Configuración de Cisco IMC Supervisor para servidores C-Series y E-Series

Contenido

Introducción

Este documento describe cómo configurar Cisco Integrated Management Controller (IMC) Supervisor para servidores C-Series y E-Series.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidores de la serie C de Cisco
- Servidores de la serie E de Cisco

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Internet Explorer 8 o superior
- Google Chrome 4.1 o superior
- Firefox 3.5 o superior
- Safari 4.0 o superior (para Apple MAC o Microsoft Windows)
- Los exploradores requieren el plug-in Adobe Flash Player versión 11 o superior.

Servidores UCS serie C

- 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

Servidores UCS serie E

- 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

Versiones de firmware mínimas

Servidores	Versión mínima del firmware
Servidores UCS serie C	1.5(4) y posteriores
Servidores UCS serie E	2.3.1 y posteriores

Tarjetas PCiE compatibles

- Tarjeta de interfaz virtual (VIC) Cisco UCS 1225
- VIC Cisco UCS 1225T

Versiones de hipervisor compatibles

- ESXi 5.1

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

Antecedentes

Cisco IMC Supervisor es un sistema de gestión que permite administrar servidores de montaje en bastidor a gran escala.

Puede utilizar Cisco IMC Supervisor para realizar estas tareas para un servidor de montaje en bastidor:

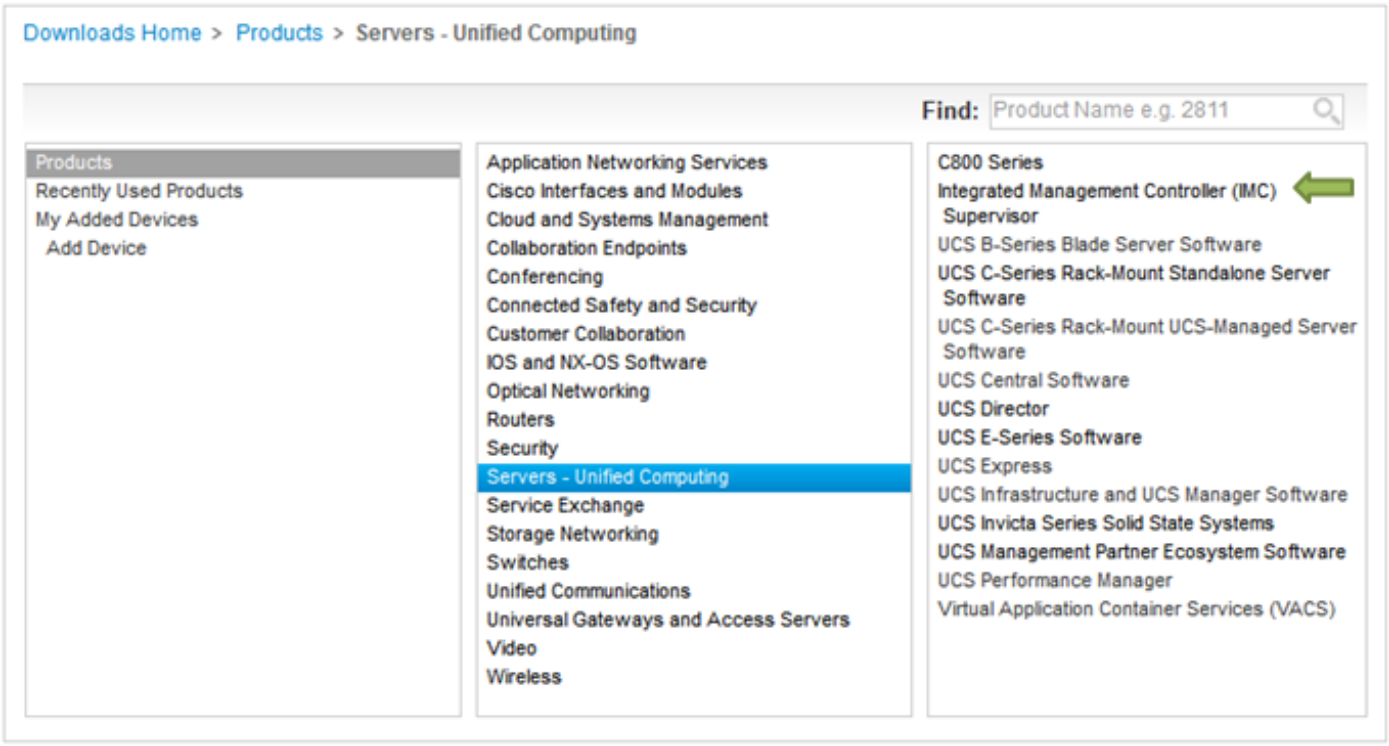
- Compatibilidad con agrupamiento lógico de servidores y vistas de resumen por grupo
- Recopilar inventario para los servidores
- Proporcionar capacidades de supervisión para servidores y grupos
- Gestión del firmware que incluye la descarga, actualización y activación del firmware
- Gestionar acciones de servidor independientes que incluyen control de alimentación, control de LED, recopilación de registros, inicio de teclado/vídeo/ratón (KVM), inicio de la interfaz de usuario CIMC y alertas de correo electrónico
- Control de acceso basado en funciones (RBAC) para restringir el acceso y las capacidades

Configurar

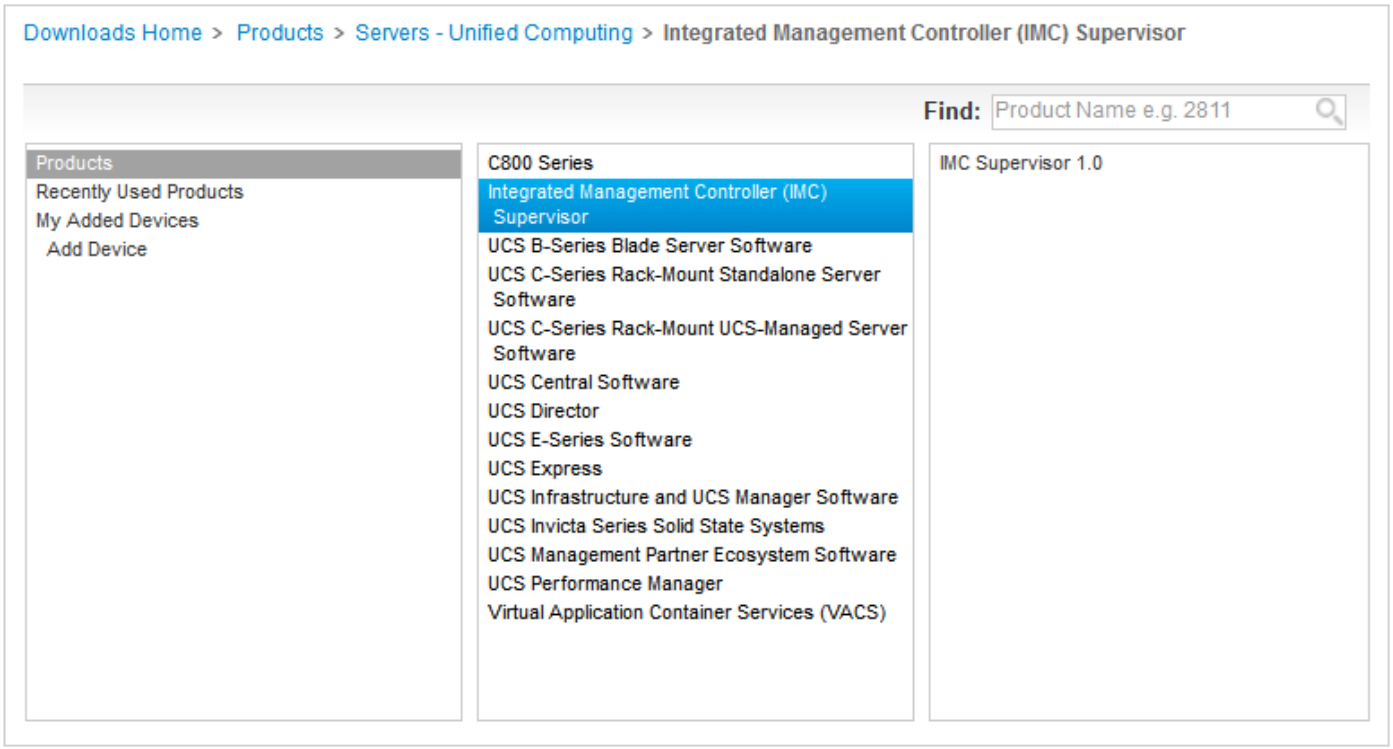
Implementación de Cisco IMC Supervisor

1. Complete estos pasos para implementar Cisco IMC Supervisor.

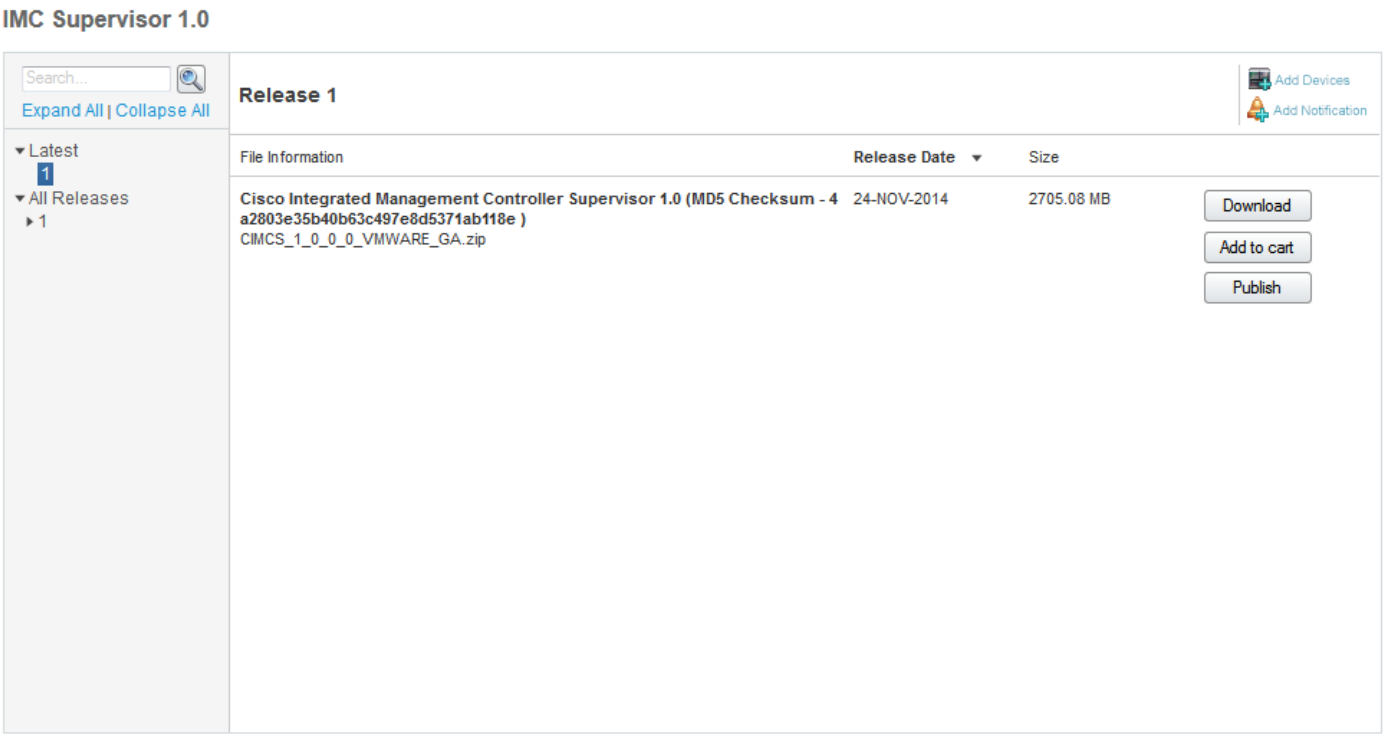
Paso 1. Para descargar el archivo zip para Cisco IMC Supervisor desde Cisco.com, navegue hasta **Productos > Servidores-Unified Computing > Supervisor de Integrated Management Controller (IMC)** como se muestra en la imagen.



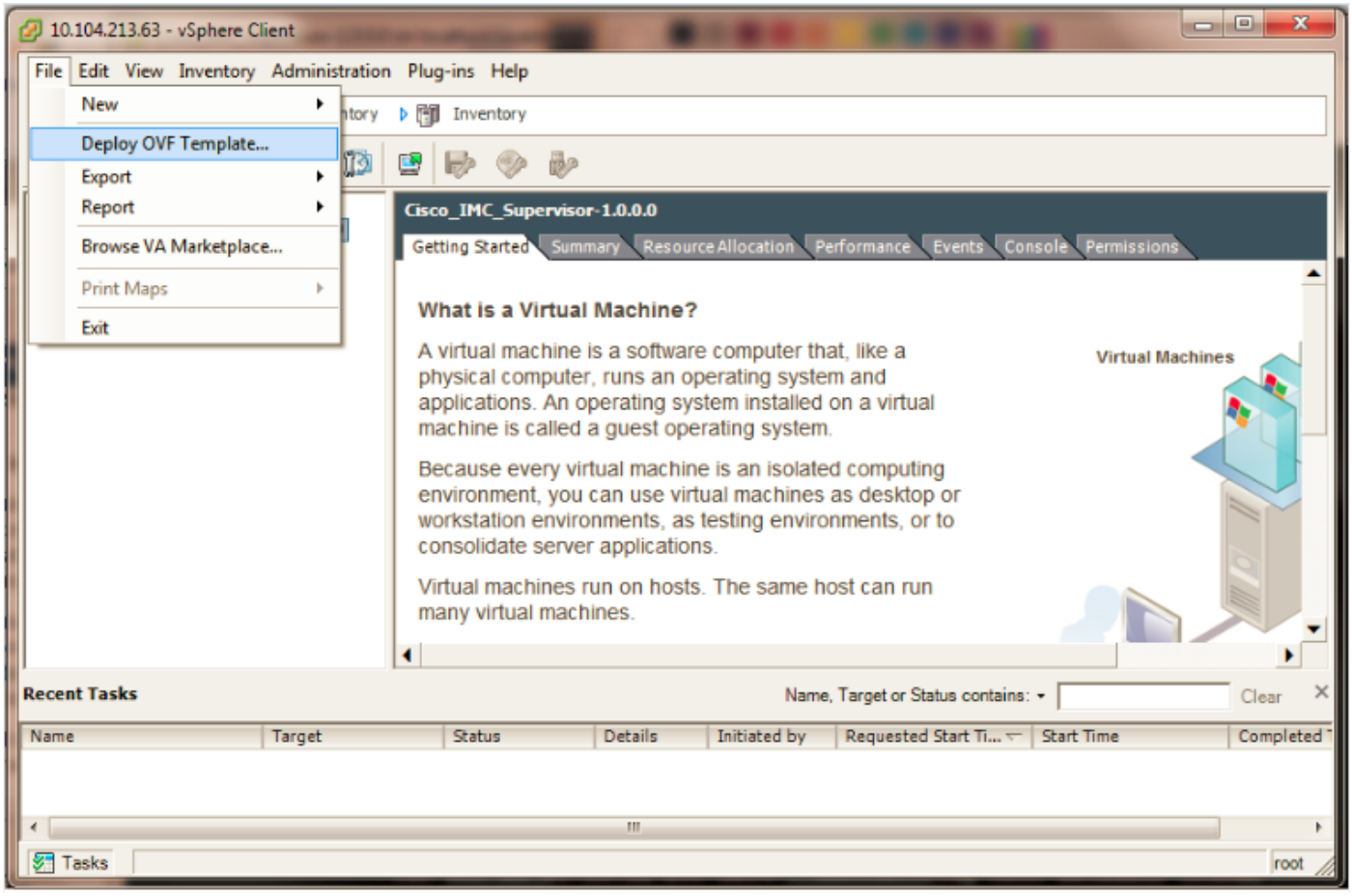
Paso 2. Seleccione **IMC Supervisor 1.0** como se muestra en la imagen.



