

Konfigurieren des Cisco IMC Supervisor für Server der Serien C und E

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Server der UCS C-Serie](#)

[Server der UCS E-Serie](#)

[Firmware-Mindestversionen](#)

[Unterstützte PCIe-Karten](#)

[Unterstützte Hypervisor-Versionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Bereitstellung von Cisco IMC Supervisor](#)

[Standardkennwort ändern](#)

[Lizenzinformationen](#)

[Server ermitteln](#)

[Rack-Gruppe hinzufügen](#)

[Rack-Konto hinzufügen](#)

[Mail-Setup-Konfiguration](#)

[Firmware-Upgrade](#)

[Daten des technischen Supports auf einen Remote-Server exportieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Konfiguration des Cisco Integrated Management Controller (IMC) Supervisor für Server der C-Serie und der E-Serie.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Server der C-Serie
- Cisco Server der E-Serie

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Internet Explorer 8 oder höher
- Google Chrome ab Version 4.1
- Firefox 3.5 oder höher
- Safari 4.0 oder höher (für Apple MAC oder Microsoft Windows)
- Browser benötigen das Adobe Flash Player Plug-in Version 11 oder höher.

Server der UCS C-Serie

- Cisco UCS C-220 M3
- Cisco UCS C-240 M3
- Cisco UCS C-220 M4
- Cisco UCS C-240 M4
- Cisco UCS C-22 M3
- Cisco UCS C-24 M3
- Cisco UCS C-420 M3
- Cisco UCS C-460 M4

Server der UCS E-Serie

- Cisco UCS E-140S M2
- Cisco UCS E-160D M2
- Cisco UCS EN120E M2
- Cisco UCS EN120S M2
- Cisco UCS E-180D M2
- Cisco UCS E-140S M1
- Cisco UCS E-140D M1
- Cisco UCS E-160D M1
- Cisco UCS E-140DP M1
- Cisco UCS E-160DP M1

Firmware-Mindestversionen

Server	Firmware-Mindestversion
Server der UCS C-Serie	1.5(4) und spätere Version
Server der UCS E-Serie	2.3.1 und höher

Unterstützte PCIe-Karten

- Cisco UCS Virtual Interface Card (VIC) 1225
- Cisco UCS VIC 1225T

Unterstützte Hypervisor-Versionen

- ESXi 5.1

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.

Hintergrundinformationen

Cisco IMC Supervisor ist ein Managementsystem, mit dem Sie Rackmount-Server in großem Umfang verwalten können.

Sie können Cisco IMC Supervisor verwenden, um diese Aufgaben für einen Rackmount-Server durchzuführen:

- Unterstützung für die logische Gruppierung von Servern und Zusammenfassungen von Ansichten pro Gruppe
- Erfassung von Beständen für die Server
- Bereitstellung von Überwachungsfunktionen für Server und Gruppen
- Firmware-Management einschließlich Firmware-Download, -Upgrade und -Aktivierung
- Verwaltung von eigenständigen Serveraktionen, einschließlich Stromüberwachung, LED-Steuerung, Protokollerfassung, KVM-Einführung (Keyboard/Video/Mouse), Start der CIMC-Benutzeroberfläche und E-Mail-Benachrichtigungen
- Rollenbasierte Zugriffskontrolle (RBAC) zur Einschränkung von Zugriff und Funktionen

Konfigurieren

Bereitstellung von Cisco IMC Supervisor

1. Führen Sie diese Schritte aus, um Cisco IMC Supervisor bereitzustellen.

Schritt 1: Um die ZIP-Datei für Cisco IMC Supervisor von Cisco.com herunterzuladen, navigieren Sie zu **Products > Servers-Unified Computing > Integrated Management Controller (IMC) Supervisor (Produkte > Server-Unified Computing > Integrated Management Controller (IMC)** wie im Bild gezeigt.

Downloads Home > Products > Servers - Unified Computing

Find: Product Name e.g. 2811

Products Recently Used Products My Added Devices Add Device	Application Networking Services Cisco Interfaces and Modules Cloud and Systems Management Collaboration Endpoints Conferencing Connected Safety and Security Customer Collaboration IOS and NX-OS Software Optical Networking Routers Security Servers - Unified Computing Service Exchange Storage Networking Switches Unified Communications Universal Gateways and Access Servers Video Wireless	C800 Series Integrated Management Controller (IMC) Supervisor ← UCS B-Series Blade Server Software UCS C-Series Rack-Mount Standalone Server Software UCS C-Series Rack-Mount UCS-Managed Server Software UCS Central Software UCS Director UCS E-Series Software UCS Express UCS Infrastructure and UCS Manager Software UCS Invicta Series Solid State Systems UCS Management Partner Ecosystem Software UCS Performance Manager Virtual Application Container Services (VACS)
---	--	---

Schritt 2: Wählen Sie **IMC Supervisor 1.0** aus, wie im Bild gezeigt.


Downloads Home > Products > Servers - Unified Computing > Integrated Management Controller (IMC) Supervisor

Find: Product Name e.g. 2811

Products Recently Used Products My Added Devices Add Device	C800 Series Integrated Management Controller (IMC) Supervisor UCS B-Series Blade Server Software UCS C-Series Rack-Mount Standalone Server Software UCS C-Series Rack-Mount UCS-Managed Server Software UCS Central Software UCS Director UCS E-Series Software UCS Express UCS Infrastructure and UCS Manager Software UCS Invicta Series Solid State Systems UCS Management Partner Ecosystem Software UCS Performance Manager Virtual Application Container Services (VACS)	IMC Supervisor 1.0
---	---	--------------------

Schritt 3: Klicken Sie auf **Download** wie im Bild gezeigt.

IMC Supervisor 1.0

Search... 

[Expand All](#) | [Collapse All](#)

▼ Latest
1

▼ All Releases
▶ 1

Release 1

File Information	Release Date	Size	
Cisco Integrated Management Controller Supervisor 1.0 (MD5 Checksum - 4 a2803e35b40b63c497e8d5371ab118e) CIMCS_1_0_0_0_VMWARE_GA.zip	24-NOV-2014	2705.08 MB	Download Add to cart Publish

Schritt 4: Um die Open Virtual Appliance (OVA) bereitzustellen, navigieren Sie zu **Datei > Bereitstellen der OVF-Vorlage** wie im Bild gezeigt.

10.104.213.63 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

- New
- Deploy OVF Template...**
- Export
- Report
- Browse VA Marketplace...
- Print Maps
- Exit

Inventory

Cisco_IMC_Supervisor-1.0.0.0

Getting Started Summary Resource Allocation Performance Events Console Permissions

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Virtual Machines

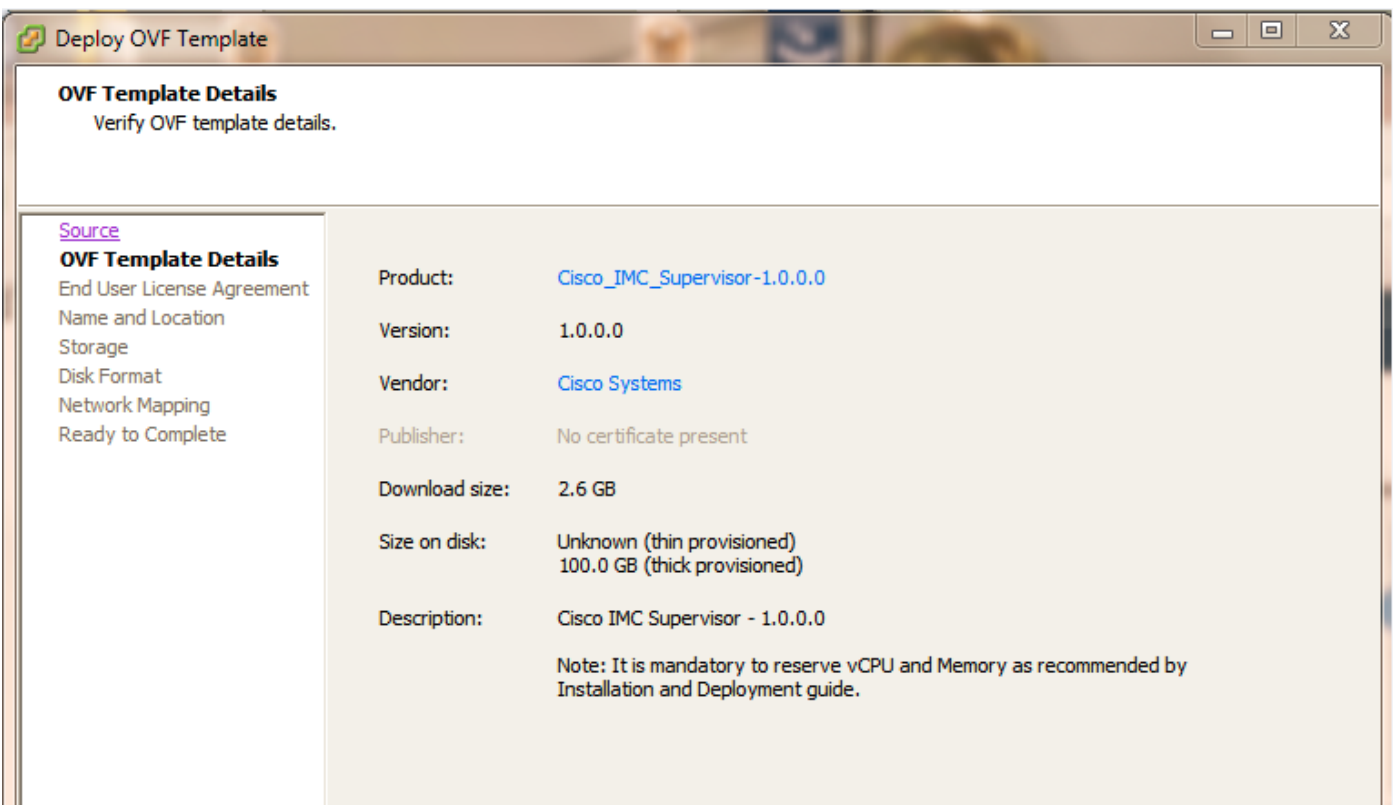
Recent Tasks

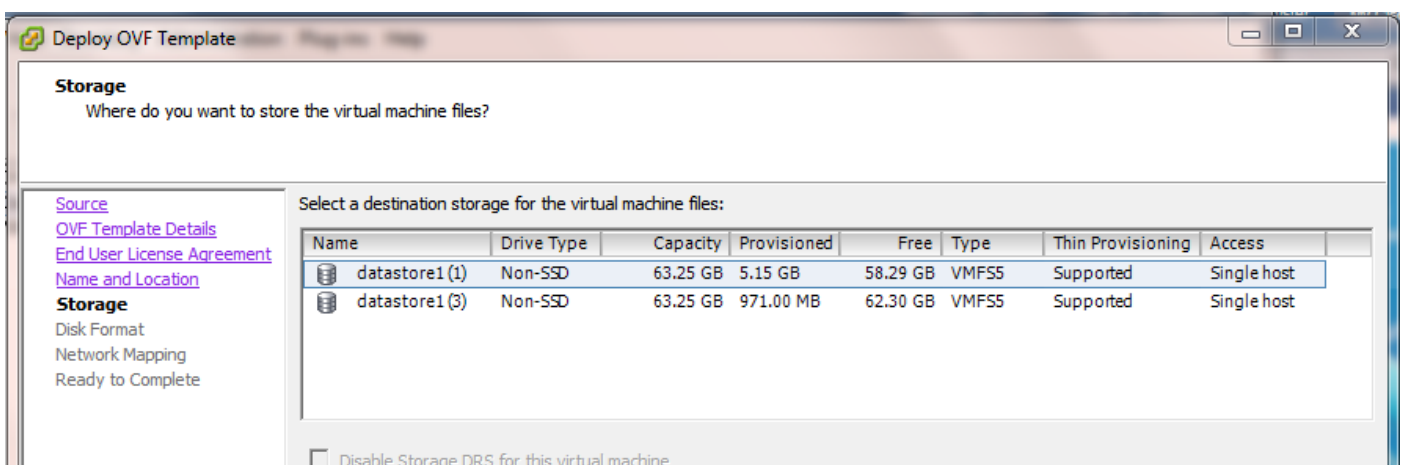
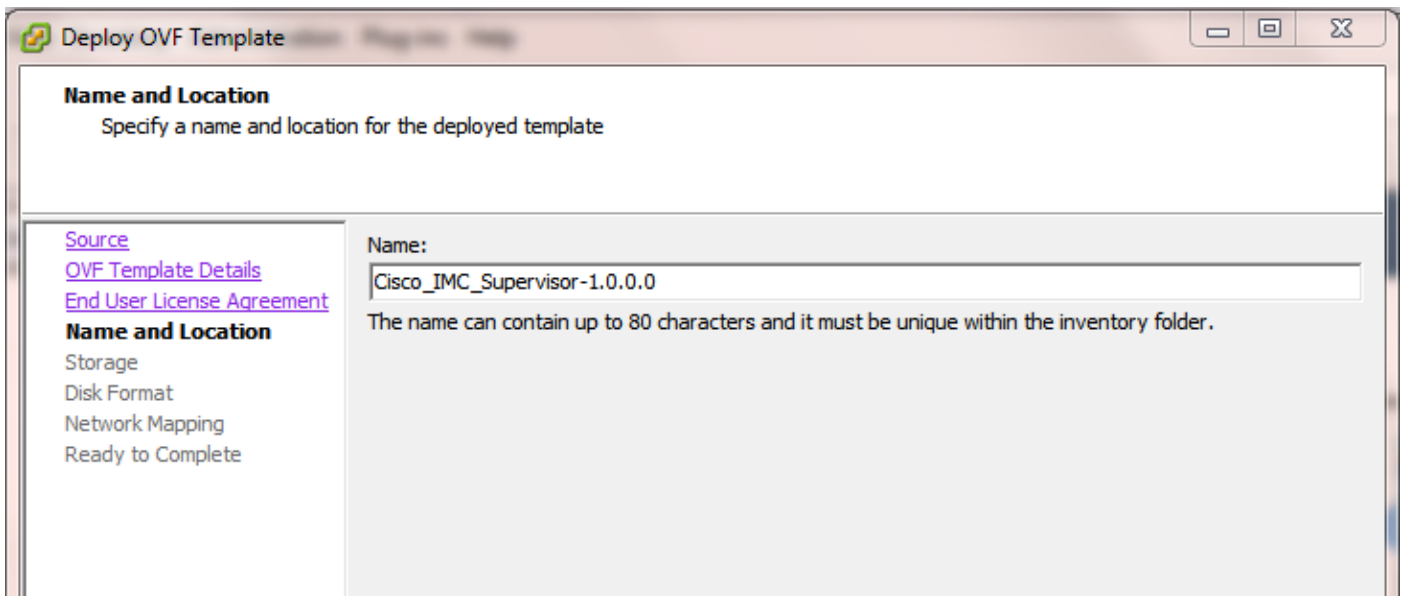
Name, Target or Status contains: Clear X

