Fedora Live CD neu formatieren.
3. Konfigurieren Sie die IP-Adresse.Wählen Sie Netzwerkadapter aus, die aktiviert und aktiv sind. Wenn Ihr Host mit mehreren Netzwerken verbunden ist, können Sie mehrere Netzwerkadapter verwenden. Sie können dieselbe IP-Adresse während der CIMC-Einrichtung festlegen. Drücken Sie beim Hochfahren F8, um die IP-Adresse einzustellen. Ändern Sie auch das Standardkennwort.

Nach der Einrichtung von ESXi können Sie zusammen mit der oben konfigurierten IP-Adresse und Anmeldeinformationen einen Windows XP- oder Windows 7-Computer verwenden, um über den vSphere-Client eine Verbindung zum ESXi-Host herzustellen.

Weitere Informationen zur Lizenzierung des ESXi-Hosts finden Sie unter Lizenzierung von ESX

4.x, ESXi 4.x und vCenter Server 4.x .

In diesen Artikeln finden Sie Informationen zum Einrichten von Datenspeichern auf ESXi:

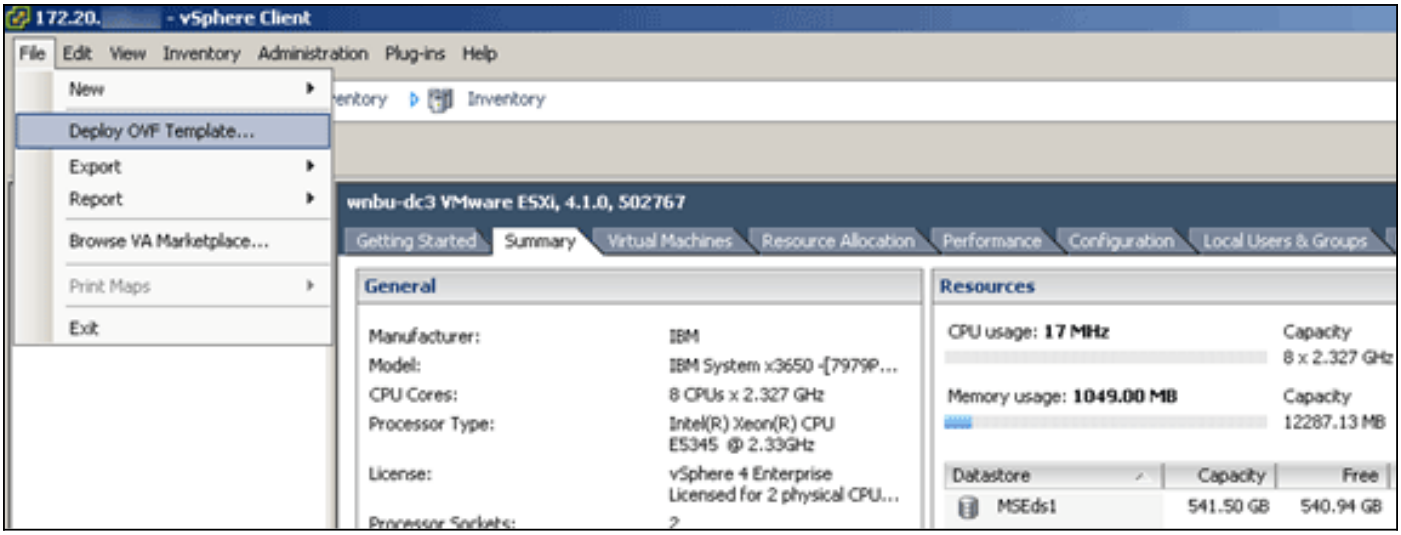
- VMFS-Datenspeicher erstellen
- Erhöhung der VMFS-Datenspeicher

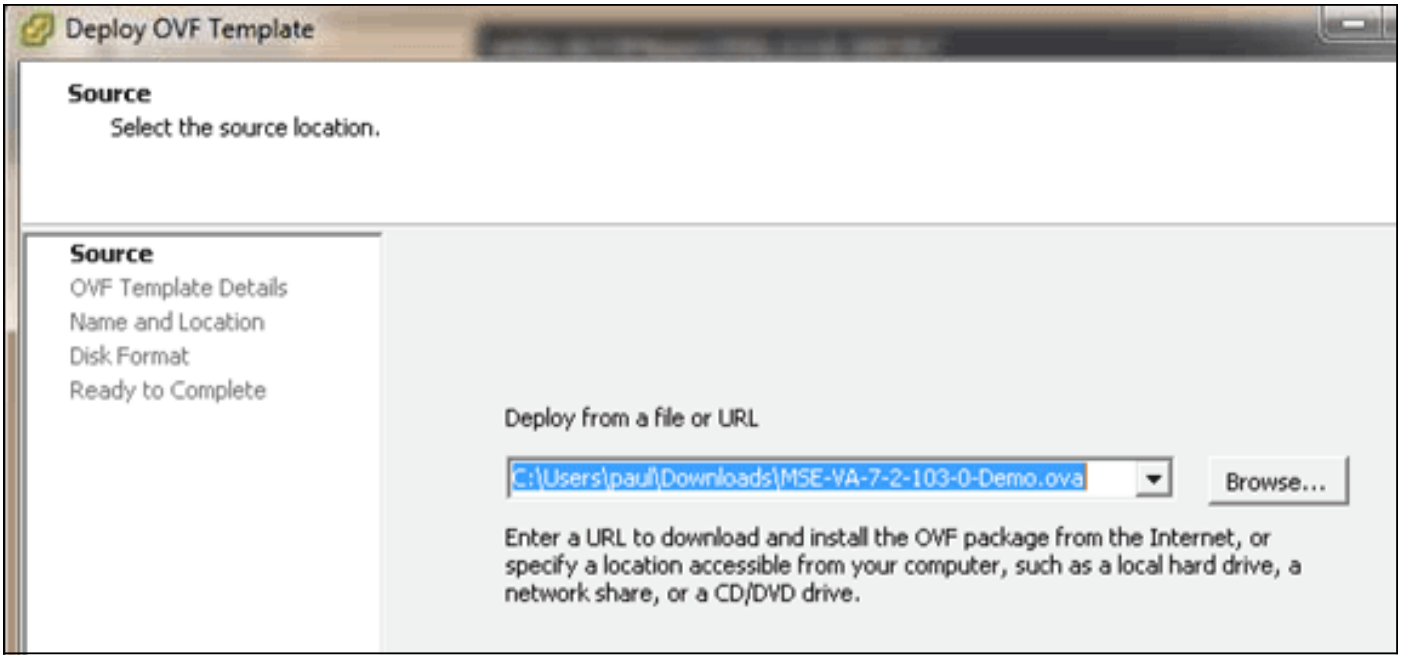
Warnung: Verwenden Sie beim Erstellen von Datenspeichern für ESXi 4.1 eine Blockgröße von mindestens 4 MB.

Installieren der MSE Virtual Appliance

Die virtuelle MSE-Appliance wird als OVA-Image (Open Virtual Appliance) verteilt, das auf einem ESXi-Host mit dem vSphere-Client bereitgestellt werden kann. Es gibt zwei verfügbare OVA-Versionen: Eine Version ist für ein Demo-Image, das nur 60 GB Speicherplatz benötigt, die andere Version ist ein generisches Produktions-Image.

Das verteilbare Produktions-Image benötigt mindestens 500 GB und mehr als den verfügbaren Speicherplatz auf dem ESXi-Hostdatenspeicher. Die OVA kann ausgewählt und über den vSphere-Client bereitgestellt werden. Wählen Sie **Datei > OVF-Vorlage bereitstellen**, um die Vorlage bereitzustellen.



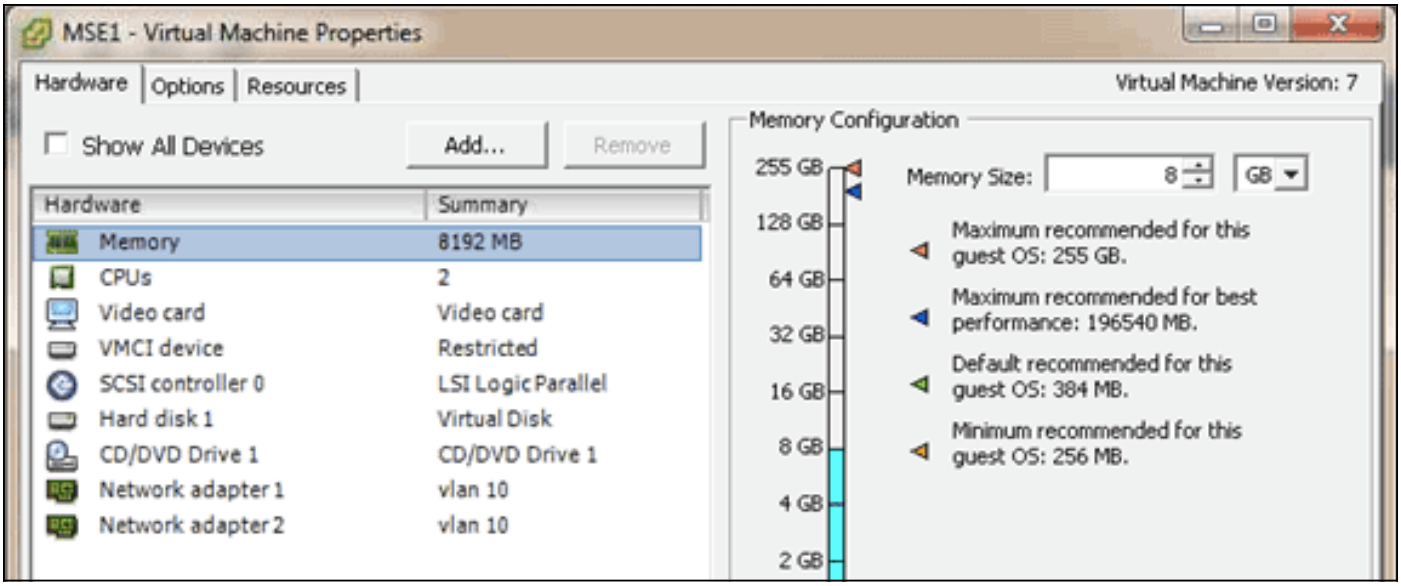


Die Bereitstellung des Images dauert in Abhängigkeit von der Netzwerkgeschwindigkeit einige Minuten. Nach der Bereitstellung können Sie die Konfiguration des virtuellen Systems (VM) bearbeiten, um die Appliance zu konfigurieren. die VM sollte bei der Konfiguration ausgeschaltet werden.

Konfigurieren der MSE Virtual Appliance-Ebenen

In der Tabelle in diesem Abschnitt sind die für die virtuelle Appliance konfigurierbaren Ebenen und die entsprechenden Ressourcenanforderungen aufgeführt. Weisen Sie der Appliance dedizierte Kerne zu, nicht die Hyper-Threading-virtuellen Kerne, da dies sich auf die Leistung auswirkt, wenn Sie davon ausgehen, dass der Host mehr virtuelle Kerne hat und mehr Appliances bereitstellen. In dem oben genannten UCS C200 sind beispielsweise acht (8) physische Kerne verfügbar, aber sechzehn (16) virtuelle Kerne mit Hyper-Threading. Gehen Sie nicht davon aus, dass sechzehn (16) Kerne verfügbar sind. nur acht (8) Kerne zuweisen, um sicherzustellen, dass die MSE bei Stress zuverlässig funktioniert.

