

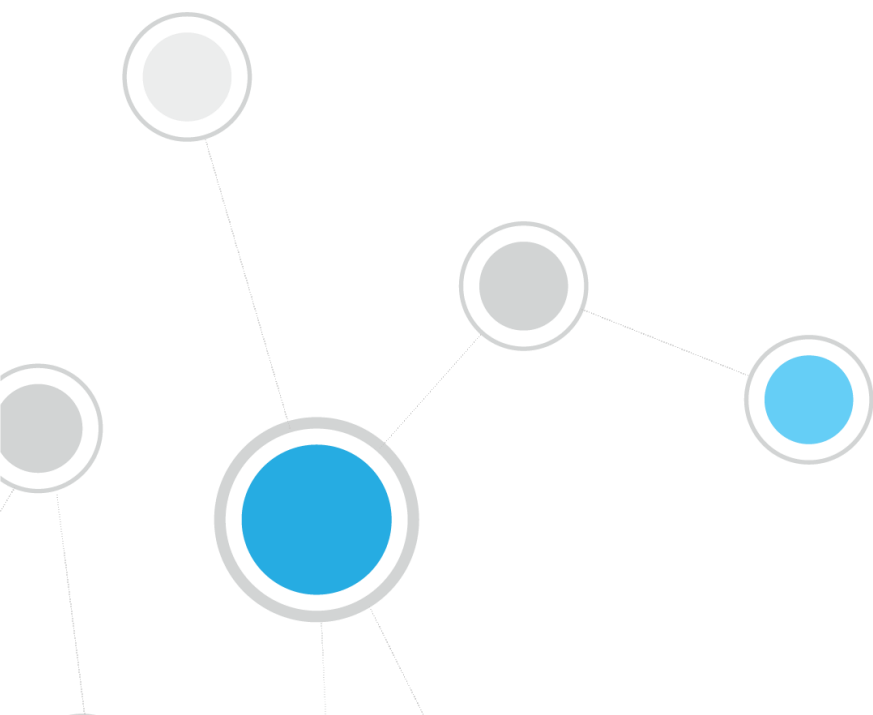


ForeScout CounterACT®

Aparelho CounterACT individual

Guia de iniciação rápida

Versão 8.0



Índice

Bem-vindo ao CounterACT Versão 8.0	4
Conteúdo do pacote CounterACT	4
Visão geral	5
1. Criar um plano de implementação	6
Decidir onde implementar o Aparelho	6
Ligações de interface do Aparelho	6
Interface de gestão	6
Interface do monitor	9
Interface de resposta	9
2. Configurar o comutador	10
A. Opções de ligação do comutador	10
1 Implementação padrão (Gestão separada, interfaces de resposta e monitor)	10
2 "Tap" em linha passiva	10
3 "Tap" em linha (com capacidade de injeção) ativa	10
4 Resposta de camada IP (para instalações de comutador de 3 camadas).....	10
B. Notas de configuração do comutador.....	11
Marcações VLAN (802.1Q)	11
Diretrizes adicionais.....	11
3. Ligar cabos de rede e cabos de alimentação.....	12
A. Desembalar o aparelho e os cabos de ligação	12
B. Registrar as atribuições de interface.....	12
C. Ligar o Aparelho.....	13
4. Configurar o aparelho.....	14
5. Gestão remota.....	18
Configuração iDRAC.....	18
Ativar e configurar o módulo iDRAC	18
Ligar o módulo à rede	21
Iniciar sessão no iDRAC.....	21
6. Verificar conectividade.....	23
Verificar a ligação da interface de gestão	23
Efetuar um teste de ping	23
7. Configurar a Consola CounterACT.....	24
Instalar a Consola CounterACT	24
Iniciar sessão	24
Efetuar configuração inicial	25

Antes de iniciar a configuração inicial26

Documentação CounterACT adicional 27

Transferência de documentação27

Portal de documentação28

Ferramentas de ajuda CounterACT.....28

Bem-vindo ao CounterACT Versão 8.0

A plataforma CounterACT fornece visibilidade do dispositivo e infraestrutura, gestão de política, orquestração e simplificação do fluxo de trabalho para melhorar a segurança da rede. O CounterACT fornece às empresas informações contextuais em tempo real sobre dispositivos e utilizadores na rede. As políticas são definidas no CounterACT utilizando estas informações contextuais que ajudam a assegurar conformidade, remediação, acesso à rede adequado e simplificação das operações de serviço.

Este guia descreve a instalação para um Aparelho CounterACT autónomo individual.



Para obter mais informações detalhadas ou informações sobre a implementação de diversos Aparelhos para proteção de rede para toda a empresa, consulte o *Guia de instalação CounterACT* e o *Guia de administração CounterACT*. Consulte [Documentação CounterACT adicional](#) para obter mais informações sobre como aceder a estes guias.

Além disso, pode navegar para o website de apoio localizado em: <http://www.forescout.com/support> para obter a documentação mais recente, artigos de base de conhecimento e atualizações para o Aparelho.

Conteúdo do pacote CounterACT

O seu pacote CounterACT inclui os seguintes componentes:

- O Aparelho CounterACT
- Aro frontal
- Kits de calha (suportes de fixação)
- Cabo(s) de alimentação
- Cabo de ligação da Consola DB9 (apenas para ligações em série)
- Informações regulamentares, ambientais e de segurança para os produtos empresariais
- Documentação introdutória (apenas dispositivos 51xx)

Visão geral

Realize os seguintes passos para configurar o CounterACT:

- [1. Criar um plano de implementação](#)
- [2. Configurar o comutador](#)
- [3. Ligar cabos de rede e cabos de alimentação](#)
- [4. Configurar o aparelho](#)
- [5. Gestão remota](#)
- [6. Verificar conectividade](#)
- [7. Configurar a Consola CounterACT](#)

1. Criar um plano de implementação

Antes de realizar a instalação, deve decidir onde vai implementar o Aparelho e tomar conhecimento sobre as ligações de interface do Aparelho.

Decidir onde implementar o Aparelho

É crucial selecionar a localização de rede correta onde o Aparelho irá ser instalado para uma implementação bem-sucedida e um desempenho ideal do CounterACT. A localização correta irá depender dos objetivos de implementação desejados e da política de acesso da rede. O Aparelho deverá ser capaz de monitorizar o tráfego que é relevante para a política pretendida. Por exemplo, se a sua política depender da monitorização de eventos de autorização de nós terminais para servidores de autenticação corporativos, o Aparelho deve ser instalado de forma a que veja o tráfego do nó terminal que flui para o(s) servidor(es) de autenticação.

Para obter mais informações sobre instalação e implementação, consulte o *Guia de instalação CounterACT*. Consulte [Documentação CounterACT adicional](#) para obter mais informações sobre como aceder a este guia.