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed
------	--------	--------	---------	--------------	-----------------------	------------	-----------

Tasks root

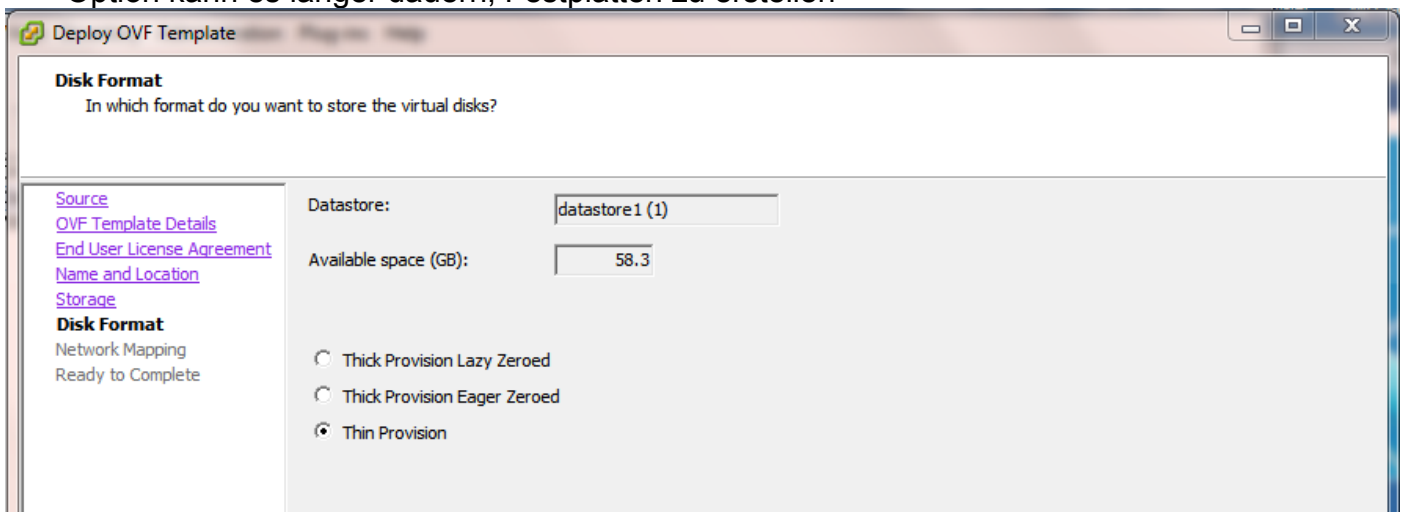
Schritt 5: Führen Sie den Schritt für Schritt durch, um die OVF-Vorlage (Open Virtualization Format) wie in den Bildern gezeigt bereitzustellen.





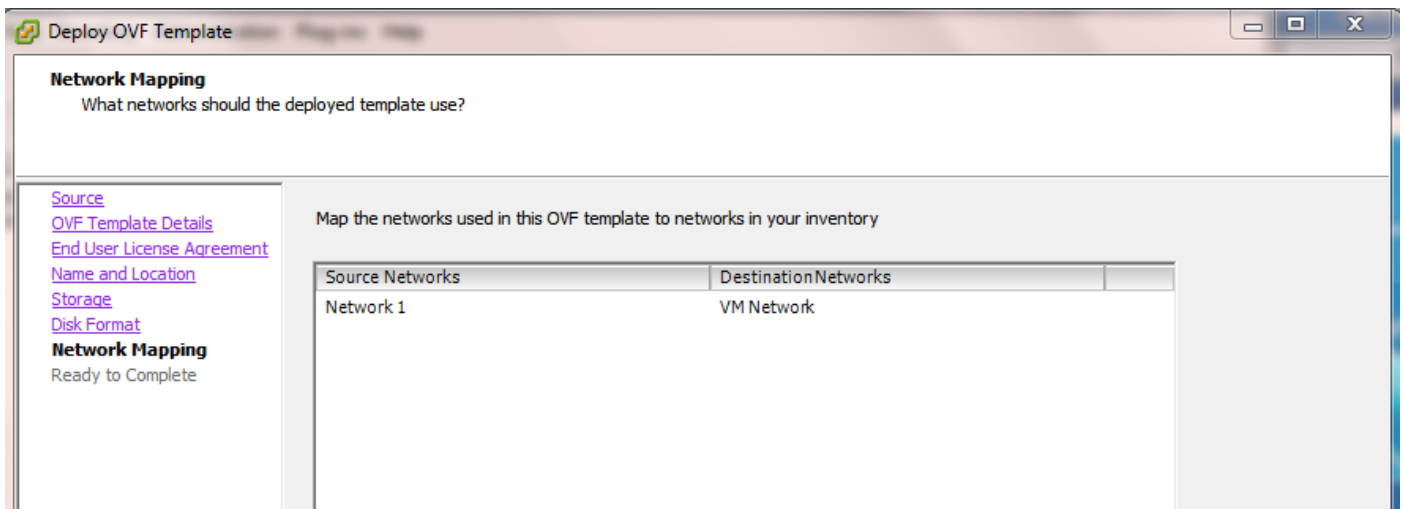
Wählen Sie im Bereich **Datenträgerformat** eine der Optionsschaltflächen aus, und klicken Sie auf **Weiter**, wie im Bild gezeigt.

- Thin Provisioning - Um Speicher bei Bedarf zuzuweisen, wenn Daten auf die Festplatte geschrieben werden
- Thick Provision Lazy Zeroed - Um Speicher sofort in dickem Format zuzuweisen
- Thick Provision Eager Zeroed - Zur Zuweisung von Storage in dicken Formaten. Mit dieser Option kann es länger dauern, Festplatten zu erstellen

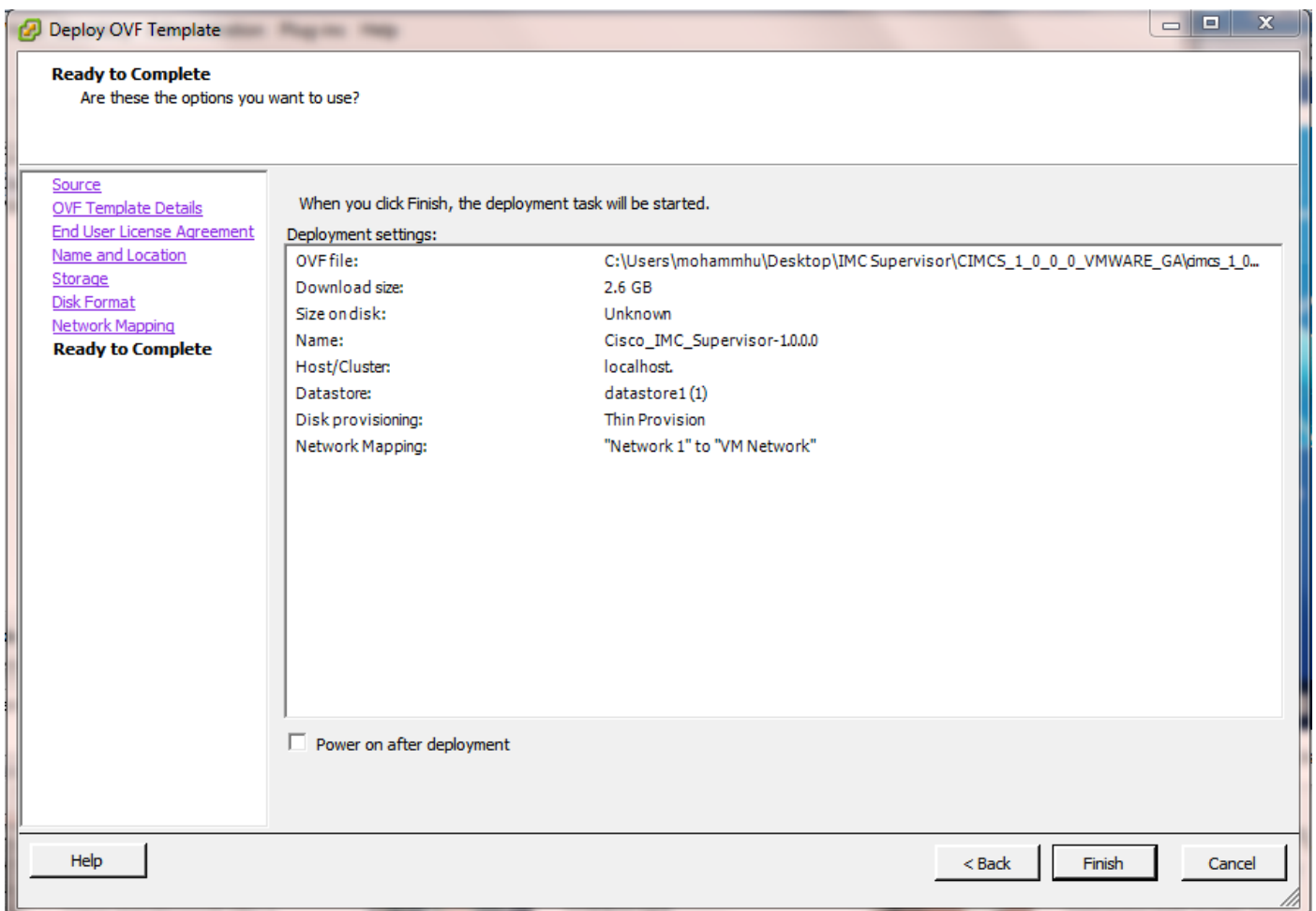


Schritt 6: Wählen Sie die entsprechende Portgruppe für das VM-Netzwerk (Virtual Machine) aus,