Primäre MSE	Ressourcen	Unterstützte Lizenz(einzeln)		Unterstützte sekundäre MSE	
Virtuelle Appliance-Ebene	Gesamter Speicher	CAS-Lizenz	wIPS-Lizenz	Virtuelle Appliance	Gehäuse
Niedrig	6 G	2000	2000	Niedrig+	Nicht unterstützt
Standard	11 G	18.000	5000	Standard+	
Hoch	20 G	50000	10.000	Hoch+	



Einrichten der MSE Virtual Appliance

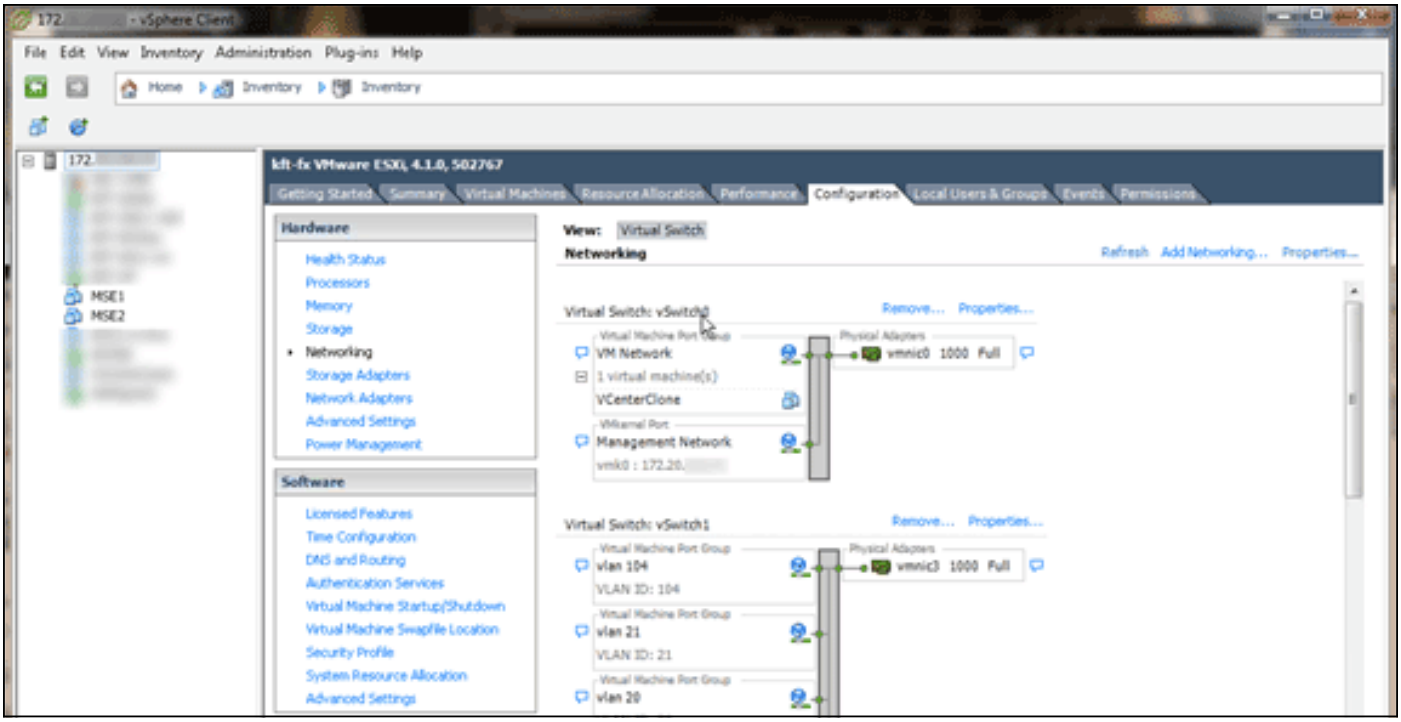
Nachdem die virtuelle Appliance bereitgestellt und konfiguriert wurde, können Sie sie hochfahren. Wenn die Appliance zum ersten Mal hochgefahren wird, müssen Sie die Standardanmeldeinformationen eingeben: root/password.

Bei der ersten Anmeldung beginnt die Appliance mit der Konfiguration der MSE-Software und installiert außerdem die Oracle-Datenbank. Dies ist ein einmaliger, zeitaufwendiger Prozess, der mindestens 30-40 Minuten in Anspruch nehmen wird. Nach Abschluss der Installation wird die Anmeldeaufforderung erneut angezeigt. Lesen Sie den Abschnitt Konfiguration der Mobility Services Engine im *Cisco 3355 Mobility Services Engine - Erste Schritte*, um mit der Konfiguration der Appliance fortzufahren.

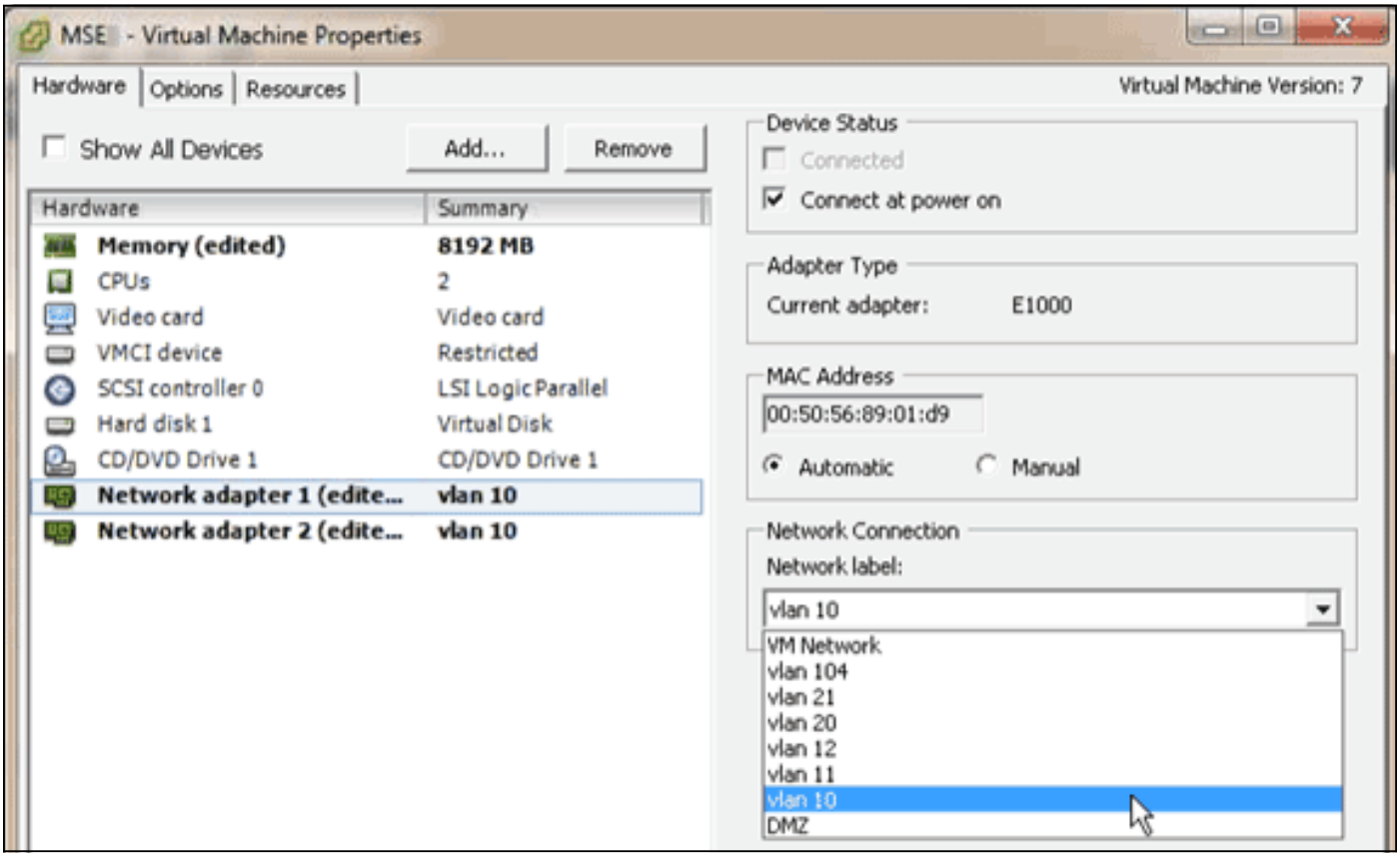
Konfigurieren des Netzwerks

Standardmäßig verwenden VMs die Host-Netzwerkeinstellungen. Daher müssen Sie die VM-Adapter nicht auf ESXi konfigurieren. Wenn jedoch sowohl öffentliche als auch private Netzwerke mit dem Host verbunden sind und die VMs Zugriff auf beide haben sollen, können Sie die VM-Adapter im vShare-Client konfigurieren.

Wählen Sie im vSphere-Client den Host aus, klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Networking**. Sie können die physischen Adapter in den Eigenschaften des virtuellen Switches anzeigen.



Erstellen Sie separate Switches mit separaten Adaptern, um die Netzwerke zu isolieren. Anschließend können Sie die VM-Adapter nach Bedarf diesen Netzwerken zuweisen.



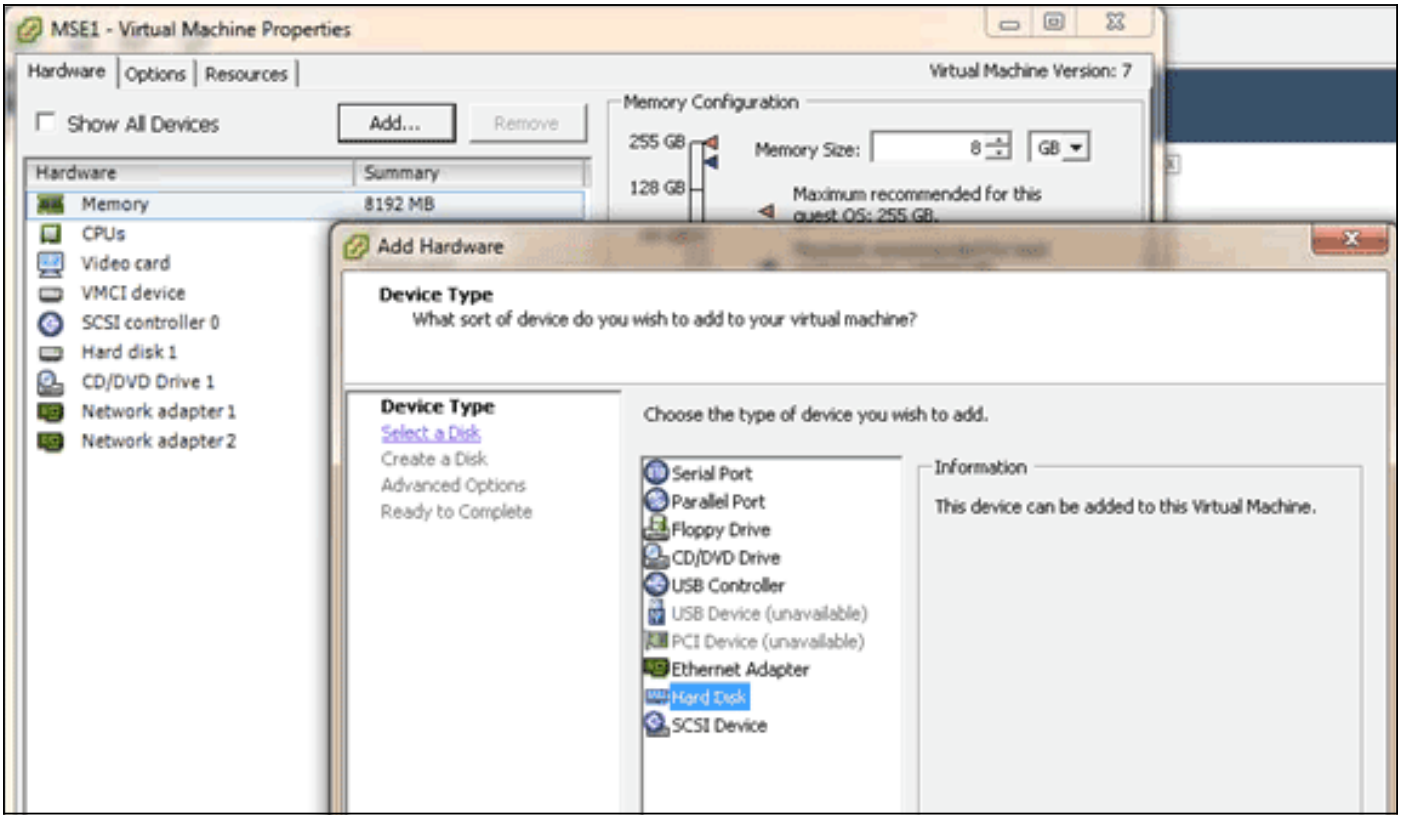
Hinzufügen von Festplattenspeicherplatz

Fügen Sie ggf. der VM zusätzliche Festplattenkapazität hinzu, und erweitern Sie die Partitionen.

