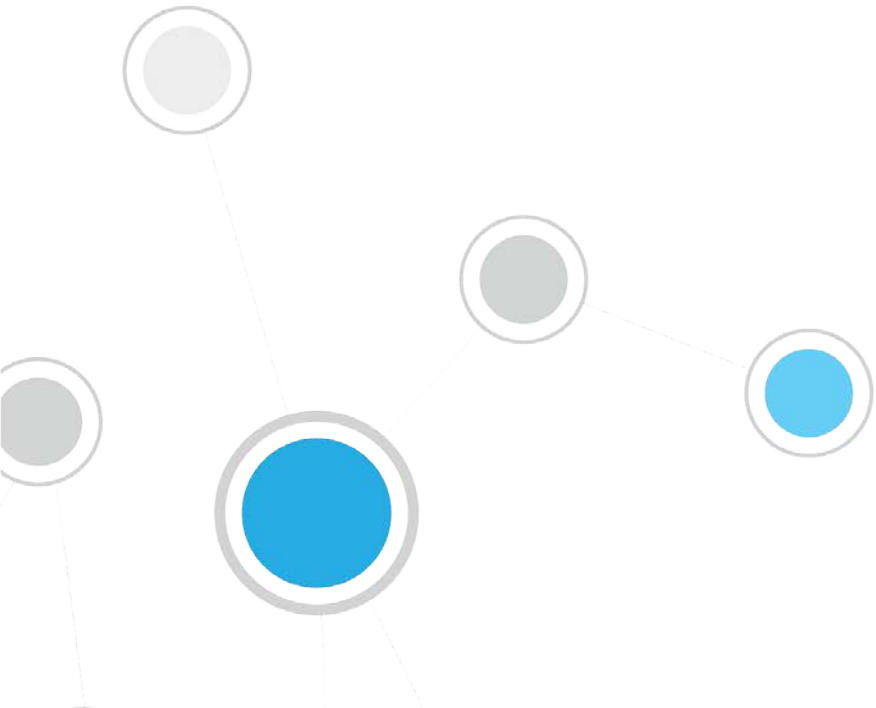
ForeScout CounterACT®

Equipo simple CounterACT

Guía de instalación rápida

Versión 8.0

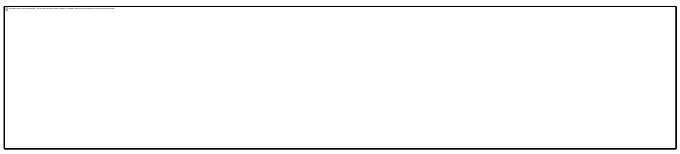


Índice

Bienvenido a CounterACT Versión 8.0

La plataforma CounterACT provee visibilidad de infraestructura y dispositivos, administración de políticas, manipulación y agilización del proceso de trabajo para mejorar la seguridad de la red. CounterACT provee a empresas información contextual en tiempo real de dispositivos y usuarios en la red. Las políticas en CounterACT se definen utilizando esta información contextual que ayuda a garantizar el cumplimiento, remedio, acceso apropiado a la red y agilización de las operaciones de servicio.

Esta guía describe la instalación de un equipo CounterACT simple e independiente.



Para más información detallada o información sobre la implementación de múltiples equipos para protección de redes en toda la empresa, consulte la *Guía de Instalación CounterACT* y *Guía de Gestión de CounterACT.* Ingrese a Documentación adicional de CounterACT para saber cómo acceder a estas guías.

Además puede navegar por el sitio web de soporte técnico ubicado en: https://www.forescout.com/support para acceder a la última documentación, los artículos de conocimiento base y actualizaciones para su equipo.

Paquete CounterACT Contenido

Su paquete CounterACT incluye los siguientes componentes:

- Equipo CounterACT
- Marco frontal
- Rieles (abrazaderas de montaje)
- Cable(s) de energía
- Cable de conexión de la consola DB9 (para conexiones en serie únicamente)
- Información de seguridad de productos, de medioambiente y regulatoria de la empresa
- Documento de Introducción general (para dispositivos 51xx únicamente)

Perspectiva general

Para configurar CounterACT realice lo siguiente:

1. Cree un plan de implementación

Antes de llevar a cabo la instalación, debe decidir dónde colocar el equipo y debe conocer las conexiones de interfaz del equipo.

Decida dónde implementar el equipo

Seleccionar la ubicación correcta de la red donde se instalará el equipo es crucial para el óptimo rendimiento y la exitosa implementación de CounterACT. La ubicación correcta dependerá de sus objetivos de implementación deseados y las políticas de acceso a la red. El equipo deberá poder controlar el tráfico relevante para la política deseada. Por ejemplo, si su política depende de los eventos de autorización de control desde las terminales hasta los servidores de autenticación corporativa, el equipo deberá estar instalado de manera que pueda ver el flujo de tráfico de las terminales al/a los servidor/es de autenticación.

Para más información sobre la instalación y la implementación, consulte la *Guía de Instalación CounterACT*. Ingrese a Documentación adicional de CounterACT para saber cómo acceder a esta guía.

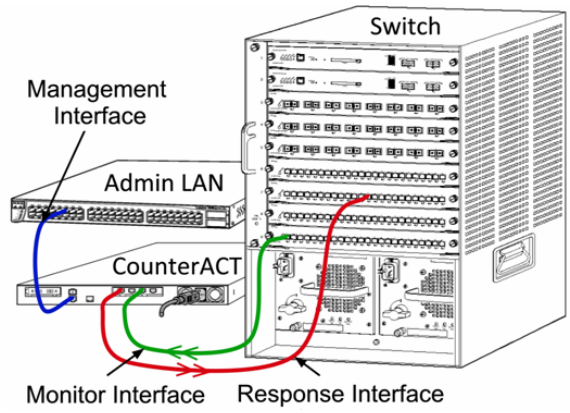
Conexiones de interfaz del equipo

El equipo está generalmente configurado con tres conexiones al interruptor de red.

Interfaz de administración

Esta interfaz le permite administrar CounterACT y realizar preguntas y una inspección profunda de las terminales. La interfaz debe estar conectada a un puerto del interruptor que tenga acceso a todas las terminales de la red.

Cada equipo exige una conexión de administración única a la red. Esta conexión necesita una dirección de IP en la red LAN local y acceso a un puerto 13000/ TCP desde las máquinas que harán funcionar la aplicación de la administración de la consola de CounterACT. El puerto de administración debe tener acceso a servicios de red adicionales.