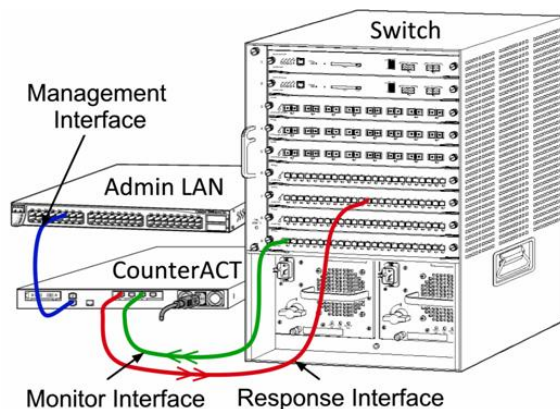
Ligações de interface do Aparelho

O Aparelho está normalmente configurado com três ligações ao comutador de rede.

Interface de gestão

A interface de gestão permite-lhe gerir o CounterACT e realizar consultas e inspeções profundas dos nós terminais. A interface deve estar ligada a uma porta de comutação com acesso a todos os nós terminais da rede.

Cada Aparelho requer uma ligação de gestão individual à rede. Esta ligação requer um endereço IP na LAN local e acesso à porta 13000/TCP a partir das máquinas que irão executar a aplicação de gestão da Consola CounterACT. A porta de gestão deve ter acesso a serviços de rede adicionais.



Requisitos de acesso à rede

Porta	Serviço	Para ou De CounterACT	Função
22/TCP	SSH	De	Permite a inspeção remota dos nós terminais OS X e de Linux. Permite ao CounterACT comunicar com comutadores de rede e routers.
		Para	Permite acesso à interface da linha de comando do CounterACT.
2222/TCP	SSH	Para	(Alta disponibilidade) Permite acesso aos dispositivos físicos do CounterACT que fazem parte da Alta disponibilidade. Use 22/TCP para aceder ao endereço IP (virtual) partilhado do par.
25/TCP	SMTP	De	Permite ao CounterACT aceder ao encaminhamento do correio da empresa.
53/UDP	DNS	De	Permite ao CounterACT resolver endereços IP internos.
80/TCP	HTTP	Para	Permite o redirecionamento de HTTP.
123/UDP	NTP	De	Permite ao CounterACT aceder a um servidor de hora local ou ntp.forescout.net. Por predefinição, o CounterACT acede a ntp.foreScout.net
135/TCP	MS-WMI	De	Permite a inspeção remota dos nós terminais Windows.
139/TCP	SMB, MS-RPC	De	Permite a inspeção remota dos nós terminais Windows (Para nós terminais que executam o Windows 7 e anterior).
445/TCP			Permite a inspeção remota dos nós terminais Windows.
161/UDP	SNMP	De	Permite ao CounterACT comunicar com comutadores de rede e routers. Para obter mais informações sobre a configuração do SNMP, consulte o <i>Guia de administração CounterACT</i> .
162/UDP	SNMP	Para	Permite ao CounterACT receber "traps" SNMP dos comutadores de rede e routers. Para obter mais informações sobre a configuração do SNMP, consulte o <i>Guia de administração CounterACT</i> .
389/TCP (636)	LDAP	De	Permite ao CounterACT comunicar com o Active Directory. Permite a comunicação com portais de base web CounterACT.

Porta	Serviço	Para ou De CounterACT	Função
443/TCP	HTTPS	Para	Permite o redirecionamento de HTTP utilizando TLS.
2200/TCP	SecureConnector para Linux	Para	Permite ao SecureConnector criar uma ligação segura (SSH encriptado) ao Aparelho a partir de máquinas Linux. <i>SecureConnector</i> é um agente baseado em script que permite a gestão dos nós terminais Linux enquanto estiverem ligados à rede.
10003/TCP	SecureConnector para Windows	Para	Permite ao SecureConnector criar uma ligação segura (TLS encriptado) ao Aparelho a partir das máquinas Windows. <i>SecureConnector</i> é um agente que permite a gestão dos nós terminais Windows enquanto estão ligados à rede. Consulte o <i>Guia de administração CounterACT</i> para obter mais informações sobre o SecureConnector. Quando o SecureConnector liga a um Aparelho ou ao Enterprise Manager, este é redirecionado para o Aparelho ao qual o respetivo anfitrião está atribuído. Certifique-se que esta porta está aberta a todos os Aparelhos e ao Enterprise Manager para permitir uma mobilidade transparente na organização.
10005/TCP	SecureConnector para OS X	Para	Permite ao SecureConnector criar uma ligação segura (TLS encriptado) para o Aparelho a partir das máquinas OS X. <i>SecureConnector</i> é um agente que permite a gestão dos nós terminais OS X enquanto estão ligados à rede. Consulte o <i>Guia de administração CounterACT</i> para obter mais informações sobre o SecureConnector. Quando o SecureConnector liga a um Aparelho ou ao Enterprise Manager, este é redirecionado para o Aparelho ao qual o respetivo anfitrião está atribuído. Certifique-se que esta porta está aberta a todos os Aparelhos e ao Enterprise Manager para permitir uma mobilidade transparente na organização.

Porta	Serviço	Para ou De CounterACT	Função
13000/TCP	CounterACT	De/Para	<p>Para ambientes com apenas um Aparelho – a partir da Consola para o Aparelho.</p> <p>Para ambientes com mais do que um Dispositivo CounterACT – a partir da Consola para o Dispositivo CounterACT e a partir de um Dispositivo CounterACT para outro. A comunicação do Dispositivo CounterACT inclui a comunicação com o Enterprise Manager e o Recovery Enterprise Manager, utilizando o TLS.</p>

Interface do monitor

A interface do monitor permite ao Aparelho monitorizar e acompanhar o tráfego de rede. Qualquer interface disponível pode ser utilizada como interface do monitor.

O tráfego está espelhado numa porta no comutador e é monitorizado pelo Aparelho. A utilização da marcação VLAN 802.1Q depende do número de VLAN a serem espelhadas.

- **VLAN individual:** Quando o tráfego monitorizado for gerado a partir de uma VLAN individual, o tráfego espelhado não precisa de marcação VLAN.
- **Múltiplas VLAN:** Se o tráfego monitorizado for proveniente de mais do que uma VLAN, o tráfego espelhado deve utilizar marcação 802.1Q VLAN.

Quando dois comutadores estiverem ligados como par redundante, o Aparelho deve monitorizar o tráfego a partir de ambos os comutadores.

Não é necessário endereço IP na interface do monitor.

Interface de resposta

O Aparelho responde ao tráfego utilizando a interface de resposta. O tráfego de resposta é utilizado para proteger contra atividade maliciosa e para realizar ações de política. Estas ações podem incluir, por exemplo, o redirecionamento de navegadores web ou realizar o bloqueio de sessões. A configuração da porta de comutação em questão depende do tráfego a ser monitorizado.