Hinweis: Das installDrive.sh-Skript (befindet sich im Verzeichnis /opt/mse/framework/bin) erkennt neue Laufwerke und partitioniert vorhandene Partitionen neu, um die neuen Laufwerke zu verwenden und zu erweitern.

Stellen Sie sicher, dass Sie Ihre VM (oder zumindest die MSE-Daten) sichern, bevor Sie versuchen, den Speicherplatz neu zu partitionieren.

Um Ihrer VM mehr Speicherplatz hinzuzufügen, fahren Sie die VM herunter, gehen Sie zu den VM-Einstellungen, und fügen Sie die zusätzliche Festplatte hinzu.

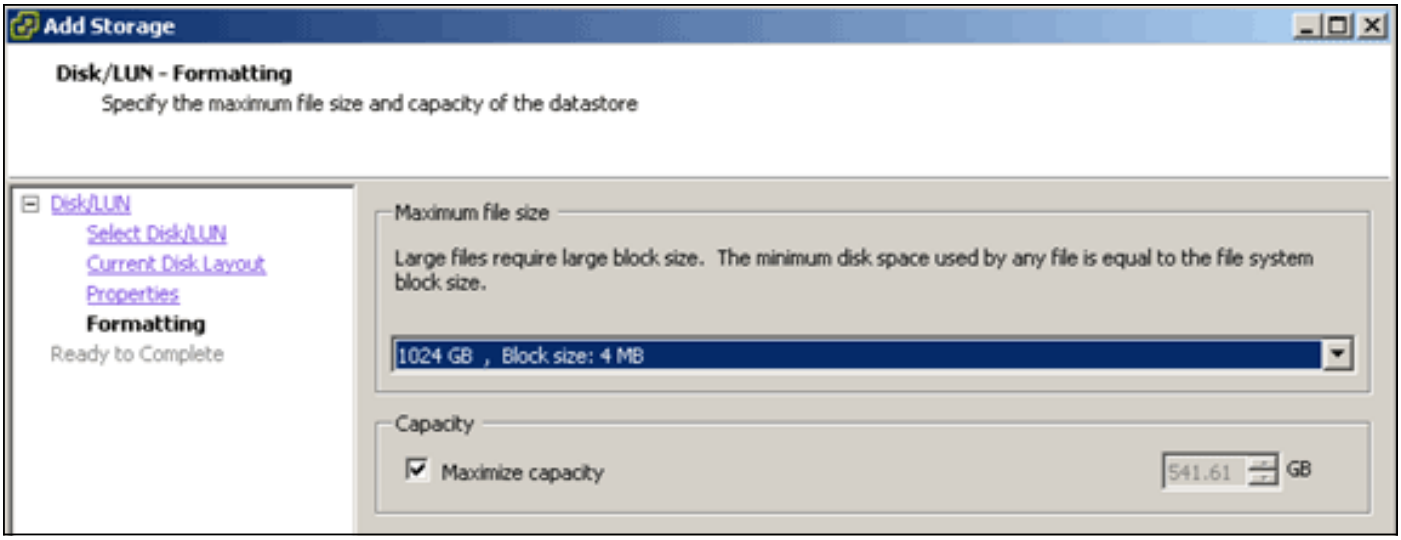


Schalten Sie nach dem Hinzufügen der Festplatte das virtuelle System ein, melden Sie sich bei der Einheit an, und führen Sie das Skript installDrive.sh aus. Das Skript sollte das neu hinzugefügte Laufwerk bereitstellen und neu partitionieren. Wenn Sie mehrere Festplatten hinzugefügt haben, führen Sie das Skript einmal für jedes neue Laufwerk aus.

Blockgröße

Für ESXi-Versionen vor 5.0 empfiehlt Cisco, dass der Datenspeicher auf dem Host eine Blockgröße von 4 MB oder mehr hat. Andernfalls kann die Bereitstellung der OVA fehlschlagen. Wenn die Bereitstellung fehlschlägt, können Sie die Blockgröße neu konfigurieren.

Um die Blockgröße neu zu konfigurieren, gehen Sie zu ESX-Hostkonfiguration > Speicher > Löschen Sie die Datenspeicher, und fügen Sie den Speicher erneut zu den neuen Datenspeichern mit einer Blockgröße von mindestens 4 MB hinzu.



VMware-Tools

Wenn die VM den folgenden Fehler auslöst, klicken Sie mit der rechten Maustaste auf die VM im vSphere-Client, und wählen Sie **Guest > Install/Upgrade VMware Tools**, um die VMware-Tools zu installieren oder zu aktualisieren:

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

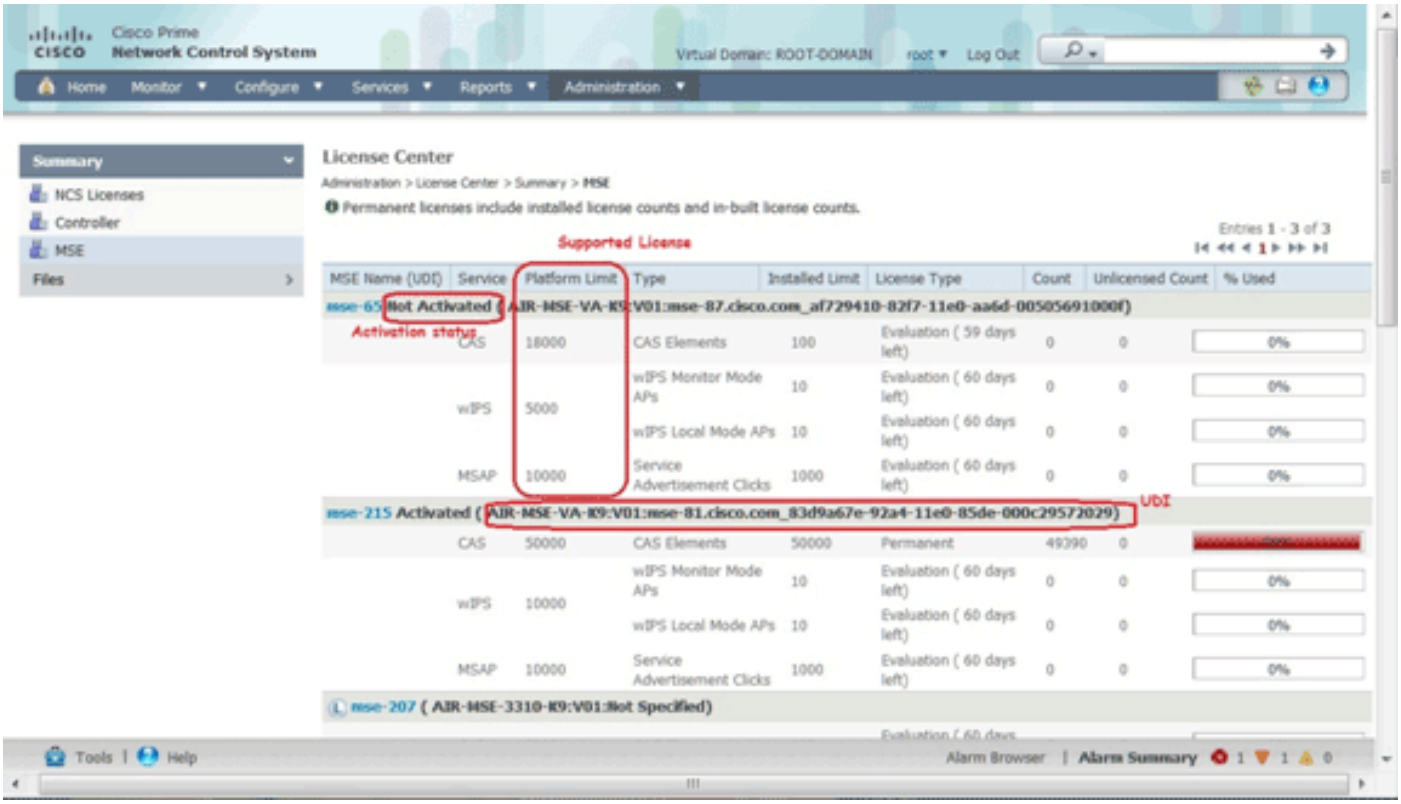
Aktualisieren der virtuellen Appliance

Nachdem Sie die virtuelle Appliance konfiguriert haben, sollte sie wie eine physische MSE-Box behandelt werden. Sie müssen nicht jedes Mal eine neue OVA bereitstellen, wenn Sie ein Upgrade auf die neueste MSE-Version durchführen möchten. Sie können das entsprechende Installationsprogramm-Image auf die Appliance herunterladen und die Schritte für ein Upgrade befolgen, wie dies bei einer physischen Appliance der Fall ist.

Lizenzierung der virtuellen Appliance

Nachdem Sie die virtuelle Appliance konfiguriert haben, kann sie im Evaluierungsmodus (standardmäßig 60 Tage) verwendet werden, ohne die Appliance zu lizenzieren. Sie müssen die virtuelle Appliance jedoch mithilfe einer Virtual Appliance-Aktivierungslizenz aktivieren, wenn Sie permanente Lizenzen bereitstellen oder Funktionen wie Hochverfügbarkeit (HA) verwenden möchten. Sie können den Unique Device Identifier (UDI) von der virtuellen Appliance (**show csludi** auf der Appliance ausführen) oder von den allgemeinen Eigenschaften der Cisco Prime Network Control System (NCS) MSE abrufen und diese Informationen verwenden, um die Aktivierungslizenz für virtuelle Appliances und permanente Service-Lizenzen zu erwerben.

Dieses Bild zeigt die kürzlich vorgenommenen Änderungen an der Benutzeroberfläche des Lizenzcenters für die virtuelle Appliance.