Requisitos de acceso a la red

Puerto	Servicio	Hacia o desde CounterACT	Función
22/TCP	SSH	Desde	Permite la inspección remota de las terminales de OS X y Linux. Permite que CounterACT se comunique con interruptores y routers de la red.
		A	Permite el acceso a la interfaz de línea del comando CounterACT.
2222/TCP	SSH	A	(Alta disponibilidad) Permite el acceso a los dispositivos físicos de CounterACT que son parte del par de terminales de alta disponibilidad. Use 22/TCP para acceder a la dirección compartida de IP (virtual) del par de terminales.
25/TCP	SMTP	Desde	Permite a CounterACT el acceso al relé de correo de la empresa.
53/UDP	DNS	Desde	Permite que CounterACT resuelva direcciones internas de IP.
80/TCP	HTTP	A	Permite la redirección de HTTP.
123/UDP	NTP	Desde	Permite el acceso de CounterACT a un servidor de tiempo local o a ntp.forescout.net. Por defecto, CounterACT accede a ntp.foreScout.net.
135/TCP	MS-WMI	Desde	Permite la inspección remota de las terminales de Windows.
139/TCP	SMB, MS-RPC	Desde	Permite la inspección remota de las terminales de Windows (para las terminales que funcionan con Windows 7 y versiones anteriores).
445/TCP			Permite la inspección remota de las terminales de Windows.
161/UDP	SNMP	Desde	Permite que CounterACT se comunique con interruptores y routers de la red. Para más información sobre la configuración de SNMP consulte la *Guía de Gestión de CounterACT*.
162/UDP	SNMP	A	Permite que CounterACT reciba trampas de SNMP desde interruptores y routers de la red. Para más información sobre la configuración de SNMP consulte la *Guía de Gestión de CounterACT*.

Puerto	Servicio	Hacia o desde CounterACT	Función
389/TCP (636)	LDAP	Desde	Permite que CounterACT se comunique con Active Directory. Permite la comunicación con portales basados en la web.
443/TCP	HTTPS	A	Permite la redirección de HTTP usando TLS.
2200/TCP	SecureConnector para Linux	A	Permite que SecureConnector cree una conexión segura (SSH encriptado) con el equipo desde las máquinas Linux. *SecureConnector* es un agente basado en una secuencia de comandos que permite la gestión de las terminales Linux mientras están conectadas a la red.
10003/TCP	SecureConnector para Windows	A	Permite que SecureConnector cree una conexión segura (TLS encriptado) con el equipo desde las máquinas Windows. *SecureConnector* es un agente que permite la gestión de las terminales Windows mientras están conectadas a la red. Consulte la *Guía de Gestión de CounterACT* para más información sobre SecureConnector. Cuando SecureConnector se conecta a un equipo o al Administrador corporativo, se redirecciona al equipo al cual su host es asignado. Asegúrese de que este puerto esté abierto a todos los equipos y al Administrador corporativo para permitir una movilidad transparente dentro de la organización.
10005/TCP	SecureConnector para OS X	A	Permite que SecureConnector cree una conexión segura (TLS encriptado) con el equipo desde las máquinas OS X. *SecureConnector* es un agente que permite la gestión de las terminales OS X mientras están conectadas a la red. Consulte la *Guía de Gestión de CounterACT* para más información sobre SecureConnector. Cuando SecureConnector se conecta a un equipo o al Administrador corporativo, se redirecciona al equipo al cual su host es asignado. Asegúrese de que este puerto esté abierto a todos los equipos y al Administrador corporativo para permitir una movilidad transparente dentro de la organización.

Puerto	Servicio	Hacia o desde CounterACT	Función
13000/TCP	CounterACT	Desde/A	Para entornos con un solo equipo: desde la consola al equipo. Para entornos con más de un dispositivo CounterACT: desde la consola al dispositivo CounterACT y desde un dispositivo CounterACT al otro. La comunicación del dispositivo CounterACT incluye la comunicación con el Administrador corporativo y Reactivación del administrador corporativo, usando TLS.

Interfaz del monitor

La interfaz del monitor permite que el equipo controle y registre el tráfico de la red. Toda interfaz disponible puede usarse como interfaz del monitor.

El equipo controla y duplica el tráfico a un puerto en el interruptor. El uso de 802.1Q VLAN marcado depende del número de VLAN reflejadas.

- ***VLAN simple***: cuando el tráfico controlado se genera desde una VLAN simple, el tráfico duplicado no necesita estar marcado en la VLAN.
- ***Múltiples VLAN***: cuando el tráfico monitoreado proviene de más de una VLAN, el tráfico duplicado debe estar marcado 802.1Q VLAN.

Cuando dos interruptores están conectados a un par redundante, el equipo debe controlar el tráfico desde ambos interruptores.

No se exige ninguna dirección de IP en la interfaz del monitor.

Interfaz de respuesta

El equipo responde al tráfico usando la interfaz de respuesta. El tráfico de respuesta se usa para protegerse contra la actividad maliciosa y para llevar a cabo acciones de las políticas. Estas acciones pueden incluir, por ejemplo, redireccionar los navegadores web o realizar un bloqueo. La configuración del puerto del interruptor relacionado depende del tráfico que se está monitoreando.

Toda interfaz disponible puede usarse como interfaz de respuesta.

- ***VLAN simple***: cuando el tráfico monitoreado se genera desde una VLAN simple, el puerto de respuesta debe pertenecer a la misma VLAN. En este caso, el equipo exige una única dirección de IP en esa VLAN.
- ***Múltiples VLAN***: si el tráfico monitoreado proviene de más de una VLAN, el puerto de respuesta debe estar también configurado con marcado VLAN 802.1Q para las mismas VLAN. El equipo necesita una dirección de IP para cada VLAN monitoreada.

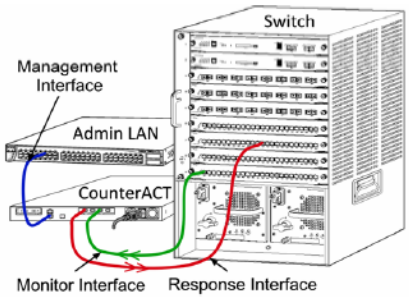
2. Configuración de su interruptor

A. Opciones de conexión del interruptor

El equipo fue diseñado para integrarse sin problemas a una amplia variedad de entornos de red. Para integrar de manera exitosa el equipo a su red, verifique que su interruptor esté configurado para supervisar el tráfico requerido.