Qualquer interface disponível pode ser utilizada como interface de resposta.

- **VLAN individual:** Quando o tráfego monitorizado é gerado a partir de uma VLAN individual, a porta de resposta deve pertencer à mesma VLAN. Neste caso, o Aparelho requer o endereço IP individual nessa VLAN.
- **Múltiplas VLAN:** Se o tráfego monitorizado for proveniente de mais do que uma VLAN, a porta de resposta deve estar igualmente configurada com as marcações 802.1Q VLAN para as mesmas VLAN. O Aparelho requer um endereço IP para cada VLAN monitorizada.

2. Configurar o comutador

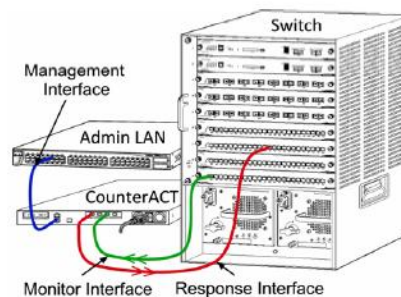
A. Opções de ligação do comutador

O Aparelho foi concebido para integrar facilmente diversos ambientes de rede. Para integrar com êxito o Aparelho na rede, verifique se o comutador está configurado para monitorizar o tráfego necessário.

Estão disponíveis diversas opções para ligar o Aparelho ao comutador.

1 Implementação padrão (Gestão separada, interfaces de resposta e monitor)

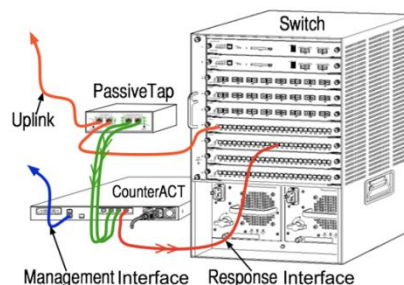
A implementação recomendada utiliza três portas separadas. Estas portas são descritas em [Ligações de interface do Aparelho](#).



2 "Tap" em linha passiva

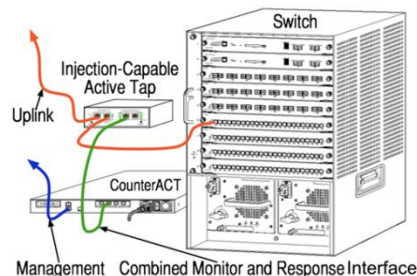
Em vez de ligar à porta do monitor do comutador, o Aparelho pode ser utilizado uma "tap" em linha passiva.

A "tap" em linha passiva requer duas portas de monitor (uma para tráfego a montante e uma para tráfego a jusante), exceto no caso de uma "tap" de *recombinação*, que combina as duas sequências duplex numa única porta. Tenha em atenção que se a porta derivada possuir marcações 802.1Q VLAN, a porta de resposta também deve possuir marcações 802.1Q VLAN.



3 "Tap" em linha (com capacidade de injeção) ativa

O Aparelho pode utilizar uma "tap" em linha ativa. Se a "tap" tiver capacidade de injeção, o Aparelho combina o monitor e as portas de resposta para que não haja necessidade de configurar uma porta de resposta separada no comutador. Esta opção pode ser utilizada independentemente do tipo da configuração do comutador a montante ou a jusante.



4 Resposta de camada IP (para instalações de comutador de 3 camadas)

O Aparelho pode utilizar a sua própria interface de gestão para responder ao tráfego. Apesar de esta opção poder ser utilizada com qualquer tráfego monitorizado, é

recomendável apenas em situações onde as portas dos monitores do Aparelho não façam parte de qualquer VLAN e não possam responder ao tráfego monitorizado utilizando qualquer outra porta de comutação. Isto é típico ao monitorizar uma ligação que liga dois routers. Esta opção não pode responder ao Protocolo de resolução de endereços (ARP), o que limita a capacidade do Aparelho para detetar as leituras direcionadas aos endereços IP incluídos na submáscara monitorizada. Este limite não se aplica quando o tráfego entre dois routers estiver a ser monitorizado.

B. Notas de configuração do comutador

Marcações VLAN (802.1Q)

- **Monitorizar uma VLAN individual:** Se o tráfego monitorizado originar de uma VLAN individual, o tráfego não precisa de marcações 802.1Q VLAN.
- **Monitorizar múltiplas VLAN:** Se o tráfego monitorizado originar de duas ou mais VLAN, *ambas* as portas monitorizadas e de resposta devem ter as marcações 802.1Q VLAN ativadas. A monitorização de múltiplas VLAN é recomendada, dado que fornece a melhor cobertura geral enquanto minimiza o número de portas de espelhamento.
- Se o comutador não puder utilizar uma marcação 802.1Q VLAN na porta de espelhamento, efetue um dos seguintes:
 - Espelhe apenas uma VLAN individual
 - Espelhe uma porta uplink individual, sem marcações
 - Utilize a opção de resposta de camada IP
- Se o comutador conseguir apenas espelhar uma porta, então deve espelhar uma porta uplink individual. Isto pode ter marcações aplicadas. No geral, se o comutador retirar as marcações 802.1Q VLAN, deve utilizar a opção de resposta da camada IP.

Diretrizes adicionais

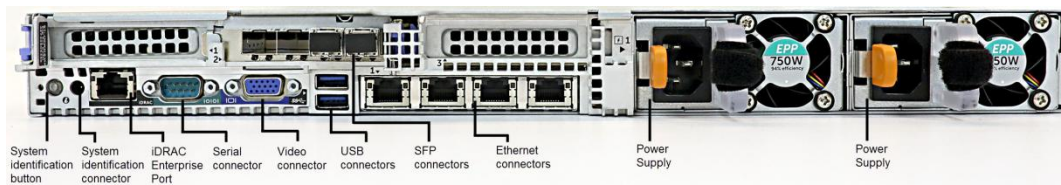
- Nos seguintes casos, deve espelhar apenas uma interface (que não permite transmitir/receber):
 - Se o comutador não conseguir espelhar os tráfegos transmitidos e recebidos
 - Se o comutador não conseguir espelhar todo o tráfego do comutador
 - Se o comutador não conseguir espelhar todo o tráfego através de uma VLAN
- Certifique-se de que não sobrecarrega a porta de espelhamento.
- Alguns comutadores (p. ex. Cisco 6509) podem exigir que a atual configuração da porta seja completamente eliminada antes de introduzir uma nova configuração. Não eliminar as antigas informações da porta faz com que o comutador remova as marcações 802.1Q.