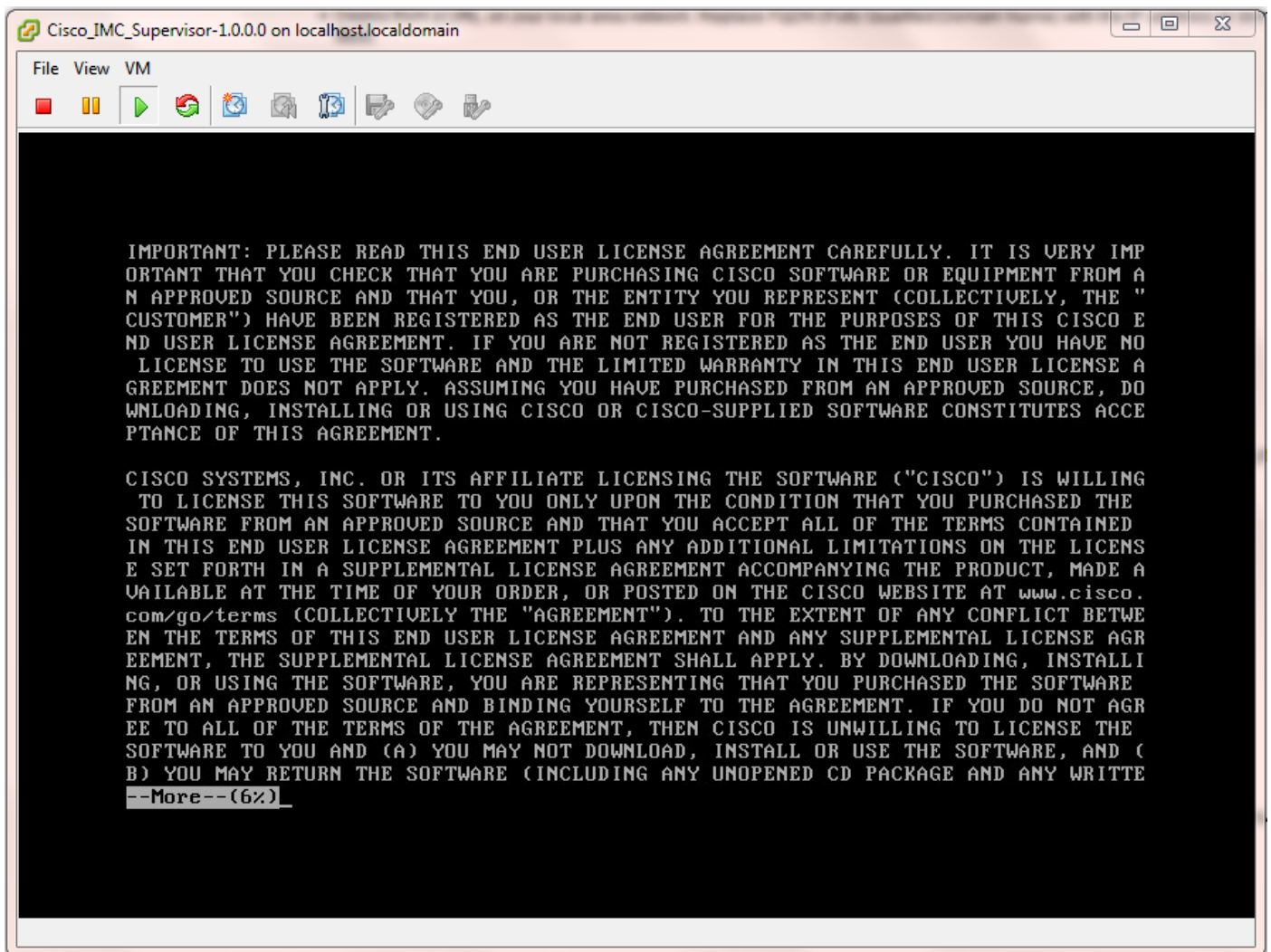
wie im Bild gezeigt.



Schritt 7: Klicken Sie auf **Fertig stellen** wie im Bild gezeigt.



Schritt 8: Öffnen Sie die Konsole des virtuellen Systems, und **akzeptieren Sie** die Lizenzvereinbarung, wie im Bild gezeigt.



Schritt 9: Geben Sie anschließend **y** ein, um eine statische IP wie im Bild gezeigt zu konfigurieren.

Schritt 10: Wenn Sie DHCP verwenden möchten, geben Sie **n** ein, um sicherzustellen, dass IP-Adressen automatisch zugewiesen werden.

```
Cisco_IMC_Supervisor-1.0.0.0 on localhost.localdomain
File View VM
not imply a partnership relationship between Cisco and any other company.

Do you agree with the terms of the End User License Agreement?
yes/no [nol]: yes

Regenerating ssh host keys...
openssh-daemon is stopped
Generating SSH1 RSA host key: [ OK ]
Generating SSH2 RSA host key: [ OK ]
Generating SSH2 DSA host key: [ OK ]
Starting sshd: [ OK ]
Regenerating keys for the root user...
Generating public/private rsa key pair.
Created directory '/root/.ssh'.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d7:34:b7:18:89:a2:27:3b:45:a6:96:72:97:7d:f3:de root@localhost
Generating SSL certificates for sfc in /opt/vmware/etc/sfc
Generating SSL certificates for lighttpd in /opt/vmware/etc/lighttpd
This script is executed on first boot only.
Configuring static IP configuration

Do you want to Configure static IP [y/n]? : y_
```

Schritt 11: Wenn Sie eine statische IP-Adresse verwenden möchten, geben Sie **y ein**, und Sie werden aufgefordert, **IPv4** oder **IPv6** auszuwählen. Geben Sie **V4** ein, um IPV4 zu konfigurieren, und geben Sie dann die in den Bildern gezeigten Informationen ein:

- IP-AdresseNetzmaskeGateway

Hinweis: Derzeit wird nur IPv4 unterstützt, um statische IP-Adressen zu konfigurieren.

```
Cisco_IMC_Supervisor-1.0.0.0 on localhost.localdomain
File View VM
Regenerating keys for the root user...
Generating public/private rsa key pair.
Created directory '/root/.ssh'.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d7:34:b7:18:89:a2:27:3b:45:a6:96:72:97:7d:f3:de root@localhost
Generating SSL certificates for sfcfb in /opt/vmware/etc/sfcfb
Generating SSL certificates for lighttpd in /opt/vmware/etc/lighttpd
This script is executed on first boot only.
Configuring static IP configuration

Do you want to Configure static IP [y/n]? : y
Do you want to configure IPv4/IPv6 [v4/v6] ? : v4

Configuring static IP for appliance. Provide the necessary access credentials

IP Address: 10.104.213.77
Netmask: 255.255.255.0
Gateway: 10.104.213.1

Configuring Network with : IP(10.104.213.77), Netmask(255.255.255.0), Gateway(10.104.213.1)

Do you want to continue [y/n]? : y_
```

```
Cisco_IMC_Supervisor-1.0.0.0 on localhost.localdomain
File View VM
Cisco_IMC_Supervisor-1.0.0.0 - 1.0.0.0
To manage this VM browse to https://10.104.213.77:443/

*Login
Configure Network
Set Timezone (Current:UTC)

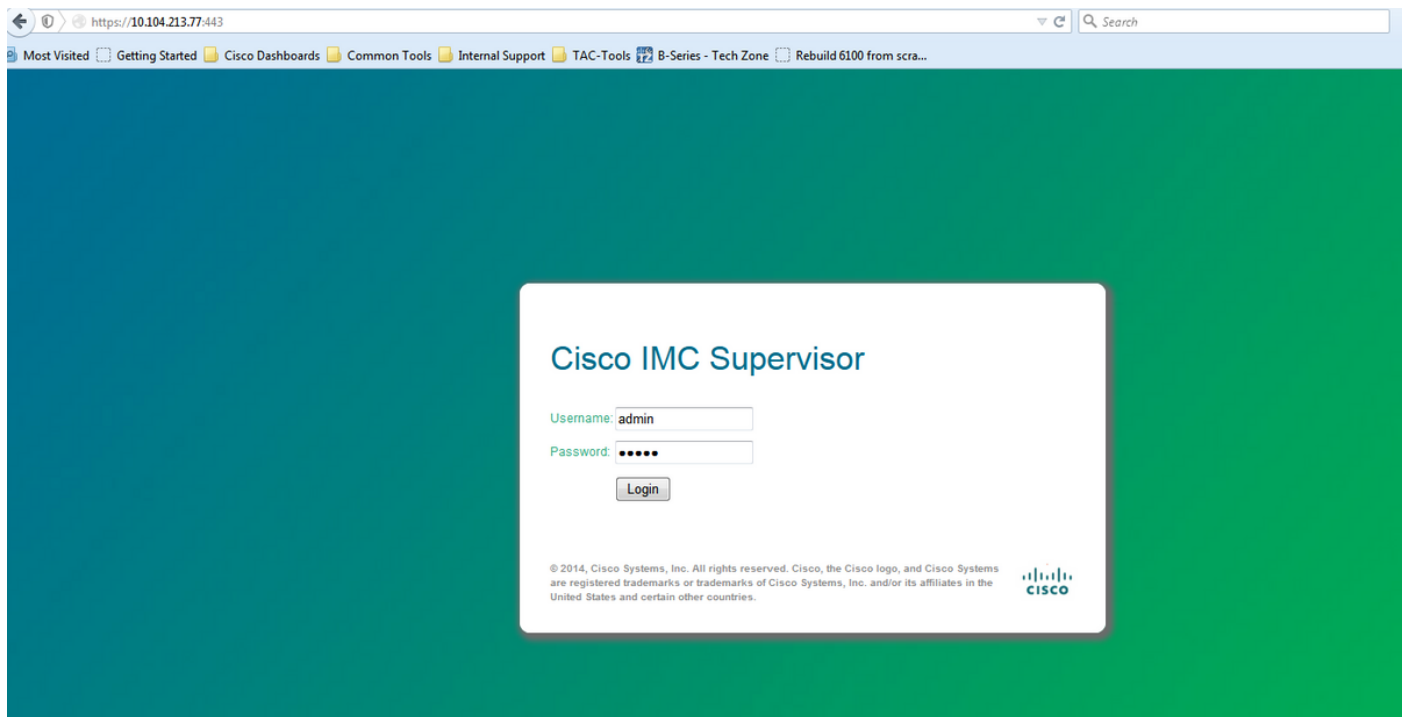
Use Arrow Keys to navigate
and <ENTER> to select your choice.
```

Schritt 12: Wenn die Appliance gestartet wurde, übertragen Sie die IP-Adresse des Cisco IMC Supervisor in einen unterstützten Webbrowser, um auf die Anmeldeseite zuzugreifen.

Geben Sie auf der Anmeldeseite **admin** als Benutzername und **admin** als Kennwort ein.

Hinweis: Nach dieser ersten Anmeldung können Sie Ihr Administratorkennwort ändern.

Die Benutzeroberfläche (UI) von Cisco IMC Supervisor ist im Bild dargestellt.



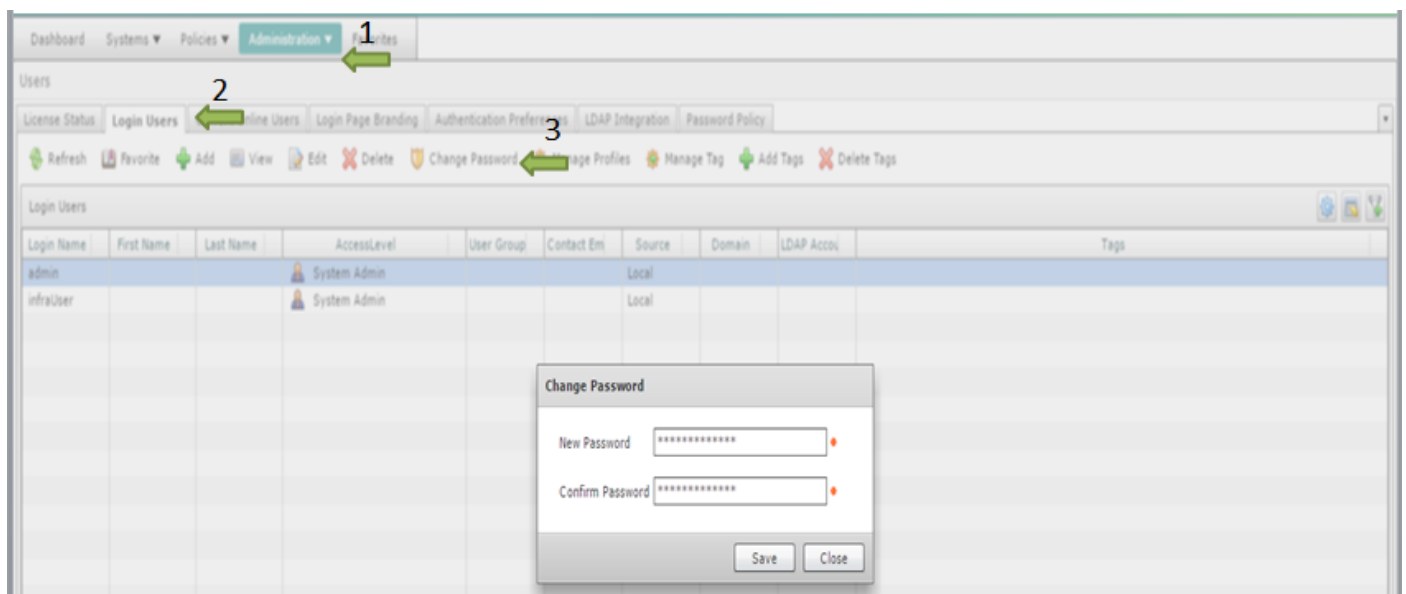
Standardkennwort ändern

2. Führen Sie diese Schritte aus, um das Standardkennwort zu ändern.

Schritt 1: Navigieren Sie zu **Administration > Users**.