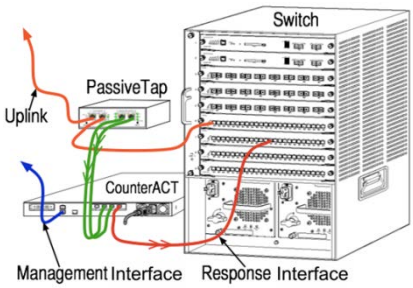
Hay varias opciones disponibles para conectar el equipo a su interruptor.

1 Implementación estándar (administración separada, interfaces de control y respuesta)



La implementación recomendada usa tres puertos separados. Estos puertos se describen en Conexiones de interfaz del equipo.

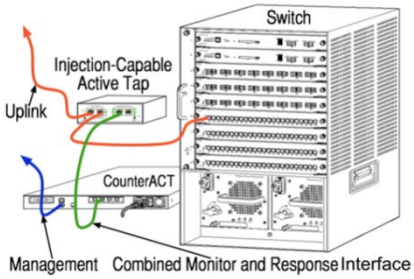
2 Punto de conexión insertado pasivo



En lugar de conectar a un puerto de monitoreo con interruptor, el equipo puede usar un punto de conexión insertado pasivo.

El punto de conexión pasivo necesita dos puertos de monitoreo (uno para el tráfico de corriente ascendente y otro para corriente descendente), excepto en el caso de unos puntos de conexión de *recombinación* que combinan las dos corrientes dobles a un único puerto. Tenga en cuenta que si el tráfico en el puerto conectado está marcado 802.1Q VLAN, el puerto de respuesta debe ser también un puerto marcado de 802.1Q VLAN.

3 Conexión en línea activa (con inyección)



El equipo puede usar una conexión en línea activa. Si la conexión tiene capacidad de inyección, el equipo combina los puertos de monitor y respuesta para que no haya necesidad de configurar un puerto de respuesta separado en el interruptor. Esta opción puede usarse para todo tipo de configuración del interruptor con corriente ascendente o descendente.

4 Respuesta de la capa de IP (para instalaciones de interruptor de 3 capas)

El equipo puede usar su propia interfaz de administración para responder al tráfico. A pesar de que esta opción puede usarse con un tráfico monitoreado, solo es recomendada cuando el equipo monitorea puertos que no son parte de ninguna VLAN y, por lo tanto, el equipo no puede responder al tráfico monitoreado usando cualquier otro puerto del interruptor. Esto ocurre generalmente cuando se controla un enlace que conecta a dos routers. Esta opción no puede responder a pedidos del Protocolo de Resolución de Direcciones (ARP, por sus siglas en inglés), que limita la capacidad del equipo de detectar escaneos dirigidos a las direcciones de IP incluidas en la subred monitoreada. Esta limitación no aplica cuando se está controlando el tráfico entre los dos routers.

B. Notas para la configuración del interruptor

Etiquetas VLAN (802.1Q)

- ***Monitoreo de una VLAN simple***: si el tráfico monitoreado proviene de una VLAN simple, el tráfico no necesita etiquetas 802.1Q.
- ***Monitoreo de múltiples VLAN***: si el tráfico monitoreado proviene de dos o más VLAN, *ambos* puertos, el de control y el de respuesta, deben tener capacidad de marcado 802.1Q VLAN. Se recomienda el monitoreo de múltiples VLAN ya que brinda la mejor cobertura general, al mismo tiempo que minimiza el número de puertos que duplica.
- Si el interruptor no puede usar una etiqueta 802.1Q VLAN en los puertos reflejados, realice una de las siguientes acciones:
  - Duplique solo una VLAN simple
  - Duplique un puerto simple, no marcado, enlazado
  - Use la opción de respuesta de capa de IP
- Si el interruptor puede duplicar solo un puerto, entonces duplique solo un puerto enlazado. Este puede estar marcado. En general, si el interruptor no incluye etiquetas 802.1Q VLAN, deberá usar la opción de respuesta de Capa de IP.

Instrucciones adicionales

- En los casos siguientes, debe multiplicar solo una interfaz (que permita recepción/transmisión):
  - Si el interruptor no puede multiplicar el tráfico recibido y transmitido al mismo tiempo
  - Si el interruptor no puede multiplicar todo el tráfico del interruptor
  - Si el interruptor no puede multiplicar todo el tráfico hacia una VLAN
- Verifique que no sobrecargue el puerto de duplicado o reflejado.

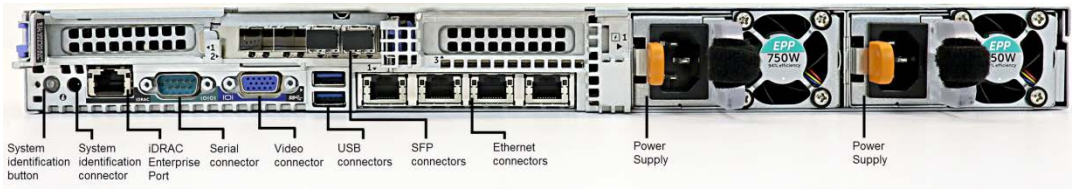
- Algunos interruptores (como Cisco 6509) pueden necesitar que se elimine completamente la configuración del puerto actual para luego ingresar una nueva configuración. No eliminar la información del puerto anterior puede causar que el interruptor quite las etiquetas 802.1Q.

3. Conexión de los cables de la red y encendido

A. Desembalaje del equipo y conexión de los cables

1. Retire el equipo y el cable de energía del contenedor de envío.
2. Retire el kit de rieles que recibió con el equipo.
3. Monte el kit de rieles en el equipo y monte el equipo a la vía.
4. Conecte los cables de la red entre las interfaces de la red en el panel trasero del equipo y los puertos del interruptor.

Muestra del panel trasero — Dispositivo CounterACT



Puede reemplazar SFP suministrado por ForeScout con SFP de Finisar que han sido probados y aprobados por ForeScout. Consulte la *Guía de Instalación CounterACT* para más información.

B. Registro de designaciones de interfaces

Luego de completar la instalación del equipo en el centro de datos y de instalar la consola CounterACT, el programa le pedirá que registre las designaciones de la interfaz. Estas designaciones, conocidas como *Definiciones de canal*, se ingresan en el Asistente de configuración inicial que se abre cuando usted ingresa por primera vez a la consola.