3. Ligar cabos de rede e cabos de alimentação

A. Desembalar o aparelho e os cabos de ligação

1. Remova o aparelho e o cabo de alimentação do contentor de transporte
2. Remova o kit de calhas fornecido com o Aparelho.
3. Monte o kit de calhas no Aparelho e monte o Aparelho no suporte.
4. Ligue os cabos de rede entre as interfaces de rede no painel traseiro do Aparelho e as portas de comutação.

Amostra do painel traseiro – dispositivo CounterACT



Pode substituir os SFP fornecidos pela ForeScout com SFP Finisar que foram testados e aprovados pela ForeScout. Consulte o *Guia de instalação CounterACT* para obter mais detalhes.

B. Registrar as atribuições de interface

Depois de concluir a instalação do Aparelho no centro de dados e instalar a Consola CounterACT, ser-lhe-á pedido para registar as atribuições de interface. Estas atribuições, referidas como *Channel definitions* (Definições de canal), são introduzidas no Initial Setup Wizard (Assistente de configuração inicial) que abre quando iniciar sessão pela primeira vez na Consola.

Registe abaixo as atribuições de interface física e utilize-as quando concluir a configuração do Canal na Consola.

Interface Eth	Atribuição da interface (p. ex. Gestão, Monitor, Resposta)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	

Eth5	
Eth6	
Eth7	

C. Ligar o Aparelho

1. Ligue o cabo de alimentação à tomada de alimentação no painel traseiro do Aparelho.
2. Ligue a outra extremidade do cabo de alimentação a uma tomada CA com ligação à terra.
3. Ligue o teclado e o monitor ao Aparelho ou configure o Aparelho para uma ligação em série. Consulte o *Guia de instalação CounterACT* para obter mais informações.
4. Ligue o Aparelho a partir do painel frontal.

4. Configurar o aparelho

Prepare as informações que se seguem antes de configurar o Aparelho.

Nome do anfitrião do aparelho	
Palavra-passe do administrador do CounterACT	Mantenha a palavra-passe num local seguro
Interface de gestão	
Endereço IP do aparelho	
Máscara da rede	
Endereço IP do portal predefinido	
Nome do domínio DNS	
Endereços do servidor DNS	

Depois de ligar, ser-lhe-á pedido para iniciar a configuração com a seguinte mensagem:

```
CounterACT Appliance boot is complete. (O arranque do aparelho
CounterACT está concluído.)
Press <Enter> to continue. (Prima <Enter> para continuar.)
```

1. Prima **Enter**. Se possuir um dispositivo 51xx CounterACT, vai surgir o seguinte menu:

```
CounterACT 8.0.0-<build> options: (Opções CounterACT 8.0.0-
<build>:)

1) Configure CounterACT (Configurar o CounterACT)
2) Restore saved CounterACT configuration (Restaurar a
configuração CounterACT gravada)
3) Identify and renumber network interfaces (Identificar e
renumerar as interfaces de rede)
4) Configure keyboard layout (Configurar a disposição do
teclado)
5) Turn machine off (Desligar a máquina)
6) Reboot the machine (Reiniciar a máquina)

Choice (1-6) :1 (Escolher (1-6) :1)
```


Se possuir um dispositivo CT-xxxx CounterACT, vai ver CounterACT 7.0.0 ou CounterACT 8.0.0 listado como a versão na parte superior do menu.

- Se o que vir indicado for CounterACT 7.0.0, pode optar entre atualizar ou efetuar uma nova instalação da versão 8.0.0. Consulte o *Guia de instalação CounterACT* para obter mais detalhes. Após instalar ou atualizar para a versão 8.0.0, vai ver o menu listado acima.
- Se o que vir indicado for CounterACT 8.0.0, o menu oferece uma opção para instalar o CounterACT 7.0.0 ou configurar o CounterACT 8.0.0, conforme indicado abaixo. Se selecionar CounterACT 7.0.0, não vai poder reinstalar o CounterACT 8.0.0 através do menu Configuration (Configuração). Consulte o *Guia de instalação CounterACT versão 7.0.0* para obter detalhes sobre a configuração do CounterACT 7.0.0.

```
CounterACT 8.0.0-<build> options: (Opções CounterACT 8.0.0-  
<build>:)
```

- 1) Install CounterACT 7.0.0-<build> (Instalar o CounterACT 7.0.0-<build>)
- 2) Configure CounterACT 8.0.0-<build> (Configurar o CounterACT 8.0.0-<build>)
- 3) Restore saved CounterACT configuration (Restaurar a configuração CounterACT guardada)
- 4) Identify and renumber network interfaces (Identificar e renumerar as interfaces de rede)
- 5) Configure keyboard layout (Configurar a disposição do teclado)
- 6) Turn machine off (Desligar a máquina)
- 7) Reboot the machine (Reiniciar a máquina)

```
Choice (1-7) : (Escolher (1-7) :)
```

 *Se a configuração for interrompida ou se selecionou a versão CounterACT errada, vai ser necessário recriar a imagem do aparelho com a versão relevante do ficheiro ISO. Consulte o Guia de instalação CounterACT para obter mais informações sobre como recriar a imagem de um aparelho.*

2. Selecione **Configure CounterACT** (Configurar CounterACT). Aquando do pedido:

```
Continue (Continuar): (yes/no) (sim/não)?
```

Prima **Enter** para iniciar a configuração.

3. O pedido de High Availability Mode (Modo de disponibilidade elevada) abre. Prima **Enter** para selecionar a Standard Installation (Instalação padrão).
4. O pedido de CounterACT Initial Setup (Configuração inicial CounterACT) é apresentado. Prima **Enter** para continuar.
5. O pedido de Select CounterACT Installation Type (Selecionar tipo de instalação CounterACT) abre. Escreva **1** e prima **Enter** para instalar um Aparelho CounterACT padrão.


A configuração é inicializada. Isto pode demorar algum tempo.

6. O pedido de Select Licensing Mode (Modo de seleção de licenciamento) abre. Selecione o modo de licenciamento que a sua implementação utiliza. O modo de licenciamento é determinado durante a compra. **Não introduza um valor até que tenha verificado qual é o modo de licenciamento que a sua implementação utiliza.** Contacte o seu representante da ForeScout para verificar o seu modo de licenciamento ou se introduziu o modo errado.
7. No pedido Enter Machine Description (Introduzir descrição da máquina), introduza um breve texto que identifique este dispositivo e prima **Enter**.

O seguinte é apresentado:

```
>>>>> Set Administrator Password (Definir palavra-passe de
administrador)<<<<<<
This password will be used to log in as 'root' to the machine
Operating System and as 'admin' to the CounterACT Console. (Esta
palavra-passe vai ser utilizada para iniciar sessão como "raiz"
no Sistema operativo da máquina e como "admin" à Consola
CounterACT.)
The password must be between 6 and 15 characters long and should
contain at least one non-alphabetic character. (A palavra-passe
deve ter entre 6 e 15 caracteres e conter pelo menos um caracter
não alfabético.)
Administrator password (Palavra-passe de administrador):
```

8. No pedido de Set Administrator Password (Definir palavra-passe de administrador), escreva a cadeia que pretende como palavra-passe (a cadeia não é apresentada no ecrã) e pressione **Enter**. É-lhe pedido que confirme a palavra-passe. A palavra-passe deve ter entre 6 e 15 caracteres e conter pelo menos um caracter não alfabético.