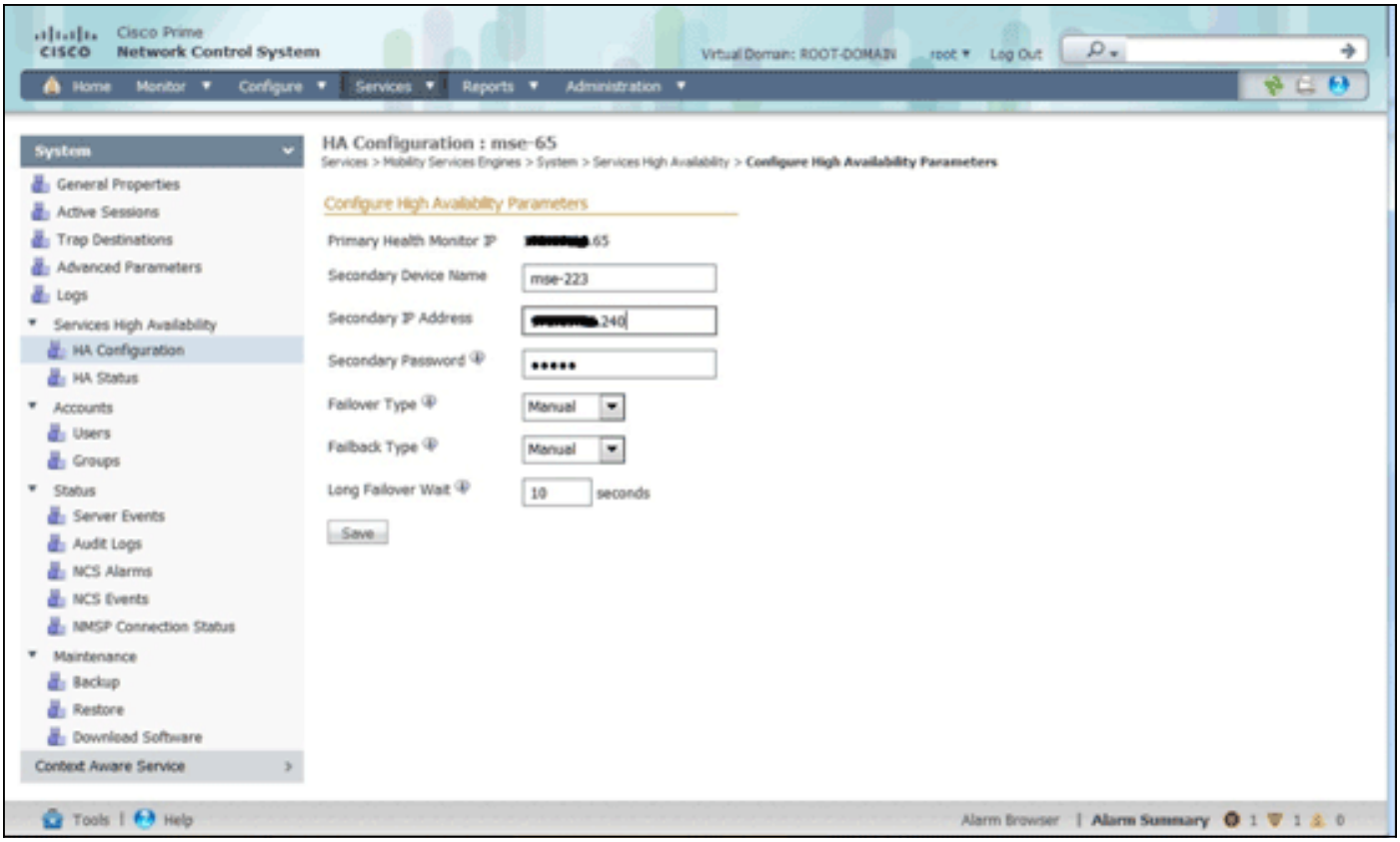
Für die virtuelle Appliance gibt eine Meldung neben dem MSE-Namen deutlich an, ob sie aktiviert ist. Darüber hinaus gibt es zwei Begrenzungsspalten: In der Spalte "Platform Limit" (Plattformbeschränkung) wird die maximal unterstützte Lizenz für diesen Dienst auf dieser Appliance (abhängig von der Ressourcenzuweisung an die VM) und in der Spalte "Installed Limit" (Installierte Grenze) die tatsächlich installierte oder durch Auswertung auf der Appliance verfügbare Lizenz aufgelistet.

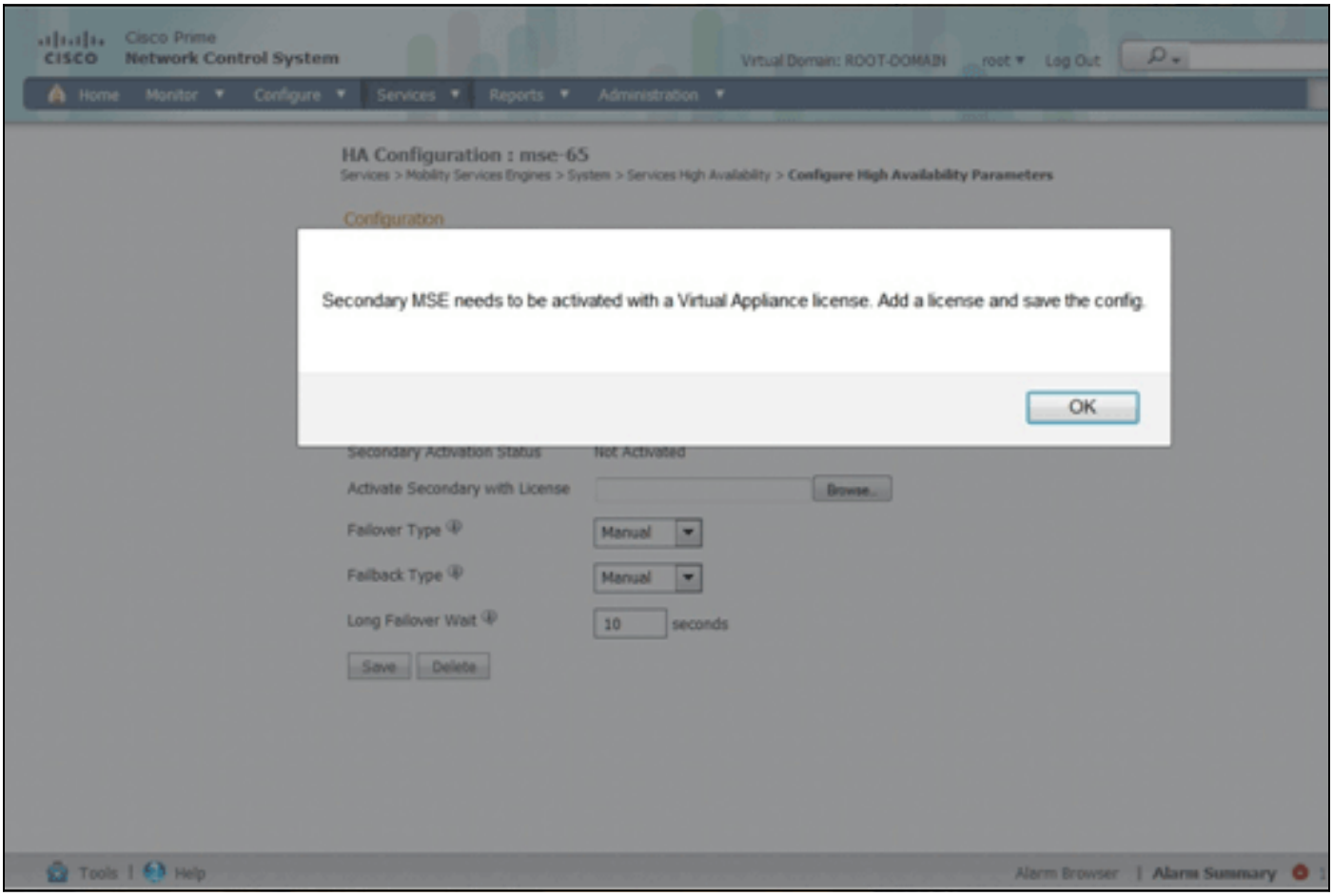
Hohe Verfügbarkeit auf der virtuellen Appliance

Um die HA-Funktion nutzen zu können, müssen sowohl die primären als auch die sekundären Appliances mit einer Aktivierungslizenz für virtuelle Appliances aktiviert werden.

Konfiguration der Hochverfügbarkeit

Sie können die HA-Konfiguration über die primäre MSE im NCS einrichten.