Registre las designaciones de la interfaz física abajo y úselas cuando complete la configuración del canal en la consola.

Interfaz de Ethernet	Designación de interfaz (p. ej. Administración, Monitoreo, Respuesta)
Eth0	
Eth1	
Eth2	
Eth3	

Eth4	
Eth5	
Eth6	
Eth7	

C. Encendido del equipo

1. Conecte el cable de energía al conector de potencia en el panel trasero del equipo.
2. Conecte el otro extremo el cable de energía a la toma a tierra de CA.
3. Conecte el teclado y el monitor al equipo o configure el equipo para una conexión en serie. Consulte la *Guía de Instalación CounterACT* para más información.
4. Encienda el equipo desde el panel frontal.

4. Configuración del equipo

Prepare la siguiente información antes de configurar el equipo:

Nombre del host del equipo	
Contraseña del administrador de CounterACT	Conserve la contraseña en un lugar seguro
Interfaz de administración	
Dirección de IP del equipo	
Máscara de la red	
Dirección de IP de la pasarela predeterminada	
Nombre del dominio DNS	
Direcciones del servidor de DNS	

Luego de conectarlo a la energía, el programa le pedirá que comience la configuración con el siguiente mensaje:

```
El arranque del equipo CounterACT está completo.
Presione <Enter> (Entrar) para continuar.
```

1. Presione **Enter (Entrar)**. Si tiene un dispositivo 51xx CounterACT, aparecerá el siguiente mensaje:

```
CounterACT 8.0.0-<build> (generar) opciones:


1) Configure CounterACT (Configurar CounterACT)
2) Restore saved CounterACT configuration (Restaurar la
configuración guardada de CounterACT)
3) Identify and renumber network interfaces (Identificar y
renumerar las interfaces de la red)
4) Configure keyboard layout (Configurar el teclado)
5) Turn machine off (Apagar la máquina)
6) Reboot the machine (Reiniciar la máquina)

Opción (1-6) :1
```

   Si tiene un dispositivo CT-xxxx CounterACT, aparecerá CounterACT 7.0.0 ó CounterACT 8.0.0 como versión al principio del menú.

   – Si aparece CounterACT 7.0.0, puede actualizarlo o instalar la versión 8.0.0. Consulte la *Guía de Instalación CounterACT* para obtener información. Luego de actualizar o instalar la versión 8.0.0, podrá ver el menú de arriba.

– Si aparece CounterACT 8.0.0, el menú ofrece la opción de instalar CounterACT 7.0.0 o configurar CounterACT 8.0.0, como se muestra a continuación. Si selecciona CounterACT 7.0.0, ya no podrá reinstalar CounterACT 8.0.0 en el menú Configuración. Consulte la *Guía de Instalación CounterACT versión 7.0.0* para más detalles sobre cómo configurar CounterACT 7.0.0.

```
CounterACT 8.0.0-<build> (generar) opciones:


1) Install (Instalar) CounterACT 7.0.0-<build> (generar)
2) Configure (Configurar) CounterACT 8.0.0-<build> (generar)
3) Restore saved CounterACT configuration (Restaurar la
configuración guardada de CounterACT)
4) Identify and renumber network interfaces (Identificar y
renumerar las interfaces de la red)
5) Configure keyboard layout (Configurar el teclado)
6) Turn machine off (Apagar la máquina)
7) Reboot the machine (Reiniciar la máquina)

Opción (1.7):
```

Si se interrumpe la configuración o si seleccionó la versión de CounterACT incorrecta, deberá reinstalar el equipo con la versión correcta del archivo ISO. Consulte la Guía de Instalación CounterACT para más información sobre cómo reinstalar un equipo.

2. Seleccionar **Configure CounterACT (Configurar CounterACT)**. Cuando se lo soliciten:

   Continuar: ¿(sí/no)?

   Presione **Enter (Entrar)** para iniciar la configuración:

3. Se abre el menú High Availability Mode (Modo de alta disponibilidad). Presione **Enter (Entrar)** para seleccionar la instalación estándar.

4. Aparece el mensaje CounterACT Initial Setup (Configuración Inicial de CounterACT). Presione **Enter (Entrar)** para continuar.

5. Se abre el menú Select CounterACT Installation Type (Seleccionar tipo de instalación de CounterACT). Ingrese **1** y presione **Enter (Entrar)** para instalar un equipo estándar CounterACT.

   Se inicia la configuración. Esto puede llevar un momento.

6. Se abre el menú Select Licensing Mode (Selección de modo de licencia). Seleccione el modo de licencia que utiliza su implementación. El modo de licencia se determina en el momento de la compra. ***No ingrese ninguna opción hasta que haya verificado el modo de licencia que su implementación utiliza***. Comuníquese con su representante de ForeScout para verificar su modo de licencia o si ingresó un modo incorrecto.

7. Cuando aparezca el mensaje Ingrese descripción de la máquina, ingrese un corto mensaje de identificación de este dispositivo y presione **Enter (Entrar)**.

   Aparecerá lo siguiente:

```
>>>>>> Establezca la contraseña del Administrador <<<<<<
```

```
Esta contraseña se usa para ingresar como ‘root’(raíz) para el
Sistema de operación de la máquina y como ‘admin’(administrador)
para la consola de CounterACT.
La contraseña deberá tener entre 6 y 15 caracteres de largo y
debe contener como mínimo un carácter no alfabético.
Contraseña del administrador:
```

8. Cuando aparece el mensaje Set Administrator Password (Establecer Contraseña del Administrador), ingrese la secuencia que será su contraseña (la secuencia no se verá en la pantalla) y presione **Enter (Entrar)**. Se le solicitará que confirme la contraseña. La contraseña deberá tener entre 6 y 15 caracteres de largo y contener como mínimo un carácter no alfabético.

Ingrese en el equipo como root (raíz)*, e ingrese en la consola como* admin (administrador)*.*

9. Cuando aparezca el mensaje Set Host Name (Establecer Nombre del Host), ingrese un nombre para el host y presione **Enter (Entrar)**. El nombre del host puede usarse cuando se inicie sesión en la consola, y se muestra en la consola para ayudar a identificar el equipo CounterACT que está visualizando. El nombre del host no debe exceder los 13 caracteres.