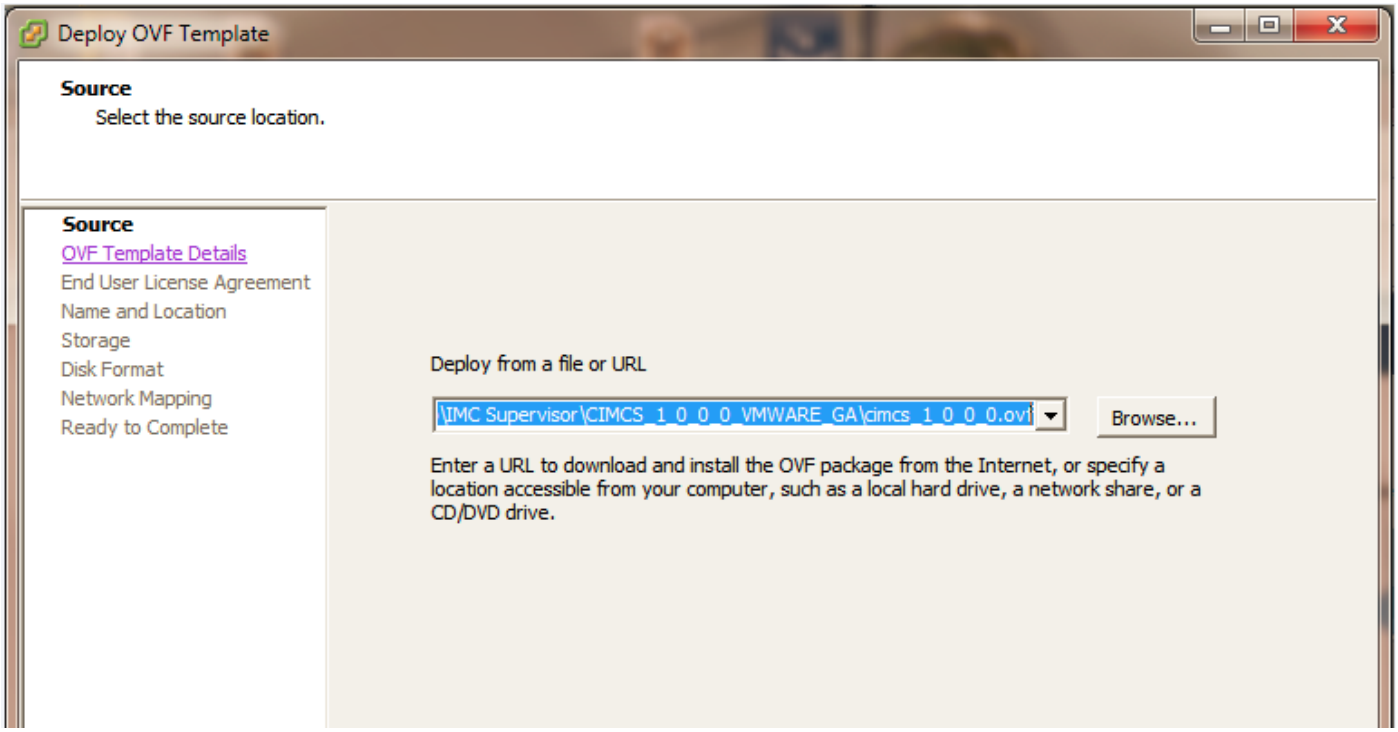
Paso 3. Haga clic en **Descargar** como se muestra en la imagen.

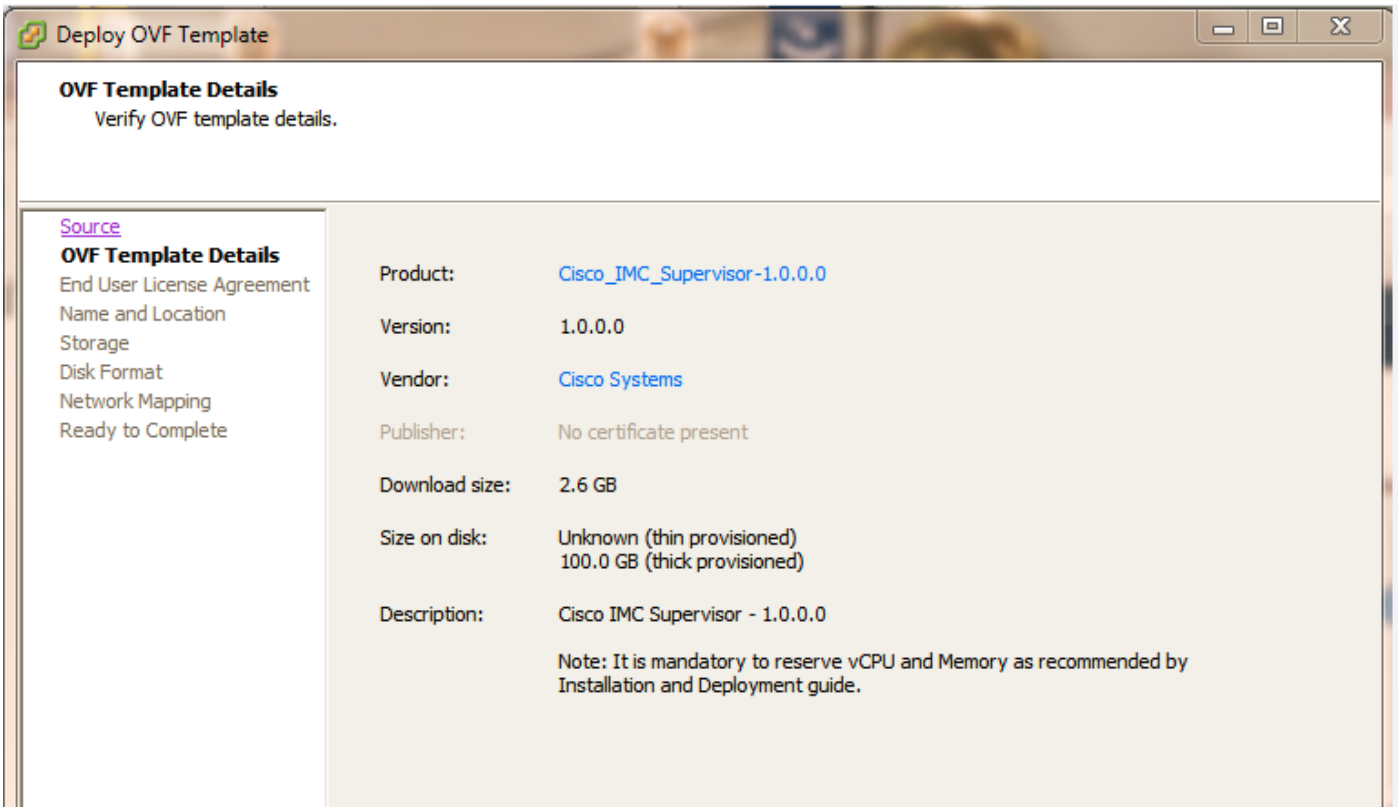


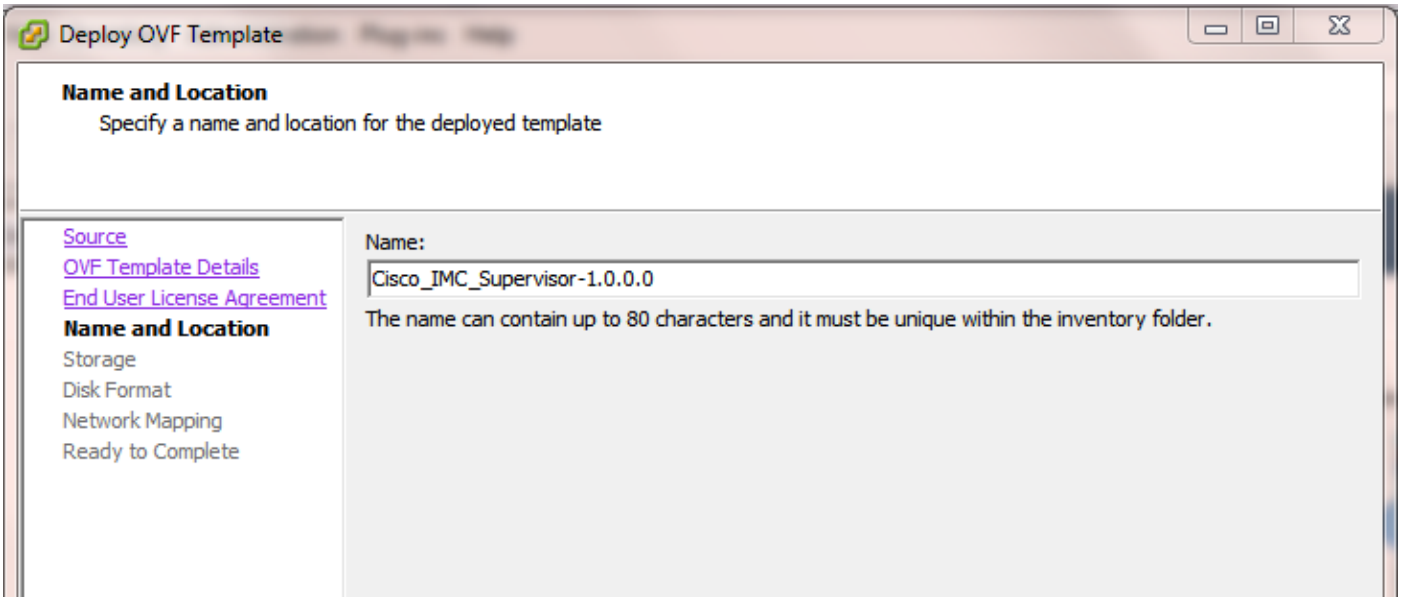
Paso 4. Para implementar el Open Virtual Appliance (OVA), navegue hasta **File >Deploy OVF Template** como se muestra en la imagen.

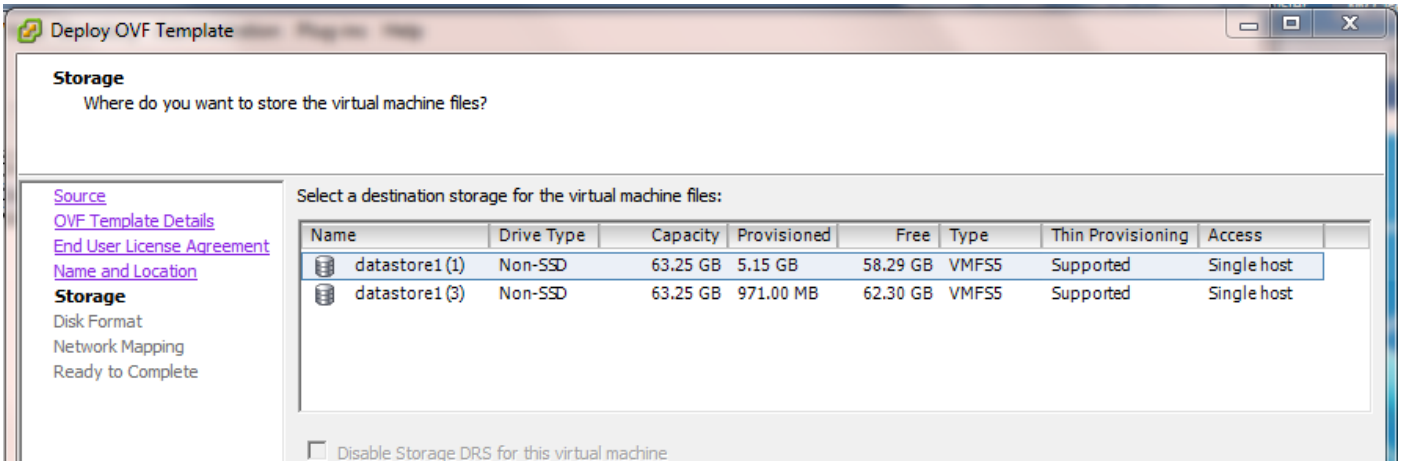


Paso 5. Continúe con el proceso paso a paso para implementar la plantilla Open Virtualization Format (OVF) como se muestra en las imágenes.


Deploy OVF Template
Source
Select the source location.
Source
OVF Template Details
End User License Agreement
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete
Deploy from a file or URL
\IMC Supervisor\CIMCS_1_0_0_0_VMWARE_GA\cimcs_1_0_0_0.ovf
Browse...
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

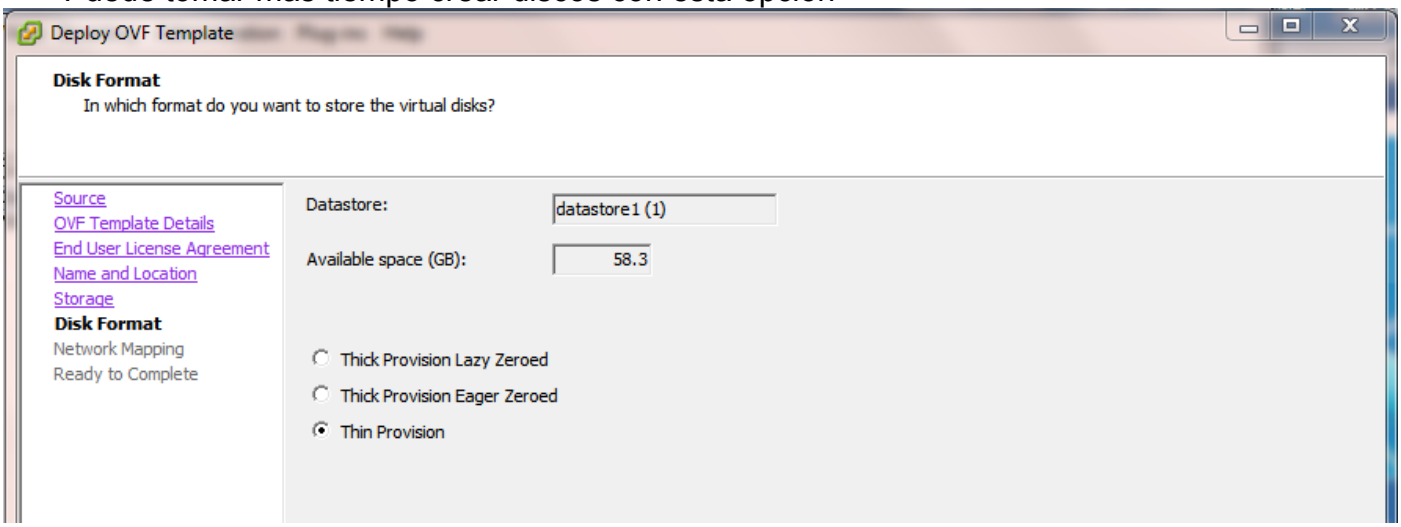

Deploy OVF Template
OVF Template Details
Verify OVF template details.
Source
OVF Template Details
End User License Agreement
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete
Product: Cisco_IMC_Supervisor-1.0.0.0
Version: 1.0.0.0
Vendor: Cisco Systems
Publisher: No certificate present
Download size: 2.6 GB
Size on disk: Unknown (thin provisioned)
100.0 GB (thick provisioned)
Description: Cisco IMC Supervisor - 1.0.0.0
Note: It is mandatory to reserve vCPU and Memory as recommended by Installation and Deployment guide.



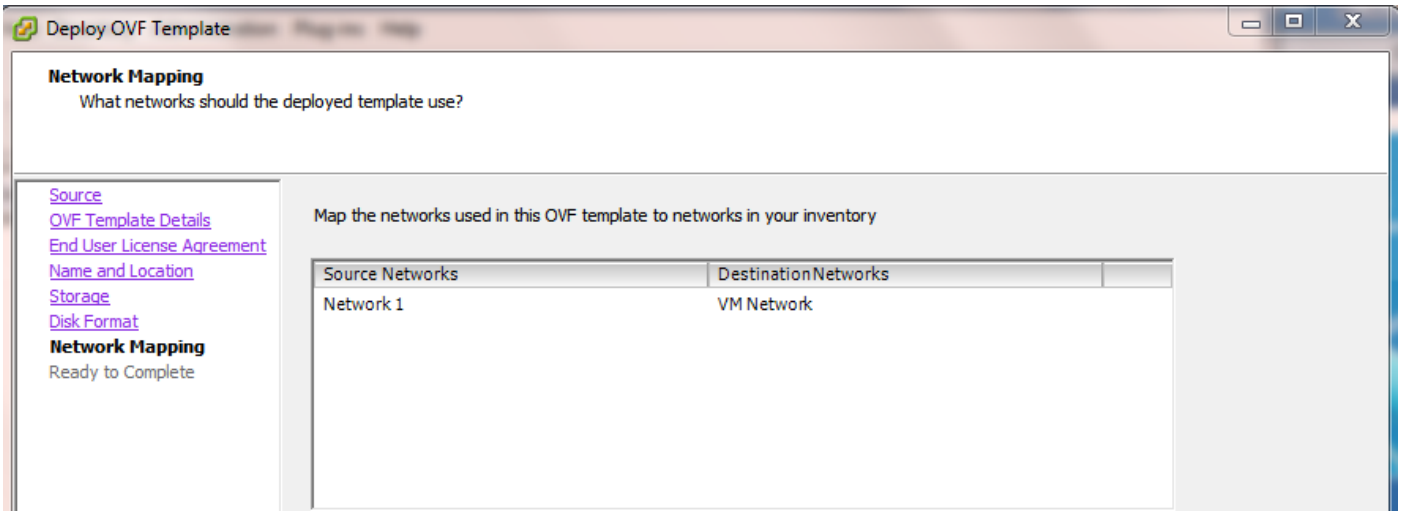


En el panel **Formato de disco**, elija uno de los botones de opción y haga clic en **Siguiente** como se muestra en la imagen.