 *Inicie sessão no aparelho como "raiz" e inicie sessão na Consola como "admin".*

9. No pedido Set Host Name (Definir nome de anfitrião), escreva um nome de anfitrião e prima **Enter**. O nome de anfitrião pode ser utilizado ao iniciar sessão na Consola e é apresentado na Consola para o ajudar a identificar o aparelho CounterACT que está a visualizar. O nome de anfitrião não deve ultrapassar 13 caracteres.
10. O ecrã Configure Network Settings (Configurar definições de rede) pede-lhe diversos parâmetros de configuração. Escreva um valor em cada pedido e pressione **Enter** para apresentar o pedido seguinte.
 - Os componentes do CounterACT comunicam através de interfaces de gestão. O número de interfaces de gestão listados depende do modelo do Aparelho.
 - O **Management IP address** (Endereço IP de gestão) é o endereço da interface através do qual os componentes do CounterACT comunicam. Apenas deve adicionar uma VLAN ID para esta interface, se a interface utilizada para comunicar entre os componentes CounterACT estiver ligada a uma porta com marcações.

- Se existir mais de um **DNS server address** (Endereço de servidor DNS), separe cada endereço com um espaço. A maioria dos servidores DNS resolve os endereços externos e internos, mas pode ser necessário incluir um servidor DNS para resolução de endereços externos. Dado que quase todas as consultas de DNS efetuadas pelo aparelho vão ser para endereços internos, o servidor DNS externo deve ser o último listado.

11. O ecrã de Setup Summary (Resumo de configuração) é apresentado. É-lhe pedido que efetue testes de conectividade gerais, reconfigure as definições ou conclua a configuração. Escreva **D** para concluir a configuração.

Licença

Após a configuração, certifique-se que o dispositivo CounterACT possui uma licença válida. O estado de licenciamento predefinido do seu dispositivo CounterACT depende do modo de licenciamento que a sua implementação utiliza.

- Se a sua implementação CounterACT estiver a funcionar em **Per-Appliance Licensing Mode** (Modo de licenciamento por aparelho), pode começar a trabalhar utilizando a licença de demonstração, que é válida por 30 dias. Durante este período, deve receber uma licença permanente da ForeScout e colocá-la numa pasta acessível no seu disco ou rede. Instale a licença para esta localização antes da licença de demonstração de 30 dias expirar (se necessário, pode solicitar uma extensão da licença de demonstração).

Vai ser alertado de diversas formas quando a sua licença de demonstração estiver perto de expirar. Consulte o *Guia de administração CounterACT* para obter mais informações sobre alertas de licenças de demonstração.

Se estiver a trabalhar com um sistema virtual CounterACT:

- A licença de demonstração não é instalada automaticamente nesta fase. Deve instalar a licença de demonstração que recebeu do seu representante ForeScout por e-mail.
- Pelo menos um dispositivo CounterACT deve ter capacidade para aceder à Internet. Esta ligação é utilizada para validar as licenças CounterACT no servidor de Licenças da ForeScout. As licenças que não for possível autenticar durante um mês vão ser revogadas. A CounterACT vai enviar um e-mail de aviso, uma vez por dia, caso ocorra um erro de comunicação com o servidor.

Consulte o *Guia de instalação CounterACT* para obter mais informações.

- Se a sua implementação CounterACT estiver a operar em **Centralized Licensing Mode** (Modo de licenciamento centralizado), o *Administrador de elegibilidade* deve receber um e-mail quando a elegibilidade da licença for criada e estiver disponível no ForeScout Customer Portal (Portal do cliente ForeScout). Uma vez disponível, o *administrador CounterACT* da implementação pode ativar a licença na Consola CounterACT. Até a licença estar ativada, as funcionalidades do CounterACT não vão funcionar corretamente. Por exemplo, as políticas não vão ser avaliadas e as ações não vão ser realizadas. *Nenhuma licença de demonstração é automaticamente instalada durante a instalação do sistema.*

Consulte o *Guia de administração CounterACT* para obter mais informações sobre gestão de licenças.

5. Gestão remota

Configuração iDRAC

O Controlador de acesso remoto Dell integrado (iDRAC) é uma solução de sistema de servidor integrado que lhe dá acesso remoto independente de localização/independente de SO através de LAN ou Internet aos aparelhos CounterACT. Utilize o módulo para efetuar o acesso KVM, para ligar/desligar/reiniciar e realizar tarefas de manutenção e resolução de problemas.

Realize o seguinte para trabalhar com o módulo iDRAC:

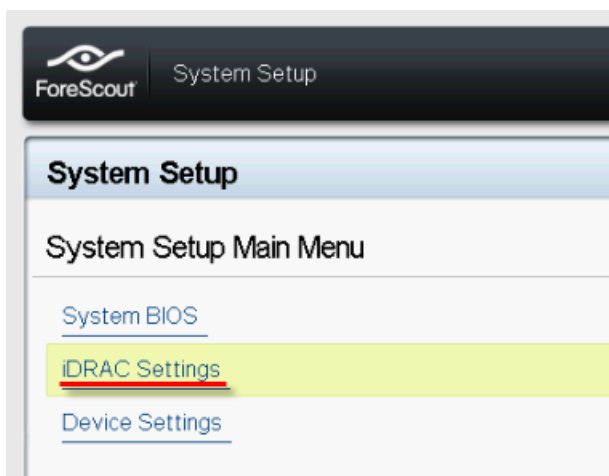
- [Ativar e configurar o módulo iDRAC](#)
- [Ligar o módulo à rede](#)
- [Iniciar sessão no iDRAC](#)

Ativar e configurar o módulo iDRAC

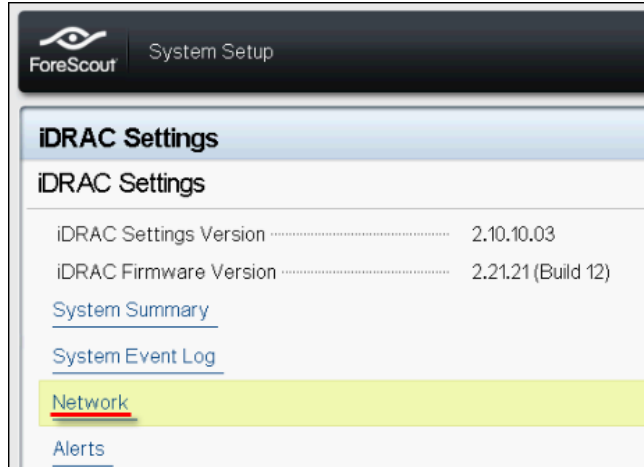
Altere as definições iDRAC para ativar o acesso remoto no dispositivo CounterACT. Esta secção descreve as definições de integração básica necessárias para trabalhar com o CounterACT.