10. La pantalla Configurar los ajustes de la red le muestra una serie de parámetros de configuración. Ingrese un valor para cada pedido y presione **Enter (Entrar)** para ver el siguiente mensaje.
    - Los componentes de CounterACT se comunican a través de interfaces de administración. El número de interfaces de comunicaciones enumerado depende del modelo del equipo.
    - La **Dirección de IP de administración** es la dirección de la interfaz a través de la cual se comunican los componentes CounterACT. Agregue una identificación VLAN para esta interfaz solamente si la interfaz usada para comunicarse entre los componentes CounterACT se conecta con un puerto marcado.
    - Si hay más de una **dirección de servidor DNS**, separe cada dirección con un espacio. La mayoría de los servidores internos DNS resuelven las direcciones externas e internas pero quizás necesite incluir un servidor DNS de resolución externa. Como casi todas las preguntas DNS realizadas por el equipo serán para direcciones internas, el servidor externo DNS deberá estar enumerado al final.

11. Aparece la pantalla de Resumen de configuración. Le indicarán que realice las pruebas generales de conectividad, reconfigure los ajustes o complete la configuración. Ingrese **D** para completar la configuración.

Licencia

Luego de la instalación, asegúrese de que su dispositivo CounterACT tenga una licencia válida. La licencia predeterminada de su dispositivo CounterACT dependerá del modo de licencia que utiliza su implementación.

- Si la implementación de su CounterACT está funcionando en ***Modo de licencia por equipo***, puede comenzar a trabajar usando esta licencia de demostración, válida por 30 días. Durante este tiempo, deberá recibir una licencia permanente de ForeScout y ubicarla en una carpeta accesible en su disco o red. Instale la licencia desde esta ubicación antes de que expire la licencia de demostración a los 30 días (si es necesario, puede solicitar una extensión de la licencia de demostración).

  Recibirá alertas cuando su licencia de demostración esté por expirar de varias maneras. Consulte la *Guía de Gestión de CounterACT* para más información sobre alertas de licencia de demostración.

  Si está trabajando con un sistema CounterACT virtual:

  – La licencia de demostración no se instalará en esta etapa. Deberá instalar la licencia de demostración que recibió de su representante de CounterACT por correo electrónico.
  – Como mínimo un dispositivo de CounterACT deberá tener acceso a internet. Esta conexión se usa para validar las licencias CounterACT con el servidor de la Licencia de ForeScout. Las licencias que no pueden ser autenticadas durante un mes serán revocadas. CounterACT le enviará un correo electrónico de advertencia una vez al día indicando que existe un error de comunicación con el servidor.

    Consulte la *Guía de Instalación CounterACT* para más información.

- Si la implementación de su CounterACT está funcionando en ***Modo de licencia centralizado***, el *Administrador de habilitación* recibirá un correo electrónico cuando se habilite la licencia y esté disponible en el Portal del usuario de ForeScout. Una vez disponible, el *administrador de CounterACT* de la implementación puede activar la licencia en la Consola de CounterACT. Hasta que la licencia esté activada, las características de CounterACT no funcionarán correctamente. Por ejemplo, las políticas no serán evaluadas y las acciones no se llevarán a cabo. *Ninguna licencia de demostración se instala automáticamente durante la instalación del sistema.*

Consulte la *Guía de Gestión de CounterACT* para más información sobre la administración de licencias.

5. Administración remota

Configuración de iDRAC

El Controlador Integrado de Acceso Remoto (iDRAC) es una solución de sistema de servidor integrado que le ofrece acceso remoto OS/ubicación independiente en la red LAN o Internet para los Equipos CounterACT. Use el módulo para acceder a KVM, encender/apagar/reiniciar y realizar tareas de mantenimiento y de resolución de problemas.

Realice lo siguiente para trabajar con el módulo iDRAC:

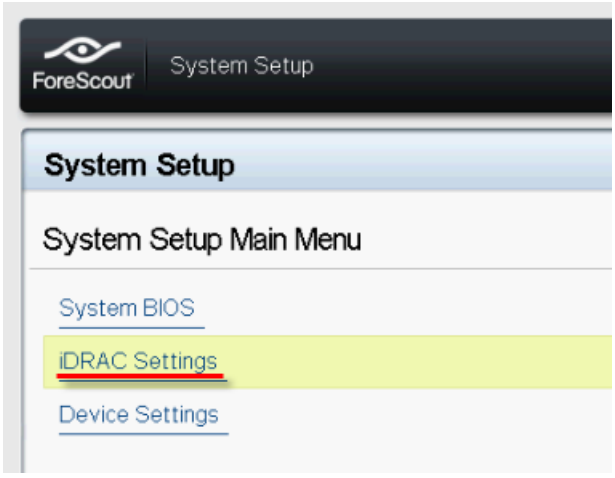
- Habilite y configure el módulo iDRAC
- Conecte el módulo a la red
- Inicie sesión en iDRAC

Habilite y configure el módulo iDRAC

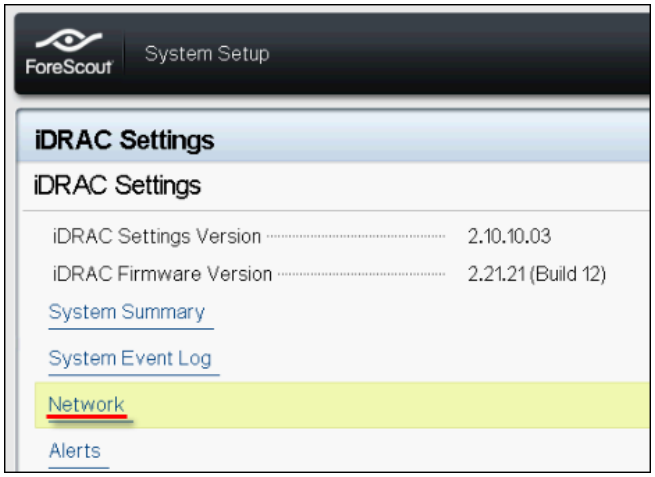
Cambie las configuraciones de iDRAC para habilitar el acceso remoto en el dispositivo CounterACT. Esta sección describe los ajustes de integración básica necesaria para trabajar con CounterACT.

Para configurar iDRAC:

1. Encienda el sistema administrado.
2. Seleccione F2 durante la Prueba Automática de Encendido.
3. En la página System Setup Main Menu (Menú Principal de la Configuración del Sistema), seleccione **iDRAC Settings (Ajustes de iDRAC)**.