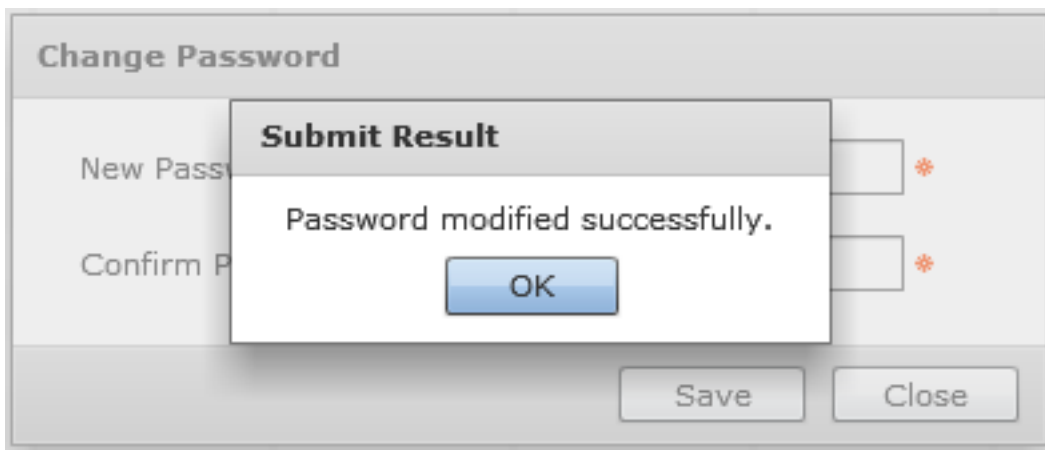
Schritt 2: Klicken Sie auf die Registerkarte **Anmelde-Benutzer**.

Schritt 3: Wählen Sie aus der Liste der Benutzer die Benutzerrolle aus, für die Sie das Kennwort wie im Bild gezeigt ändern möchten.



Schritt 4: Nachdem Sie das neue Kennwort festgelegt haben, klicken Sie auf **Speichern** und

klicken Sie im **Ergebnis** senden wie im Bild gezeigt auf **OK**.



Lizenzinformationen

3. Für Cisco IMC Supervisor benötigen Sie folgende gültige Lizenzen:

- Eine Basislizenz für Cisco IMC Supervisor.
- Eine Cisco IMC Supervisor Bulk-Enablement-Lizenz, die Sie nach der Basislizenz für Cisco IMC Supervisor installieren, wie im Bild gezeigt.

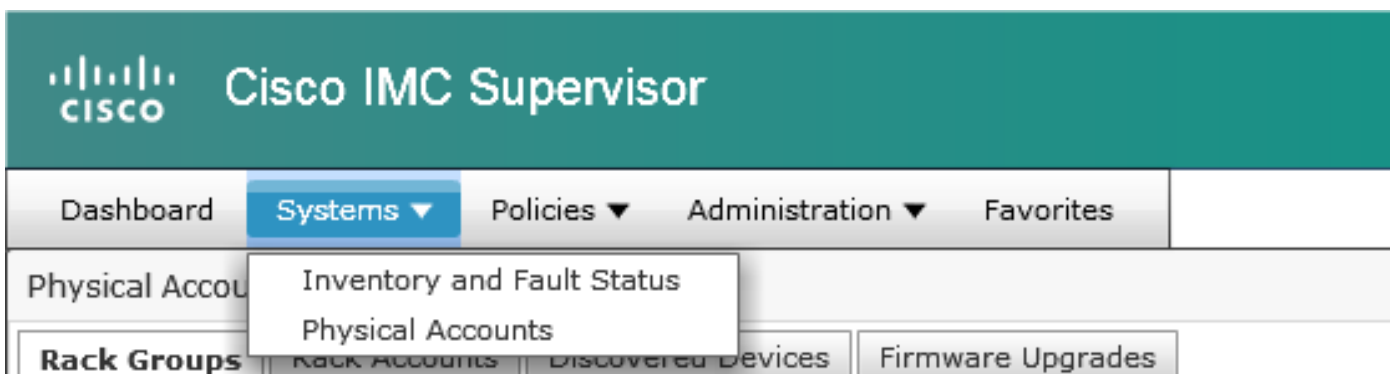
License	Licensed Lim	Available	Used	Status	Remarks
CIMC SUP Base	1		1	✔ Licensed	
Physical Servers	200	200	0	✔ Licensed	Licensed Limit = CIMC-SUP-B01(=2) * 100+ CIMC-SUP-B02(=0) * 250+ CIMC-SUP-B10(=0) * 1000

Hinweis: Ohne diese Lizenzen können Aufgaben wie das Gruppieren von Servern in einem Rack-Konto usw. nicht ausgeführt werden.

Server ermitteln

4. Führen Sie diese Aktionen aus, um Server zu ermitteln.

Schritt 1: Navigieren Sie zu **System > Physical Accounts (System > Physische Konten) > Discovered Devices (Entdeckte Geräte)**, wie im Bild gezeigt.



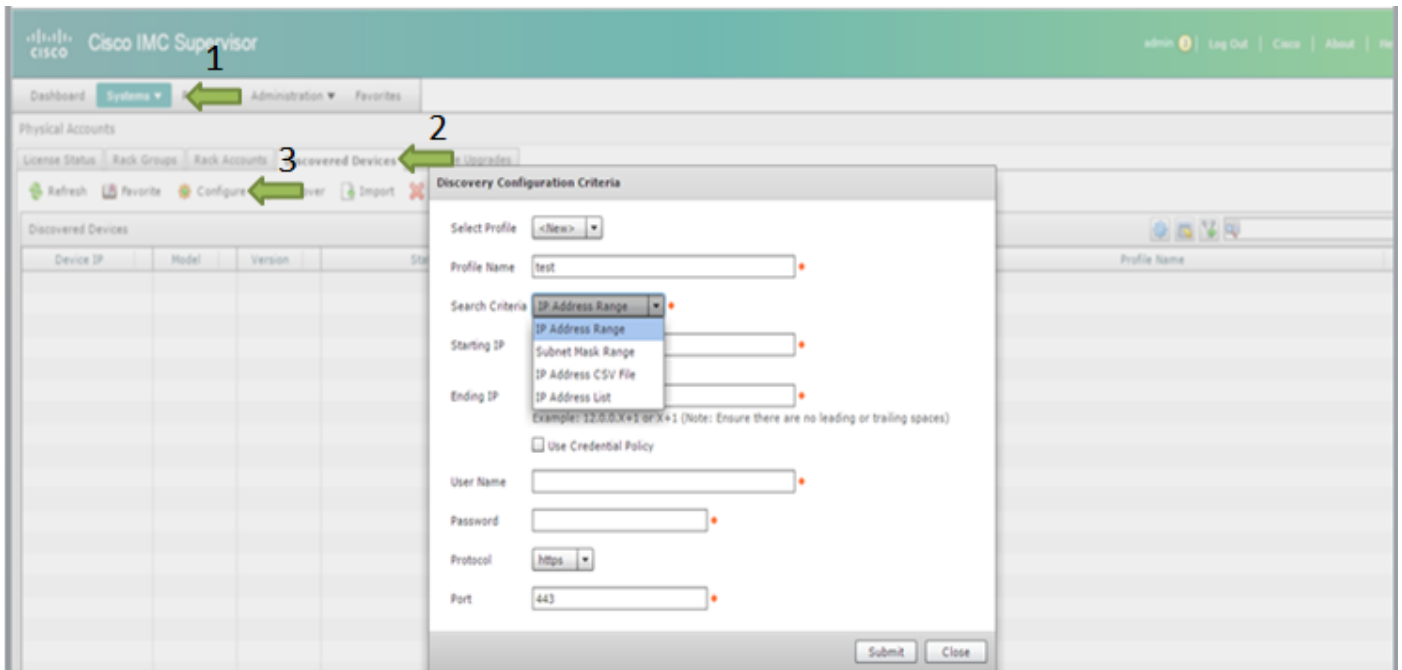
Schritt 2: Klicken Sie auf **Konfigurieren**.

Schritt 3: Im Dialogfeld **Discovery Configuration Criteria** können Sie entweder ein neues Profil erstellen oder ein vorhandenes Profil bearbeiten.

Schritt 4: Die Erstellung eines **neuen** Profils erfolgt wie im Bild gezeigt.

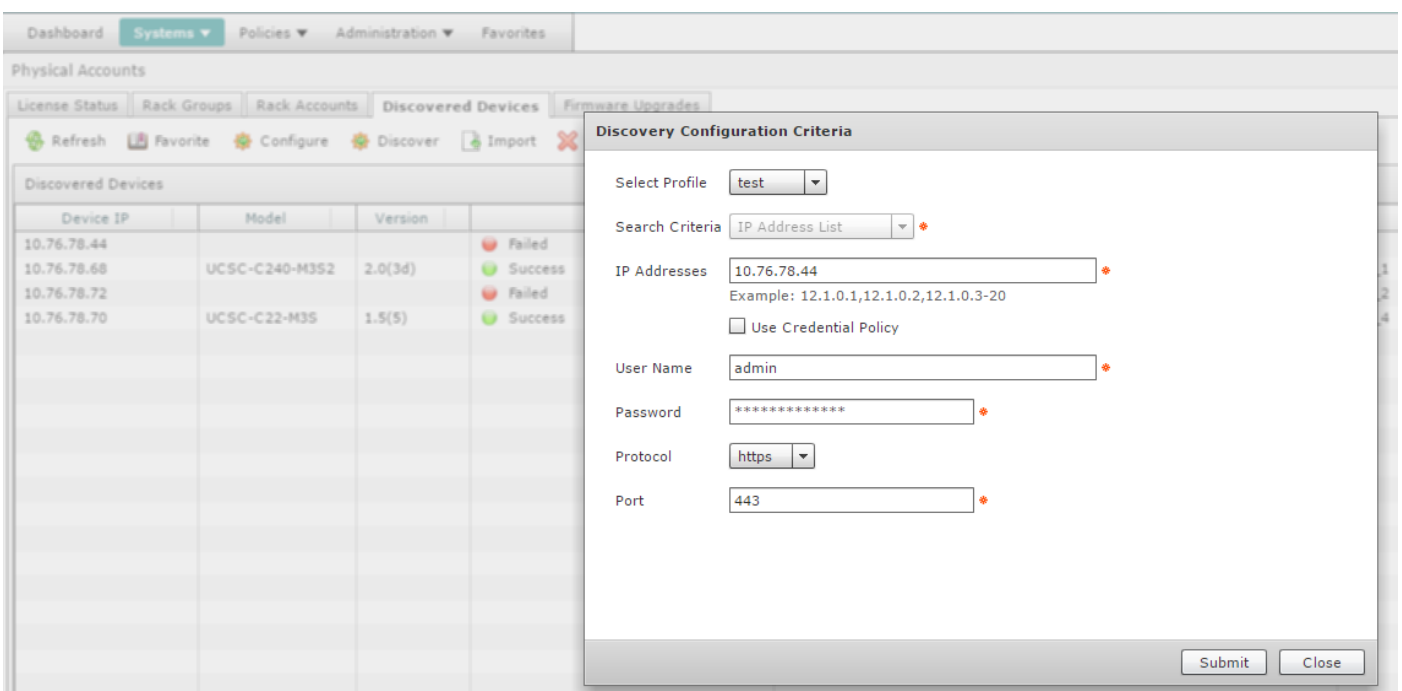
Schritt 5: Unter Suchkriterien können Sie die geeignete Methode zum Ermitteln der Server auswählen.

Schritt 6: Wählen Sie für dieses Beispiel **IP-Adressliste** aus.

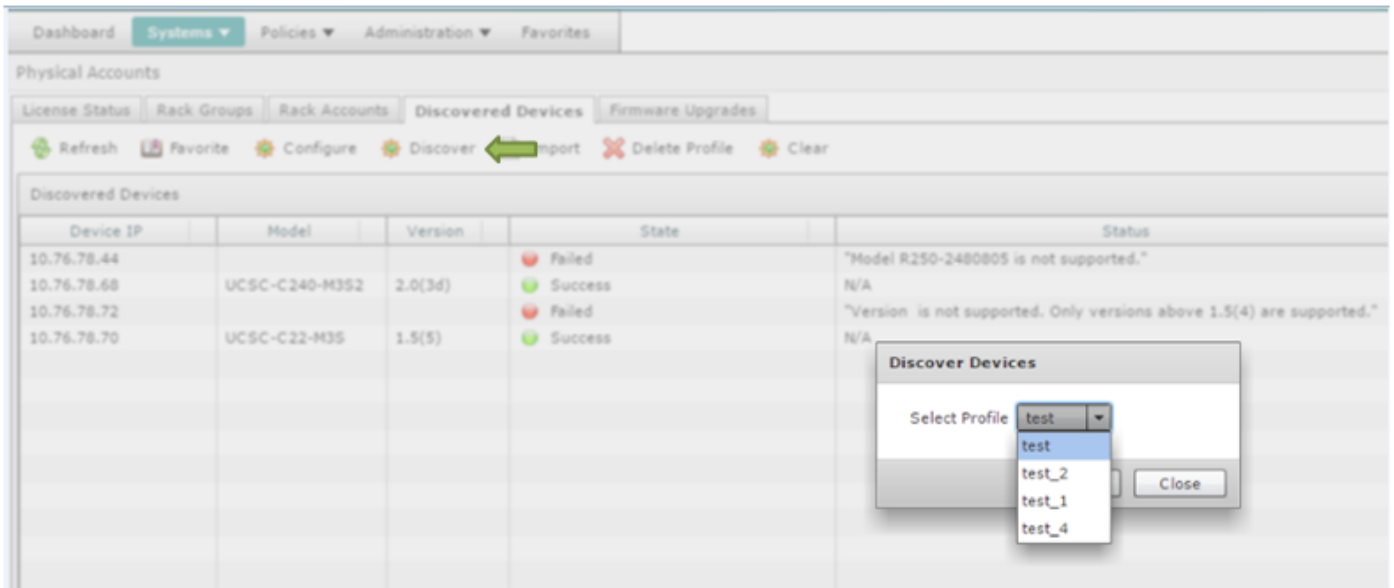


Schritt 7: Geben Sie die IP-Adresse des Servers ein, den Sie ermitteln möchten.

