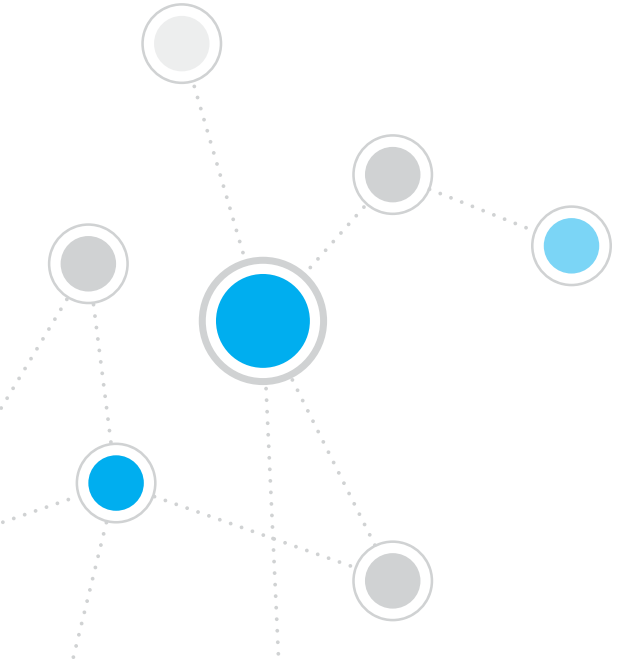
ForeScout

ForeScout CounterACT® 7

Dispositivo CounterACT Único

Guia de Instalação Rápida



Sumário

Bem-vindo ao ForeScout CounterACT® Versão 7

O ForeScout CounterACT é um dispositivo de segurança físico ou virtual que identifica e avalia de forma dinâmina dispositivos e aplicativos de rede no momento em que se conectam à sua rede. Como o CounterACT não precisa de agentes, funciona com todos os seus dispositivos—gerenciados e não gerenciados, conhecidos e desconhecidos, desktop ou móveis, integrados e virtuais. O CounterACT determina rapidamente o usuário, o proprietário, o sistema operacional, a configuração do dispositivo, o software, os serviços, o estado do patch e a presença de agentes de segurança. Em seguida, ele corrige, controla e monitora de forma contínua esses dispositivos à medida que entram e saem da rede. Além do mais, faz tudo isso sem deixar de se integrar facilmente à sua infraestrutura de TI existente.

Este guia descreve a instalação de um Dispositivo CounterACT único e autônomo.

Para obter informações mais detalhadas ou informações sobre como implantar diversos Dispositivos para a proteção de rede em nível empresarial, consulte o *Guia de Instalação do CounterACT* e o *Manual do Usuário do Console*. Esses documentos estão localizados no CD CounterACT no diretório /docs.

Além disso, você pode navegar até o site de suporte, localizado em: http://www.forescout.com/support para obter a última documentação, artigos da base de conhecimento e atualizações para seu Dispositivo.

Incluído no Pacote CounterACT

- Dispositivo CounterACT
- Guia de Instalação Rápida
- CD CounterACT com software do Console, Manual do Usuário e Guia de Instalação do Console do CounterACT
- Documento de garantia
- Suportes de montagem
- Cabo de alimentação
- Cabo de conexão do console DB9 (somente para conexões seriais)

Visão Geral

Execute os passos a seguir para configurar o CounterACT:

1. Criar um Plano de Implantação
2. Configurar seu Comutador
3. Conectar Cabos de Rede e Ligar
4. Configurar o Dispositivo
5. Gerenciamento Remoto
6. Verificar Conectividade
7. Configurar o Console do CounterACT

1. Criar um Plano de Implantação

Antes de realizar a instalação, é necessário decidir onde implantar o Dispositivo e aprender sobre as conexões da interface do Dispositivo.

Decidir onde Implantar o Dispositivo

Selecionar o local de rede correto para o Dispositivo é fundamental para uma implantação bem-sucedida e para o desempenho ideal do CounterACT. A localização correta depende das metas de implementação desejadas e das políticas de acesso à rede. O Dispositivo deve ser capaz de monitorar o tráfego que seja relevante para a política desejada. Por exemplo, caso sua política dependa do monitoramento dos eventos de autorização de pontos de extremidade para os servidores de autenticação corporativos, o Dispositivo precisará ser instalado de forma que enxergue o fluxo de tráfego do ponto de extremidade para os servidores de autenticação.

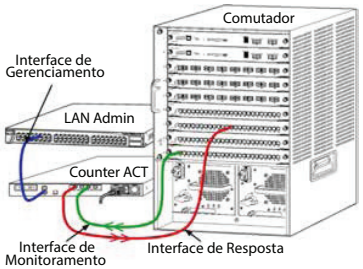
Para obter informações sobre instalação e implantação, consulte o Guia de Instalação do CounterACT, localizado no CD do CounterACT que você recebeu com este pacote.

Conexões da Interface do Dispositivo

Geralmente, o Dispositivo é configurado com três conexões ao comutador de rede.

Interface de Gerenciamento

Essa interface permite que você gerencie o CounterACT e realize consultas e inspeções profundas dos pontos de extremidade. A interface deve ser conectada à porta do comutador que tenha acesso a todos os pontos de extremidade da rede.