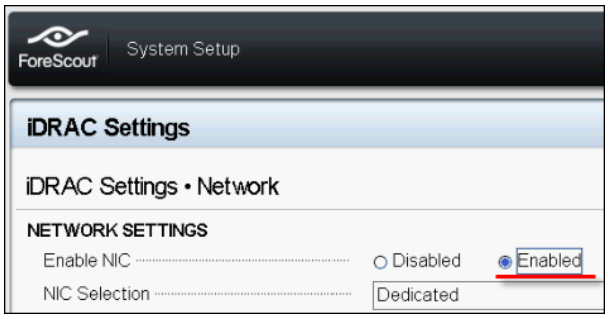


4. En la página iDRAC Settings (Ajustes de iDRAC), seleccione **Network (Red)**.



5. Configure los siguientes ajustes de la Red:

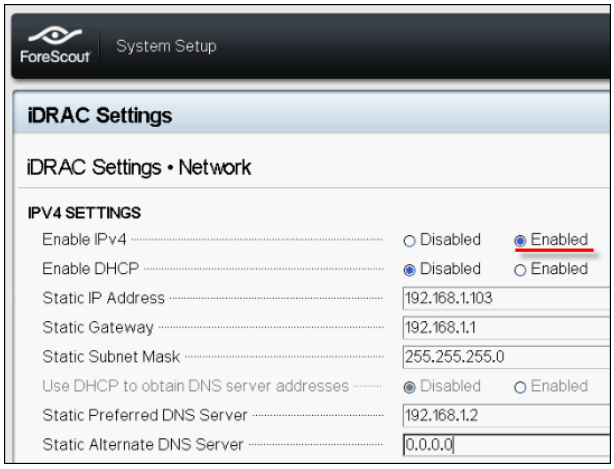
   – ***Network Settings (Ajustes de la Red)***. Verifique que el campo **Enable NIC (Habilitar NIC)** esté en **Enabled (Habilitado)**.



   – ***Common Settings (Ajustes comunes)***. En el campo DNS DRAC Name (Nombre de DNS DRAC), puede actualizar un DNS dinámico (opcional).

   – ***IPV4 Settings (Ajustes de IPV4)***. Verifique que el campo **Enable IPv4 (Habilitar IPv4)** esté en **Enabled (Habilitado)**.

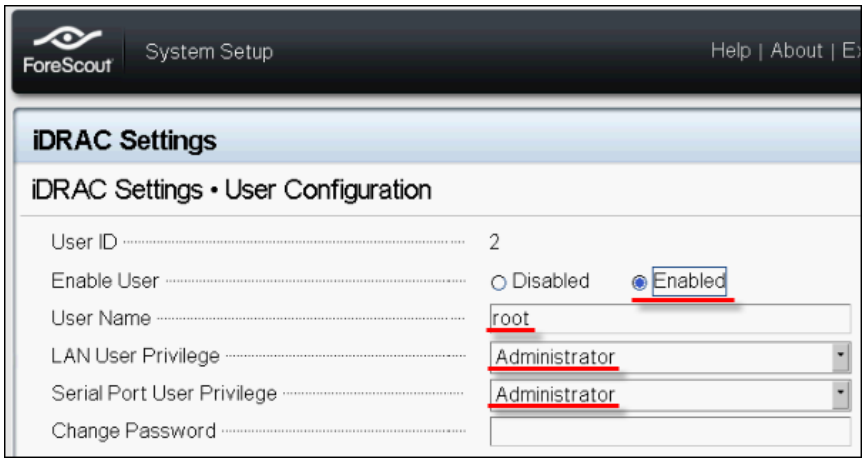
     Marque el campo **Enable DHCP (Habilitar DHCP)** como **Enabled (Habilitado)** para usar la Dirección de IP Dinámica o como **Disabled (Deshabilitado)** para usar la Dirección de IP Estática. Si está habilitado, el DHCP automáticamente asignará la dirección de IP, la pasarela y la máscara de subred a iDRAC. Si se desactiva, ingrese los valores para los campos de **Static IP Address (Dirección de IP Estática)**, **Static Gateway (Pasarela Estática)** y **Static Subnet Mask (Máscara de Subred Estática)**.



6. Seleccione **Back (Regresar)**.
7. Seleccione **User Configuration (Configuración del Usuario)**.
8. Configure los siguientes campos de Configuración del Usuario para el usuario raíz:
   - ***Enable User (Habilite el usuario)***. Verifique que este campo esté en Enabled (Habilitado).

     El nombre de usuario ingresado aquí no puede ser el mismo que el usuario de CounterACT.

   - ***LAN and Serial Port User Privileges (Privilegios de Usuario de Puerto en Serie y LAN)***. Establezca los niveles de privilegio al Administrador.
   - ***Change Password (Cambie la contraseña)***. Establezca una contraseña para iniciar sesión con el usuario.

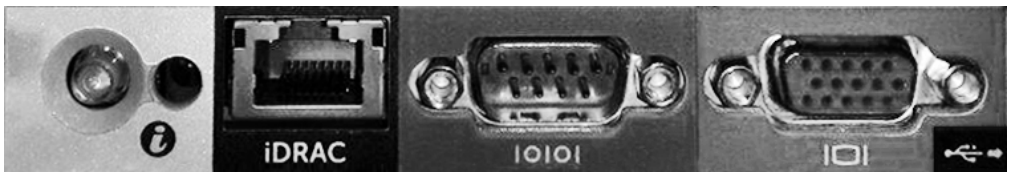


9. Seleccione **Back (Regresar)** y luego seleccione **Finish (Finalizar)**. Confirme los ajustes cambiados.

   Se guardan los ajustes de la red y el sistema se reinicia.