Para configurar o iDRAC:

1. Ligue o aparelho gerido.
2. Selecione F2 durante o processo de arranque.
3. Na página de System Setup Main Menu (Menu principal de configuração de sistema), selecione **iDRAC Settings** (Definições iDRAC).

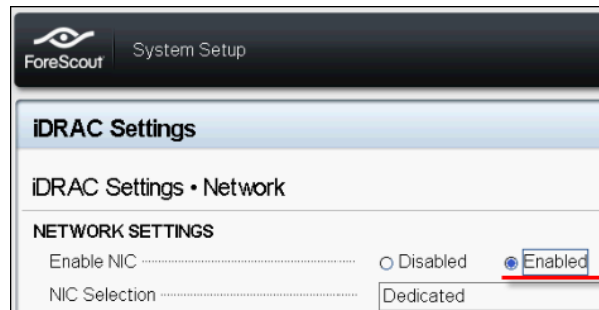


4. Na página de iDRAC Settings (Definições iDRAC), selecione **Network** (Rede).



5. Configure as definições de Rede que se seguem:

- **Network Settings** (Definições de rede). Verifique que o campo **Enable NIC** (Ativar NIC) está definido para **Enabled** (Ativado).



- **Common Settings** (Definições comuns). No campo de DNS DRAC Name (Nome DNS DRAC), pode atualizar um DNS dinâmico (Opcional).
- **IPv4 Settings** (Definições IPV4). Verifique que o campo **Enable IPv4** (Ativar Ipv4) está definido para **Enabled** (Ativado).

Defina o campo **Enable DHCP** (Ativar DHCP) para **Enabled** (Ativado) para utilizar o Endereçamento IP dinâmico ou para **Disabled** (Desativado) para utilizar o Endereçamento IP estático. Se ativado, o DHCP vai atribuir automaticamente o endereço IP, gateway e máscara de sub-rede ao iDRAC. Se desativado, introduza valores para os campos **Static IP Address** (Endereço IP estático), **Static Gateway** (Gateway estático) e **Static Subnet Mask** (Máscara de sub-rede estática).

The screenshot shows the 'iDRAC Settings' page in the ForeScout System Setup. The sub-section is 'iDRAC Settings • Network'. Under 'IPV4 SETTINGS', the following options are visible:

- Enable IPv4: Disabled, Enabled
- Enable DHCP: Disabled, Enabled
- Static IP Address: 192.168.1.103
- Static Gateway: 192.168.1.1
- Static Subnet Mask: 255.255.255.0
- Use DHCP to obtain DNS server addresses: Disabled, Enabled
- Static Preferred DNS Server: 192.168.1.2
- Static Alternate DNS Server: 0.0.0.0

6. Selecione **Back** (Anterior).
7. Selecione **User Configuration** (Configuração de utilizador).
8. Configure os seguintes campos de User Configuration (Configuração de utilizador) para o utilizador "raiz":
 - **Enable User** (Ativar utilizador). Verifique que este campo está definido para Enabled (Ativado).
 - *O nome de utilizador aqui configurado não é o mesmo que o nome de utilizador CounterACT.*
 - **LAN and Serial Port User Privileges** (Privilégios de utilizador de porta de série e LAN). Defina o nível de privilégios para Administrator (Administrador).
 - **Change Password** (Alterar palavra-passe). Defina uma palavra-passe para o início de sessão do utilizador.

The screenshot shows the 'iDRAC Settings' page in the ForeScout System Setup. The sub-section is 'iDRAC Settings • User Configuration'. The following fields are visible:

- User ID: 2
- Enable User: Disabled, Enabled
- User Name: root
- LAN User Privilege: Administrator
- Serial Port User Privilege: Administrator
- Change Password: (empty field)

9. Selecione **Back** (Anterior) e, em seguida, selecione **Finish** (Concluir). Confirme para alterar as definições.

As definições configuradas são guardadas e o sistema reinicia.

Ligar o módulo à rede

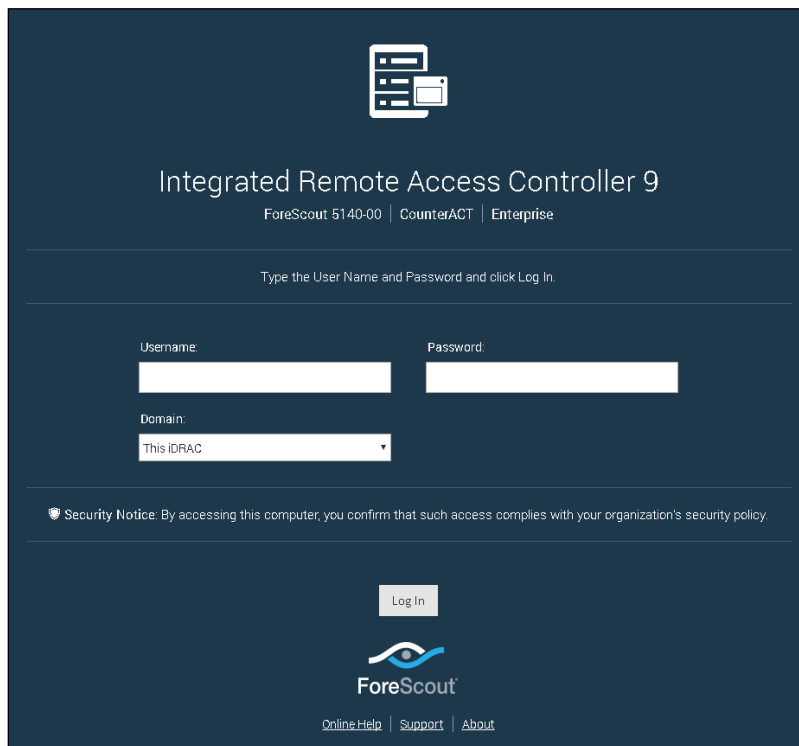
O iDRAC liga-se a uma rede de Ethernet. O normal é ser ligado a uma rede de gestão. A imagem que se segue mostra a localização da porta do iDRAC no painel traseiro do aparelho CT-1000:



Iniciar sessão no iDRAC

Para iniciar sessão no iDRAC:

1. Navegue até ao endereço IP ou nome de domínio configurado em **iDRAC Settings** (Definições iDRAC) > **Network** (Rede).