Cada Dispositivo requer uma única conexão de gerenciamento à rede. Essa conexão requer um endereço IP na LAN local e acesso à porta 13000/TCP das máquinas que executarão o aplicativo de gerenciamento do Console do CounterACT. A interface de gerenciamento deve ter acesso aos seguintes itens da sua rede:

Porta	Serviço	De ou Para o CounterACT	Função
22/TCP	SSH	Para	Permite acesso à interface da linha de comando do CounterACT.
2222/TCP			(Alta Disponibilidade) Permite acesso aos dispositivos físicos do CounterACT que façam parte do cluster de Alta Disponibilidade. Use a 22/TCP para acessar o endereço IP compartilhado (virtual) do cluster.

Porta	Serviço	De ou Para o CounterACT	Função
25/TCP	SMTP	De	Usado para enviar e-mail do CounterACT
53/UDP	DNS	De	Permite que o CounterACT resolva endereços IPs internos.
80/TCP	HTTP	Para	Permite o redirecionamento HTTP.
123/UDP	NTP	De	Permite o acesso do CounterACT a um servidor de tempo NTP. Por padrão, o CounterACT usa ntp.foreScout.net.
135/TCP	MS-WMI	De	Permite a inspeção remota dos pontos de extremidade do Windows.
139/TCP	SMB, MS-RPP	De	Permite a inspeção remota dos pontos de extremidade do Windows (Para pontos de extremidade sendo executados no Windows 7 e em versões anteriores).
445/TCP			Permite a inspeção remota dos pontos de extremidade do Windows.
161/UDP	SNMP	De	Permite que o CounterACT comunique-se com equipamentos de infraestrutura de rede, como comutadores e roteadores. Para obter informações sobre como configurar o SNMP, consulte o *Manual do Usuário do Console do CounterACT.*
162/UDP	SNMP	Para	Permite que o CounterACT receba interceptações SNMP de equipamentos de infraestrutura de rede, como comutadores e roteadores. Para obter informações sobre como configurar o SNMP, consulte o *Manual do Usuário do Console do CounterACT.*
443/TCP	HTTPS	Para	Permite o redirecionamento HTTP usando TLS.
2200/TCP	Secure Connector	Para	Permite que o SecureConnector crie uma conexão segura (criptografada por SSH) ao Dispositivo a partir de máquinas Macintosh/Linux. O *SecureConnector* é um agente baseado em script que permite o gerenciamento de pontos de extremidade dos sistemas Macintosh e Linux enquanto estiverem conectados à rede.
10003/TCP	Secure Connector para Windows	Para	Permite que o SecureConnector crie uma conexão segura (criptografada por TLS) ao Dispositivo a partir de máquinas Windows. O *SecureConnector* é um agente que permite o gerenciamento de pontos de extremidade do Windows enquanto estiverem conectados à rede. Consulte o *Manual do Usuário do Console do CounterACT* para obter mais informações sobre o SecureConnector.

			Quando o SecureConnector se conecta a um Dispositivo ou ao Enterprise Manager, ele é redirecionado ao Dispositivo para o qual seu host é atribuído. Verifique se essa porta está aberta para todos os Dispositivos e para o Enterprise Manager para permitir uma mobilidade transparente dentro da organização.
13000/TCP	CounterACT	Para	Permite a conexão entre o Console e o Dispositivo. Para sistemas com diversos Dispositivos CounterACT, permite a conexão entre o Console e o Enterprise Manager e entre o Enterprise Manager e cada Dispositivo.

Interface de Monitoramento

Essa conexão permite que o Dispositivo monitore e rastreie o tráfego de rede.

O tráfego é espelhado para uma porta no comutador e monitorado pelo Dispositivo. Dependendo do número de VLANs que estiverem sendo espelhadas, o tráfego pode ou não ser marcado como VLAN 802.1Q.

- **VLAN única (não marcada):** Quando o tráfego monitorado é gerado de uma única VLAN, o tráfego espelhado não precisa ser marcado como VLAN.
- **VLANs múltiplas (marcadas):** Quando o tráfego monitorado é de mais de uma VLAN, o tráfego espelhado *deve* ser marcado como VLAN 802.1Q.

Quando dois comutadores forem conectados como um par redundante, o Dispositivo deve monitorar o tráfego de ambos os comutadores.

Não é necessário endereço IP na interface de monitoramento.

Interface de Resposta

O Dispositivo responde ao tráfego usando essa interface. O tráfego de resposta é usado para proteger contra atividade maliciosa e realizar ações de política de NAC. Essas ações podem incluir, por exemplo, o redirecionamento de navegadores da Web ou execução de bloqueio de firewall. A configuração da porta do comutador relacionada depende do tráfego monitorado.

- **VLAN única (não marcada):** Quando o tráfego monitorado é gerado de uma única VLAN, a interface de resposta deve ser configurada para que faça parte da mesma VLAN. Nesse caso, o Dispositivo exige um único endereço IP nessa VLAN.
- **VLANs múltiplas (marcadas):** Se o tráfego monitorado for de mais de uma VLAN, a interface de resposta também deve ser configurada com a marcação de 802.1Q para essas VLANs. O Dispositivo requer um endereço IP para cada VLAN protegida.

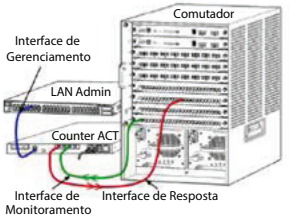
2. Configurar Seu Comutador

A. Opções de Conexão do Comutador

O Dispositivo foi projetado para integrar-se de maneira ininterrupta com uma grande variedade de ambientes de rede. Para uma integração bem-sucedida do Dispositivo com sua rede, verifique se seu comutador está configurado para monitorar o tráfego necessário.