Conecte el módulo a la red

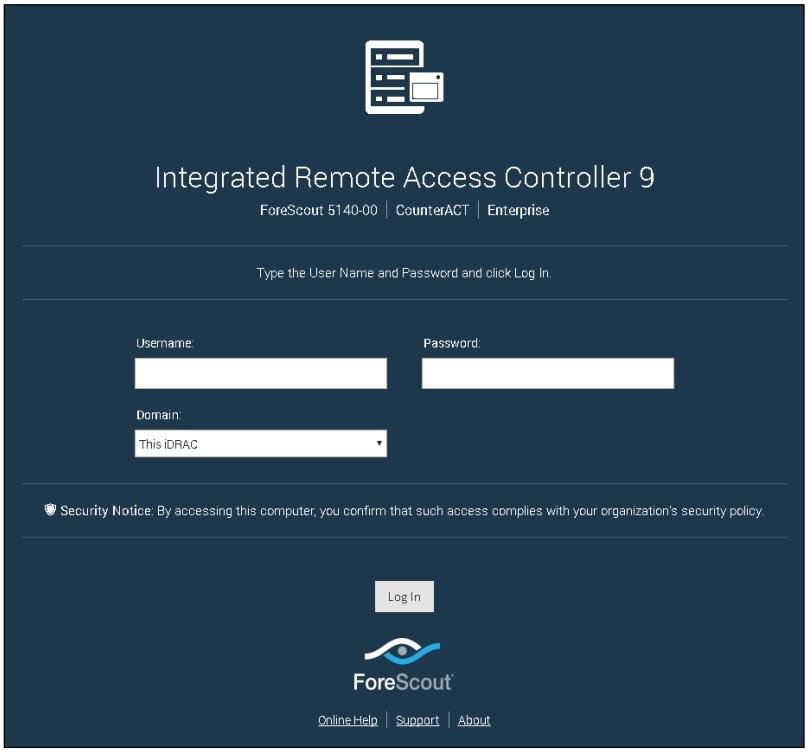
El iDRAC se conecta a una red de Ethernet. Es común que se conecte a una red de administración. La siguiente imagen muestra la ubicación del puerto iDRAC en el panel trasero del equipo CT-1000:



Inicie sesión en iDRAC

Para iniciar sesión en iDRAC:

1. Navegue por la dirección de IP o el nombre de dominio configurado en **iDRAC Settings (Ajustes de iDRAC)** > **Network (Red)**.



2. Ingrese el Nombre de usuario y la Contraseña configurada en la página de User Configuration (Configuración del Usuario) de la configuración del sistema iDRAC.
3. Seleccione **Submit (Enviar)**.

Para más información sobre iDRAC, consulte la *Guía del Usuario de iDRAC*. Puede acceder a esta guía en uno de los siguientes lugares, dependiendo del modo de licencia que su implementación esté usando:

- Modo de licencia por equipo - https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf
- Modo de licencia centralizado – Página de documentación del Portal del usuario.

Consulte la Documentación adicional de CounterACT (*Identificación del modo de licencia en la Consola*) para ver qué modo de licencia su implementación esté usando.

Es muy importante actualizar la contraseña raíz predeterminada, si aún no lo ha hecho.

6. Verificación de conectividad

Verificar la conexión de la interfaz de administración

Para probar la conexión de la interfaz de administración, inicie sesión en el equipo y ejecute el siguiente comando:

fstool linktest

Aparecerá la siguiente información:

```
Estado de la interfaz de administración
Rastreo de la información de la pasarela predeterminada
Estadística de rastreo
Llevando a cabo la prueba de resolución de nombre
Resumen de la prueba
```

Realizar la prueba de rastreo

Ejecute la prueba de rastreo desde el equipo al escritorio de la red para verificar la conectividad:

Rastreo <network_desktop_IP_address> (IP_del_escritorio_de_la_red)

7. Configure la consola de CounterACT

Instale la consola de CounterACT

La consola es la aplicación de administración de CounterACT que se usa para visualizar información detallada importante sobre terminales y controlarlas. Esta información es recopilada por dispositivos CounterACT. Consulte la *Guía de Gestión de CounterACT* para más información.

Debe suministrar una máquina para alojar el software de aplicación de la Consola CounterACT. Los requisitos mínimos de hardware son:

- Máquinas no dedicadas, en funcionamiento:
  - Windows 7/8/8.1/10
  - Windows Server 2008/2008 R2/2012/2012 R2/2016
  - Linux RHEL/CentOS 7
- Memoria de 2GB
- Espacio en disco de 1GB

El método siguiente está disponible para realizar la instalación de la consola:

Use el software de instalación incorporado en su equipo.

1. Abra una ventana del navegador desde la computadora de la consola.
2. Ingrese lo siguiente en la línea de dirección del navegador:

   `http://<Appliance_ip>/install`

   Donde Appliance_ip es la dirección de IP de este equipo. El navegador mostrará la ventana de instalación de la consola.
3. Siga las instrucciones que aparecen en la pantalla.

Inicie sesión

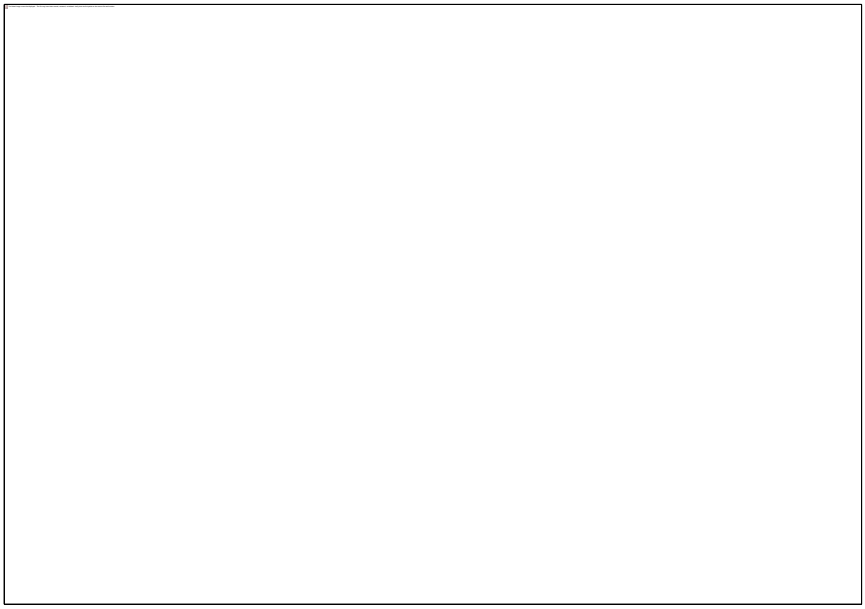
Luego de completar la instalación, puede iniciar sesión en la consola de CounterACT.

1. Seleccione el icono de CounterACT desde la ubicación del atajo que creó.

2. Ingrese la dirección de IP o nombre del host del equipo en el campo **IP/Name (IP/Nombre)**.
3. En el campo **User Name (Nombre de usuario)**, ingrese admin (administrador).
4. En el campo **Password (Contraseña)**, ingrese la contraseña que usted creó durante la instalación del equipo.
5. Seleccione **Login (Iniciar sesión)** para lanzar la consola.