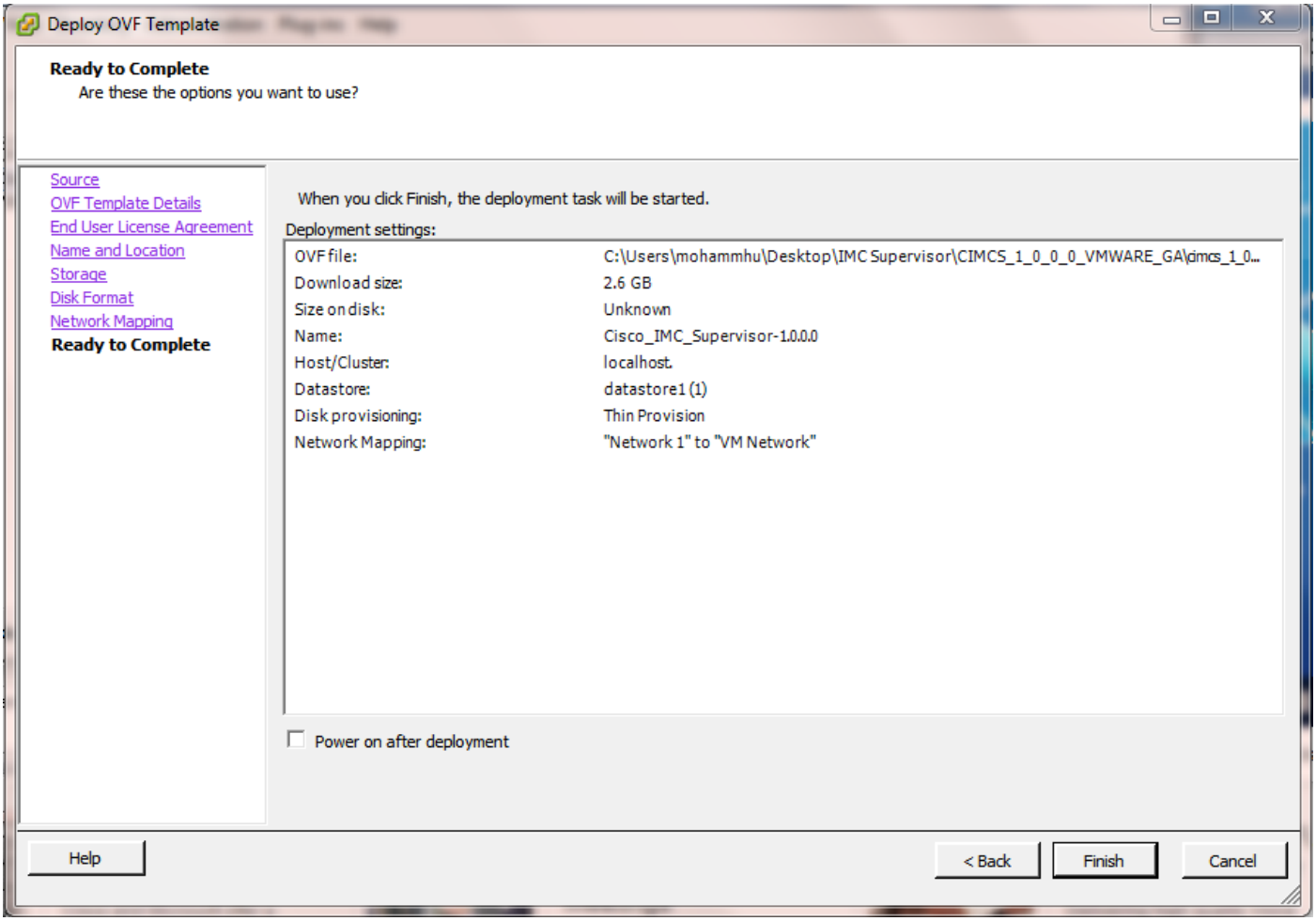
- Aprovisionamiento dinámico: para asignar el almacenamiento a demanda a medida que los datos se escriben en el disco
- Provisión gruesa con cero flojo - Para asignar el almacenamiento inmediatamente en formato grueso
- Aprovisionamiento grueso con cero: para asignar el almacenamiento en formato grueso. Puede tomar más tiempo crear discos con esta opción



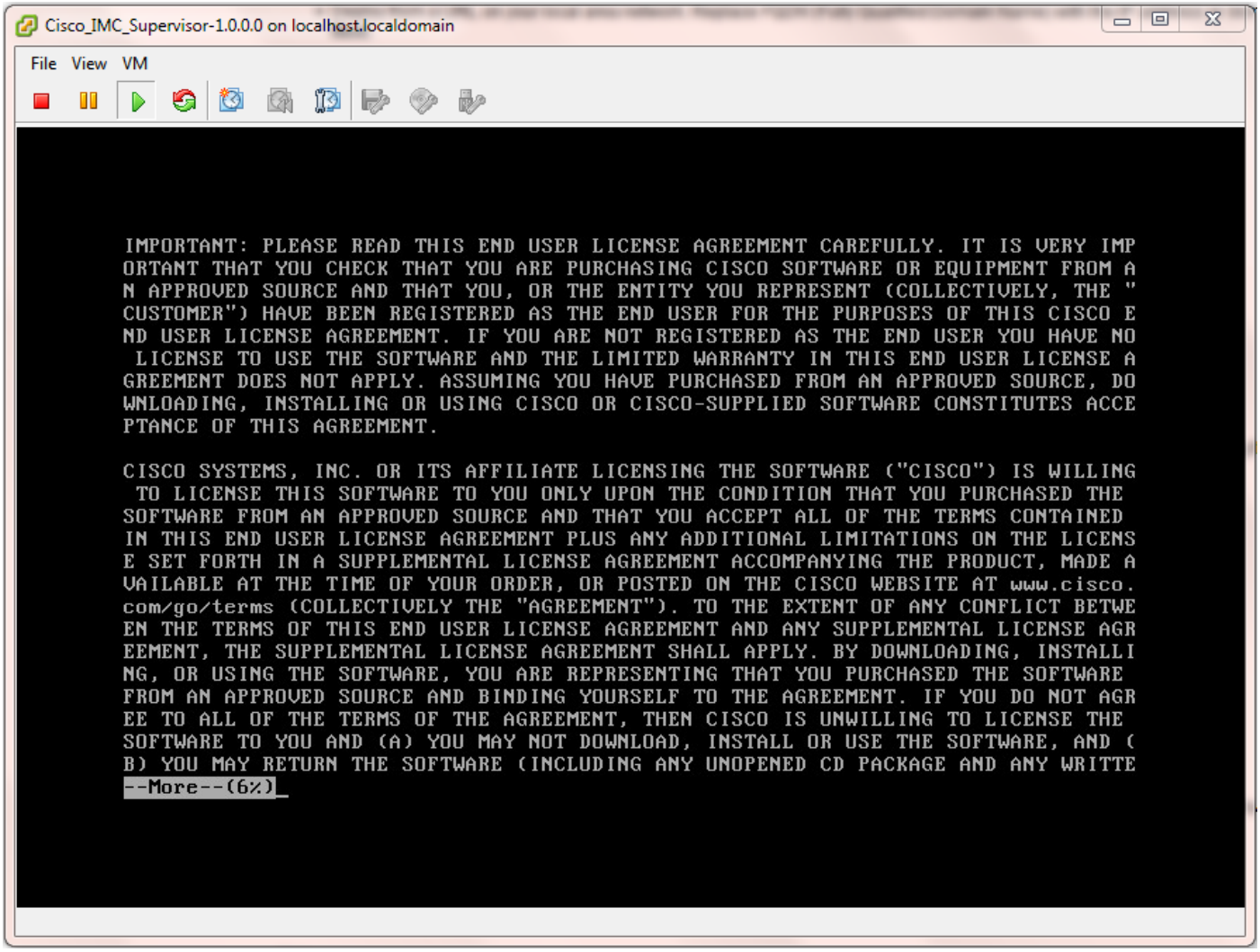
Paso 6. Seleccione el grupo de puertos adecuado para la red de máquina virtual (VM) como se muestra en la imagen.



Paso 7. Haga clic en **Finalizar** como se muestra en la imagen.

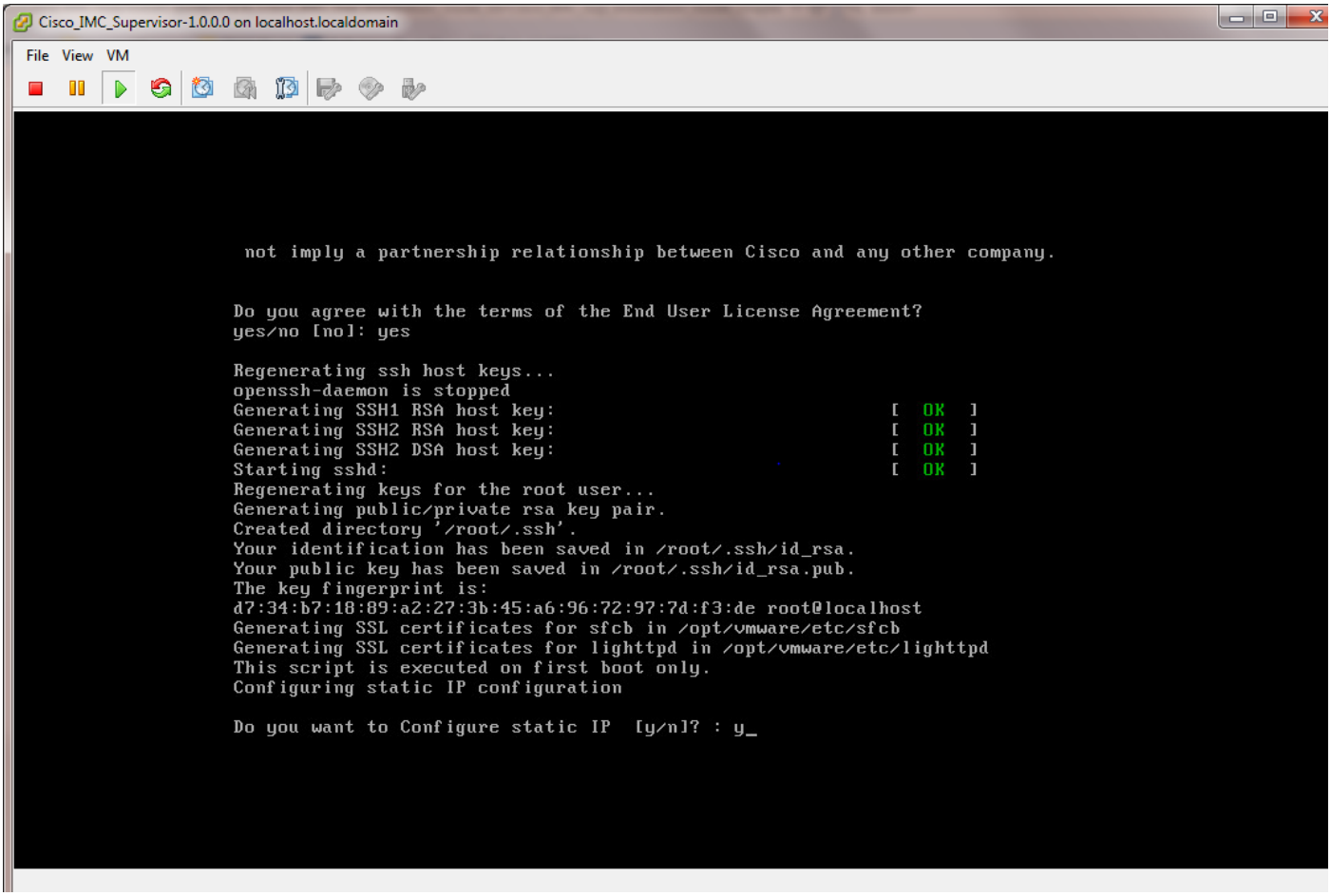


Paso 8. Abra la consola de la máquina virtual y **Acepte** el contrato de licencia como se muestra en la imagen.



Paso 9. Una vez hecho, ingrese **y** para configurar una IP estática como se muestra en la imagen.

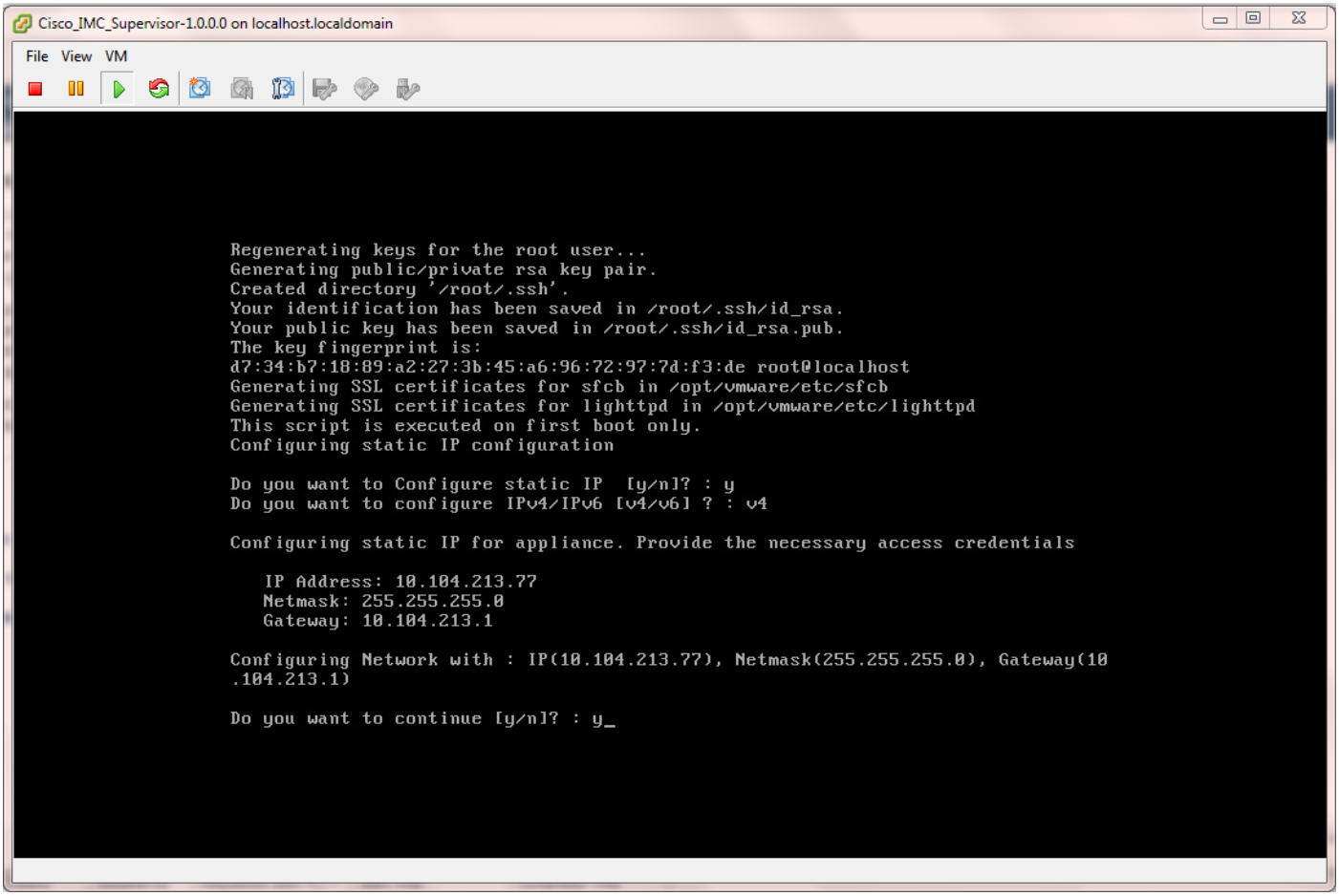
Paso 10. Si desea utilizar DHCP, introduzca **n** para asegurarse de que las direcciones IP se asignan automáticamente.