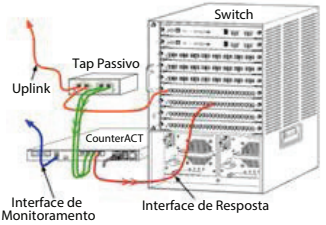
Diversas opções estão disponíveis para conectar o Dispositivo ao seu comutador.

1. **Implantação Padrão (Interfaces Separadas de Gerenciamento, Monitoramento e Resposta)**
   A implantação recomendada usa três portas separadas. Essas portas são descritas em *Conexões da Interface do Dispositivo*.

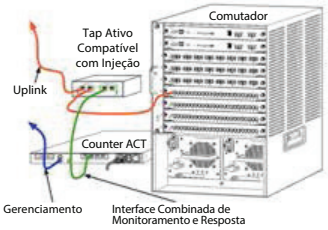


2. **Tap Passivo Embutido**
   Em vez de conectar-se a uma porta de monitoramento de comutador, o Dispositivo pode usar um tap passivo embutido.

   Um tap passivo requer duas portas de monitoramento, exceto no caso de taps de "recombinação", que combinam dois fluxos duplex em uma única porta. O tráfego na porta derivada e o tráfego na interface de resposta devem ser configurados da mesma forma. Por exemplo, se o tráfego na porta derivada for marcado como VLAN (802.1Q), a interface de resposta também deverá ser uma porta marcada como VLAN.



3. **Tap Ativo Embutido (Compatível com Injeção)**
   Quando o Dispositivo usa um tap embutido que seja *compatível com injeção*, as interfaces de monitoramento e de resposta podem ser combinadas. Não há necessidade de configurar uma porta de resposta separada no comutador. Essa opção pode ser usada para qualquer tipo de configuração de comutador upstream ou downstream.



4. **Resposta de Camada IP (para Instalações de Comutadores com Camada 3)**
   O Dispositivo pode usar sua própria interface de gerenciamento para responder ao tráfego. Embora essa opção possa ser usada com qualquer tráfego monitorado, é recomendada para quando o Dispositivo monitora portas que não façam parte de qualquer VLAN, e portanto o Dispositivo não pode responder ao tráfego monitorado usando qualquer outra porta do comutador. Isso é normal ao monitorar um link que conecta dois roteadores.

   Essa opção não pode responder a solicitações de ARP (Protocolo de Resolução de Endereço), o que limita a capacidade do Dispositivo de detectar varreduras focadas nos endereços IP incluídos na sub-rede monitorada. Essa limitação não se aplica quando o tráfego entre dois roteadores estiver sendo monitorado.

B. Observações sobre Configuração do Comutador

Marcações VLAN (802.1Q)

- **Monitoramento de uma Única VLAN (tráfego não marcado)** Se o tráfego monitorado é de uma única VLAN, o tráfego não precisa de marcações 802.1Q.
- **Monitoramento de VLANs Múltiplas (tráfego marcado)** Se o tráfego monitorado é de duas ou mais VLANs, as *duas* interfaces, de monitoramento e de resposta, devem ter a marcação 802.1Q habilitada. Monitorar diversas VLANs é a recomendada opção, pois fornece a melhor cobertura geral, ao mesmo tempo em que minimiza o número de portas espelhadas.
- Se o comutador não puder usar uma marcação VLAN 802.1Q nas portas espelhadas, faça uma das seguintes opções:
  - Espelhe somente uma VLAN
  - Espelhe uma única porta de uplink não marcada
  - Use a opção de resposta da camada IP
- Se o comutador puder espelhar somente uma porta, espelhe uma única porta de uplink. O espelhamento pode ser marcado. Em geral, se o comutador remover as marcações VLAN 802.1Q, será necessário usar a opção de resposta da Camada IP

Adicional

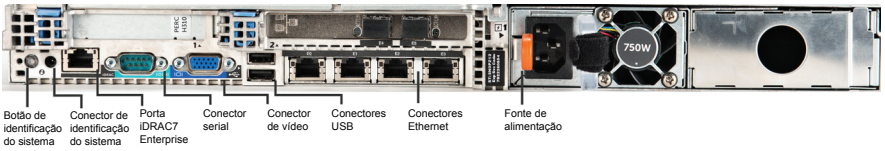
- Se o comutador não puder espelhar o tráfego de transmissão e recepção, monitore o comutador inteiro, as VLANs completas (isso fornece transmissão/recepção) ou apenas uma interface (o que permite a transmissão/recepção). Cuidado para não sobrecarregar a porta espelhada.
- Alguns comutadores (como o Cisco 6509) podem precisar que as configurações de porta anteriores sejam completamente limpas antes de inserir novas configurações. O resultado mais comum quando as informações antigas de porta não são limpas é a remoção das marcações 802.1Q pelo comutador.

3. Conectar Cabos de Rede e Ligar

A. Desembalar o Dispositivo e Conectar os Cabos

1. Remova o Dispositivo e o cabo de alimentação do contêiner de remessa.
2. Remova o kit de montagem recebido com o Dispositivo.
3. Monte o kit de montagem no Dispositivo e monte o Dispositivo no rack.
4. Conecte os cabos de rede entre as interfaces de rede no painel traseiro do Dispositivo e nas portas do comutador.

Exemplo de Painel Traseiro — Dispositivo CounterACT



B. Registrar as Atribuições da Interface

Depois de concluir a instalação do Dispositivo no data center e instalar o Console do CounterACT, será pedido que você registre as atribuições da interface. Essas atribuições, chamadas de *Channel definitions* (Definições de canal), são inseridas no Initial Setup Wizard (Assistente de Configuração Inicial) que é aberto quando você faz login pela primeira vez no Console.