A screenshot of the login page for the Integrated Remote Access Controller 9. The page has a dark blue background. At the top center is a white icon of a server rack. Below it, the text reads 'Integrated Remote Access Controller 9' followed by 'ForeScout 5140-00 | CounterACT | Enterprise'. A line of text says 'Type the User Name and Password and click Log In.' Below this are two input fields for 'Username' and 'Password'. Underneath the 'Username' field is a 'Domain:' label and a dropdown menu currently showing 'This iDRAC'. At the bottom of the form area is a 'Log In' button. Below the button is the ForeScout logo and the text 'ForeScout'. At the very bottom, there are links for 'Online Help', 'Support', and 'About'. A security notice is visible above the 'Log In' button: 'Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.'

2. Introduza o Username (Nome de utilizador) e a Password (Palavra-passe) configurados na página de User Configuration (Configuração de utilizador) da configuração do sistema iDRAC.
3. Selecione **Submit** (Submeter).

Para obter mais informações sobre o iDRAC, consulte o *Guia do utilizador iDRAC*. Pode aceder a este guia numa das seguintes localizações, dependendo do modo de licenciamento que a sua implementação utiliza:

- Modo de licenciamento por aparelho - https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf
- Modo de licenciamento centralizado – [Portal do cliente](#), página de documentação.

Consulte [Documentação CounterACT adicional](#) (*Identificar o seu modo de licenciamento na consola*) para descobrir qual o modo de licenciamento que a sua implementação utiliza.

- 📄 *É muito importante atualizar a palavra-passe de "raiz" predefinida, caso ainda não o tenha feito.*

6. Verificar conectividade

Verificar a ligação da interface de gestão

Para testar a ligação da interface de gestão, inicie sessão no aparelho e execute o comando que se segue:

```
fstool linktest
```

É apresentada a seguinte informação:

```
Management Interface status (Estado da interface de gestão)
Pinging default gateway information (Informações de ping do
gateway predefinido)
Ping statistics (Estatísticas de ping)
Performing Name Resolution Test (Efetuar teste de resolução de
nome)
Test summary (Resumo de teste)
```

Efetuar um teste de ping

Execute o comando que segue a partir do aparelho para um ambiente de trabalho da rede para verificar a conectividade:

```
Ping <endereço_IP_ambiente_de_trabalho_de_rede>
```

7. Configurar a Consola CounterACT

Instalar a Consola CounterACT

A Consola é a aplicação de gestão CounterACT que é utilizada para visualizar importantes informações detalhadas sobre os nós terminais e controlá-los. Estas informações são recolhidas pelos dispositivos CounterACT. Consulte o *Guia de administração CounterACT* para obter mais informações.

Deve providenciar uma máquina para hospedar o software da aplicação da Consola CounterACT. Os requisitos de hardware mínimos são:

- Máquina não dedicada, a executar:
 - Windows 7/8/8.1/10
 - Windows Server 2008/2008 R2/2012/2012 R2/2016
 - Linux RHEL/CentOS 7
- 2 GB RAM
- 1 GB de espaço em disco

O método que se segue encontra-se disponível para efetuar a instalação da Consola:

Utilize o software de instalação integrado no seu Aparelho.

1. Abra uma janela do navegador a partir do computador da Consola.

2. Escreva o seguinte na linha de endereço do navegador:

```
http://<Ip_aparelho>/install
```


Onde Ip_aparelho é o endereço IP deste Aparelho. O navegador apresenta a janela de instalação da Consola.

3. Siga as instruções no ecrã.

Iniciar sessão

Após concluir a instalação, pode iniciar sessão na Consola CounterACT.

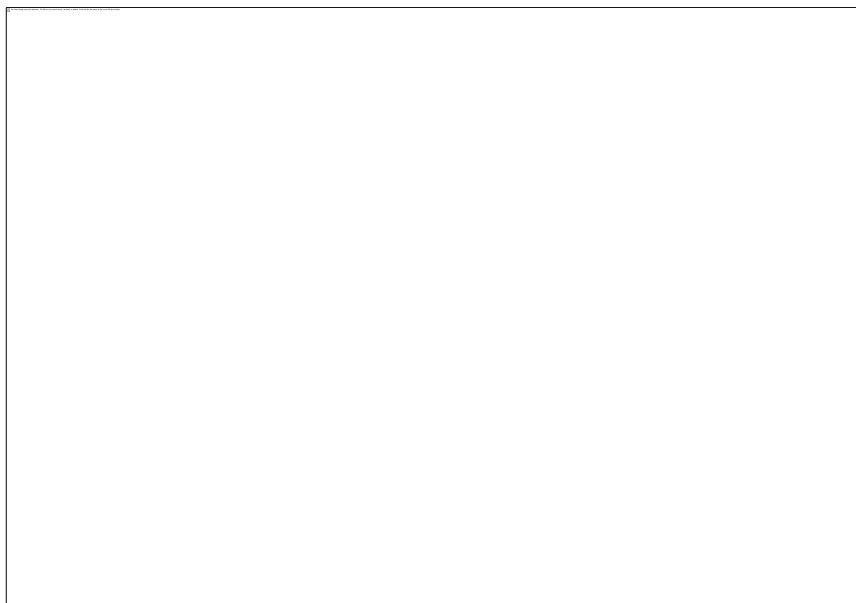
1. Selecione o ícone CounterACT a partir da localização do atalho que criou.



2. Introduza o endereço de IP ou nome de anfitrião do aparelho no campo **IP/Name** (IP/Nome).
3. No campo **User Name** (Nome de utilizador), introduza admin.
4. No campo **Password** (Palavra-passe), introduza a palavra-passe que criou durante a instalação do aparelho.
5. Selecione **Login** (Iniciar sessão) para iniciar a Consola.

Efetuar configuração inicial

Quando inicia sessão pela primeira vez, o Initial Setup Wizard (Assistente de configuração inicial) abre. O Assistente vai guiá-lo através dos passos de configuração essenciais para colocar o CounterACT em funcionamento de forma rápida e eficiente.



Antes de iniciar a configuração inicial

Prepare as informações que se seguem antes de trabalhar com o Assistente:

Informação necessária para o Assistente	Valor
Endereço do servidor NTP utilizado pela sua organização (opcional)	
Endereços IP de encaminhamento de correio interno que permitem a entrega de alertas de e-mail caso o tráfego SMTP não for permitido a partir do Aparelho (opcional)	
Endereços de e-mail do administrador CounterACT	
Interfaces de resposta e de monitorização	
Em caso de VLAN/segmentos sem DHCP, o VLAN/segmento de rede ao qual a interface de resposta é ligada diretamente e um endereço IP para ser utilizado pelo CounterACT em cada um destes VLAN	
Intervalo de endereço IP que este Aparelho vai monitorizar (todos os endereços internos, incluindo endereços não utilizados)	
Informações de conta de utilizador LDAP e o endereço IP do servidor LDAP	
Credenciais de domínio, incluindo a palavra-passe e o nome da conta administrativa do domínio	
Servidores de autenticação, para que o CounterACT possa analisar qual o anfitrião de rede que foi autenticado com sucesso	
Computador de endereço IP, vendedor e parâmetros SNMP	

Consulte o *Guia de administração CounterACT* ou a ajuda online para obter mais informações sobre como trabalhar com o assistente.