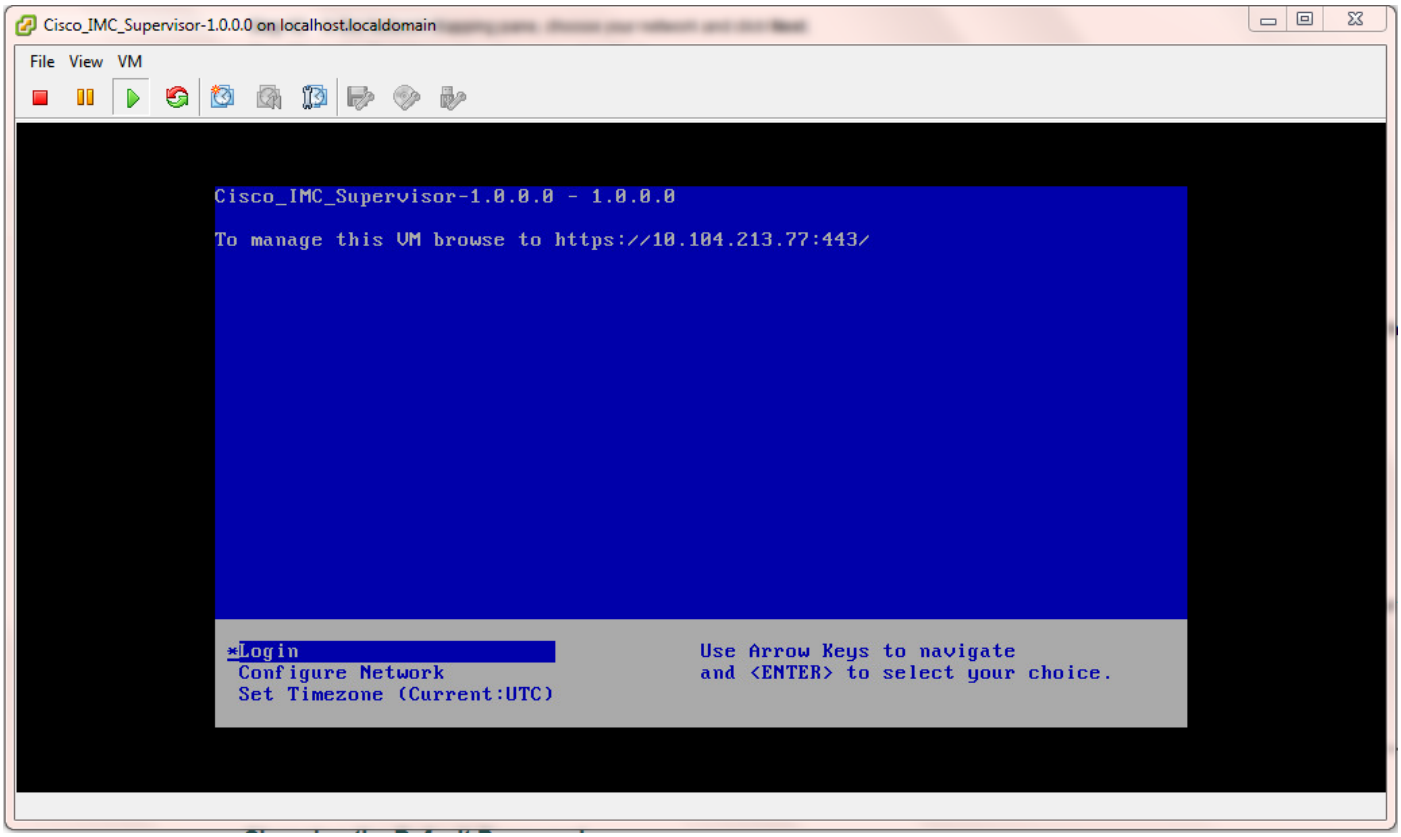


Paso 11. Si desea utilizar una dirección IP estática, introduzca **y** y, a continuación, se le pedirá que seleccione **IPv4** o **IPv6**. Ingrese **V4** para configurar IPV4 y luego ingrese la información como se muestra en las imágenes:

- Dirección IPMáscara de redGateway

Nota: Actualmente, sólo se soporta IPv4 para configurar las direcciones IP estáticas.



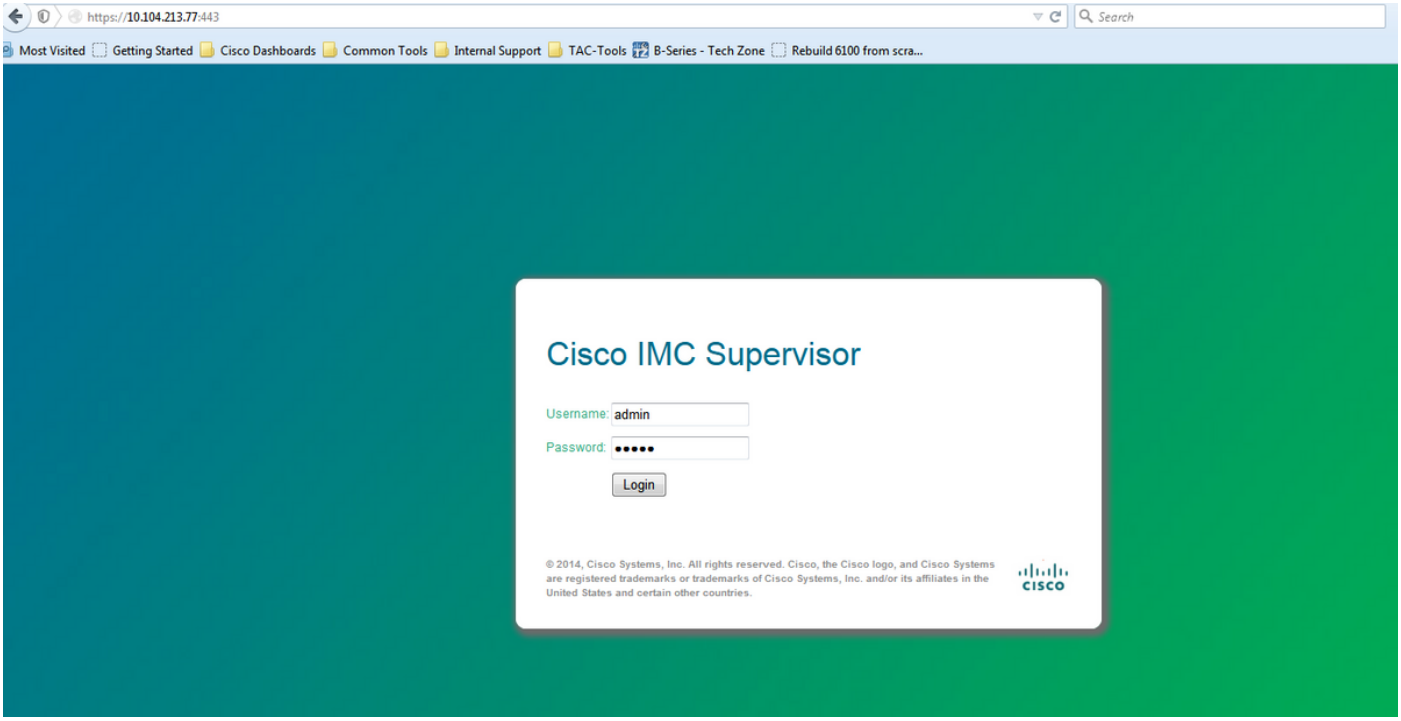


Paso 12. Después de que el dispositivo se haya iniciado, transfiera la dirección IP del supervisor de Cisco IMC a un navegador web compatible para acceder a la página de inicio de sesión.

En la página Inicio de sesión, ingrese **admin** como el nombre de usuario y ***admin*** como contraseña.

Nota: Puede cambiar su contraseña de administrador después de este inicio de sesión inicial.

La interfaz de usuario de Cisco IMC Supervisor es la que se muestra en la imagen.



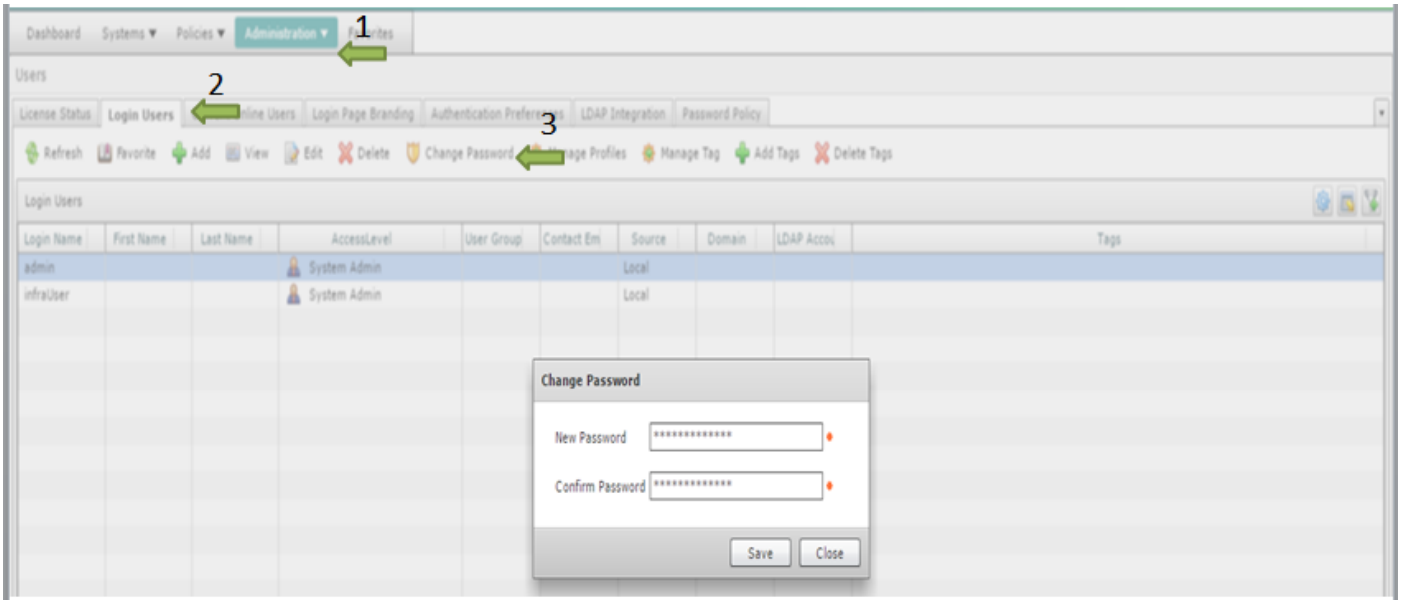
Cambiar contraseña predeterminada

2. Complete estos pasos para cambiar la contraseña predeterminada.

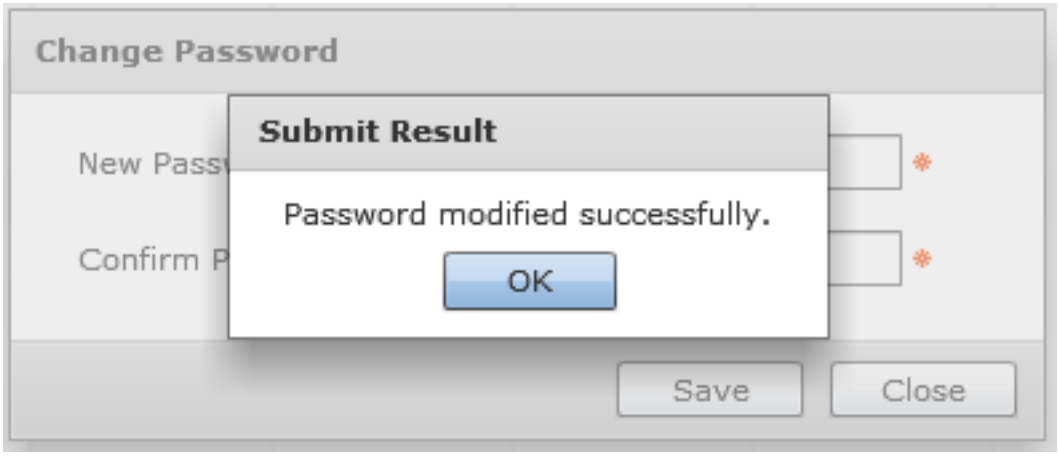
Paso 1. Vaya a **Administración > Usuarios**.

Paso 2. Haga clic en la pestaña **Usuarios de Inicio de Sesión**.

Paso 3. En la lista de usuarios, seleccione la función de usuario para la que desea cambiar la contraseña como se muestra en la imagen.



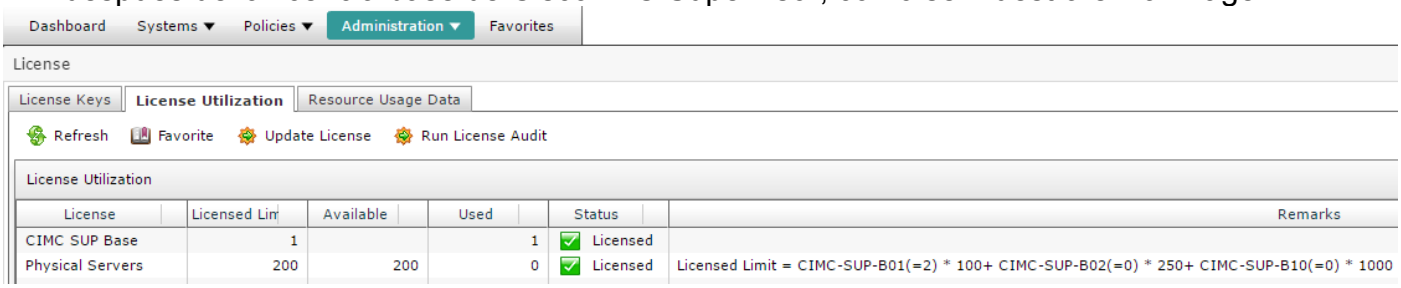
Paso 4. Después de especificar la nueva contraseña, haga clic en **Guardar** y en **Aceptar** en el **Resultado de envío** como se muestra en la imagen.



Información de licencia

3. Cisco IMC Supervisor requiere que tenga estas licencias válidas:

- Licencia básica de Cisco IMC Supervisor.
- Licencia de habilitación de terminales masivos de Cisco IMC Supervisor que se instala después de la licencia base de Cisco IMC Supervisor, como se muestra en la imagen.

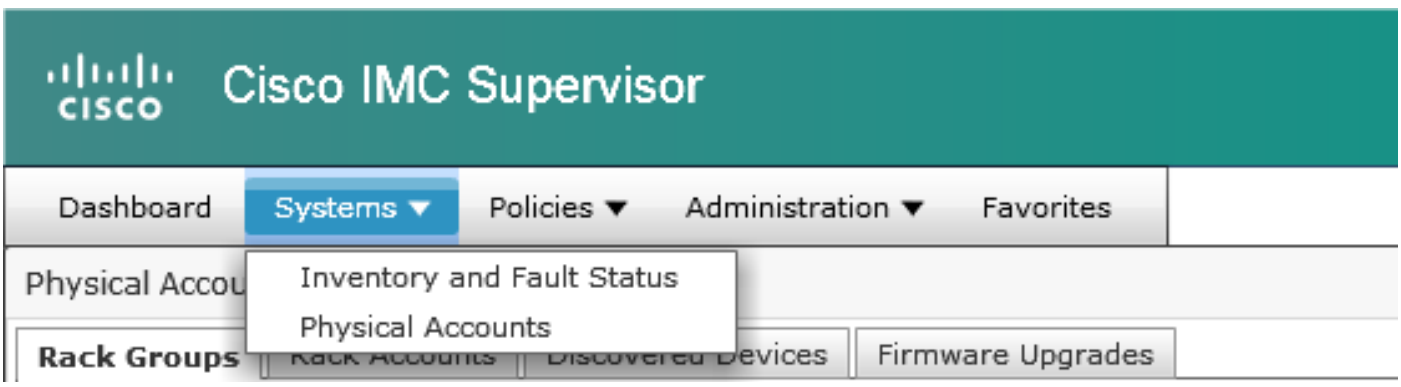


> **Nota:** A menos que tenga estas licencias, no se pueden realizar tareas como agrupar servidores en una cuenta de rack, etc.

Detectar servidor

4. Realice estas acciones para detectar servidores.

Paso 1. Vaya a **Sistema > Cuentas físicas > Dispositivos descubiertos** como se muestra en la imagen.