Registre as atribuições da interface física abaixo e use-as ao concluir a configuração do Canal no Console.

Interface Ethernet	Atribuição de Interface (por exemplo, Gerenciamento, Monitoramento, Resposta)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. Ligar o Dispositivo

1. Conecte o cabo de alimentação ao conector de alimentação no painel traseiro do Dispositivo.
2. Conecte a outra extremidade do cabo de alimentação a uma tomada com aterramento CA.
3. Conecte o teclado e o monitor ao Dispositivo ou configure o Dispositivo para conexão serial. Consulte o *Guia de Instalação do CounterACT,* localizado no CD do CounterACT.
4. Ligue o Dispositivo no painel frontal.

Importante: Desligue a máquina antes de desconectá-la.

4. Configurar o Dispositivo

Prepare as informações a seguir antes de configurar o Dispositivo.

☐ Nome do host do Dispositivo	
☐ Senha de Administrador do CounterACT	**Mantenha a senha em um local seguro**
☐ Interface de gerenciamento	
☐ Endereço IP do Dispositivo	
☐ Máscara de rede	
☐ Endereço IP padrão do Gateway	
☐ Nome do Domínio DNS	
☐ Endereço do servidor DNS	

Depois de ligar o dispositivo, será pedido que você inicie a configuração com a seguinte mensagem:

```
CounterACT Appliance boot is complete
  (A inicialização do Dispositivo CounterACT
  foi concluída).
Press <Enter> to continue (Pressione <Enter> para
  continuar).
```

1. Pressione **Enter** para exibir o seguinte menu:

```
1) Configure CounterACT (Configurar CounterACT)
2) Restore saved CounterACT configuration
   (Restaurar configuração salva do CounterACT)
3) Identify and renumber network interfaces
   (Identificar e renumerar interfaces de rede)
4) Configure keyboard layout (Configurar layout do
   teclado)
5) Turn machine off (Desligar máquina)
6) Reboot the machine (Reiniciar máquina)
Choice (1-6) :1 (Escolha [1-6]: 1)
```

2. Selecione **1** – Configure CounterACT (Configurar CounterACT). No prompt:
   `Continue: (yes/no) (Continuar [sim/não])?`
   Pressione **Enter** para iniciar a configuração.
3. O menu **`High Availability Mode`** (Modo de Alta Disponibilidade) é aberto. Pressione **Enter** para selecionar a Instalação Padrão.
4. O prompt **`CounterACT Initial Setup`** (Configuração Inicial do CounterACT) é exibido. Pressione **Enter** para continuar.
5. O menu **`Select CounterACT Installation Type`** (Selecionar Tipo de Instalação do CounterACT) é aberto. Digite **1** e pressione **Enter** para instalar um Dispositivo CounterACT padrão.
   A configuração é inicializada. Isso pode demorar um pouco.

6. No prompt **`Enter Machine Description`** (Inserir Descrição da Máquina), digite um texto curto que identifique esse dispositivo e pressione **Enter**. A seguinte mensagem é exibida:

```
>>>>>> Set Administrator Password <<<<<<
(Definir Senha de Administrador)

This password is used to log in as 'root' to
the machine Operating System and as 'admin' to
the CounterACT Console (Esta senha é usada para
fazer login como "raiz" no Sistema Operacional
da máquina e como "administrador" no Console do
CounterACT).
The password should be between 6 and 15
characters long and should contain at least one
non-alphabetic character (A senha deve ter de
6 a 15 caracteres e pelo menos um caractere não
alfabético).

Administrator password(Senha de Administrador):
```

7. No prompt **`Set Administrator Password`** (Definir Senha de Administrador), digite a sequência que será sua senha (a sequência não aparece na tela) e pressione **Enter**. É pedido que você confirme a senha. A senha deve ter de 6 a 15 caracteres e pelo menos um caractere não alfabético).

   Faça login no Dispositivo como raiz e faça login no Console como administrador.

8. No prompt **`Set Host Name`** (Definir Nome do Host), digite um nome de host e pressione **Enter**. O nome de host pode ser usado ao fazer login no Console e é exibido no Console para ajudar a identificar o Dispositivo CounterACT que você está visualizando.
9. A tela **`Configure Network Settings`** (Definir Configurações de Rede) pede uma série de parâmetros de configuração. Digite um valor em cada prompt e pressione **Enter** para avançar.
   - Os componentes do CounterACT se comunicam por meio das interfaces de gerenciamento. O número de interfaces de gerenciamento listadas depende do modelo do Dispositivo.
   - O **Management IP address** (Endereço IP de gerenciamento) é o endereço da interface por meio da qual os componentes do CounterACT se comunicam. Adicione um ID de VLAN para essa interface somente se a interface usada para comunicação entre os componentes do CounterACT estiver conectada a uma porta marcada.
   - Se houver mais de um **DNS server address** (Endereço de servidor DNS), separe cada endereço com um espaço — a maioria dos servidores DNS internos resolve endereços externos e internos, mas talvez seja necessário incluir um servidor DNS de resolução externa. Quase todas as consultas DNS realizadas pelo Dispositivo será para endereços internos, o servidor DNS externo deve ser listado por último.
10. A tela **`Setup Summary`** (Resumo de Configuração) é exibida. É pedido que você realize testes de conectividade gerais, redefina as configurações ou conclua a configuração. Digite **D** para concluir a configuração.