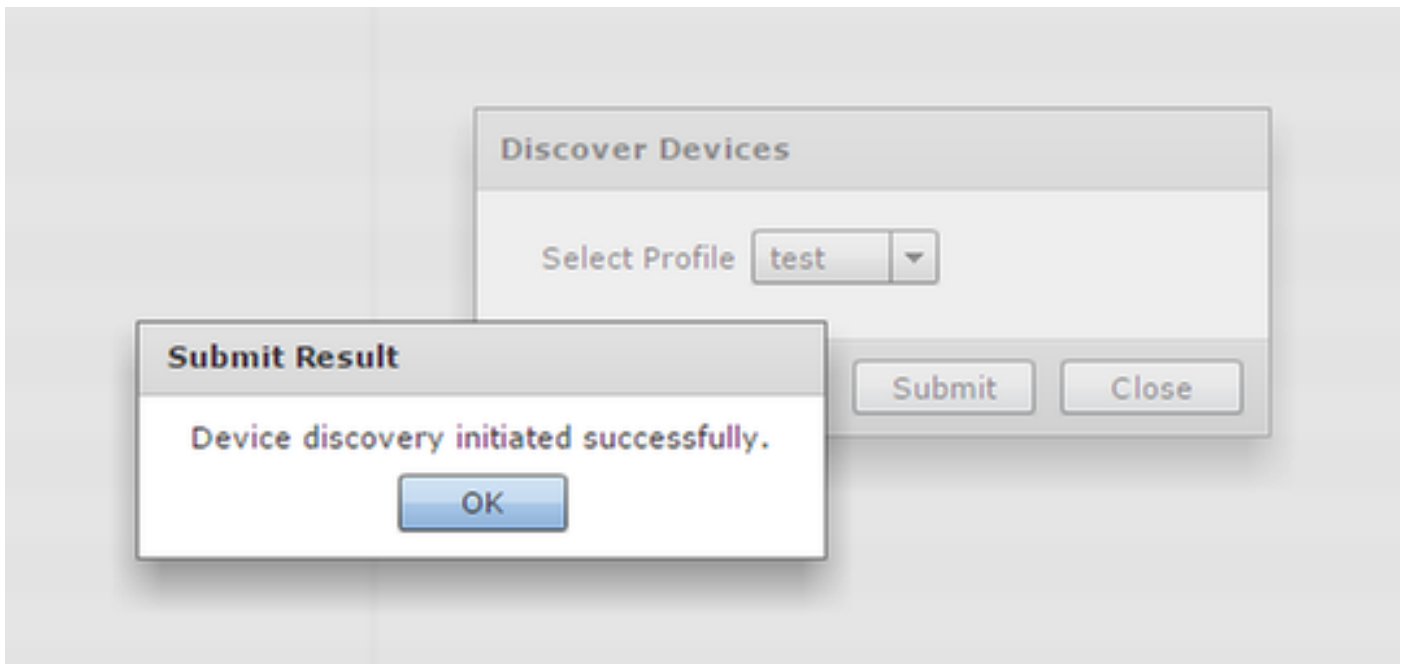
Schritt 8: Geben Sie den Benutzernamen und das Kennwort ein, das Sie für die Anmeldung am Server (CIMC-Anmeldeinformationen) verwenden, wie im Bild gezeigt.



Schritt 9: Nachdem das Profil erstellt wurde, klicken Sie wie im Bild gezeigt in der Dropdown-Liste auf Profil **ermitteln** und auswählen.



Schritt 10: Nachdem Sie das entsprechende Profil ausgewählt haben, klicken Sie auf **Senden** und klicken Sie auf **OK** auf Ergebnis senden, wie im Bild gezeigt.



Schritt 11: Wenn die Geräte in Ihrem Profil nicht mit den minimalen unterstützten Kriterien übereinstimmen, ist der Grund für das nicht erkannte Gerät im Abschnitt **Status** aufgeführt, wie im Bild gezeigt.

Dashboard Systems Policies Administration Favorites					
Physical Accounts					
License Status		Rack Groups		Rack Accounts	
Discovered Devices Firmware Upgrades					
Refresh Favorite Configure Discover Import Delete Profile Clear					
Discovered Devices					
Device IP	Model	Version	State	Status	
10.76.78.44			Failed	"Model R250-2480805 is not supported."	test
10.76.78.68	UCSC-C240-M352	2.0(3d)	Success	N/A	test_1
10.76.78.72			Failed	"Version is not supported. Only versions above 1.5(4) are supported."	test_2
10.76.78.70	UCSC-C22-M35	1.5(5)	Success	N/A	test_4

Rack-Gruppe hinzufügen

5. Führen Sie dieses Verfahren aus, wenn Sie eine neue Rack-Gruppe in Cisco IMC Supervisor hinzufügen möchten.

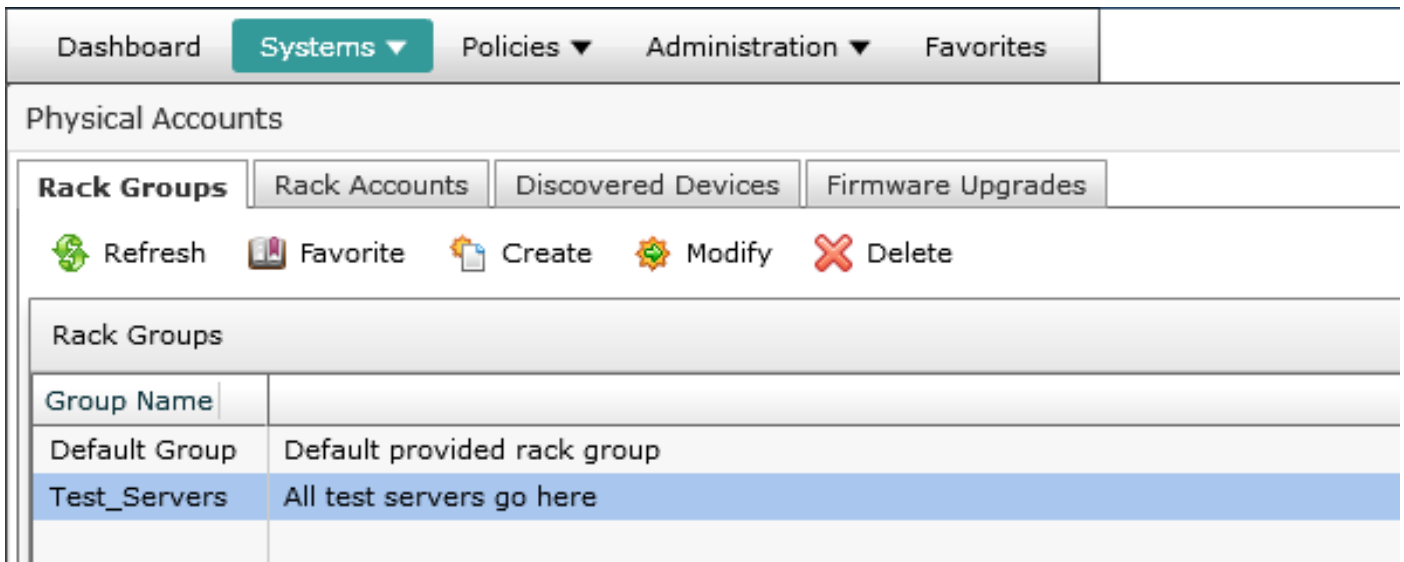
Schritt 1: Navigieren Sie zu **Systeme > Physical Accounts > Rack Groups (Systeme > physische Konten > Rackgruppen)**.

Schritt 2: Klicken Sie auf **Erstellen**.

Schritt 3: Geben Sie im Feld Create Rack Group (Rack-Gruppe erstellen) einen **Gruppennamen** und eine **Beschreibung** an.

Schritt 4: Klicken Sie auf **Erstellen** wie im Bild gezeigt.

Schritt 5: Nach der Erstellung muss der Gruppenname wie im Bild dargestellt angezeigt werden.



Rack-Konto hinzufügen

6. Führen Sie dieses Verfahren aus, wenn Sie eine neue Rack-Gruppe in Cisco IMC Supervisor hinzufügen möchten.

Schritt Wählen Sie in der Menüleiste **System** aus.

1:

Schritt Klicken Sie auf die Registerkarte.

2:

Schritt Klicken Sie auf.

3:

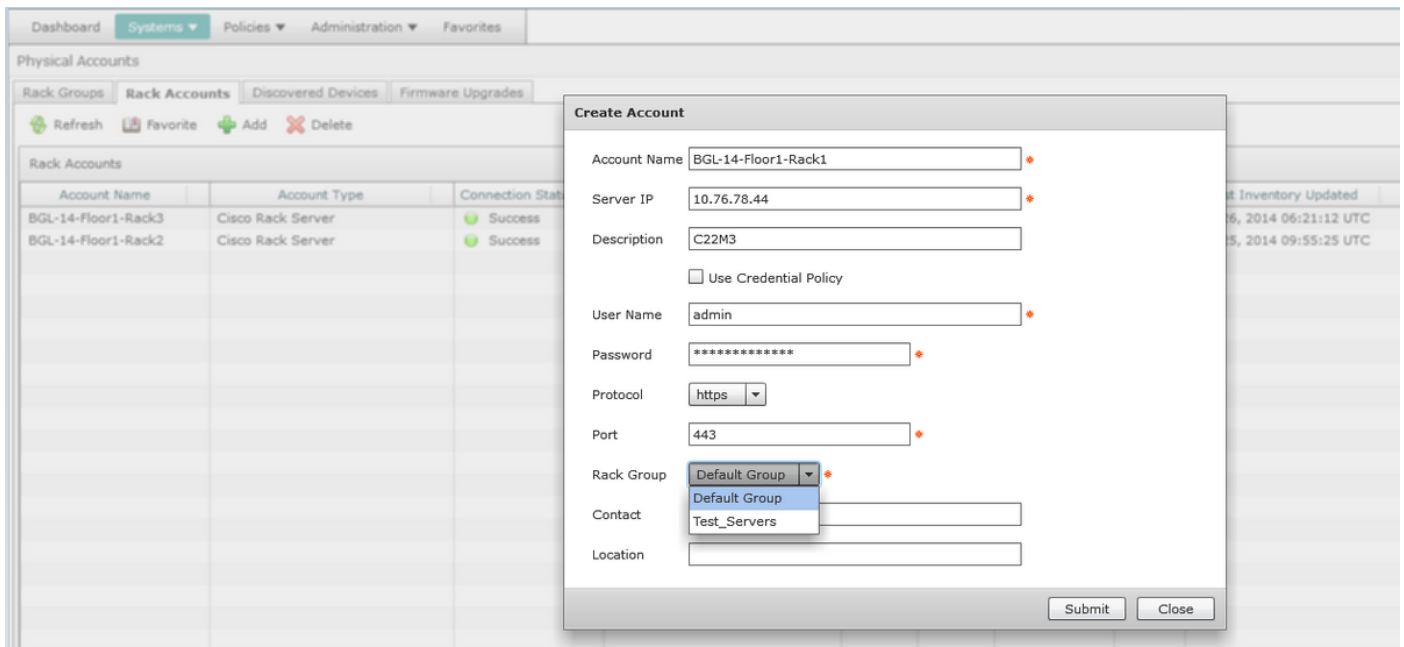
Schritt Füllen Sie im Dialogfeld Konto erstellen die folgenden Felder aus:

4:

Feld	Beschreibung
Feld	Ein beschreibender Name für das Rack-Konto
Feld	Die IP-Adresse des Rackmount-Servers
Beschreibung	(Optional) Beschreibung des Rack-Kontos
Kontrollkästchen	(Optional) Wenn Sie bereits Richtlinien für Anmeldeinformationen erstellt haben, aktivieren Sie dieses Kontrollkästchen, um die Richtlinie aus der Dropdown-Liste auszuwählen.
Wenn Sie das Kontrollkästchen aktivieren	
Dropdown-Liste	Wählen Sie eine Richtlinie aus der Dropdown-Liste aus.
Wenn Sie das Kontrollkästchen deaktivieren	
Feld	Anmelde-ID für den Rackmount-Server
Kennwortfeld	Kennwort für die Anmelde-ID des Rackmount-Servers
Protokoll-Dropdown-Liste	Wählen Sie https oder http aus der Liste aus.
Port-Feld	Die dem ausgewählten Protokoll zugeordnete Portnummer
Rack Group-Dropdown-Liste	Wählen Sie eine Rack-Gruppe aus der Liste aus.
Kontaktfeld	(Optional) Die E-Mail-Adresse des Kunden
Ortsfeld	(Optional) Der Standort des Kontos

Schritt 1: In der Dropdown-Liste für Rack-Gruppe können Sie entweder die **Standardgruppe** oder die Gruppe auswählen, die zuvor wie im Bild gezeigt definiert wurde.