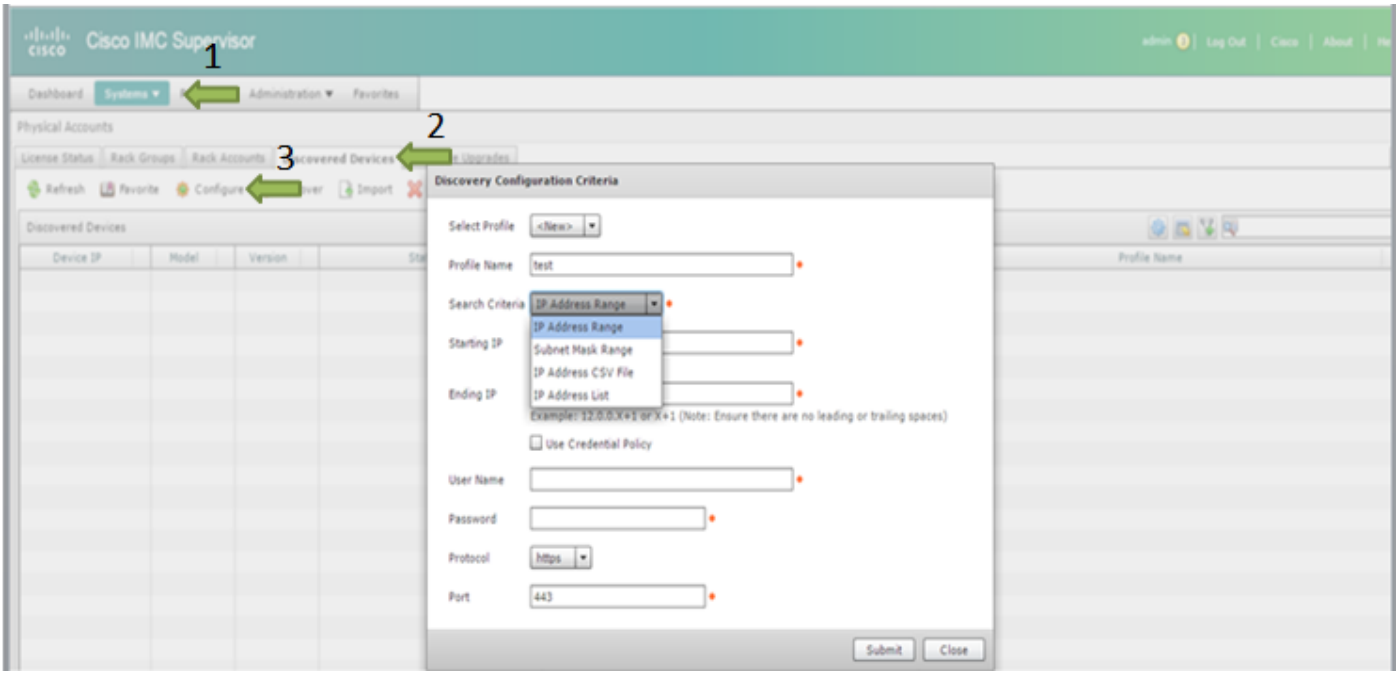
Paso 2. Haga clic en Configure (Configurar).

Paso 3. En el cuadro de diálogo **Criterios de configuración de detección**, puede crear un nuevo perfil o editar un perfil existente.

Paso 4. La creación de un perfil **Nuevo** es como se muestra en la imagen.

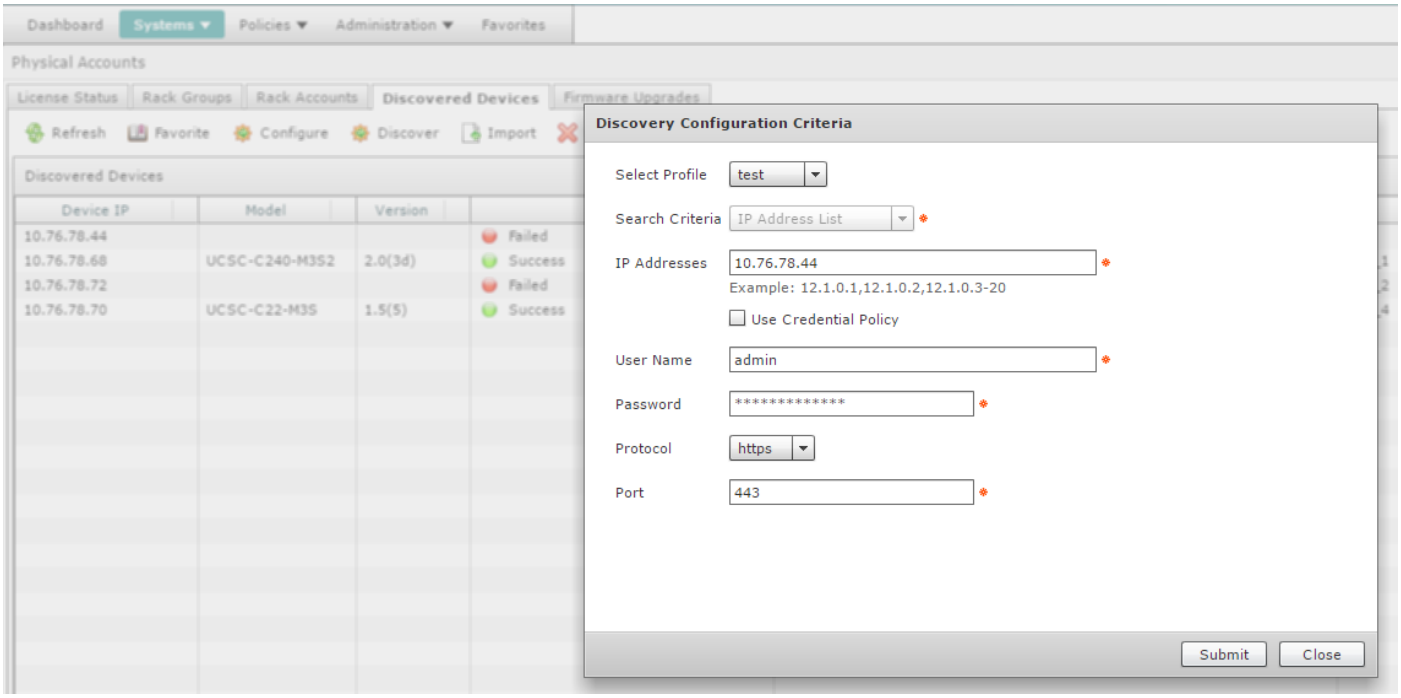
Paso 5. En los criterios de búsqueda, puede elegir el método adecuado para detectar los servidores.

Paso 6. Elija **Lista de Direcciones IP** para este ejemplo.

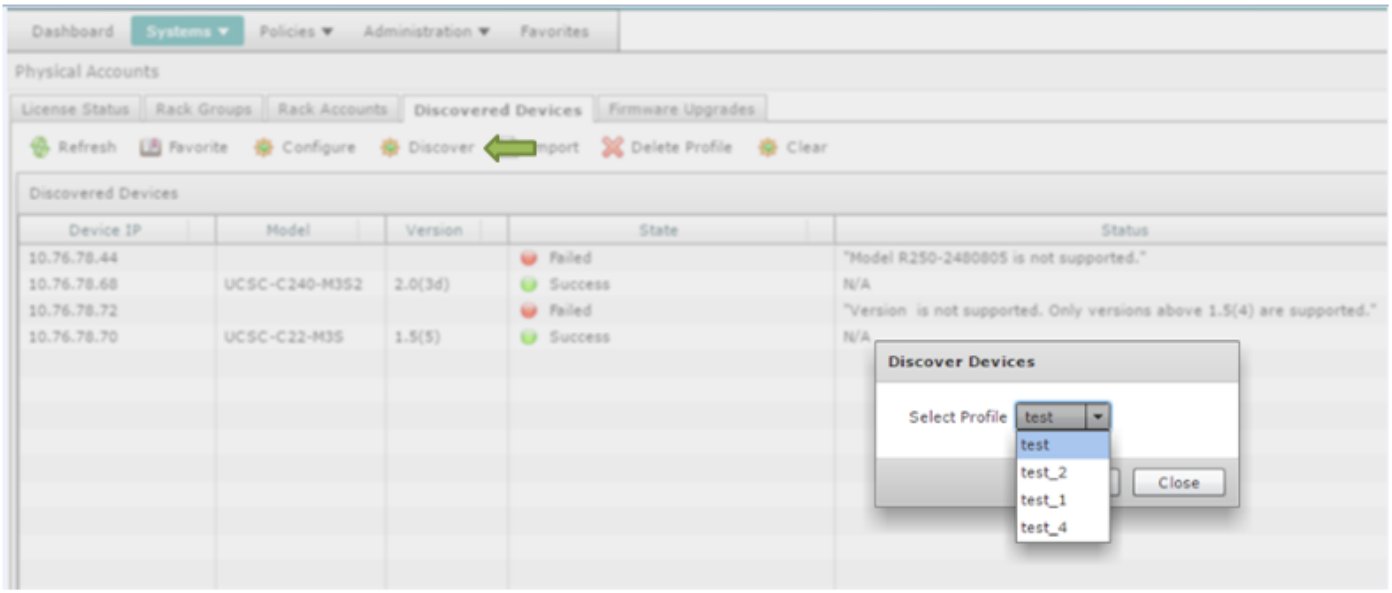


Paso 7. Introduzca la dirección IP del servidor que desea descubrir.

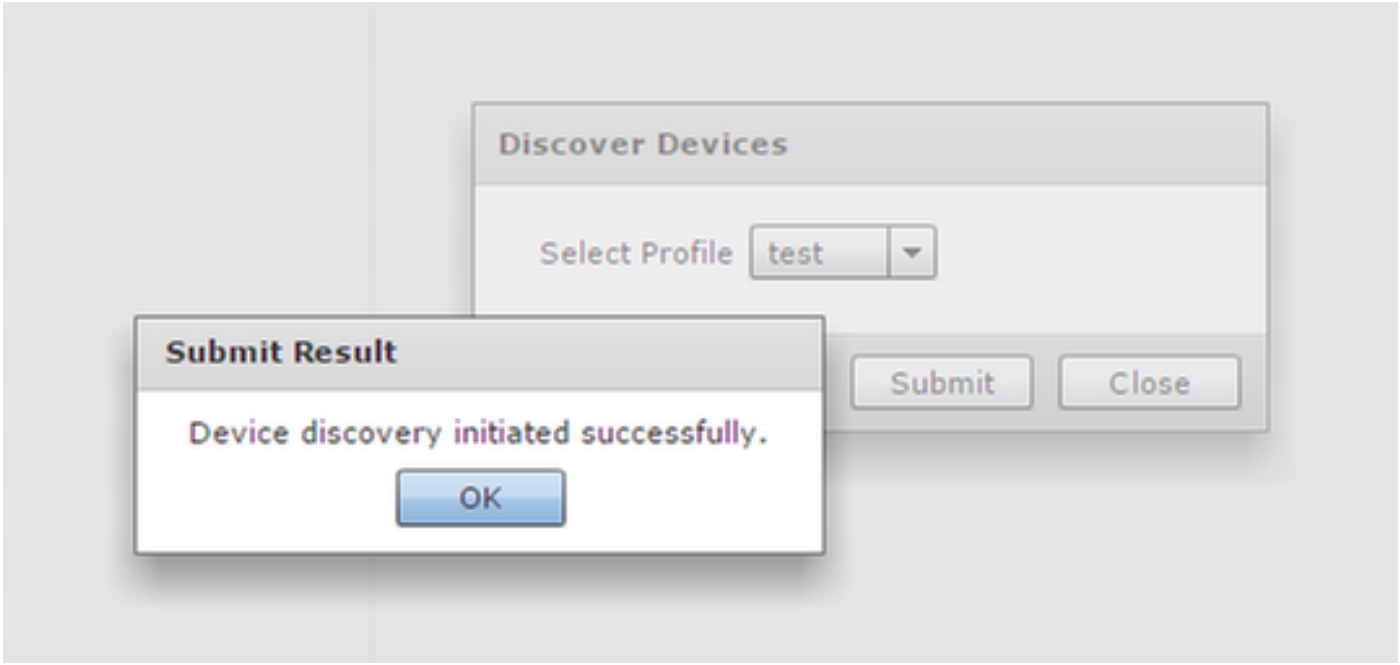
Paso 8. Introduzca el nombre de usuario y la contraseña que utiliza para iniciar sesión en el servidor (credenciales CIMC), como se muestra en la imagen.



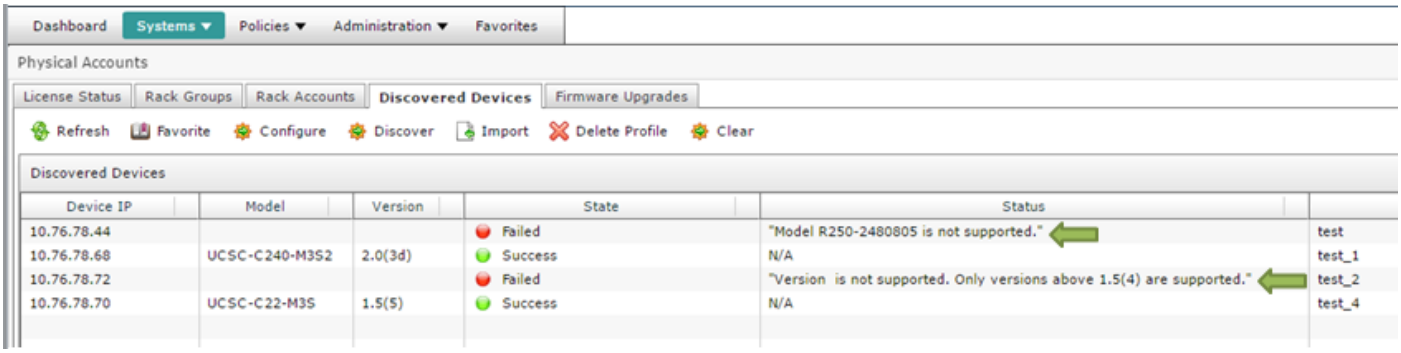
Paso 9. Una vez creado el perfil, haga clic en **Discover** y Select Profile en la lista desplegable, como se muestra en la imagen.



Paso 10. Después de seleccionar el perfil adecuado, haga clic en **Enviar** y haga clic en **Aceptar** en Enviar resultado, como se muestra en la imagen.



Paso 11. Si los dispositivos de su perfil no coinciden con los criterios mínimos admitidos, la razón por la que el dispositivo no fue descubierto es la que aparece en la sección **Estado** como se muestra en la imagen.



Agregar grupo de rack

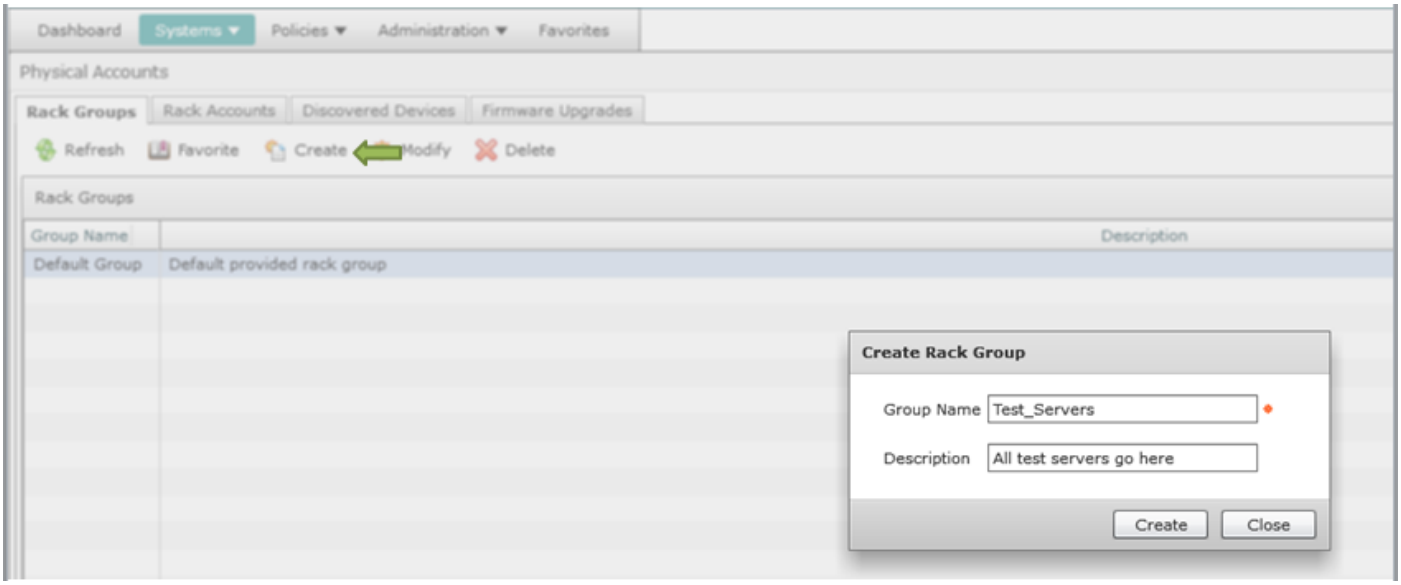
5. Realice este procedimiento cuando desee agregar un nuevo grupo de rack en Cisco IMC Supervisor.