Licença

Depois da instalação, é preciso instalar a licença de demonstração inicial fornecida pelo representante do CounterACT. A licença é instalada durante a configuração inicial do Console. Essa licença de demonstração inicial é válida por determinado número de dias. É necessário instalar uma licença permanente antes do término desse período. Você será contatado por e-mail sobre a data de expiração. Além disso, as informações sobre a data de expiração e a licença de status é exibida no painel Appliances/Devices (Dispositivos) do Console.

Depois de receber uma licença permanente, a licença é validada diariamente pelo ForeScout License Server. Alertas e violações de licença são exibidas no painel Device Details (Detalhes do Dispositivo).

As licenças que não puderem ser validadas por um mês serão revogadas. Consulte o Guia de Instalação do CounterACT para obter mais detalhes sobre licenças.

Requisitos de Conexão de Rede

Pelo menos um dispositivo CounterACT (Appliance ou Enterprise Manager) deve ser capaz de acessar a Internet. Essa conexão é usada para validar as licenças do CounterACT no ForeScout License Server.

As licenças que não puderem ser autenticadas por um mês serão revogadas. O CounterACT enviará um e-mail de aviso diariamente indicando que há um erro de comunicação com o servidor.

5. Gerenciamento Remoto

Configuração do iDRAC

O iDRAC (Integrated Dell Remote Access Controller) é uma solução de sistema de servidor integrado que fornece acesso remoto independente do local/sistema operacional por meio da LAN ou da Internet aos Appliances/Enterprise Managers do CounterACT. Use o módulo para realizar acesso KVM, ligar/desligar/reiniciar e realizar tarefas de resolução de problemas e manutenção.

Realize as tarefas a seguir para trabalhar com o módulo iDRAC:

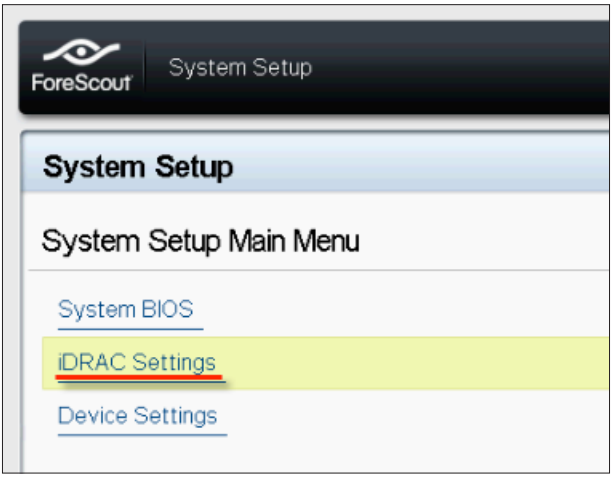
- *Ativar e Configurar o Módulo iDRAC*
- *Conectar o Módulo à Rede*
- *Login no iDRAC*

Ativar e Configurar o Módulo iDRAC

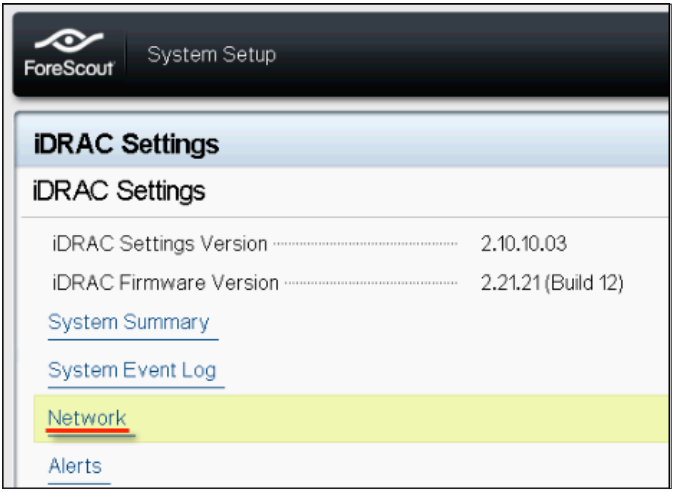
Altere as configurações do iDRAC para ativar o acesso remoto no dispositivo CounterACT. Esta seção descreve as configurações básicas de integração necessárias para trabalhar com o CounterACT.

Para configurar o iDRAC:

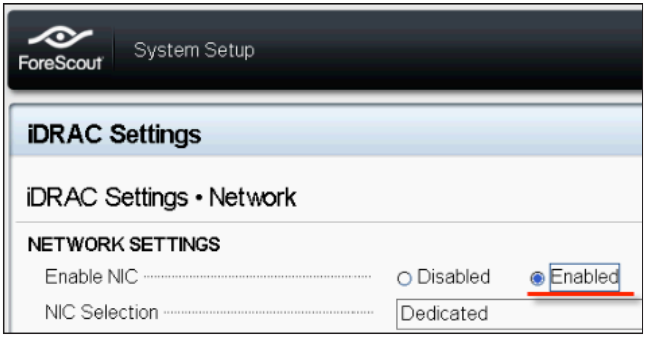
1. Ligue o sistema gerenciado.
2. Selecione F2 durante o POST (Power-on Self-test).
3. Na página System Setup Main Menu (Menu Principal de Configuração do Sistema), selecione **iDRAC Settings** (Configurações do Sistema).