Schritt 2: Nach Abschluss dieser Aktion müssen die angegebenen Server unter die ausgewählte Rack-Gruppe fallen.



Mail-Setup-Konfiguration

7. Führen Sie dieses Verfahren aus, um Ihre Setup-Mail-Adresse zu konfigurieren.

Schritt 1: Navigieren Sie zu **Administration > Mail Setup**.

Schritt 2: Geben Sie die erforderlichen Details ein.

Schritt 3: Sie können das Kontrollkästchen **Test-E-Mail senden** auswählen und überprüfen, ob Sie die Testmail mit der von Ihnen angegebenen E-Mail-Adresse erhalten haben, wie im Bild gezeigt.

[Dashboard](#)[Systems ▼](#)[Policies ▼](#)[Administration ▼](#)[Favorites](#)

System

[System Information](#)**Mail Setup**[System Tasks](#)[User Roles](#)[Email Alert Rules](#)

Outgoing Email Server (SMTP)



Outgoing SMTP Port



Outgoing SMTP User

Outgoing SMTP Password

Outgoing Email Sender Email Address



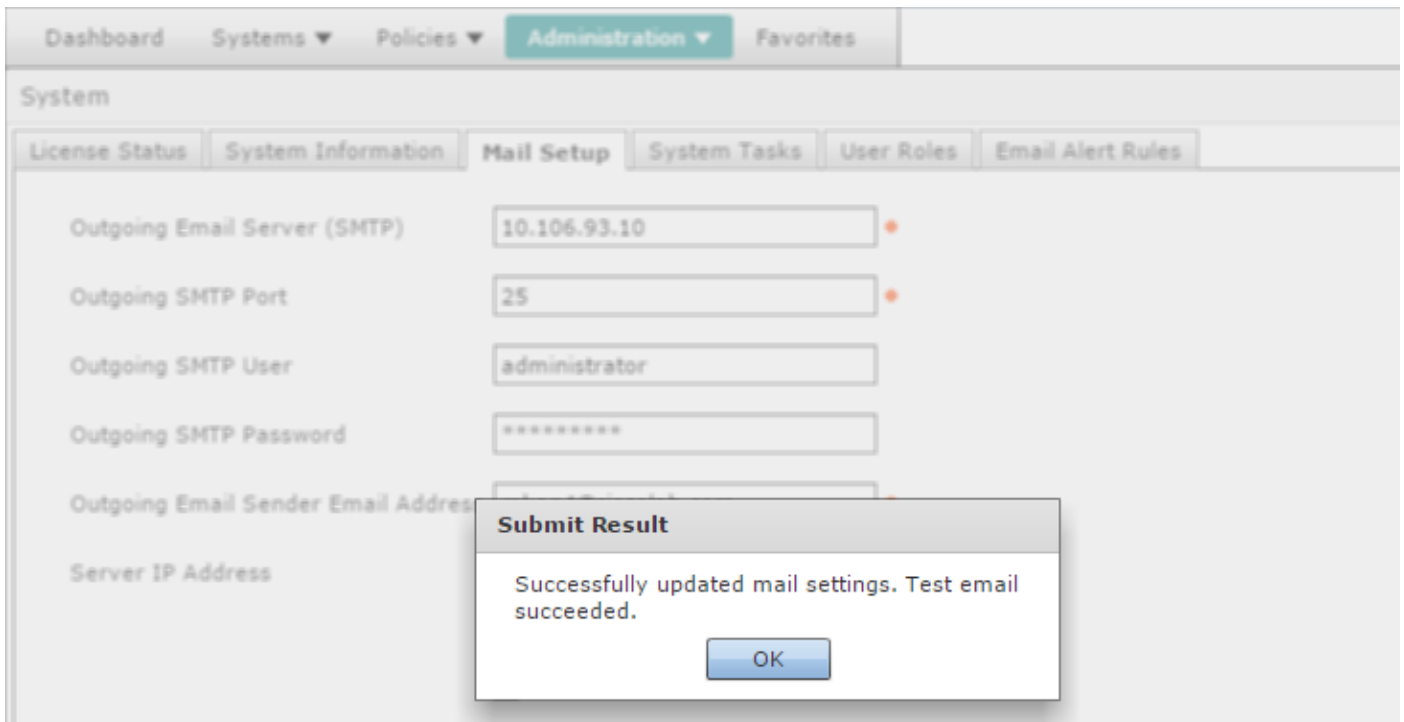
Server IP Address

 Send Test Email

Test Email Address

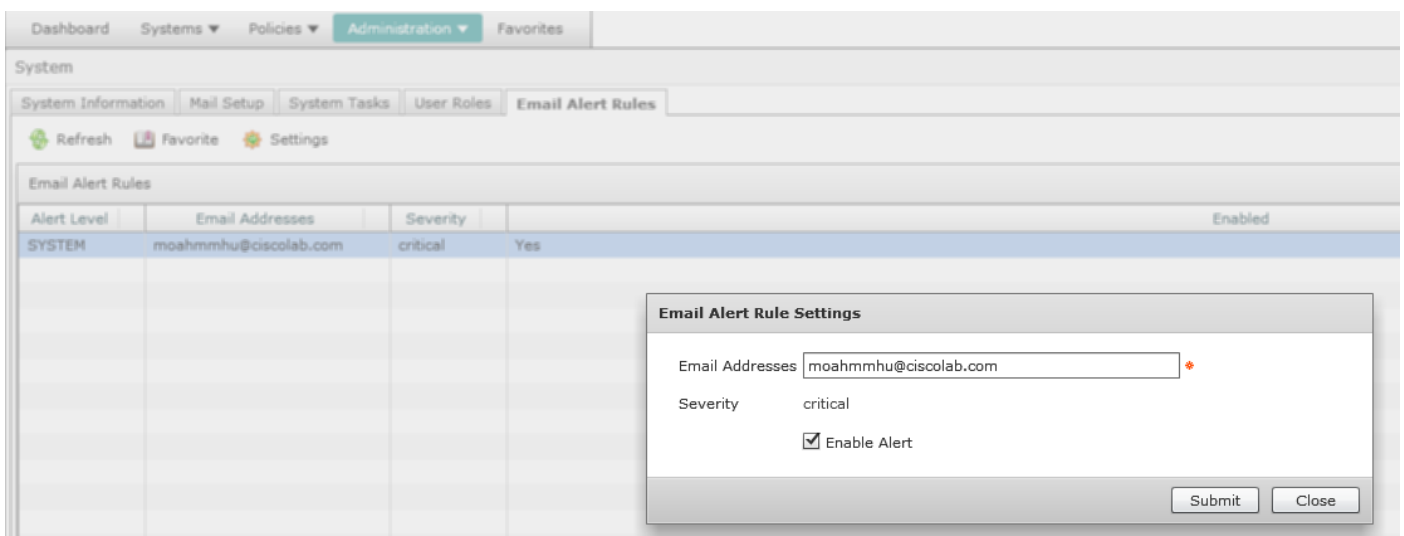


Schritt 4: Sie müssen dann die Test-E-Mail wie im Bild gezeigt erhalten.



Schritt 5: Navigieren Sie im gleichen Abschnitt zu **Einstellungen für E-Mail-Warmmeldungsregeln**, und aktivieren Sie das Kontrollkästchen **Warmmeldung aktivieren**, wie im Bild gezeigt.

Hinweis: Zu diesem Zeitpunkt (mit Version 1.0 des Cisco IMC Supervisor) werden Benachrichtigungen nur für kritische und schwerwiegende Fehler unterstützt.



Schritt 6: Wenn bei Ihrem System ein kritischer Fehler auftritt, müssen Sie eine E-Mail erhalten, wie im Bild gezeigt, vorausgesetzt, Ihre E-Mail-Einrichtung funktioniert einwandfrei.

Server IP	Host name	Severity	Code	Cause	Description	Created	Affected DN
10.76.78.70	bgl-sv-c22-m3-01	critical	F1007	equipment-inoperable	Storage Virtual Drive 0 is inoperable: Check storage controller, or reseal the storage drive	Thu Dec 25 12:10:19 2014	sys/rack-unit-1/board /storage-SAS-SLOT-2/vd-0

Firmware-Upgrade

8. Führen Sie dieses Verfahren aus, wenn Sie die Firmware aktualisieren möchten.

Schritt 1: Navigieren Sie zu **Systems > Physical Accounts (Systeme > physische Konten)**.

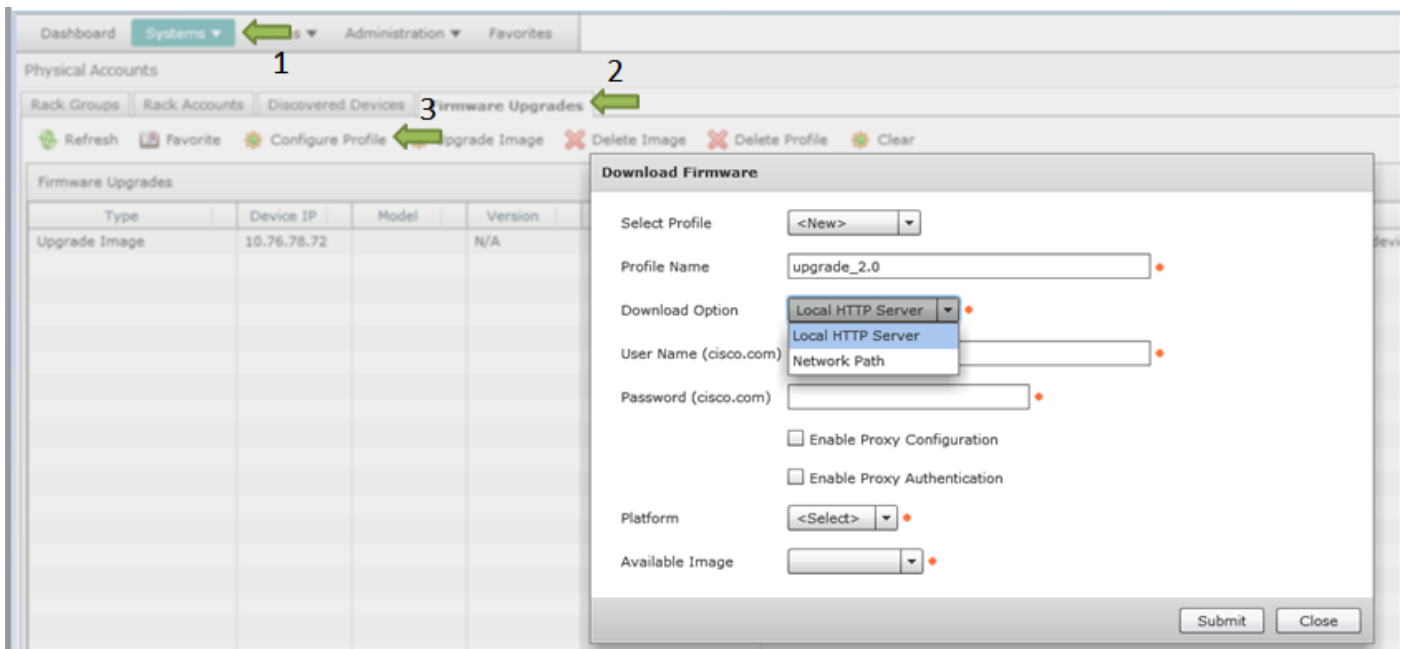
Schritt 2: Klicken Sie auf die **Registerkarte**.

Schritt 3: Klicken Sie auf **Profil konfigurieren**.

Schritt 4: Im Dialogfeld **Firmware herunterladen** können Sie entweder ein neues Profil erstellen oder ein vorhandenes Profil bearbeiten.