Paso 1. Navegue hasta **Sistemas > Cuentas físicas > Grupos en rack**.

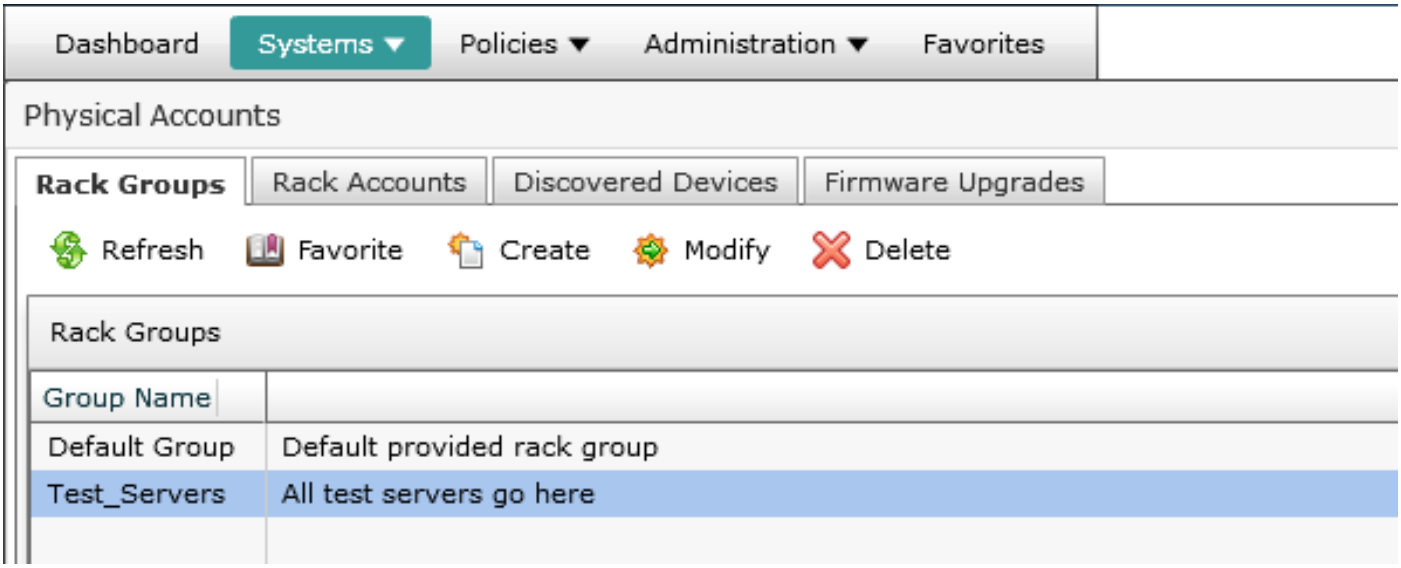
Paso 2. Haga clic en **Crear**.

Paso 3. Especifique un **nombre de grupo** y una **descripción** en el cuadro Crear grupo de rack.

Paso 4. Haga clic en **Crear** como se muestra en la imagen.



Paso 5. Una vez creado, el nombre del grupo debe aparecer como se muestra en la imagen.



Agregar cuenta de rack

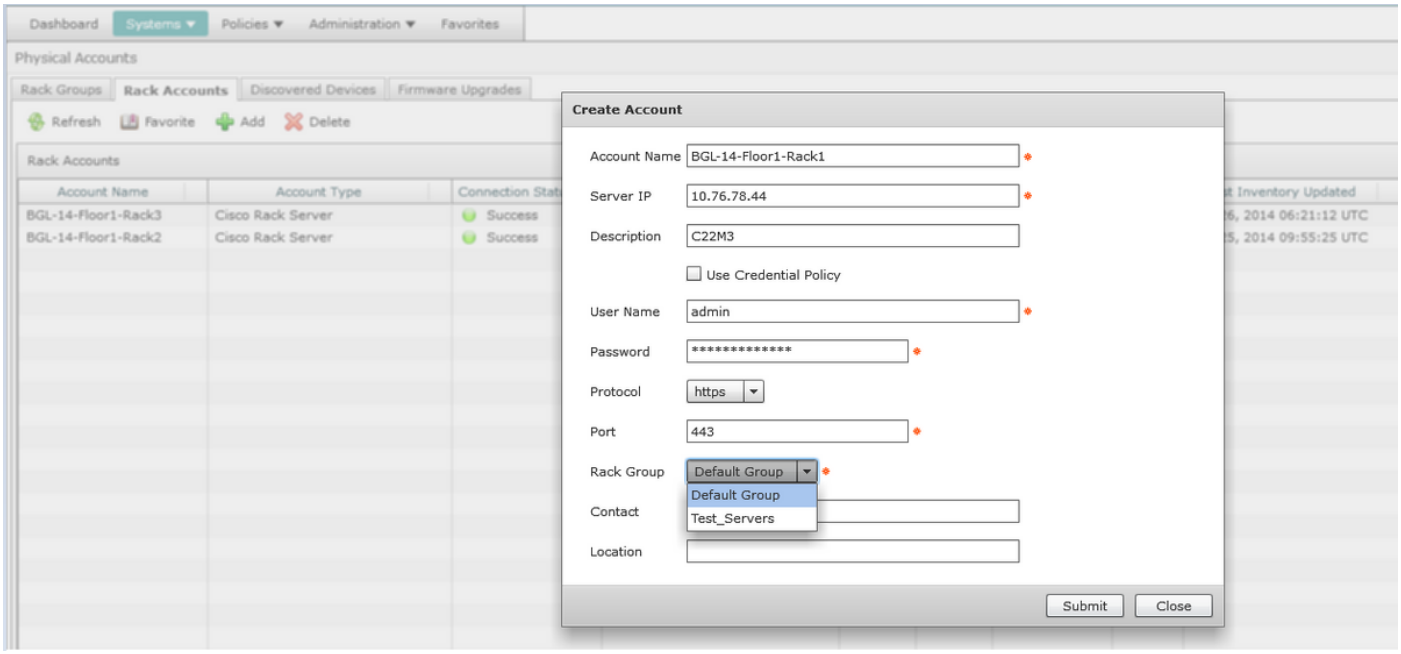
6. Realice este procedimiento cuando desee agregar un nuevo grupo de rack en Cisco IMC Supervisor.

Paso 1.	En la barra de menús, elija **System**.
Paso 2.	Haga clic en la ficha.
Paso 3.	Haga clic.
Paso 4.	En el cuadro de diálogo Crear cuenta, complete estos campos:

Campo	Descripción
campo	Nombre descriptivo de la cuenta de rack
campo	La dirección IP del servidor de montaje en bastidor
Campo Descripción	(Opcional) Una descripción de la cuenta de rack
casilla de verificación	(Opcional) Si ya ha creado directivas de credenciales, active esta casilla seleccionar la directiva de la lista desplegable.
Si marca la casilla de verificación	
lista desplegable	Elija una política de la lista desplegable
Si desmarca la casilla de verificación	
campo	ID de inicio de sesión para el servidor de montaje en bastidor
Campo Contraseña	Contraseña para el ID de inicio de sesión del servidor de montaje en bas
Lista desplegable Protocolo	Elija https o http de la lista
Campo de puerto	El número de puerto asociado al protocolo seleccionado
Lista desplegable Grupo de rack	Elija un grupo en rack de la lista.
Campo de contacto	(Opcional) La dirección de correo electrónico de contacto de la cuenta
Campo de ubicación	(Opcional) La ubicación de la cuenta

Paso 1. En la lista desplegable Grupo en rack, puede elegir el **Grupo predeterminado** o el Grupo definido anteriormente, como se muestra en la imagen.

Paso 2. Una vez finalizada esta acción, los servidores especificados deben estar bajo el grupo de rack que seleccione.



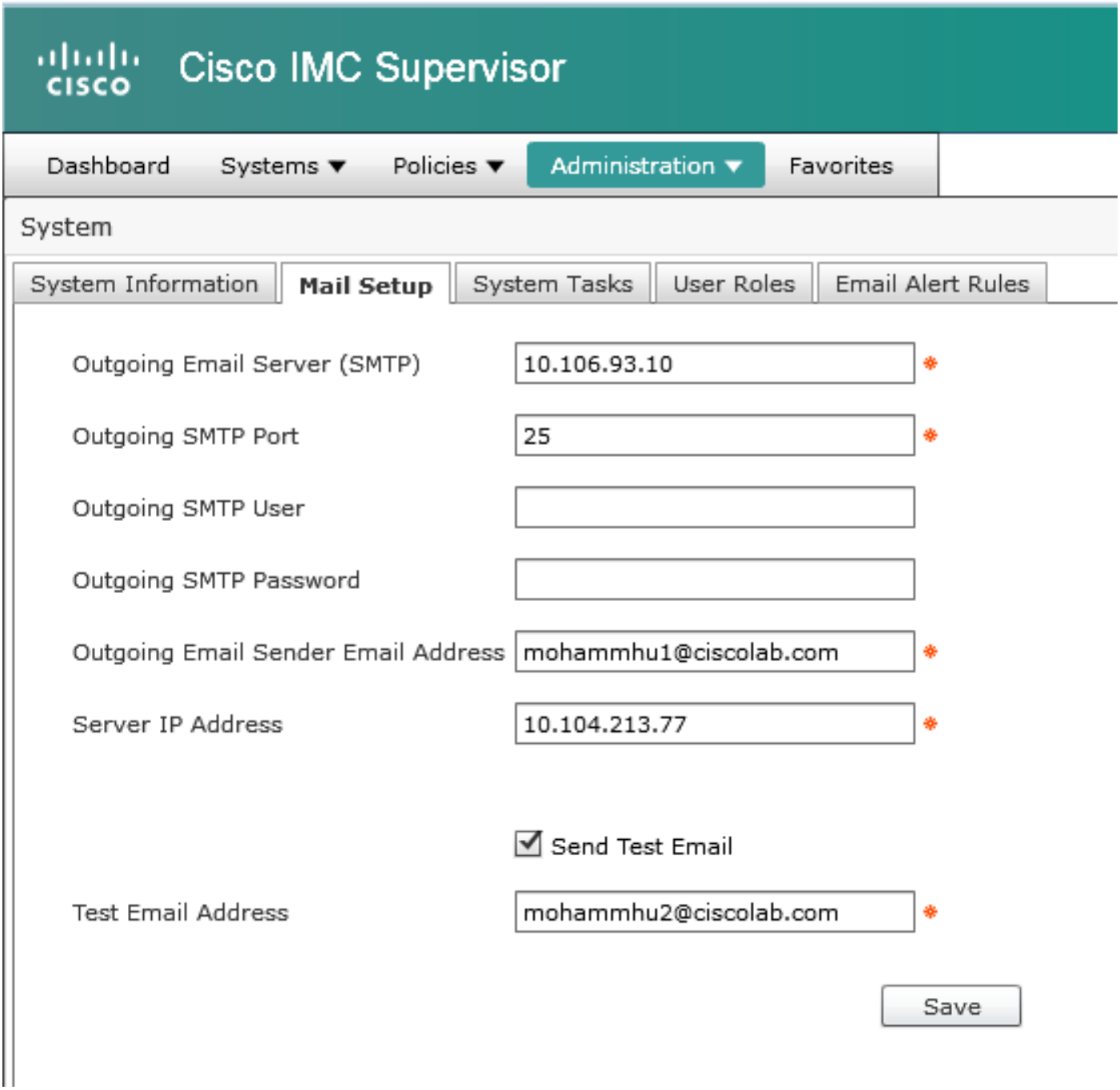
Configuración de correo

7. Realice este procedimiento para configurar el correo de configuración.

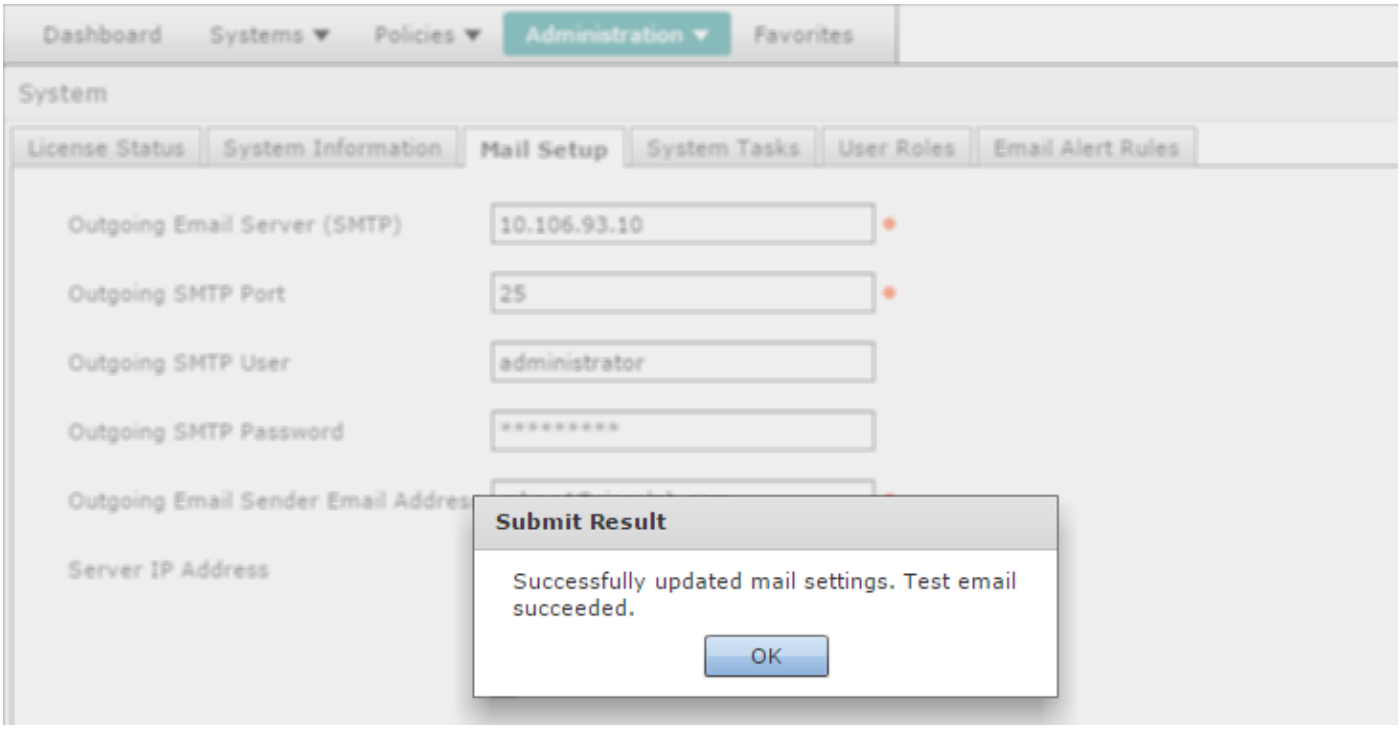
Paso 1. Vaya a **Administration > Mail Setup**.

Paso 2. Introduzca los detalles solicitados.

Paso 3. Puede seleccionar la casilla de verificación **Enviar correo electrónico de prueba** y comprobar si ha recibido el correo de prueba en la dirección de correo electrónico proporcionada, como se muestra en la imagen.