4. Na página iDRAC Settings (Configurações do iDRAC), selecione **Network** (Rede).

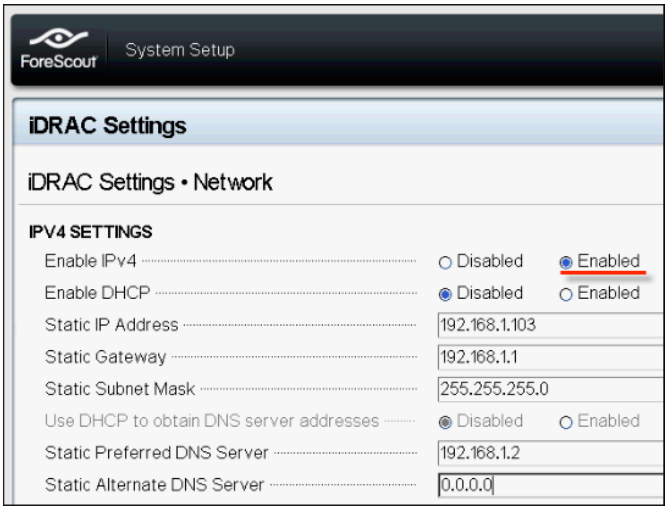


5. Defina as seguintes configurações de rede:
   - ***Network Settings (Configurações de Rede).*** Verifique se o campo **Enable NIC** (Ativar NIC) está configurado como **Enabled** (Ativado).

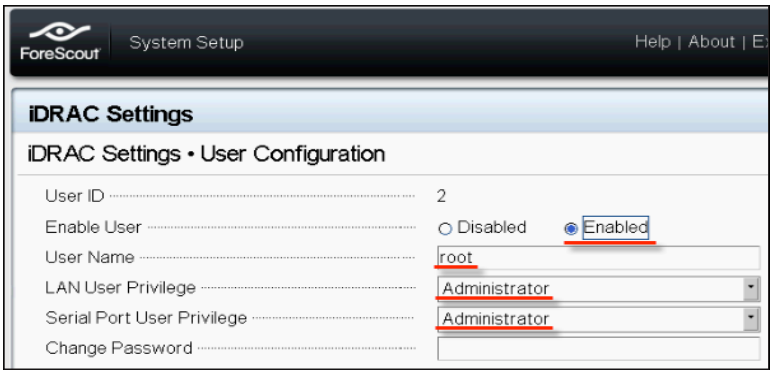


   - ***Common Settings (Configurações Comuns).*** No campo DNS DRAC Name (Nome do DNS DRAC), você pode atualizar um DNS dinâmico (opcional).

- ***IPV4 Settings (Configurações IPV4).*** Verifique se o campo **Enable IPv4** (Ativar IPv4) está configurado como **Enabled** (Ativado). Configure o campo **Enable DHCP** (Ativar DHCP) para **Enabled** (Ativado) para usar Endereçamento IP Dinâmico, ou Disabled (Desativado) para usar Endereçamento IP Estático. Se ativado, o DHCP atribuirá automaticamente o endereço IP, gateway e máscara de sub-rede ao iDRAC. Se desativado, insira valores para os campos **Static IP Address (Endereço IP Estático), Static Gateway (Gateway Estático)** e **Static Subnet Mask** (Máscara de Sub-rede Estática).



6. Selecione **Back** (Voltar).
7. Selecione **User Configuration** (Configuração do Usuário).
8. Configure os seguintes campos de User Configuration (Configuração do Usuário):
   - ***Enable User (Ativar Usuário).*** Verifique se esse campo está definido como Enabled (Ativado).
   - ***User Name (Nome de Usuário).*** Digite um nome de usuário.
   - ***LAN e Serial Port User Privileges (Privilégios de Usuário de LAN e de Porta Serial).*** Defina os níveis de privilégio para Administrator (Administrador).



- **Change Password (Alterar Senha).** Defina uma senha para o login do usuário.

9. Selecione **Back** (Voltar) e depois selecione **Finish** (Concluir). Confirme as configurações alteradas. As configurações de rede são salvas e o sistema é reiniciado.

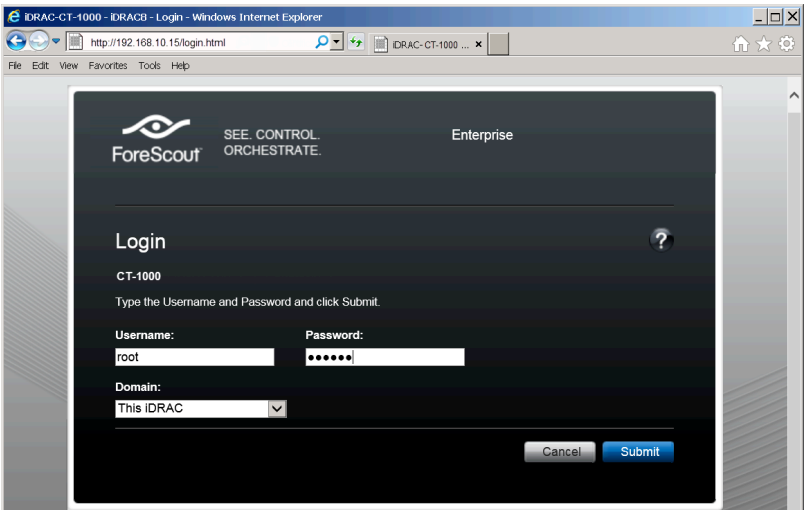
Conectar o Módulo à Rede

O iDRAC conecta-se a uma rede Ethernet. É habitual conectá-lo a uma rede de gerenciamento. A imagem a seguir mostra a localização da porta iDRAC no painel traseiro do dispositivo CT-1000:

Login no iDRAC

Para fazer login no iDRAC:

1. Navegue até o Endereço IP ou nome de domínio configurado em **iDRAC Settings > Network (Configurações iDRAC > Rede)**.