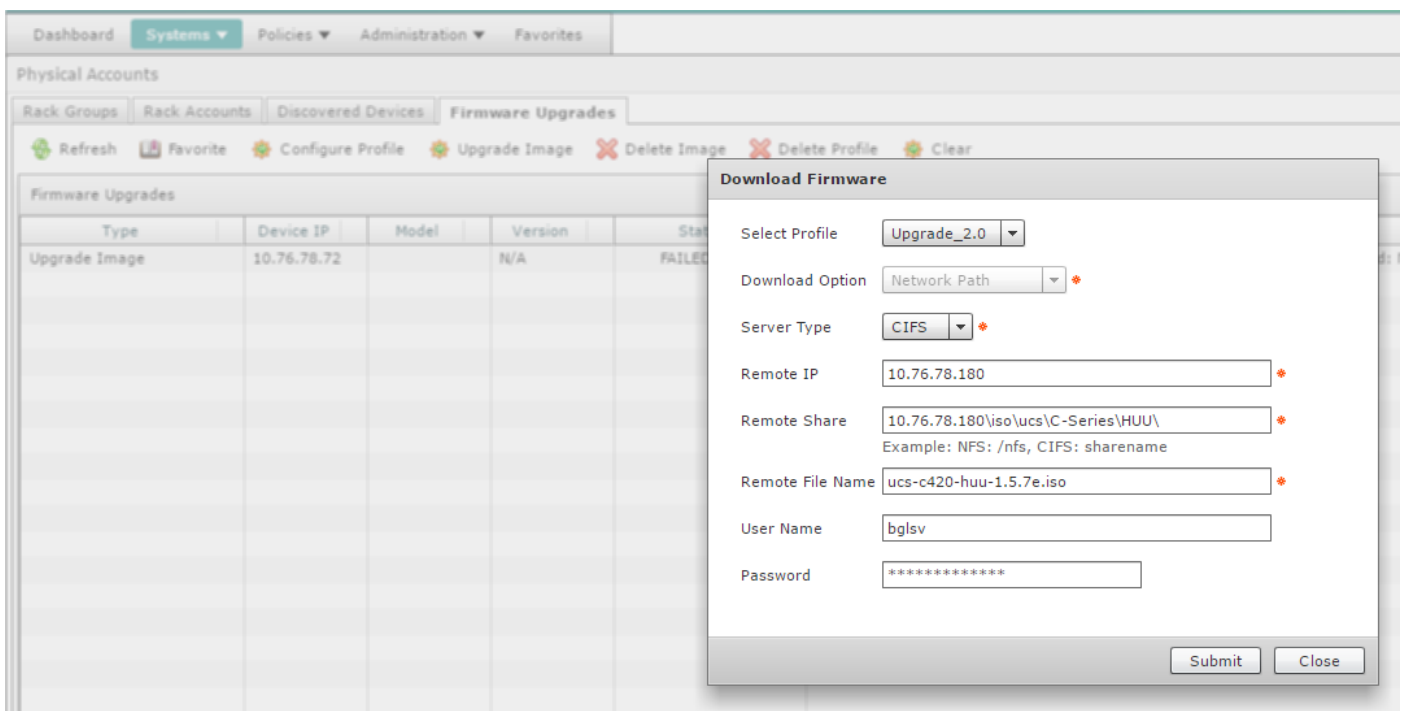
Feld	Beschreibung
Feld	Wählen Sie New aus der Dropdown-Liste aus.
Feld	Ein beschreibender Name für das Profil.
Dropdown-Liste	Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> • Lokaler HTTP-Server - Das ISO-Image wird im lokalen Cisco IM Supervisor gespeichert. • Netzwerkpfad: Das ISO-Image wird im Netzwerk gespeichert.
Feld	Geben Sie Ihren Cisco Benutzernamen ein.
Feld	Geben Sie Ihr Cisco Anmeldekennwort ein.
Kontrollkästchen	(Optional) Aktivieren Sie dieses Kontrollkästchen, um die Proxy-Konfiguration zu aktivieren und die folgenden Felder auszufüllen: <ul style="list-style-type: none"> • Feld "Hostname" - Geben Sie einen Hostnamen für die Proxykonfiguration ein. • Port-Feld - Geben Sie den Port für die Proxy-Konfiguration ein.
Kontrollkästchen Proxy-Authentifizierung aktivieren	(Optional) Aktivieren Sie dieses Kontrollkästchen, um die Proxy-Authentifizierung zu aktivieren und die folgenden Felder auszufüllen: <ul style="list-style-type: none"> • Feld "Proxy User Name" (Proxy-Benutzername) - Geben Sie einen Proxy-Benutzernamen für die Proxy-Authentifizierung ein. • Proxy Password (Proxy-Kennwort) - Geben Sie das Kennwort für den Proxy-Benutzernamen ein.
Plattform-Dropdown-Liste	Wählen Sie aus der Dropdown-Liste eine Plattform aus.
Dropdown-Liste	Wählen Sie das ISO-Image aus der Dropdown-Liste aus.

Schritt 5: Konfigurieren Sie ein **neues** Profil, wie im Bild gezeigt.



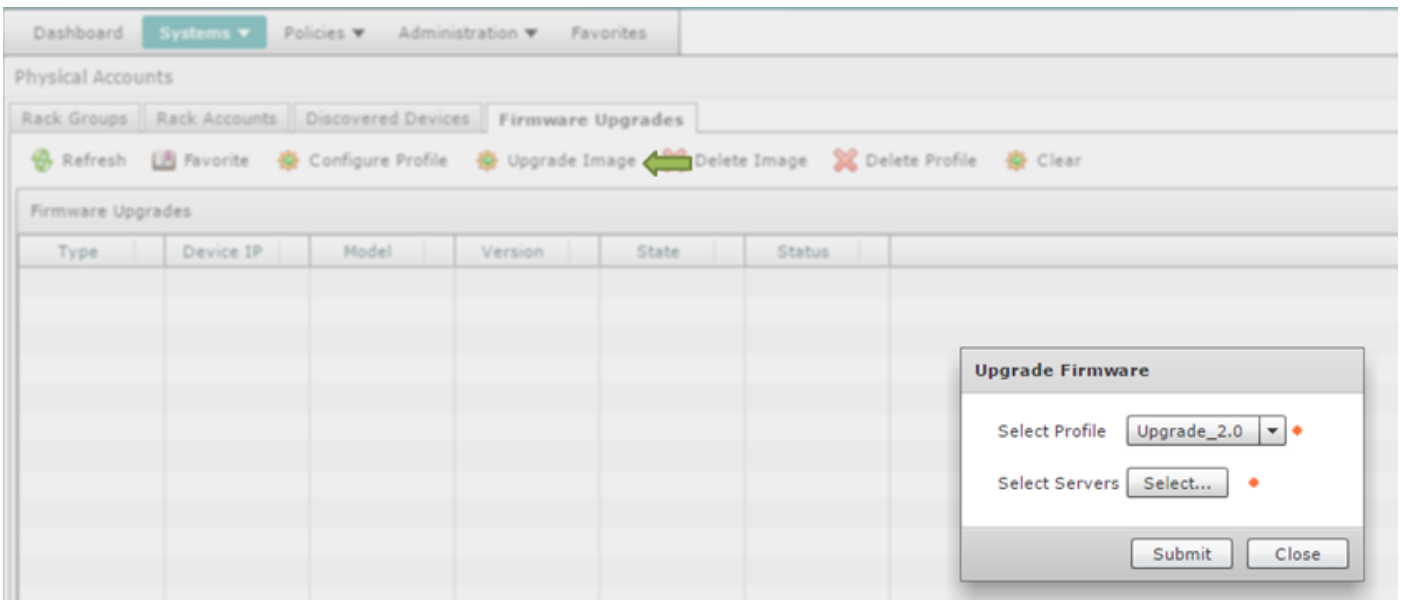
Schritt 6: Wählen Sie **Network Path** als Download Option für dieses Beispiel aus. (Sie haben CIFS und NFS als Optionen)

Schritt 7: Klicken Sie wie im Bild gezeigt auf **Senden**.



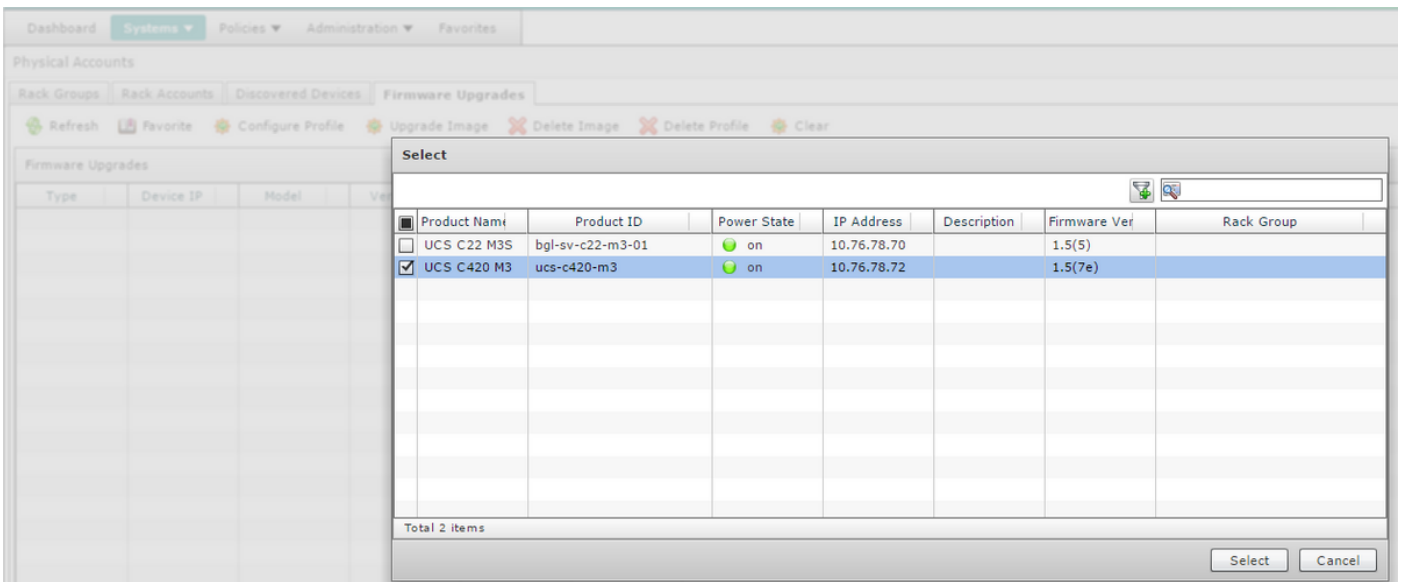
Schritt 8: Klicken Sie auf **Image aktualisieren**.

Schritt 9: Klicken Sie auf **Auswählen...** um die Server auszuwählen, die Sie aktualisieren möchten, wie im Bild gezeigt.



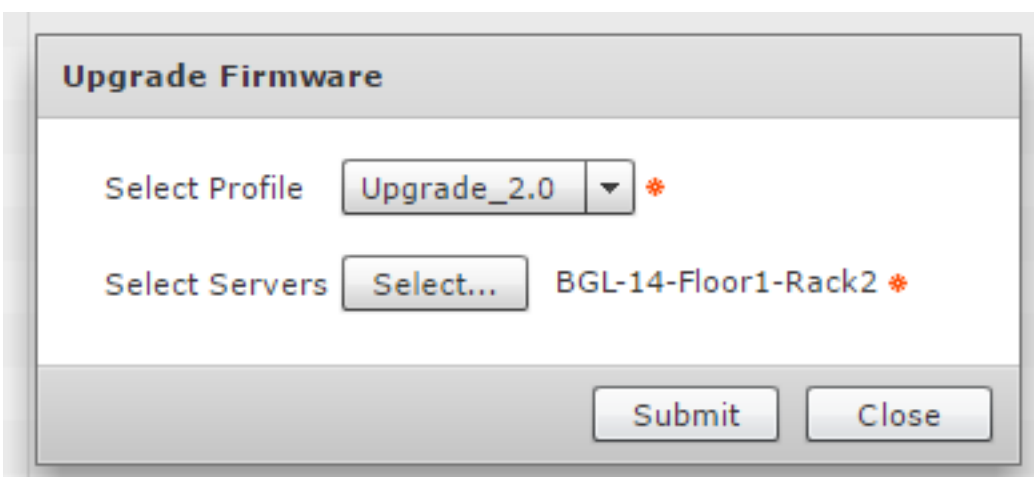
Schritt 10: Für dieses Beispiel wird ein einzelner Server ausgewählt.

Schritt 11: Klicken Sie wie im Bild gezeigt auf **Auswählen**.



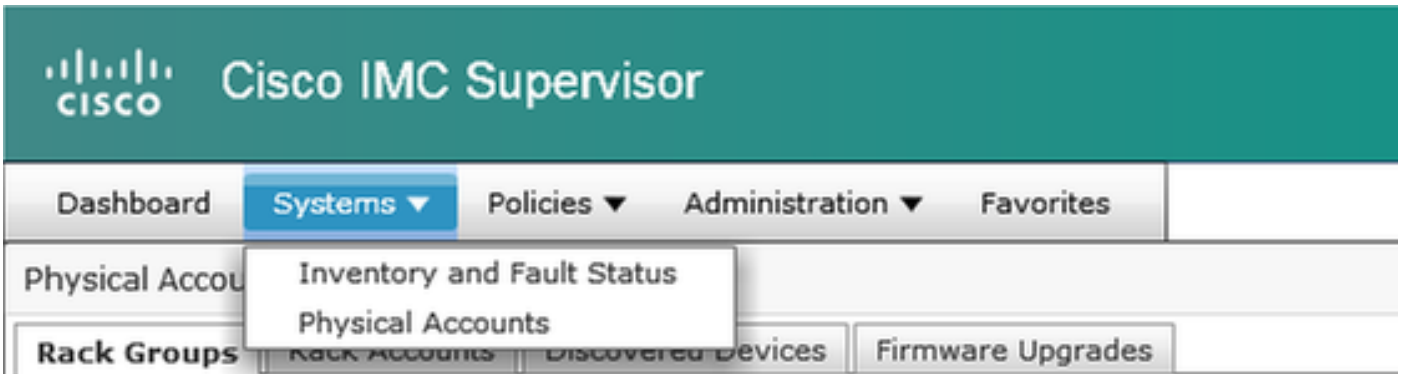
Schritt 12: Der ausgewählte Server wird angezeigt.