Configuración inicial

Luego de iniciar sesión por primera vez, aparecerá el Asistente de configuración inicial. El Asistente lo guiará por los pasos esenciales de configuración para que CounterACT funcione de manera rápida y eficiente.



Antes de comenzar con la Configuración inicial

Prepare la siguiente información antes de trabajar con el Asistente:

Información necesaria para el Asistente	**Valor**
Direcciones de servidor NTP que usa su organización (opcional)	
Dirección de IP de relé de correo interno que permite la entrega de alertas por correo electrónico si el tráfico SMTP no está permitido desde el equipo (opcional)	
Dirección de correo electrónico del administrador de CounterACT	
interfaces de respuesta y control	
Para segmentos o VLAN sin DHCP, el segmento de la red o VLAN a la que la interfaz de respuesta está directamente conectada y una dirección de IP permanente va ser usada por CounterACT en cada VLAN	
Variaciones de la dirección de IP que el equipo protegerá (todas las direcciones internas, incluyendo las direcciones no usadas)	
Información de cuenta de usuario LDAP y dirección de IP de servidor LDAP	
Credenciales de dominio, incluyendo la contraseña y nombre de la cuenta administrativa del dominio	
Servidores de autenticación para que CounterACT pueda analizar qué hosts de red se han autenticado exitosamente	
Dirección de IP del interruptor, proveedor y parámetros de SNMP	

Consulte la *Guía de Gestión de CounterACT* para más información o la Ayuda en línea para recibir información sobre cómo trabajar con el Asistente.

Documentación adicional de CounterACT

Para más información sobre otras características y módulos de CounterACT, consulte los siguientes recursos:

- Descarga de documentación
- Portal de documentación
- Herramientas de ayuda de CounterACT

Descarga de documentación

Puede acceder a las descargas de documentación desde uno de los dos portales de ForeScout, depende del modo de licencia que su implementación usa.

- ***Modo de licencia por equipo*** - Portal de actualizaciones del producto
- ***Modo de licencia centralizado*** - Portal del usuario

Las descargas de software también están disponibles en estos portales.

Para saber qué modo de licencia está usando su implementación, consulte Identificación del modo de licencia en la Consola.

Portal de actualizaciones del producto

El Portal de actualizaciones del producto ofrece enlaces de lanzamientos de versiones de CounterACT, Módulos base y de contenido y Módulos extendidos, así como documentación relacionada. El portal también ofrece una variedad de documentación adicional.

Para acceder al Portal de actualizaciones del producto:

1. Ingrese a https://updates.forescout.com/support/index.php?url=counteract.
2. Seleccione la versión de CounterACT que está buscando.

Portal del usuario

Esta página de descargas en el Portal del usuario de CounterACT ofrece enlaces de lanzamientos de versiones de CounterACT pagas, Módulos base y de contenido y Módulos extendidos, así como documentación relacionada. El software y la documentación relacionada solo aparecerán en la página de Descargas si tiene la licencia habilitada para el software. La página de Documentación en el portal ofrece una variedad de documentación adicional.

Para acceder a la documentación en el Portal del usuario de ForeScout:

1. Ingrese a https://forescout.force.com/support/.
2. Seleccione **Downloads (Descargas)** o **Documentation (Documentación)**.

Portal de documentación

El Portal de documentación de ForeScout es una biblioteca de búsqueda basada en la web que contiene información sobre herramientas, características, funcionalidades e integraciones de CounterACT.

Si su implementación usa el Modo de licencia centralizado, no tendrá las credenciales para acceder a este portal.

Para acceder al Portal de Documentación:

1. Ingrese a www.forescout.com/docportal.
2. Use sus credenciales de soporte técnico para iniciar sesión.
3. Seleccione la versión de CounterACT que está buscando.

Herramientas de ayuda de CounterACT

Acceda a la información directamente desde su Consola CounterACT.

Botones de ayuda de la consola

Utilice los botones de *Help (Ayuda)* contextual para acceder rápidamente a información sobre tareas y temas sobre los que está trabajando.

Guía de Gestión de CounterACT

Seleccione **CounterACT Help (Ayuda CounterACT)** desde el menú **Help (Ayuda)**.

Archivos de ayuda en plugin

1. Una vez instalado el plugin, seleccione **Options (Opciones)** desde el menú **Tools (Herramientas)** y luego seleccione **Modules (Módulos)**.
2. Seleccione el plugin y luego seleccione **Help (Ayuda)**.

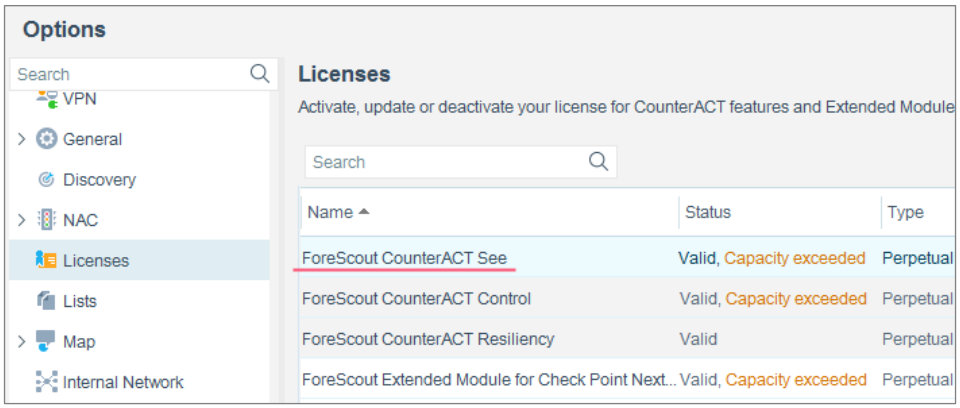
Portal de documentación

Seleccione **Documentation Portal (Portal de documentación)** desde el menú **Help (Ayuda)**.

Identificación del modo de licencia en la Consola

Si su Administrador corporativo tiene una licencia *ForeScout CounterACT* consulte la licencia enumerada en su consola, su implementación está funcionando en Modo de licencia centralizado. Si no, su implementación está funcionando en Modo de licencia por equipo.

Seleccione **Options (Opciones) > Licenses (Licencias)** para ver si tiene una licencia *ForeScout CounterACT* consulte la licencia enumerada en la tabla.



Comuníquese con su representante de ForeScout si tiene preguntas sobre cómo identificar el modo de licencia.

Aviso legal

Envíe sus comentarios y preguntas sobre este documento a: support@forescout.com

2018-03-2715:03