Documentação CounterACT adicional


Para informações sobre outras funcionalidades e módulos CounterACT, consulte os recursos que se seguem:

- [Transferência de documentação](#)
- [Portal de documentação](#)
- [Ferramentas de ajuda CounterACT](#)

Transferência de documentação

A transferência de documentação pode ser acessada a partir de um de dois portais ForeScout, dependendo do modo de licenciamento que a sua implementação está a utilizar.

- **Modo de licenciamento por aparelho** - [Portal de atualizações de produto](#)
- **Modo de licenciamento centralizado** - [Portal do cliente](#)

 *As transferências de software também estão disponíveis a partir destes portais.*

Para aprender que modo de licenciamento a sua implementação está a utilizar, consulte [Identificar o seu modo de licenciamento na consola](#).

Portal de atualizações de produto

O Product Updates Portal (Portal de atualizações de produto) proporciona ligações para módulos alargados, módulos de conteúdo e de base e lançamento de versões CounterACT, assim como documentação relacionada. O portal também proporciona diversas documentações adicionais.

Para aceder ao Product Updates Portal (Portal de atualizações de produto):

1. Aceda a <https://updates.forescout.com/support/index.php?url=counteract>.
2. Selecione a versão CounterACT que pretende descobrir.

Portal do cliente

A página Downloads (Transferências) no ForeScout Customer Portal (Portal de cliente ForeScout) proporciona ligações para módulos alargados, módulos de conteúdo e de base e lançamento de versões CounterACT, assim como documentação relacionada. O software e a documentação relacionada vão apenas aparecer na página Downloads (Transferências) se possuir uma licença elegível para o software. A página Documentation (Documentação) no portal proporciona diversa documentação adicional.

Para aceder a documentação no ForeScout Customer Portal (Portal de cliente ForeScout):

1. Aceda a <https://forescout.force.com/support/>.
2. Selecione **Downloads** (Transferências) ou **Documentation** (Documentação).

Portal de documentação

O ForeScout Documentation Portal (Portal de documentação ForeScout) é uma biblioteca baseada em web, pesquisável e que contém informações sobre as ferramentas CounterACT, funcionalidades, características e integrações.

- 📖 *Se a sua implementação estiver a utilizar o Modo de licenciamento centralizado, pode não possuir credenciais para aceder a este portal.*

Para aceder ao Documentation Portal (Portal de documentação):

1. Aceda a www.forescout.com/docportal.
2. Utilize as credenciais de apoio ao cliente para iniciar sessão.
3. Selecione a versão CounterACT que pretende descobrir.

Ferramentas de ajuda CounterACT

Aceda a informações diretamente da Consola CounterACT.

Botões de ajuda da consola

Utilize botões de *Ajuda* sensíveis ao contexto para rapidamente aceder a informação sobre as tarefas e tópicos com os quais está a trabalhar.

Guia de administração CounterACT

Selecione **CounterACT Help** (Ajuda CounterACT) a partir do menu **Help** (Ajuda).

Ficheiros de ajuda do plugin

1. Após o plugin ser instalado, selecione **Options** (Opções) a partir do menu **Tools** (Ferramentas) e, em seguida, selecione **Modules** (Módulos).
2. Selecione o plugin e, em seguida, selecione **Help** (Ajuda).

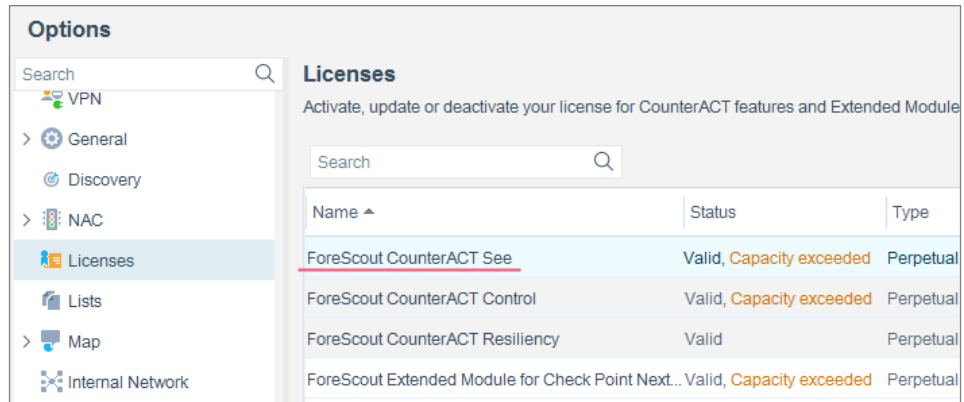
Portal de documentação

Selecione **Documentation Portal** (Portal de documentação) a partir do menu **Help** (Ajuda).

Identificar o seu modo de licenciamento na consola

Se o seu Enterprise Manager possuir uma licença *ForeScout CounterACT See* listada na Consola, a sua implementação está a operar no Centralized Licensing Mode (Modo de licenciamento centralizado). Caso contrário, a sua implementação está a operar em Per-Appliance Licensing Mode (Modo de licenciamento por aparelho).

Selecione **Options** (Opções) > **Licenses** (Licenças) para ver as licenças *ForeScout CounterACT See* listadas na tabela.



Options

Search

- VPN
- General
- Discovery
- NAC
- Licenses**
- Lists
- Map
- Internal Network

Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Search

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contacte o seu representante ForeScout se tiver quaisquer questões sobre como identificar o seu modo de licenciamento.

Aviso legal

Copyright © ForeScout Technologies, Inc. 2000-2018. Todos os direitos reservados. ForeScout, o logotipo ForeScout, ActiveResponse, ControlFabric, CounterACT, CounterACT Edge e SecureConnector são marcas comerciais ou registadas da ForeScout. É estritamente proibido copiar, duplicar, vender, emprestar ou de outra forma utilizar este documento sob qualquer forma ou formato sem o consentimento prévio por escrito da ForeScout. Quaisquer outras marcas comerciais utilizadas neste documento são propriedade dos respetivos proprietários.

Estes produtos são baseados em software desenvolvido pela ForeScout. Os produtos descritos neste documento podem estar protegidos por uma ou mais das patentes dos EUA que se seguem: #6.363.489, #8.254.286, #8.590.004, #8.639.800 e #9.027.079 e podem estar protegidas por outras patentes dos EUA e patentes estrangeiras.

Envie comentários e questões relacionados com este documento para: support@forescout.com

2018-03-27 15:03