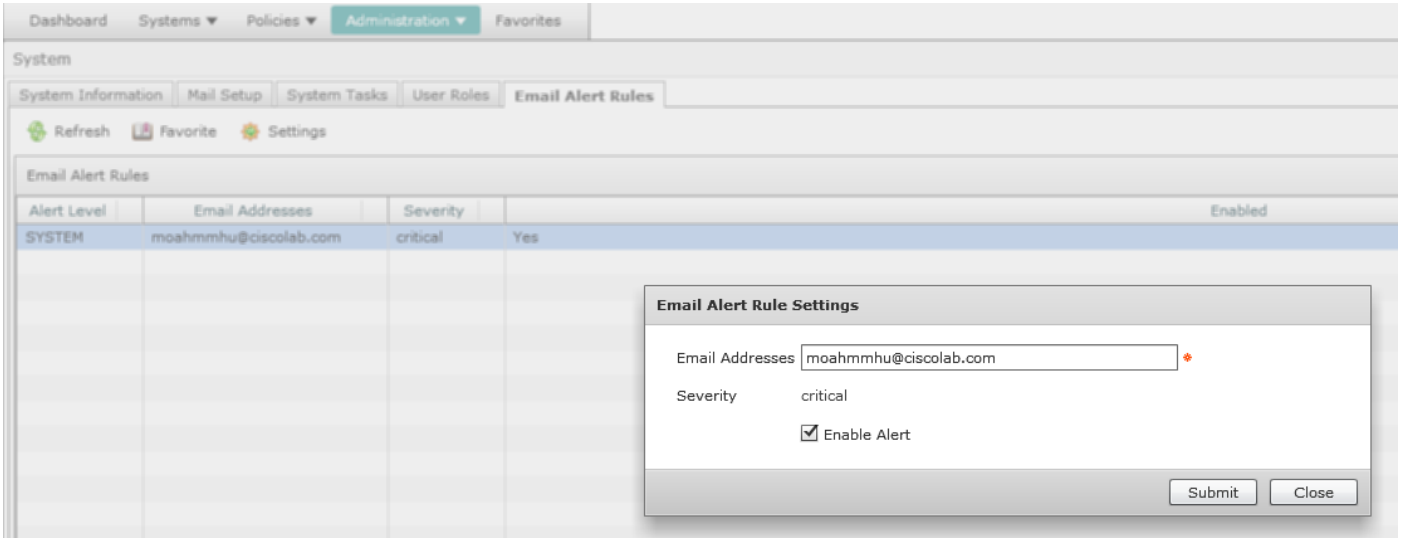


Paso 4. A continuación, debe recibir el correo de prueba como se muestra en la imagen.



Paso 5. En la misma sección, navegue hasta **Configuración de reglas de alerta de correo electrónico** y marque la **casilla de verificación Habilitar alerta** como se muestra en la imagen.

> **Nota:** En este momento (con la versión 1.0 de Cisco IMC Supervisor), solo se admiten notificaciones de fallos críticos y de nivel superior.



Paso 6. Si el sistema detecta un error grave, debe recibir un correo como se muestra en la imagen, siempre que la configuración del correo funcione correctamente.

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 reseat the storage drive	Thu Dec 25 12:10:19 2014	sys/rack-unit-1/board/storage-SAS-SLOT-2/vd-0

Actualización del firmware

8. Realice este procedimiento cuando desee actualizar el firmware.

Paso 1. Navegue hasta **Sistemas > Cuentas físicas**.

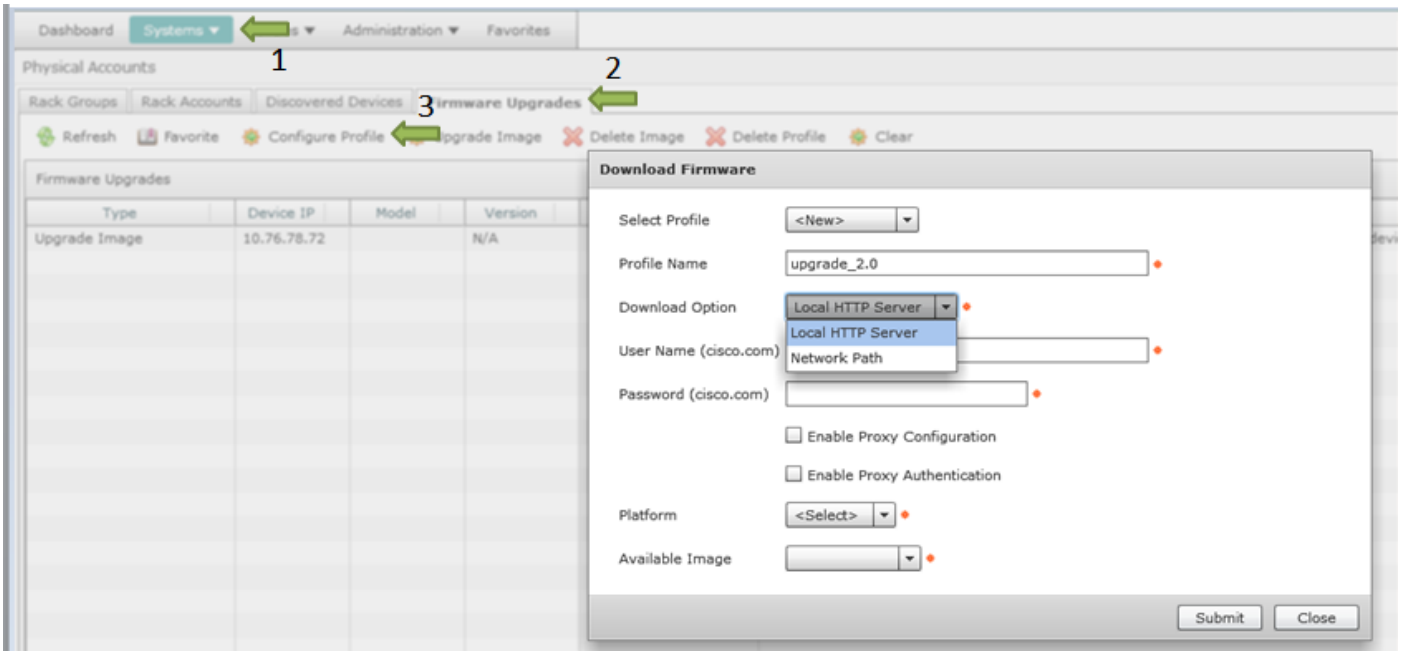
Paso 2. Haga clic en la **pestaña**.

Paso 3. Haga clic en **Configurar perfil**.

Paso 4. En el cuadro de diálogo **Descargar firmware**, puede crear un perfil nuevo o editar un perfil existente.

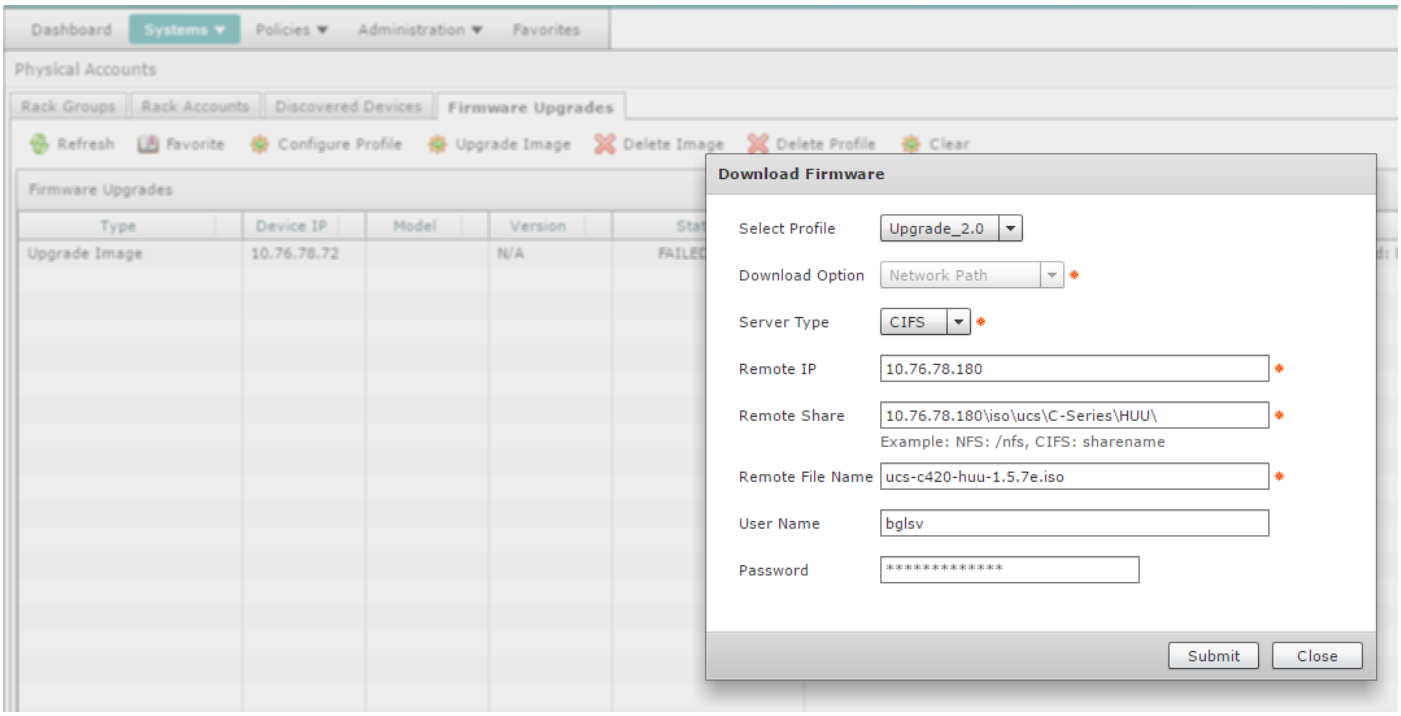
Campo	Descripción
	Seleccione **Nuevo** en la lista desplegable.
Campo	Un nombre descriptivo para el perfil.
lista desplegable	Elija una de estas opciones: • Servidor HTTP local: la imagen .iso se almacena en el supervis local de Cisco IMC. • Ruta de red: la imagen .iso se almacena en la red.
campo	Introduzca su nombre de usuario de inicio de sesión de Cisco.
campo	Introduzca su contraseña de inicio de sesión de Cisco.
casilla	(Opcional) Marque esta casilla de verificación para habilitar la configuración de proxy y completar estos campos: • Campo Nombre de host: introduzca un nombre de host para la configuración de proxy • Campo Puerto: introduzca el puerto para la configuración del p
casilla de verificación Habilitar autenticación de proxy	(Opcional) Marque esta casilla de verificación para habilitar la autenticación de proxy y completar estos campos: • Campo Nombre de usuario de proxy: introduzca un nombre de usuario de proxy para la autenticación de proxy • Campo Contraseña del proxy: introduzca la contraseña del nor de usuario del proxy.
Lista desplegable Plataforma	Elija una plataforma de la lista desplegable.
lista desplegable	Elija la imagen .iso en la lista desplegable.

Paso 5. Configure un perfil **Nuevo** como se muestra en la imagen.



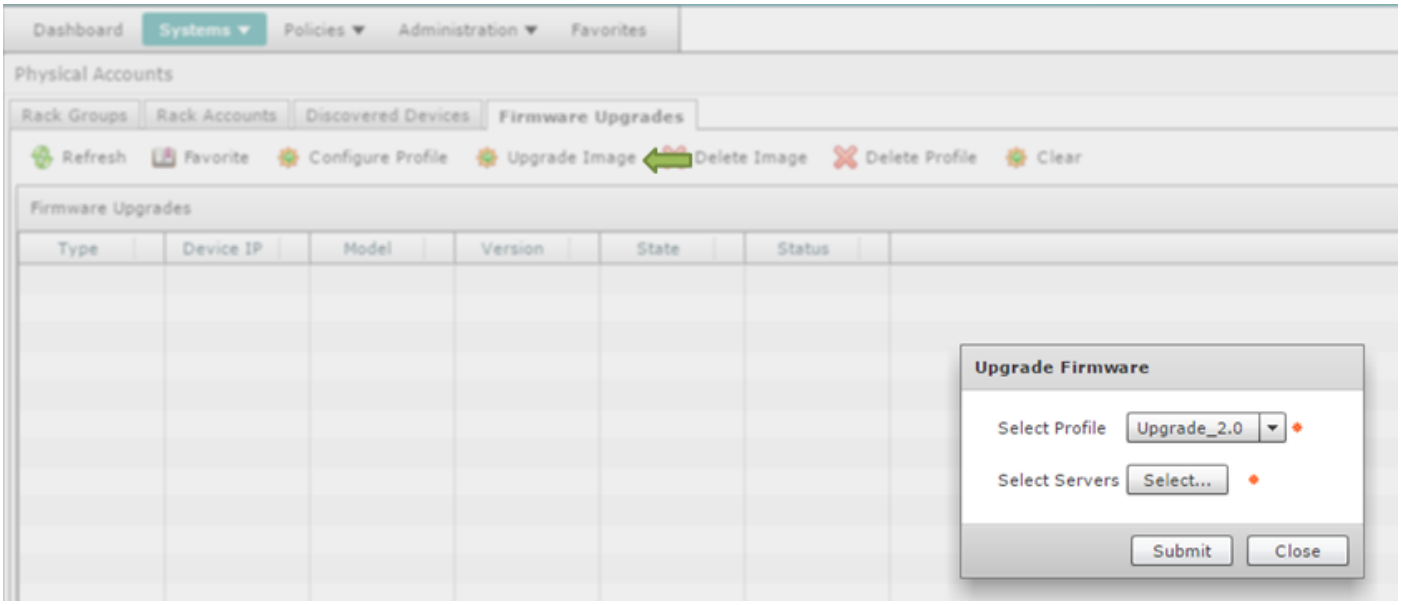
Paso 6. Elija **Ruta de red** como la Opción de descarga para este ejemplo. (Tiene CIFS y NFS como opciones)

Paso 7. Haga clic en **Enviar** como se muestra en la imagen.



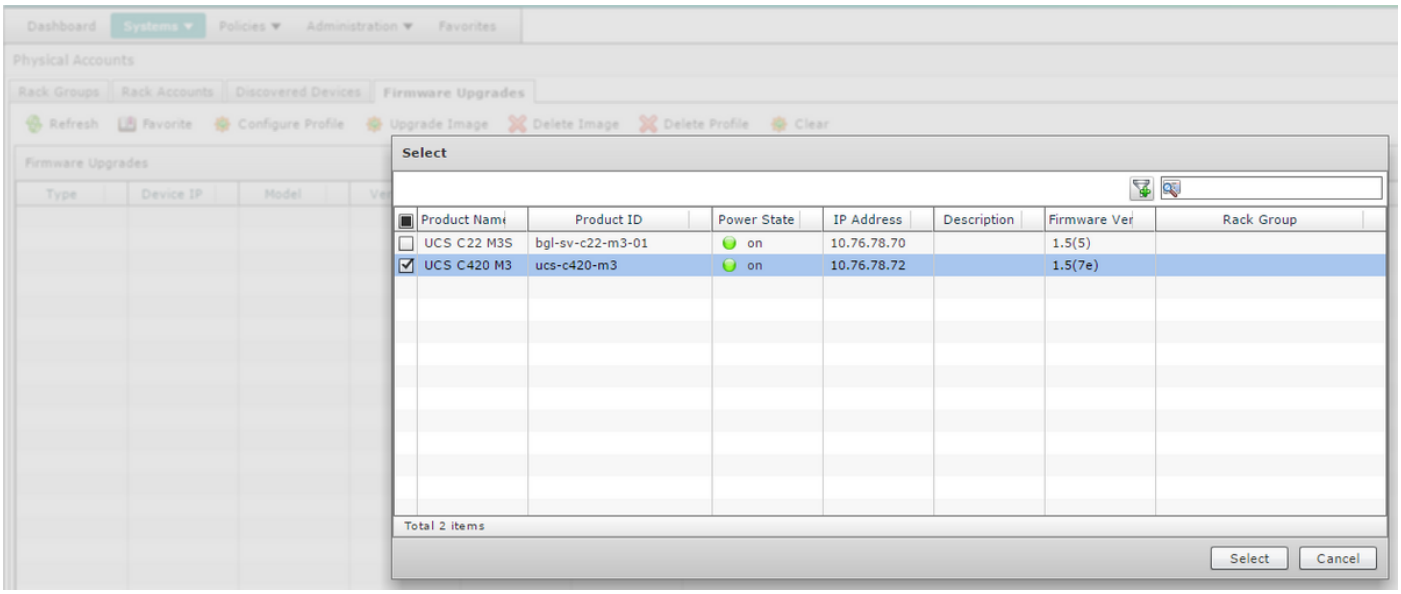
Paso 8. Haga clic en **Actualizar imagen**.

Paso 9. Haga clic en **Seleccionar...** para seleccionar los servidores que desea actualizar como se muestra en la imagen.