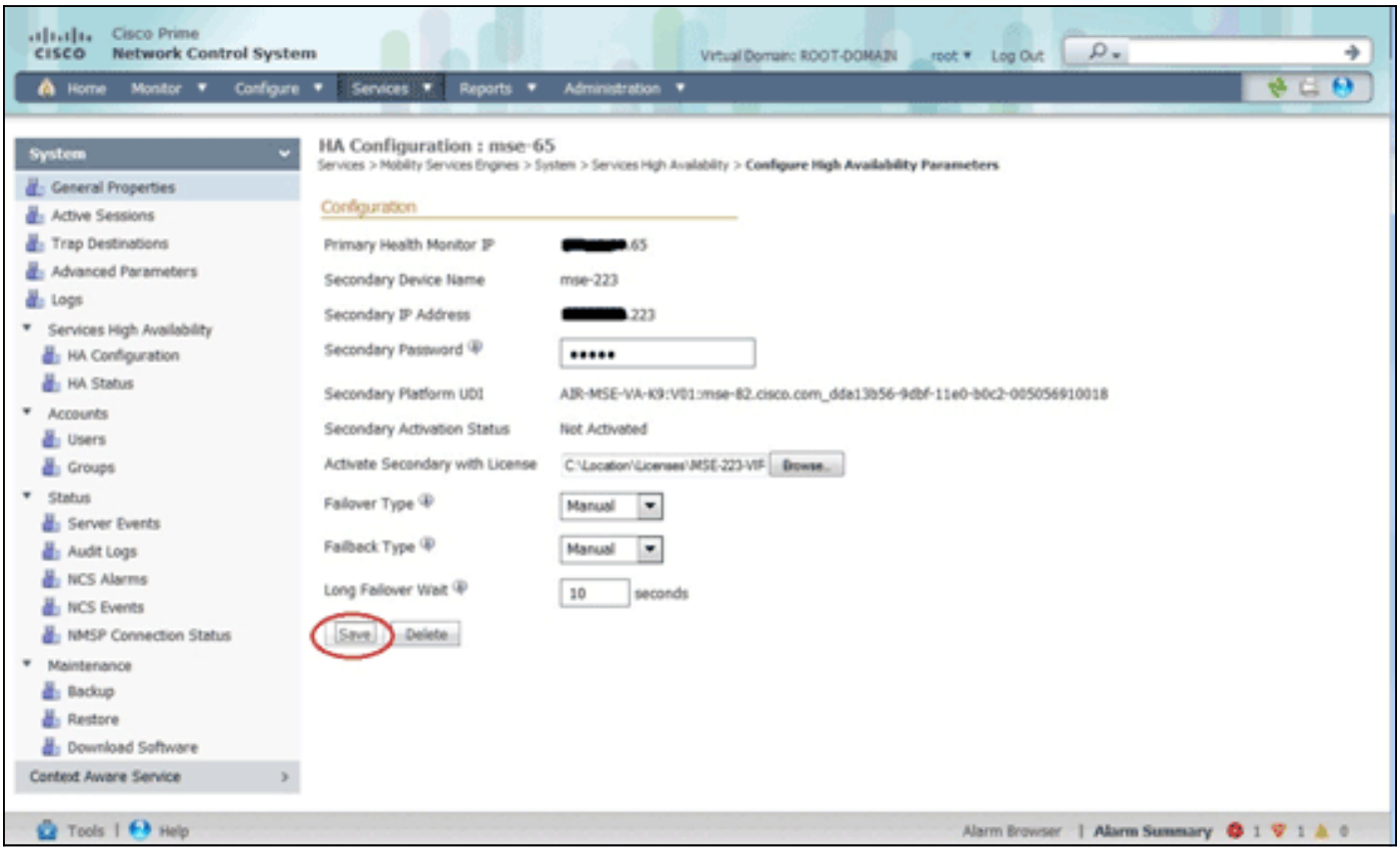




Aktivieren der sekundären MSE

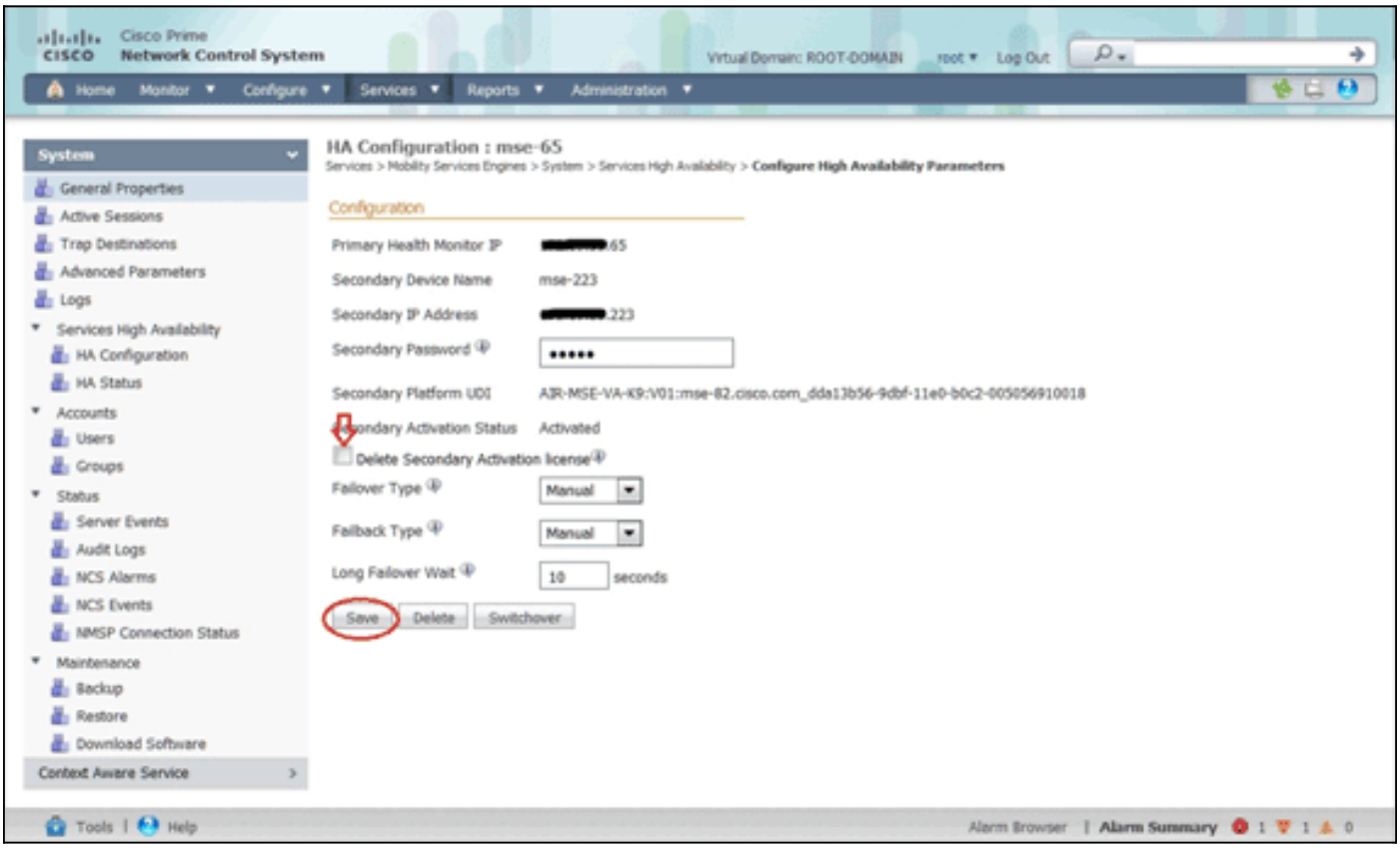
Die sekundäre Appliance muss aktiviert werden. Sie können die UDI-Informationen verwenden, um eine Aktivierungslizenz für die sekundäre MSE anzufordern. Suchen Sie auf der Seite HA-Konfiguration nach der Lizenz, und klicken Sie auf **Speichern**. HA wird eingerichtet, sobald die

sekundäre MSE erfolgreich aktiviert wurde.



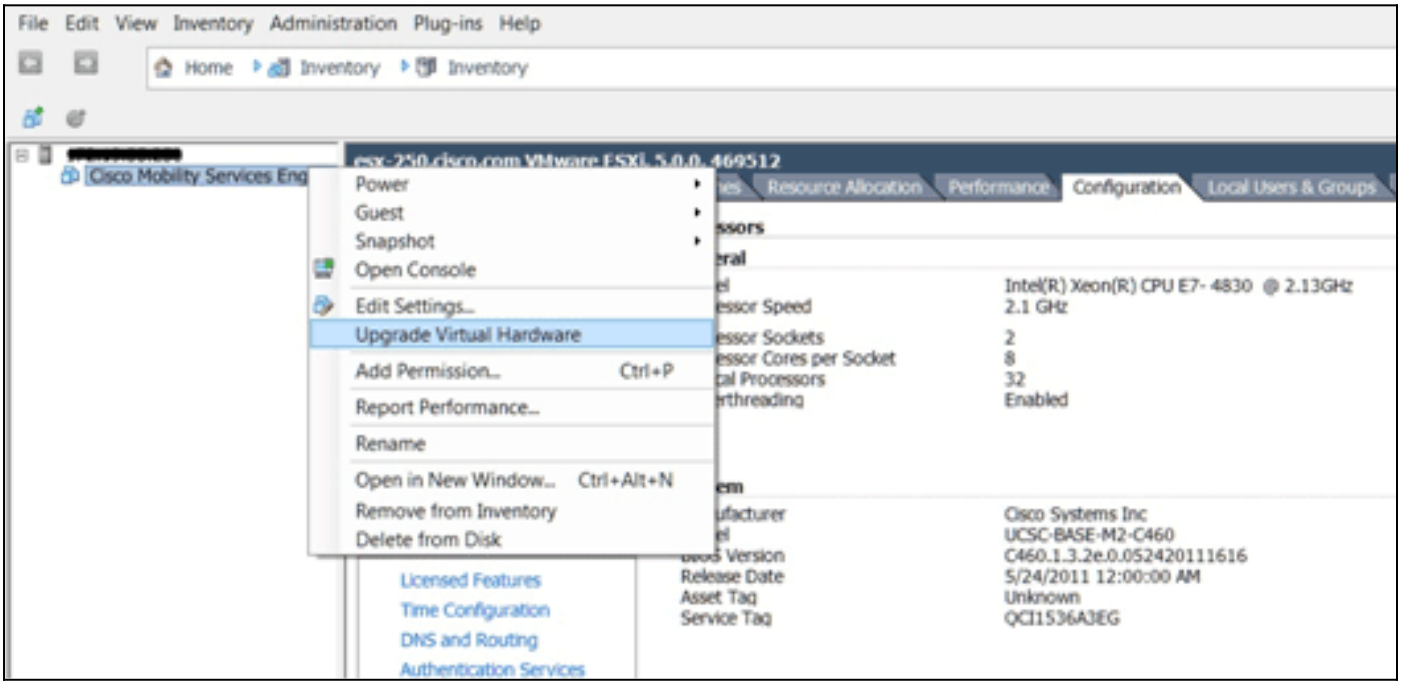
Deaktivieren der sekundären MSE

Falls Sie die Aktivierungslizenz von der sekundären MSE löschen müssen, können Sie auf das Kontrollkästchen klicken und auf **Speichern** klicken, um die sekundäre MSE zu deaktivieren.



Virtuelle Appliance auf ESXi 5.0

Beim ESXi 5.0 ist die Blockgröße auf 1 MB festgelegt, da große VM-Bereitstellungen unterstützt werden. Um der virtuellen Appliance mehr als acht (8) Kerne zuweisen zu können, müssen Sie die virtuelle Hardware aktualisieren. Um die virtuelle Hardware zu aktualisieren, wählen Sie die MSE aus, und wählen Sie **Upgrade Virtual Hardware (Virtuelle Hardware aktualisieren)** aus, wie in diesem Image gezeigt:



MSE-Konsolenverfahren

1. Melden Sie sich mit den folgenden Anmeldeinformationen bei der Konsole an: root/password.Beim erstmaligen Booten fordert die MSE den Administrator auf, das Setup-Skript zu starten.
2. Geben Sie **yes** für diese Eingabeaufforderung ein.

```
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]: _
```

Hinweis: Wenn die MSE nicht zur Einrichtung auffordert, geben Sie den folgenden Befehl ein: /opt/mse/setup/setup.sh

3. Konfigurieren Sie den Hostnamen:

```
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. Konfigurieren Sie den DNS-Domänennamen:

```
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. Konfigurieren Sie die primäre HA-Rolle:

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

6. Ethernet-Schnittstellenparameter konfigurieren:

```
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. Wenn Sie zur Eingabe der eth1-Schnittstellenparameter aufgefordert werden, geben Sie **Überspringen ein**, um mit dem nächsten Schritt fortzufahren, da für den Betrieb keine zweite NIC erforderlich ist.

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

Hinweis: Die konfigurierte Adresse muss IP-Verbindungen zu den in dieser Appliance

verwendeten perspektivischen WLCs und WCS Management System bereitstellen.

8. Geben Sie DNS-Server-Informationen ein. Für eine erfolgreiche Domänenauflösung ist nur ein DNS-Server erforderlich. Geben Sie zur Gewährleistung der Ausfallsicherheit Backup-Server
   ein.

```
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. Konfigurieren Sie die Zeitzone. Cisco empfiehlt, UTC (koordinierte universelle Zeit) zu verwenden.Wenn die standardmäßige Zeitzone von New York nicht für Ihre Umgebung anwendbar ist, suchen Sie in den Standortmenüs nach der richtigen
   Zeitzone.

```
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. Wenn Sie aufgefordert werden, den zukünftigen Neustart zu konfigurieren, geben Sie **Überspringen**
    ein.

```
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. Konfigurieren Sie ggf. den Remote-Syslog-
    Server.

```
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. Konfigurieren Sie das Network Time Protocol (NTP) oder die Systemzeit.NTP ist optional, gewährleistet jedoch, dass Ihr System die korrekte Systemzeit erhält. Wenn Sie NTP aktivieren, wird die Systemzeit von den ausgewählten NTP-Servern konfiguriert. Andernfalls werden Sie aufgefordert, das aktuelle Datum und die Uhrzeit
    einzugeben.

```
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. Wenn Sie aufgefordert werden, das Anmeldebanner zu konfigurieren, geben Sie **Überspringen** ein.

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

14. Aktivieren Sie die lokale Konsolenroot-Anmeldung.Dieser Parameter wird verwendet, um den lokalen Konsolenzugriff auf das System zu aktivieren/deaktivieren. Die lokale Konsolenroot-Anmeldung sollte aktiviert sein, damit eine lokale Fehlerbehebung möglich ist. Der Standardwert ist Überspringen.

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

15. Aktivieren Sie Secure Shell (SSH)-Root-Anmeldung.Dieser Parameter wird verwendet, um den Remote-Konsolenzugriff auf das System zu aktivieren/deaktivieren. Die SSH-Root-Anmeldung sollte aktiviert werden, damit eine Remote-Fehlerbehebung durchgeführt werden kann. Sicherheitsrichtlinien des Unternehmens erfordern jedoch möglicherweise, dass diese Option deaktiviert wird.

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

16. Konfigurieren Sie den Modus für einen einzelnen Benutzer und die Kennwortstärke.Diese Konfigurationsparameter sind nicht erforderlich. Der Standardwert ist Überspringen.

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

17. Ändern Sie das Root-Kennwort.Dieser Schritt ist entscheidend für die Gewährleistung der Systemsicherheit. Wählen Sie unbedingt ein sicheres Kennwort aus Buchstaben und Zahlen ohne Wörterbuchwörter. Die Kennwortlänge beträgt mindestens acht (8) Zeichen. Die Standardanmeldeinformationen sind root/password.

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

18. Konfigurieren Sie die Parameter für Anmeldung und Kennwort:

```
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. Konfigurieren Sie ein Boot-Passwort (Grub). (*Optional*)Dieser Konfigurationsparameter ist nicht erforderlich. Der Standardwert ist Überspringen.

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

20. Konfigurieren Sie den NCS-Kommunikations-Benutzernamen.

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

21. Nehmen Sie die Änderung der Konfiguration an.

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

Dieses Bild zeigt ein Beispiel für den Abschlussbildschirm:

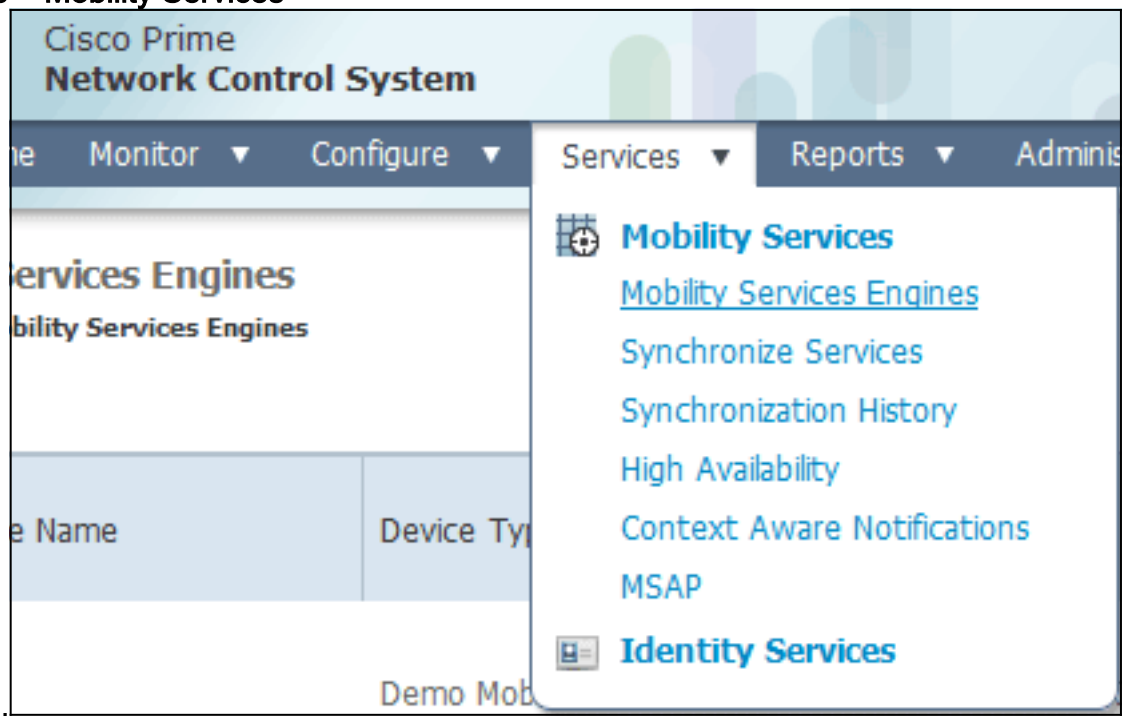
```
Stopping MSE Platform
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: nat filter                [  OK  ]
Unloading iptables modules: Removing netfilter NETLINK layer.
                                                           [  OK  ]
ip_tables: (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. Führen Sie den Befehl **getserverinfo** aus, um die Konfiguration zu überprüfen.