2. Digite o Username (Nome de Usuário) e Password (Senha) configurados na página User Configuration (Configuração de Usuário) da configuração do sistema iDRAC.
3. Selecione **Submit** (Enviar).

Para mais informações sobre o iDRAC, consulte o Guia de Usuário do iDRAC 7.

É muito importante atualizar as credenciais padrão.

6. Verificar Conectividade

Verificar a Conexão da Interface de Gerenciamento

Para testar a conexão da interface de gerenciamento, faça login no Dispositivo e execute o seguinte comando:

`fstool linktest`

As seguintes informações serão exibidas:

```
Management Interface status (Status de
  Interface de Gerenciamento)
Pinging default gateway information
  (Informações de ping de gateway padrão)
Ping statistics (Estatísticas de ping)
Performing Name Resolution Test (Executar Teste
  de Resolução de Nome)
Test summary (Resumo de Teste)
```

Verificar Conectividade do Comutador/Dispositivo

Verifique se o comutador está conectado adequadamente ao Dispositivo antes de sair do data center. Para fazer isso, execute o comando fstool ifcount no Dispositivo para cada interface detectada.

`fstool ifcount eth0 eth1 eth2`
(Separe cada interface com um espaço.)

Esta ferramenta exibe continuamente o tráfego de rede nas interfaces especificadas. Funciona em dois modos: por interface ou por VLAN. O modo pode ser alterado na tela. O total de bits por segundo e a porcentagem de cada uma das seguintes categorias de tráfego são mostrados:

- A interface de monitoramento deve enxergar principalmente o tráfego espelhado — acima de 90%.
- A interface de resposta deve enxergar principalmente o tráfego de broadcast.
- As interfaces de monitoramento e de resposta devem enxergar as VLANs esperadas.

Opções de comando:

`v – exibe o modo VLAN`
`v – exibe o modo de interface`
`P – mostra o anterior`
`N – mostra o próximo`
`q – para de exibir`

Modo VLAN:

```
update=[4]      [eth3: 14 vlans]
Interface/Vlan  Total   Broadcast  Mirrored  *To my MAC  *From my MAC
eth3.untagged   4Mbps   0.2%       99.8%     0.0%        0.0%
eth3.1          9Mbps   0.0%       100.0%    0.0%        0.0%
eth3.2          3Mbps   0.1%       99.9%     0.0%        0.0%
eth3.4          542bps  100.0%     0.0%      0.0%        0.0%
eth3.20         1Kbps   100.0%     0.0%      0.0%        0.0%
Show [v]lans [i]nterfaces <-[p]rev [n]ext->     [q]uit
```

Modo de Interface:

```
update=[31]     [eth0: 32 vlans] [eth1: 1 vlans]
Interface       Total   Broadcast  Mirrored  *To my MAC  *From my MAC
eth0            3Kbps   42.3%      0.0%      14.1%       43.7%
eth1            475bps  0.0%       100.0%    0.0%        0.0%
```

*To my MAC (Para meu MAC) — O MAC de Destino é o MAC do Dispositivo.

*From my MAC (Do meu MAC) — Tráfego enviado por este Dispositivo (O MAC de Origem é o MAC do Dispositivo. O destino pode ser broadcast ou unicast).

Caso não veja nenhum tráfego, verifique se a interface está funcionando. Use o comando a seguir no Dispositivo:

`ifconfig [interface name] up`

Executar Teste de Ping

Execute um teste de ping do Dispositivo para uma área de trabalho de rede para verificar a conectividade.

Para executar o teste:

1. Faça login no Dispositivo.
2. Execute o comando a seguir: **`Ping [network desktop IP]`**
   Por padrão, o Dispositivo não responde ao ping.

7. Configurar o Console do CounterACT

Instalar o Console do CounterACT

O Console do CounterACT é um aplicativo de gerenciamento central usado para visualizar, rastrear e analisar a atividade detectada pelo Dispositivo. Políticas de NAC, Proteção contra Ameaças, Firewall e outras podem ser definidas do Console. Consulte o *Manual do Usuário do Console do CounterACT* para obter mais informações.

Você deve fornecer uma máquina para hospedar o software do aplicativo do Console do CounterACT. Os requisitos mínimos de hardware são:

- Máquina não dedicada, que execute:
  - Windows XP, Windows Vista ou Windows 7
  - Windows Server 2003 ou Server 2008
  - Linux
- Pentium 3, 1GHz
- Memória de 2 GB
- Espaço em disco de 1 GB

Dois métodos estão disponíveis para realizar a instalação do Console:

Use o software de instalação embutido no seu Dispositivo.

1. Abra uma janela de navegador no computador Console.

   Digite o seguinte na linha de endereço do navegador
   `http://<Appliance_ip>/install`
   Em que <Appliance ip> é o endereço IP desse Dispositivo. O navegador exibe a janela de instalação do Console.
2. Siga as instruções da tela.

Instale a partir do CD-ROM do CounterACT

1. Insira o CD-ROM do CounterACT no drive de DVD.
2. Abra o arquivo **`ManagementSetup.htm`** do CD ROM com um navegador.
3. Siga as instruções da tela.