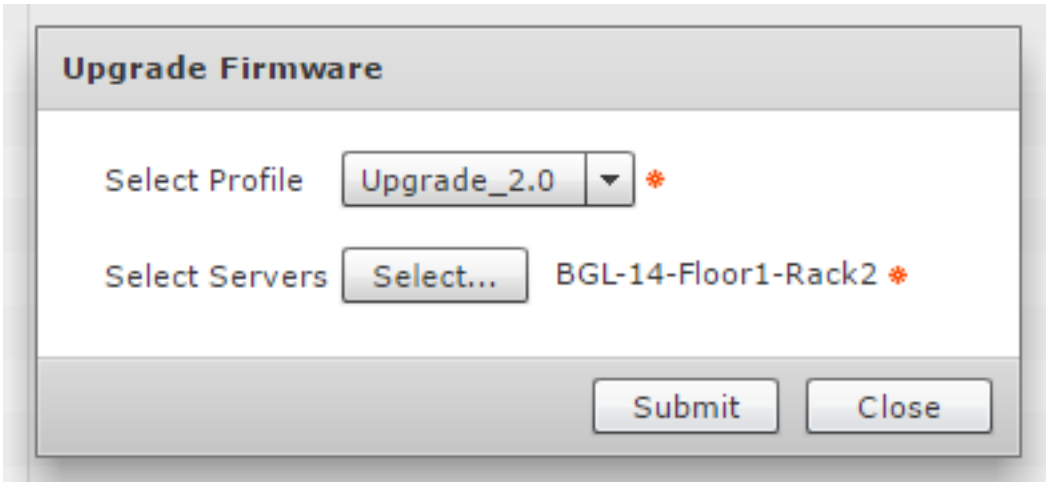
Paso 10. Se selecciona un único servidor para este ejemplo.

Paso 11. Haga clic en **Seleccionar** como se muestra en la imagen.



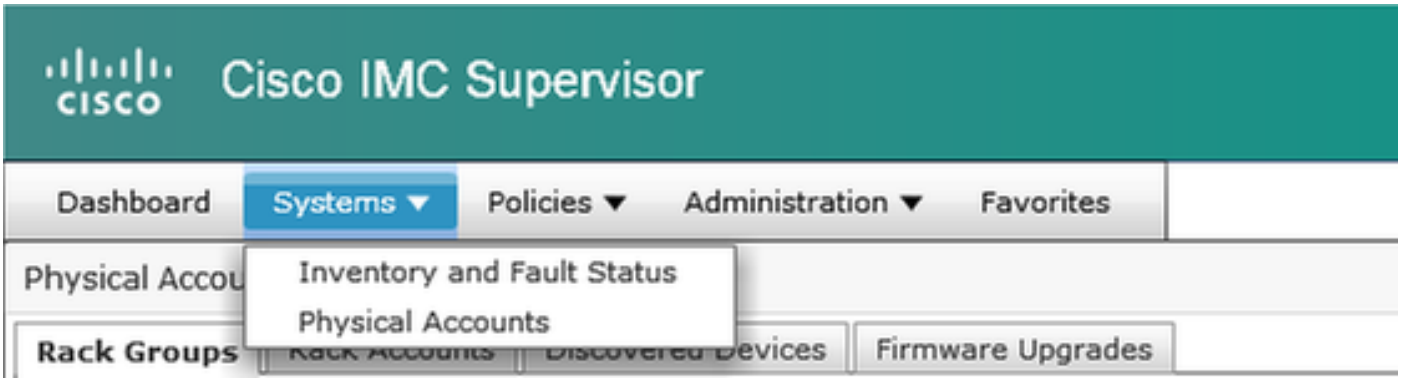
Paso 12. Se muestra el servidor seleccionado.

Paso 13. Haga clic en **Enviar** como se muestra en la imagen.



Nota: Si actualiza Cisco IMC versión 2.0(x), debe cambiar la contraseña predeterminada de Cisco IMC.

Paso 14. Para verificar el estado de la actualización, navegue hasta **Sistema > Inventario y estado de falla** como se muestra en la imagen.

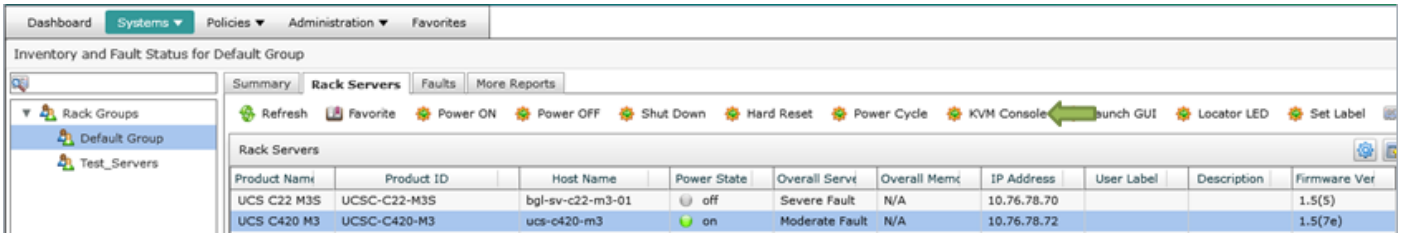


Paso 15. Expanda **Grupos de Rack**, elija el grupo apropiado en el cual los servidores se llenaron antes.

Paso 16. Haga clic en **Rack Servers** y elija el servidor apropiado.

Paso 17. Una vez hecho esto, debe aparecer una fila adicional con opciones remotas.

Paso 18. Haga clic en **Consola KVM** en esta fila y podrá ver la actualización en acción, como se muestra en la imagen.



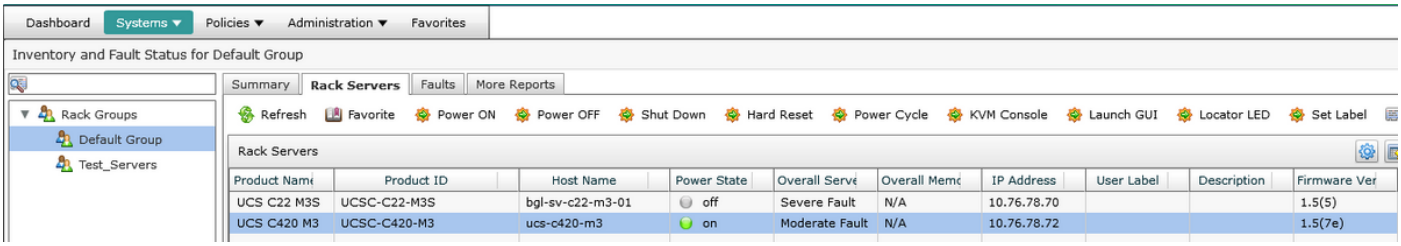
Exportar datos de soporte técnico al servidor remoto

9. Realice estas acciones para extraer los datos de soporte técnico.

Paso 1. Navegue hasta **Sistemas > Inventario y Estado de Fallas para Grupo Predeterminado**.

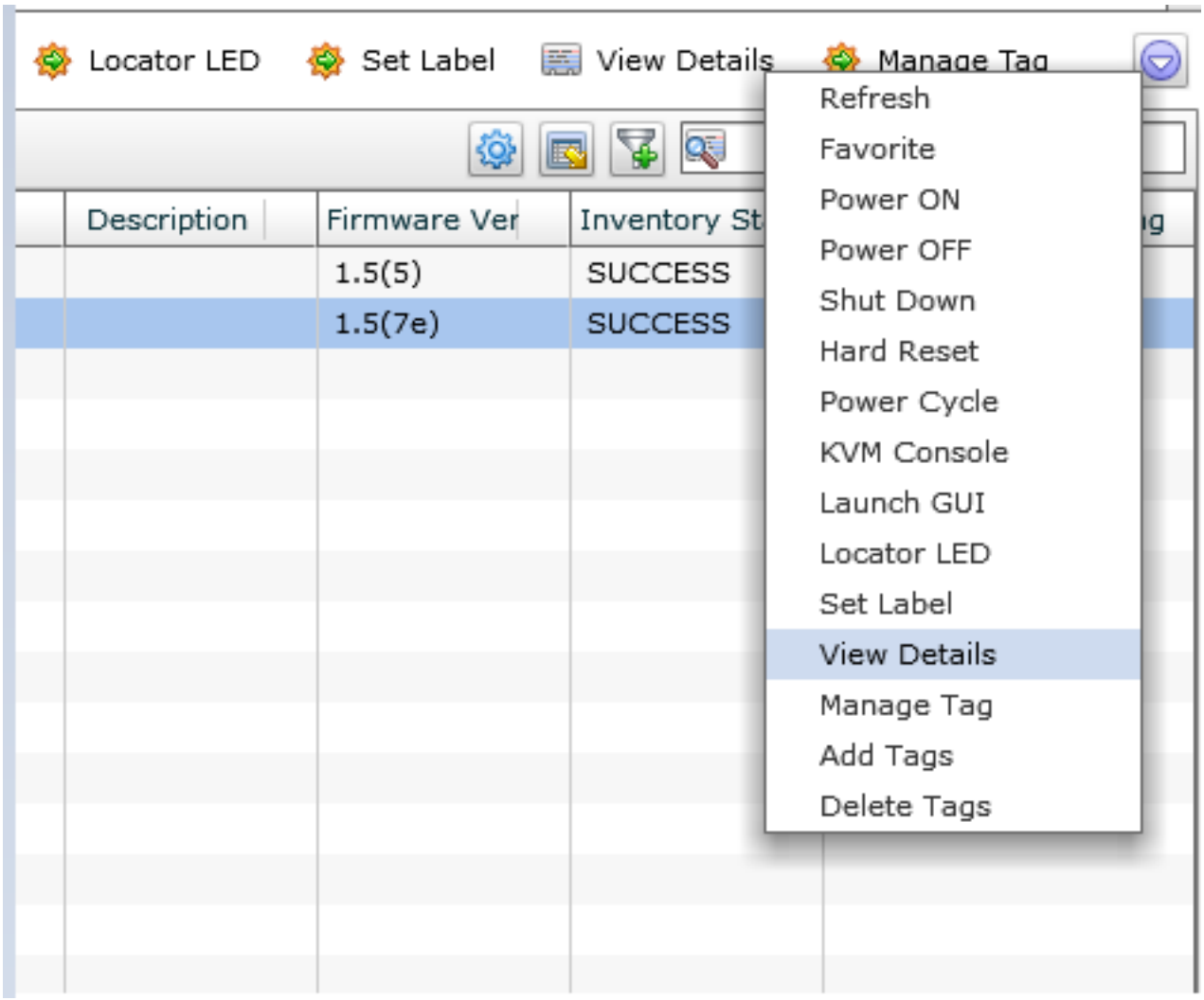
Paso 2. Expanda **Grupos de Rack** y seleccione el Grupo de Rack que contiene los servidores.

Paso 3. Seleccione la pestaña **Servidores en rack** como se muestra en la imagen.



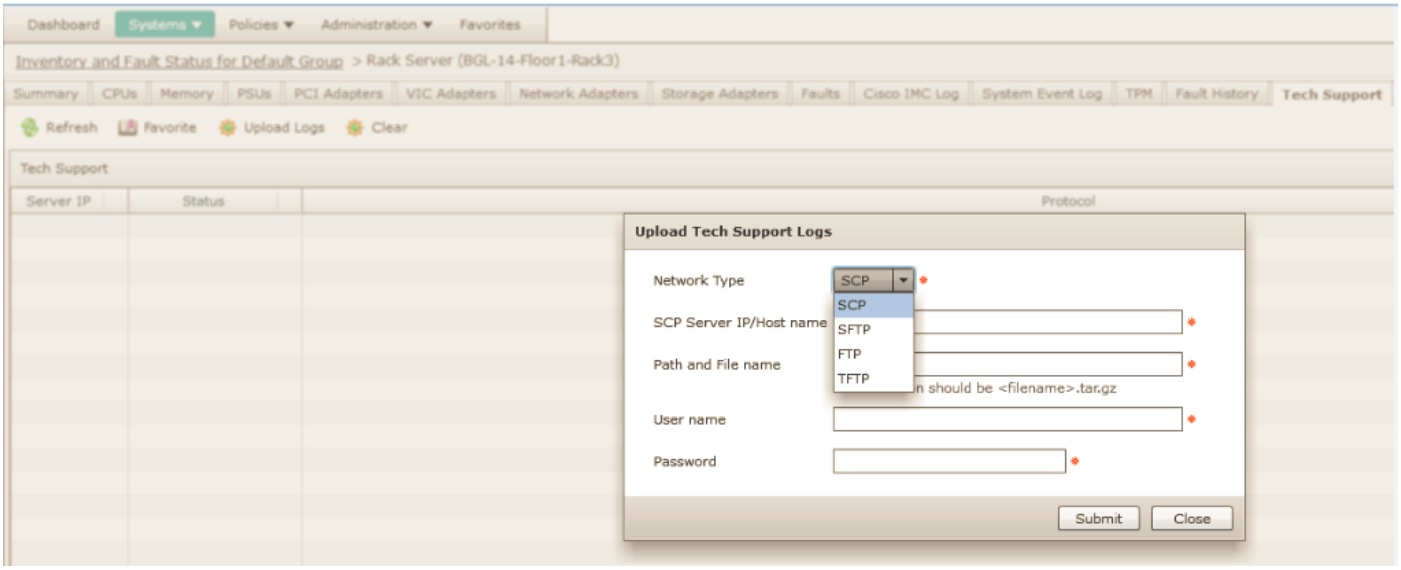
Paso 4. Haga doble clic en el servidor de la lista para ver los detalles o haga clic en el servidor de

la lista y, a continuación, en la flecha hacia abajo del extremo derecho, haga clic en **Ver detalles** como se muestra en la imagen.



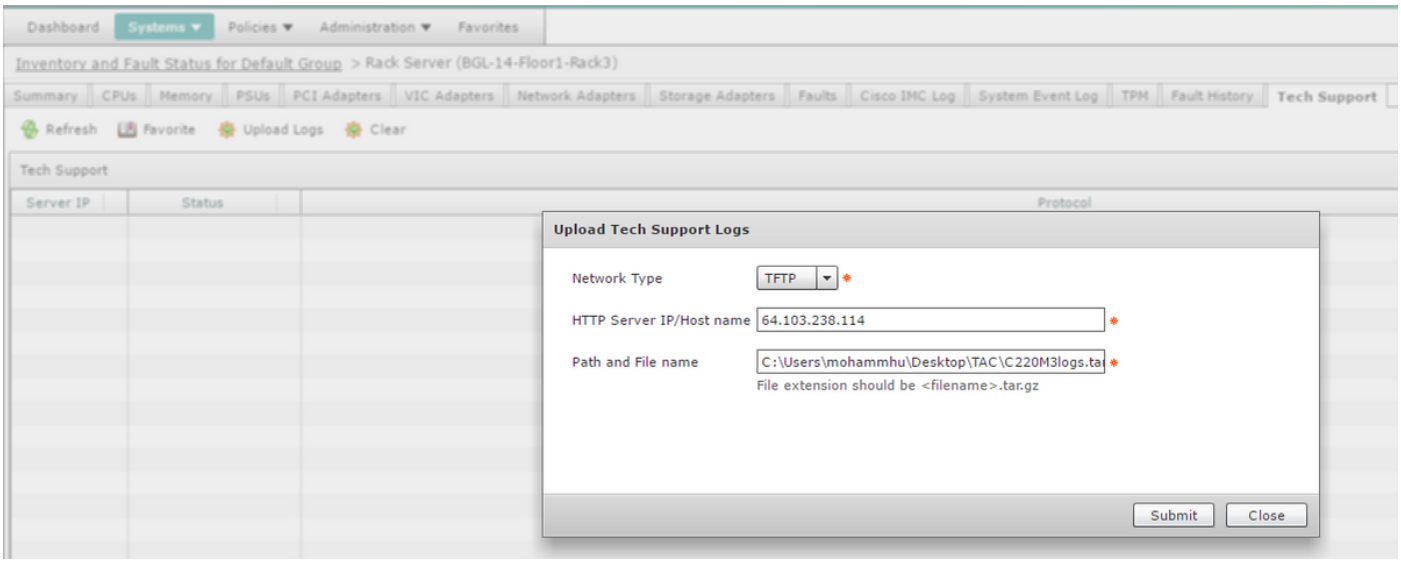
Paso 5. Haga clic en la pestaña **Soporte Técnico**.

Paso 6. Elija el tipo de red adecuado para cargar los archivos como se muestra en la imagen.



Paso 7. Elija **TFTP** para este ejemplo.

Paso 8. Haga clic en **Enviar** como se muestra en la imagen.



Paso 9. La captura de pantalla muestra que los registros se cargaron correctamente en la ubicación especificada.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.