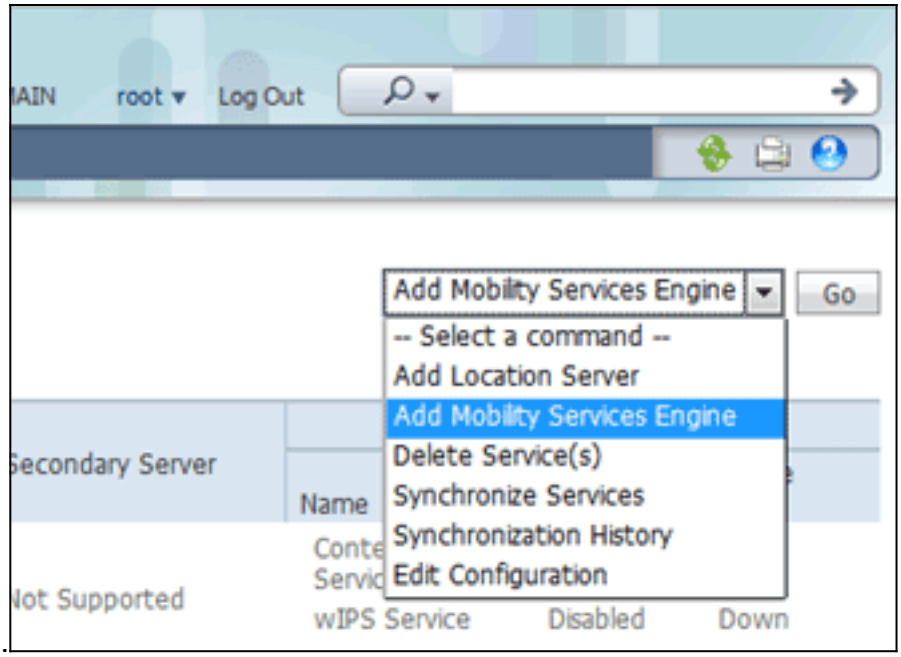
```
Active Wired Clients: 0
Active Elements(Wireless Clients, Rogue APs, Rogue Clients,
lients, Tags) Limit: 115
Active Sessions: 1
Wireless Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogue APs Not Tracked due to the limiting: 0
Rogue Clients Not Tracked due to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

Hinzufügen von MSE VA zum NCS

1. Melden Sie sich beim NCS an, und wählen Sie **Services > Mobility Services Engines (Services > Mobility Services Engines)**.

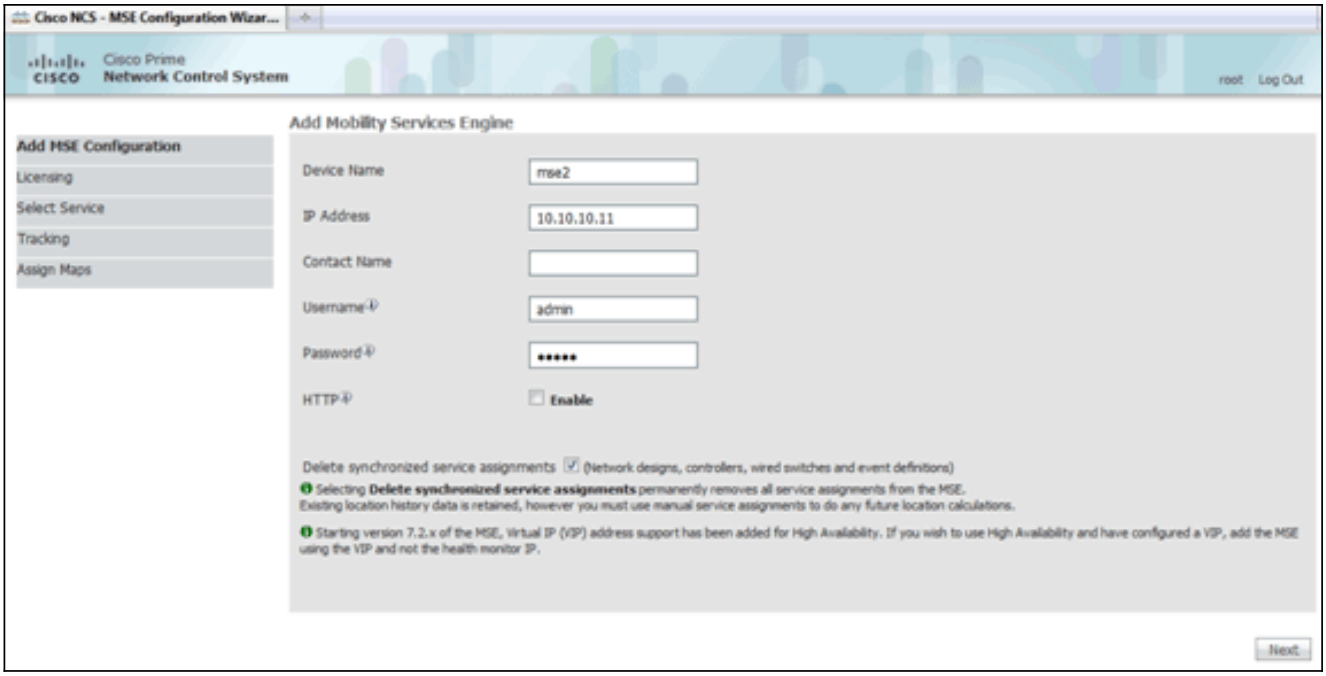


2. Wählen Sie aus der Dropdown-Liste rechts auf der Seite die Option **Add Mobility Services Engine (Engine für Mobilitätsdienste hinzufügen) aus**, und klicken Sie auf **Go**

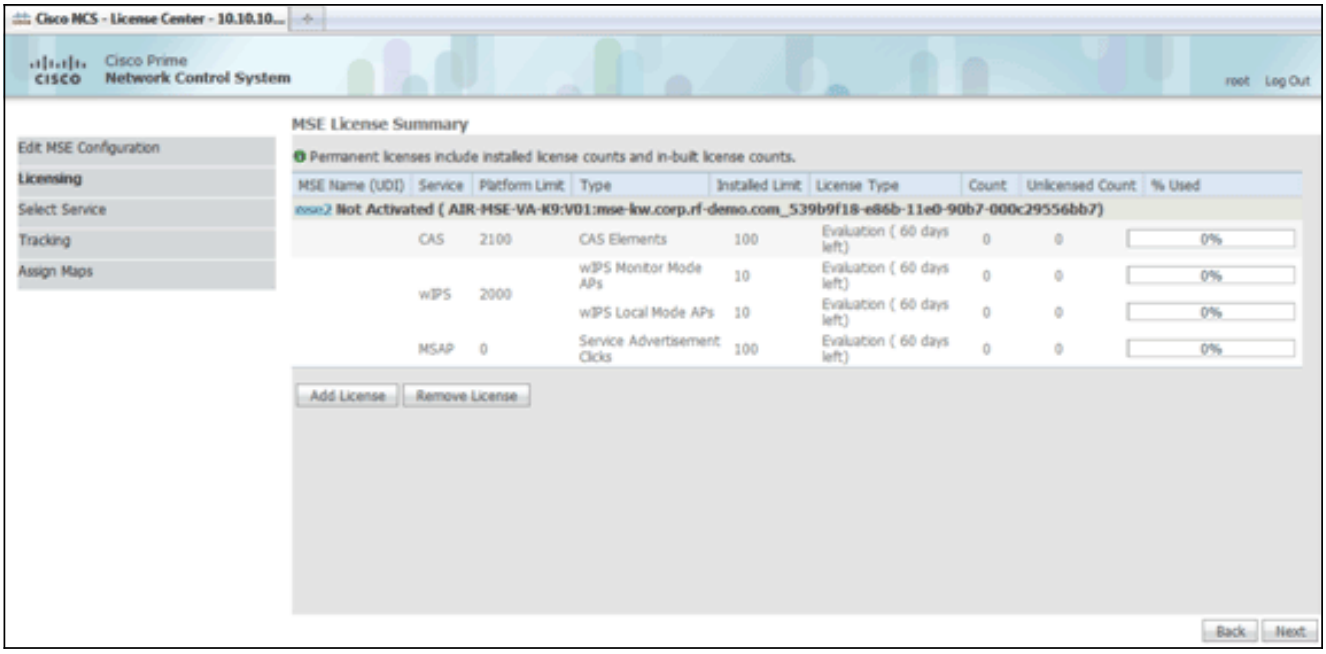


(Los).

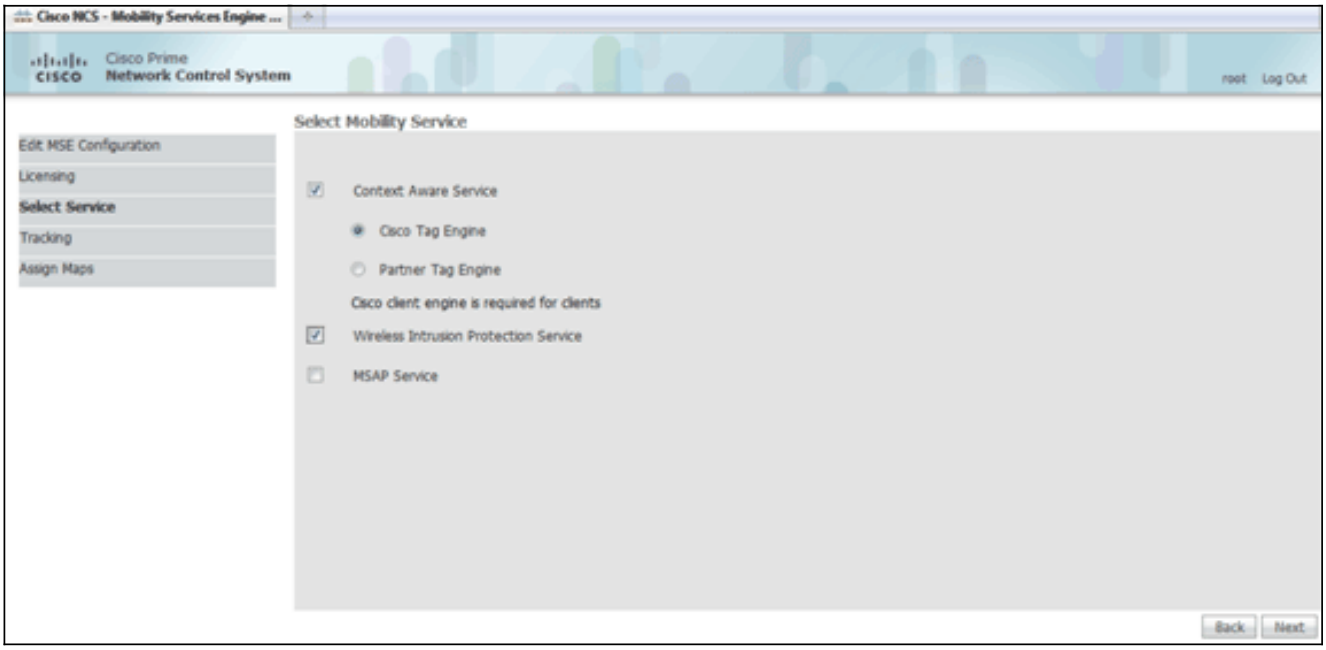
3. Geben Sie einen eindeutigen Gerätenamen für die MSE, die IP-Adresse, die zuvor während der MSE-Einrichtung konfiguriert wurde, und einen Kontaktnamen für den Support ein. sowie den während der MSE-Einrichtung konfigurierten Benutzernamen und das Kennwort für das NCS.Ändern Sie den Benutzernamen nicht von der Standardeinstellung *admin*. Sie können die Standardeinstellung
verlassen.



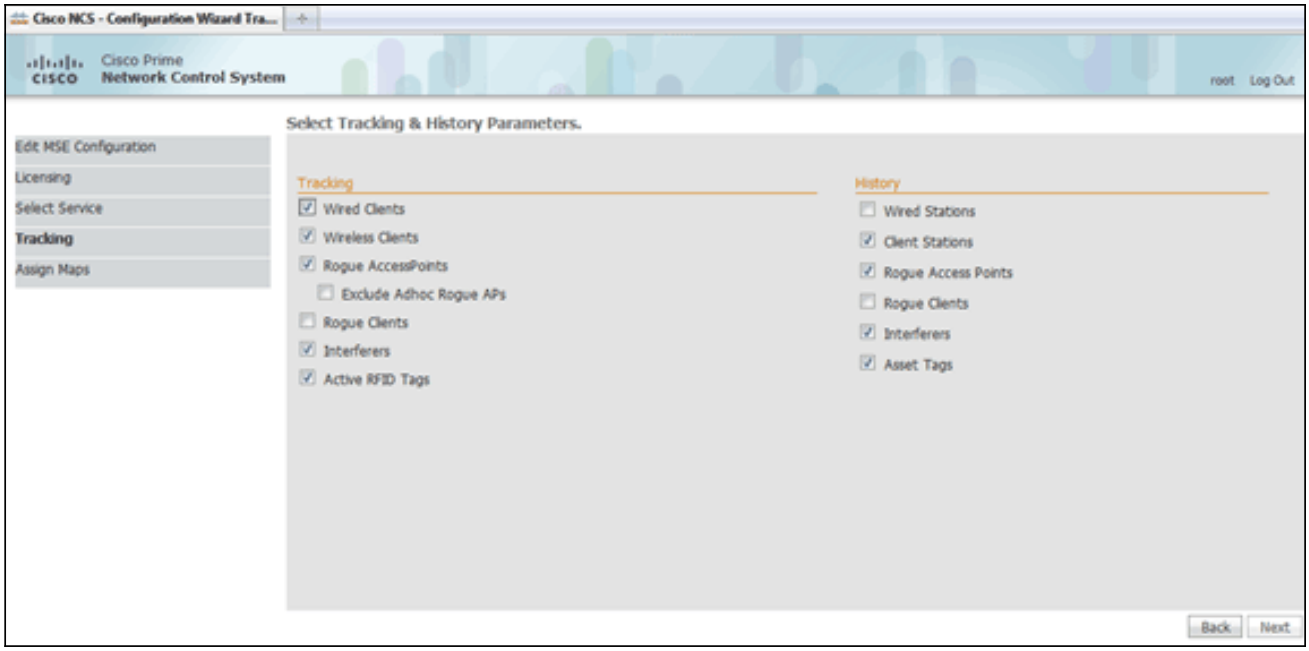
4. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Lizenzierung**, und überprüfen Sie die Lizenzierung. Bei der Installation reicht die Standard-Demolizenz für das Testen aus. Auf der Lizenzierungsseite können Sie weitere erworbene Lizenzen hinzufügen oder Lizenzen
entfernen.



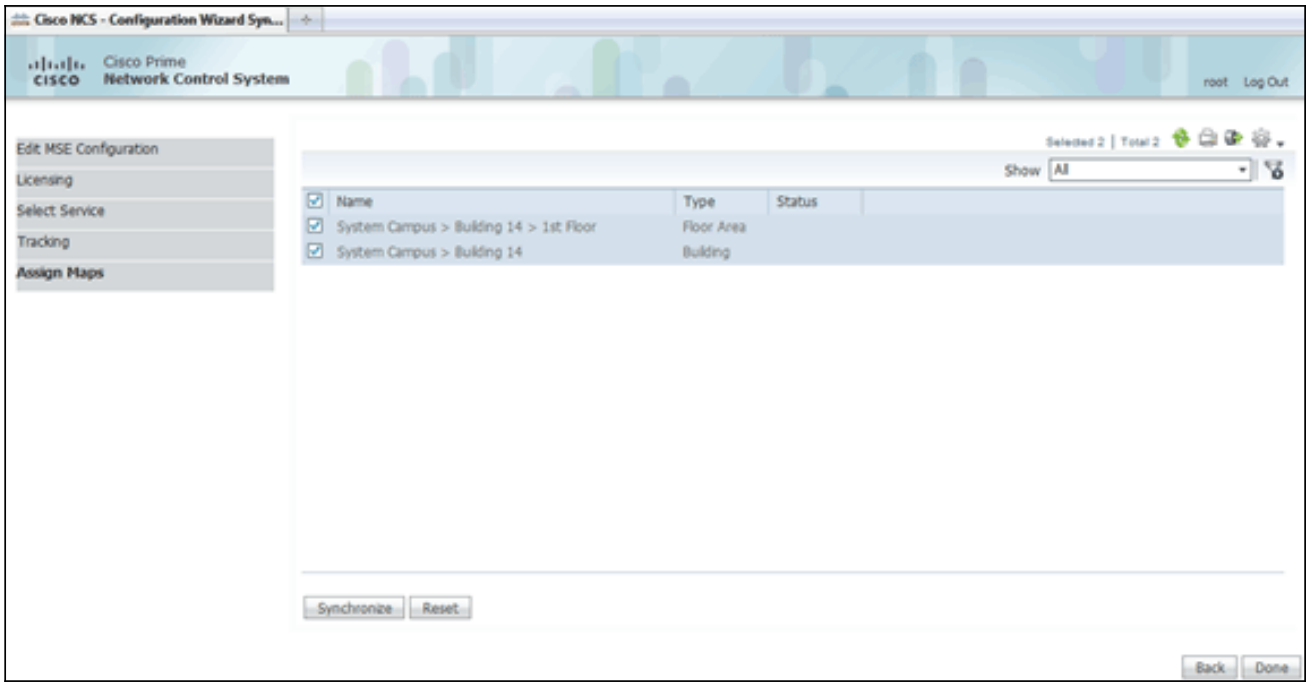
6. Klicken Sie auf **Weiter**.



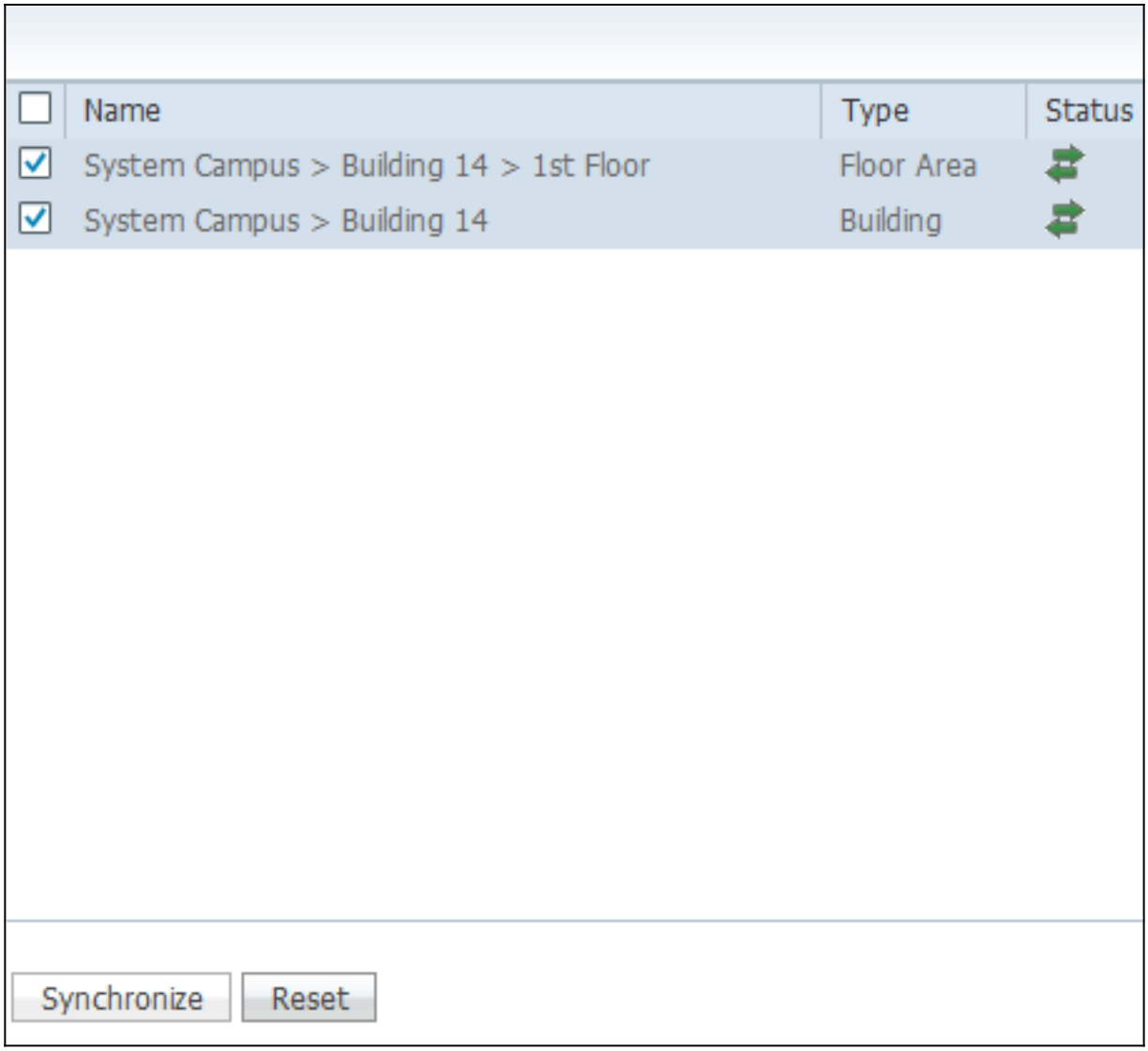
7. Klicken Sie auf der Seite "Select Mobility Service" (Mobility-Service auswählen) auf das Optionsfeld **Cisco Tag Engine** (verfügbar seit 7.0 MR) (für Client- und RFID-Tag-Unterstützung), oder klicken Sie auf das Optionsfeld **Partner Tag Engine** (für Aeroscout usw.).
8. Klicken Sie auf das Kontrollkästchen **Wireless Intrusion Protection Service**, um die wIPS-Sicherheitsfunktion des Überwachungsmodus und der Funktionen des erweiterten lokalen Modus zu testen.
9. Klicken Sie auf **Weiter**.
10. Aktivieren Sie die Kontrollkästchen für Elemente, die für die Nachverfolgung aktiviert werden sollen, und für Verlaufsparameter für diese Elemente, die für Verlaufsberichte verfügbar sein
    sollen.



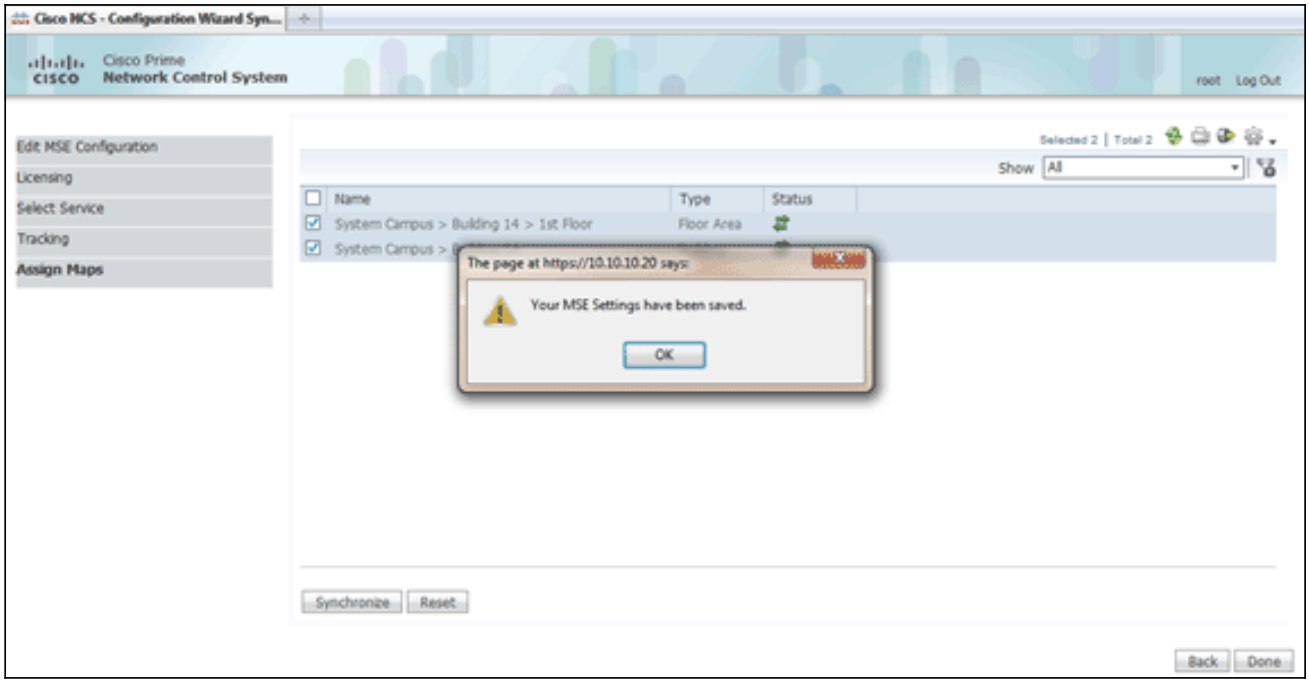
11. Klicken Sie auf **Weiter**.



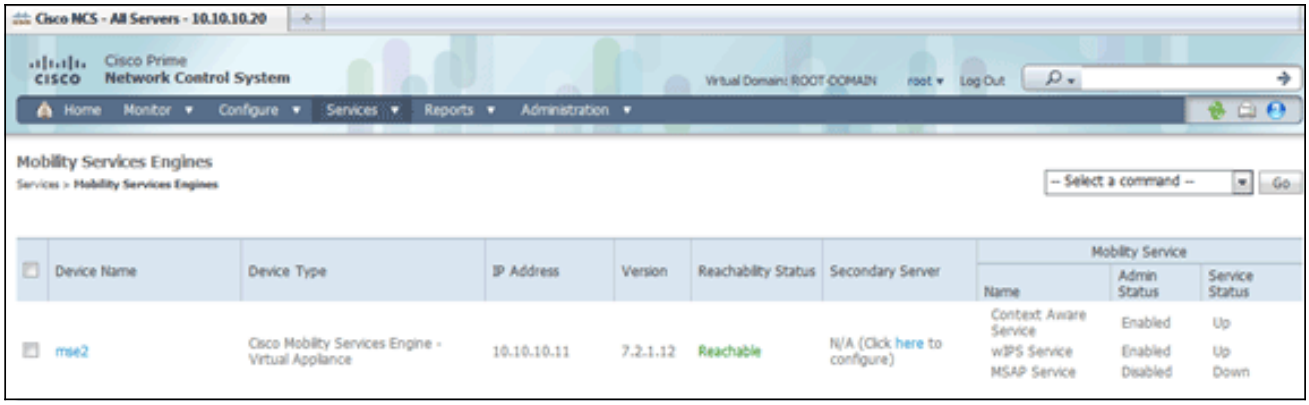
12. Aktivieren Sie die Kontrollkästchen für das vorhandene Gebäude und die vorhandene Etage, und klicken Sie auf **Synchronisieren**.Nach der Synchronisierung wird die Statusspalte aktualisiert, um anzuzeigen, dass das anfängliche Netzwerkdesign synchronisiert
wurde.



13. Wenn die Synchronisierung abgeschlossen ist, klicken Sie auf **Fertig**.Es wird ein Dialogfeld angezeigt, in dem die MSE-Einstellungen gespeichert wurden.

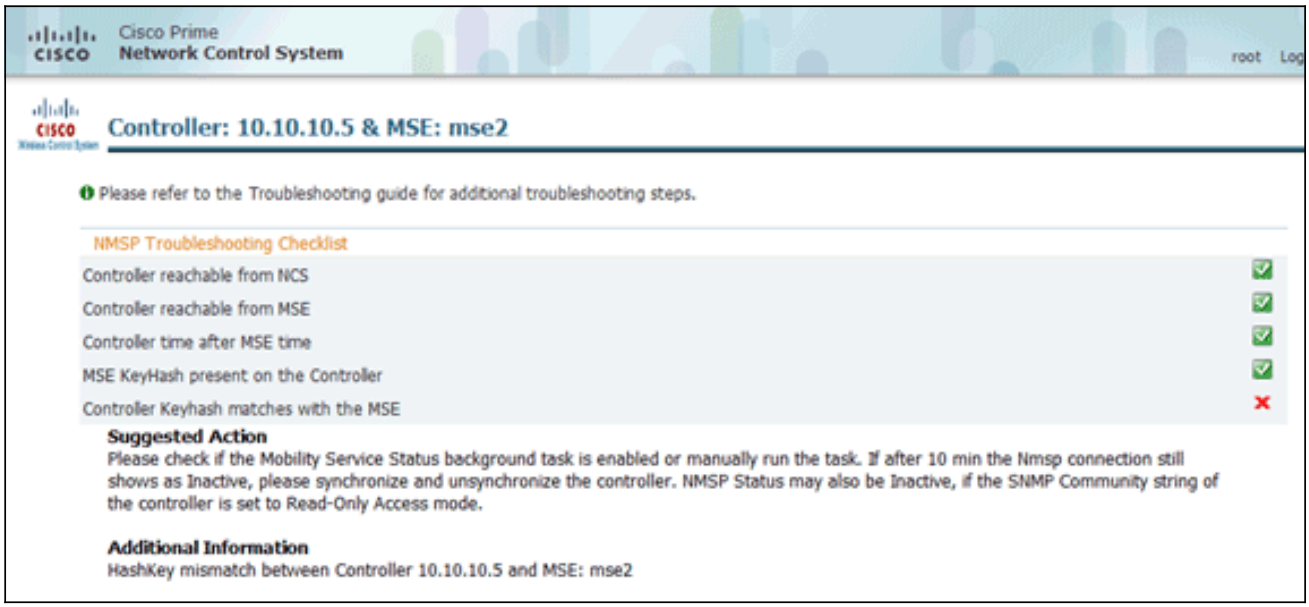


14. Bestätigen Sie die Konfiguration auf der Haupt-MSE-Seite des NCS.



Stellen Sie sicher, dass die übrigen Netzwerkdesigns, Controller, kabelgebundenen Switches und Ereignisgruppen, soweit verfügbar, synchronisiert werden.**Hinweis:** Der Cisco Context-Aware Service ist in hohem Maße von einer synchronisierten Uhr zwischen WLC, NCS und MSE abhängig. Wenn alle drei Systeme nicht auf denselben NTP-Server zeigen und mit denselben Zeitzoneneinstellungen konfiguriert sind, funktioniert der kontextsensitive Dienst nicht ordnungsgemäß. Bevor Sie Fehlerbehebungsverfahren durchführen, stellen Sie sicher, dass die Systemuhr für alle Komponenten des kontextsensitiven Systems identisch ist.

15. Überprüfen Sie die MSE- und Controller-Kommunikation für ausgewählte Services.Stellen Sie sicher, dass die MSE nur für den ausgewählten Service mit den einzelnen Controllern kommuniziert. Der Status des Network Mobility Service Protocol (NMSP) muss *aktiv* sein.Dieses Bild enthält ein Beispiel dafür, wie der Tastenanschlag nicht zum WLC hinzugefügt
wird.



Verwenden Sie auf der WLC-Konsole den Befehl **show auth-list**.Das folgende Beispiel zeigt von der WLC-Konsole, dass kein Standortserver verfügbar
ist:

```
(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
```

G

ehen Sie wie folgt vor, um die MSE manuell hinzuzufügen und eine NMSP-Verbindung zum WLC herzustellen:Führen Sie auf der MSE-Konsole den Befehl **cmdshell** und anschließend den Befehl **show server-auth-info aus**.Dieses Beispiel zeigt die MAC-Adresse und den Tastenanschlag, der zum Hinzufügen zum WLC verwendet werden soll.

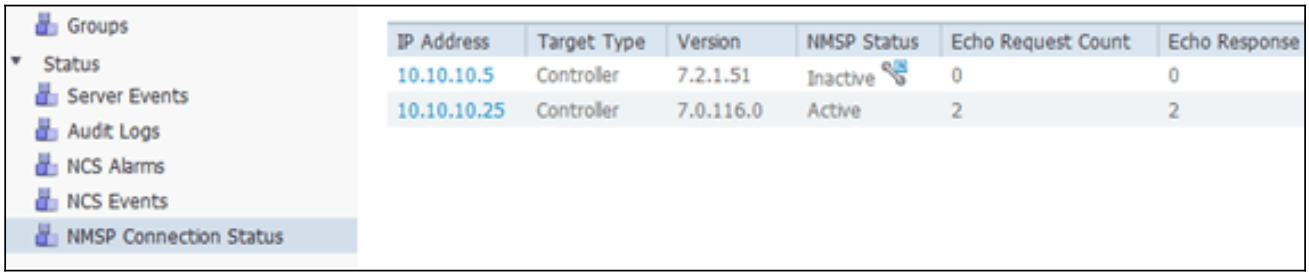
```
cmd> show server-auth-info
invoke command: com.aes.server.cli.CmdGetServerAuthInfo
----------------
Server Auth Info
----------------
MAC Address: 00:0c:29:55:6b:b7
Key Hash: 1469187db14ac53ac6108e56b04d48015bdd70d7
Certificate Type: SSC
```

F

ühren Sie den Befehl **config auth-list add ssc <*mac address*> <*MSE keyhash*>** aus, und führen Sie dann den Befehl **show auth-list aus**.Dieses Beispiel zeigt, dass die MSE dem WLC (manuell) hinzugefügt
wurde.