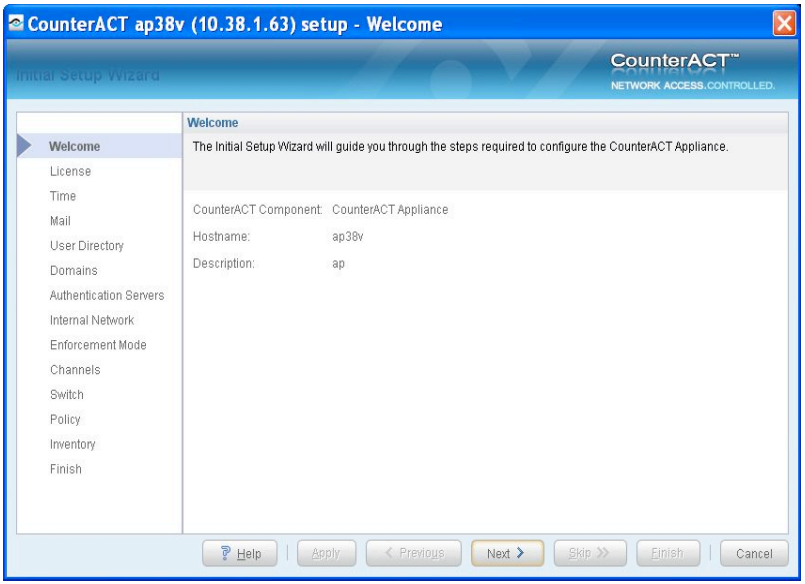
Fazer Login

Depois de concluir a instalação, você pode fazer login no Console do CounterACT.

1. Selecione o ícone do CounterACT a partir do atalho de local que você criou.
2. Digite o endereço IP ou nome de host do Dispositivo no campo **IP/Name** (IP/Nome).
3. No campo **User Name** (Nome de Usuário), digite **admin**.
4. No campo **Password** (Senha), digite a senha que você criou durante a instalação do Dispositivo.
5. Selecione **Login** para iniciar o Console.

Executar Configuração Inicial

Depois que você fizer login pela primeira vez, o Initial Setup Wizard (Assistente de Configuração Inicial) aparecerá. O Assistente o orientará pelas etapas de configuração essenciais para assegurar que o CounterACT funcione de maneira rápida e eficiente.



Antes de Começar a Configuração Inicial

Prepare as informações a seguir antes de trabalhar com o Assistente.

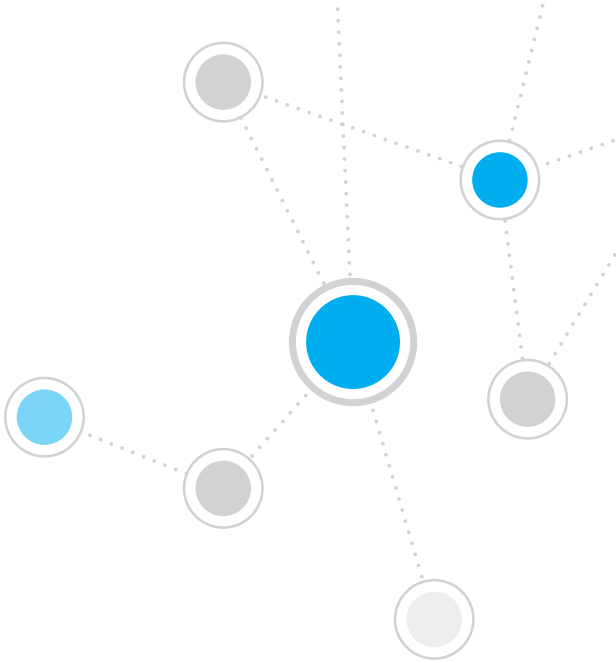
Informações	Valores
☐ Endereço do servidor NTP usado pela sua organização (opcional).	
☐ Endereço IP de retransmissão de e-mail interno. Permite a entrega de e-mail do CounterACT se o tráfego SMTP não for permitido a partir do Dispositivo (opcional).	
☐ Endereço de e-mail do administrador do CounterACT.	
☐ Atribuições das interfaces de monitoramento e de resposta definidas no Data Center.	
☐ Para segmentos ou VLANs sem DHCP, o segmento de rede ou VLANs aos quais a interface de monitoramento está conectada diretamente e um endereço IP permanente a ser usado pelo CounterACT em cada uma dessas VLANs. Essas informações não são necessárias para a configuração do Enterprise Manager.	
☐ As faixas de endereço IP que o Dispositivo protegerá (todos os endereços internos, incluindo os endereços não usados).	
☐ Informações de conta do Diretório do Usuário e o endereço IP do servidor do Diretório do Usuário.	
☐ Credenciais do domínio, incluindo nome e senha da conta administrativa do domínio.	
☐ Servidores de autenticação para que o CounterACT possa analisar quais hosts de rede foram autenticados com êxito.	
☐ Endereço IP do comutador principal, fornecedor e parâmetros de SNMP.	

Consulte o *Manual do Usuário do Console do CounterACT* ou a Ajuda On-line para obter informações sobre como trabalhar com o Assistente.

Informações de Contato

Para suporte técnico da ForeScout, envie um e-mail para support@forescout.com ou ligue para:

- Ligação gratuita (EUA): 1.866.377.8771
- Telefone (Intern): 1.408.213.3191
- Suporte: 1.708.237.6591
- Fax: 1.408.371.2284



ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 EUA

Ligação Gratuita: 1.866.377.8771
Telefone (Intern): 1.408.213.3191
Suporte: 1.708.237.6591
Fax: 1.408.371.2284

400-00020-01