Schritt 13: Klicken Sie auf **Senden**, wie im Bild gezeigt.



Hinweis: Wenn Sie ein Upgrade von Cisco IMC Version 2.0(x) durchführen, müssen Sie das Cisco IMC-Standardkennwort ändern.

Schritt 14: Um den Status des Upgrades zu überprüfen, navigieren Sie zu **System > Inventory and Fault Status (System > Bestand und Fehlerstatus)**, wie im Bild gezeigt.



Schritt 15: Erweitern Sie **Rack-Gruppen**, und wählen Sie die entsprechende Gruppe aus, in die die Server zuvor eingefüllt wurden.

Schritt 16: Klicken Sie auf **Rack-Server** und wählen Sie den gewünschten Server aus.

Schritt 17: Anschließend muss eine zusätzliche Zeile mit Remoteoptionen angezeigt werden.

Schritt 18: Klicken Sie in dieser Zeile auf **KVM Console**, und Sie können die Aktualisierung wie im Bild gezeigt in Aktion sehen.



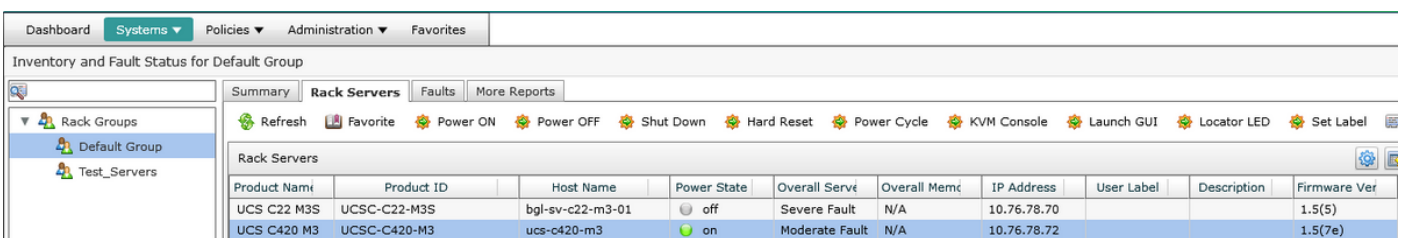
Daten des technischen Supports auf einen Remote-Server exportieren

9. Führen Sie diese Aktionen aus, um Daten des technischen Supports zu extrahieren.

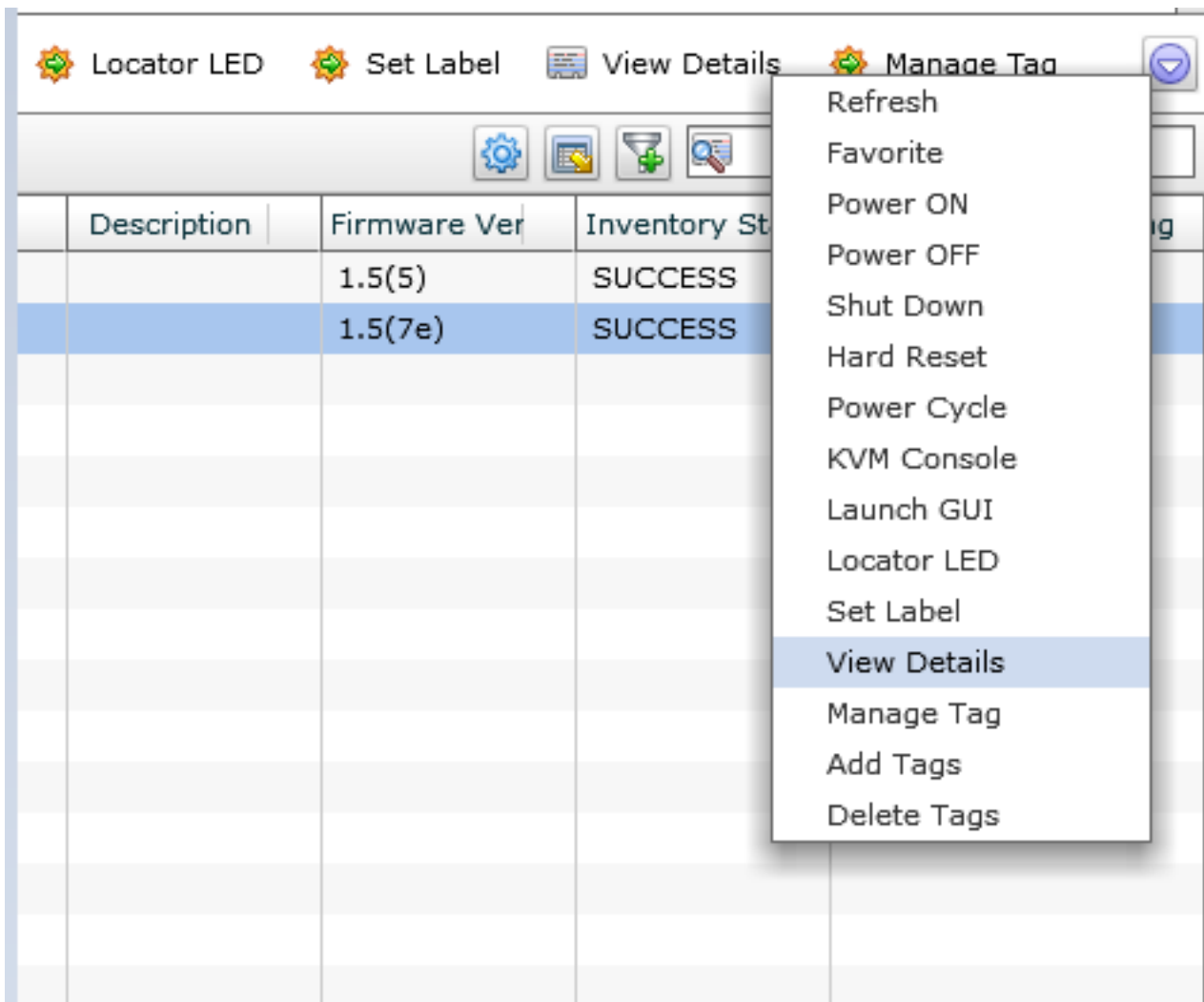
Schritt 1: Navigieren Sie zu **Systems > Inventory and Fault Status (Systeme > Bestand und Fehlerstatus für Standardgruppe)**.

Schritt 2: Erweitern Sie **Rack-Gruppen**, und wählen Sie die Rack-Gruppe aus, die die Server enthält.

Schritt 3: Wählen Sie die Registerkarte **Rack-Server** aus, wie im Bild gezeigt.

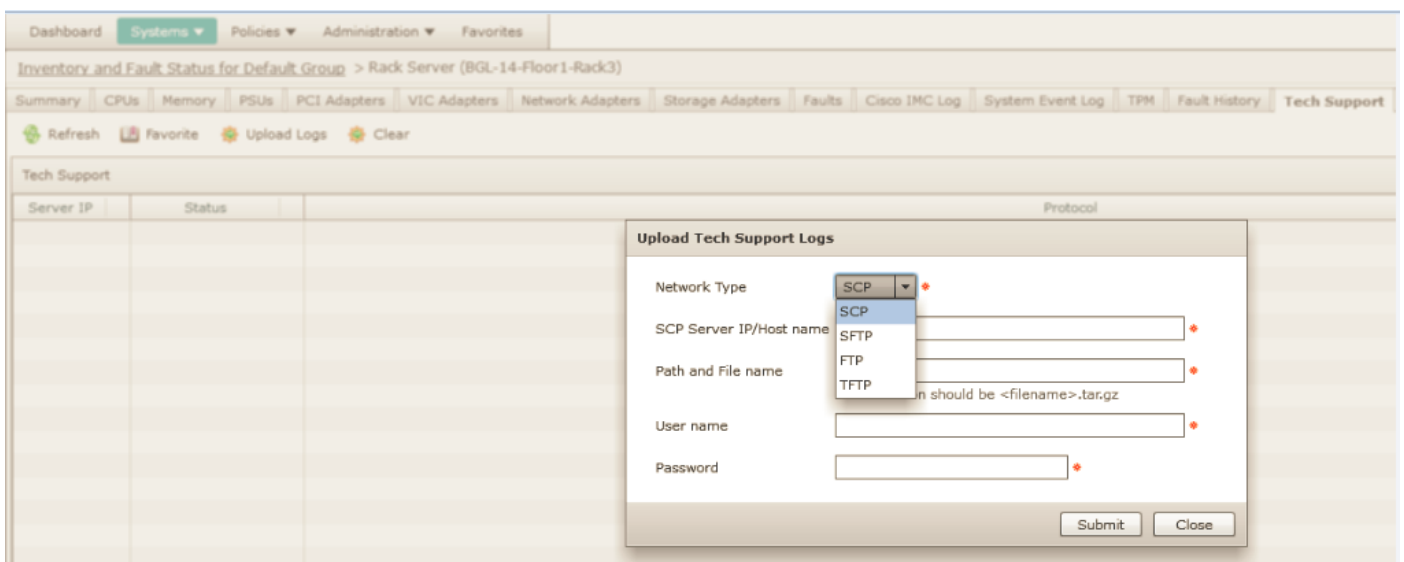


Schritt 4: Doppelklicken Sie auf den Server in der Liste, um die Details anzuzeigen, oder klicken Sie auf den Server in der Liste. Klicken Sie dann ganz rechts über den Pfeil nach unten auf **Details anzeigen**, wie im Bild gezeigt.



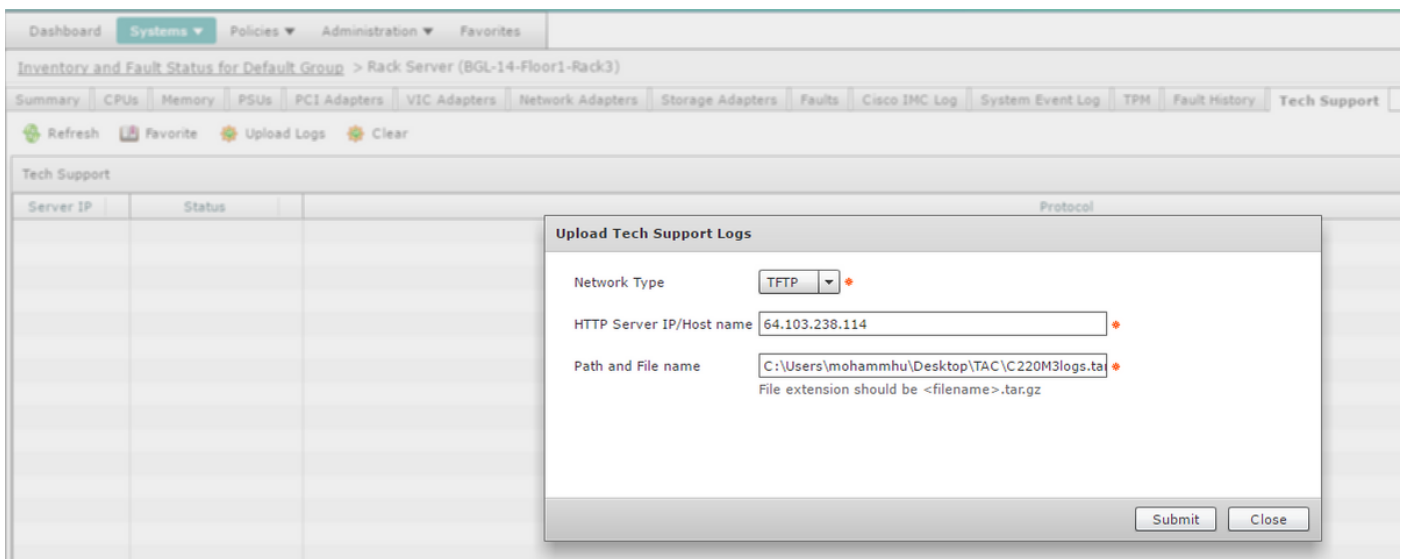
Schritt 5: Klicken Sie auf die Registerkarte **Technischer Support**.

Schritt 6: Wählen Sie den entsprechenden Netzwerktyp aus, um die Dateien wie im Bild gezeigt hochzuladen.



Schritt 7: Wählen Sie für dieses Beispiel **TFTP** aus.

Schritt 8: Klicken Sie auf **Senden**, wie im Bild gezeigt.



Schritt 9: Der Screenshot hier zeigt, dass die Protokolle erfolgreich an den angegebenen Speicherort hochgeladen wurden.

Server IP	Status	Protocol
10.76.78.70	completed (100 %)	TFTP

The screenshot shows the same web-based interface as before, but the "Upload Tech Support Logs" dialog is closed. The "Tech Support" table is now visible and contains one entry. The table has three columns: "Server IP", "Status", and "Protocol". The entry shows "10.76.78.70" in the "Server IP" column, "completed (100 %)" in the "Status" column, and "TFTP" in the "Protocol" column. The background interface remains the same as in the previous screenshot.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.