```
(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
```

Überprüfen Sie auf dem NCS, ob die NMSP-Verbindung als *aktiv* angezeigt
wird.



Befehlszeilenreferenz

WLC-Befehle

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
```

MSE-Befehle

Führen Sie diesen Befehl aus, um den Status der MSE-Dienste zu bestimmen:

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

Führen Sie diesen Befehl aus, um die kontextsensitive Engine für die Client-Nachverfolgung zu starten:

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

Führen Sie diesen Befehl aus, um den Status der kontextsensitiven Engine für die Client-Nachverfolgung zu ermitteln:

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

Führen Sie diesen Befehl aus, um die kontextsensitive Engine für die Client-Nachverfolgung zu beenden:

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

Führen Sie diesen Befehl aus, um die Diagnose durchzuführen:

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

Hinweis: Mit dem **Rundiag**-Befehl können auch MSE UDI-Informationen angezeigt werden, die zum Abrufen der Lizenzdatei für kontextsensitive Engine für Clients erforderlich sind.

Zugehörige Informationen

- MSE-Konfigurationsleitfaden (virtuelle und physische Appliance)
- Konfiguration der MSE mit hoher Verfügbarkeit
- Cisco WIPS - Implementierungsleitfaden
- Produktbestellung
- Technischer Support und Dokumentation - Cisco Systems