SonicWall® Secure Mobile Access 12.1 Túnel de conexão

Guia do usuário

SONICWALL®

Sumário

1

Introdução

Sobre o Túnel de conexão

O *Guia do usuário do Túnel de conexão do Secure Mobile Access (SMA)* 12.1 fornece informações sobre a instalação e o uso dos clientes Serviço do túnel de conexão e Túnel de conexão.Também é incluída uma seção sobre a Solução de problemas.

NOTA: O SMA 12.1 fornece o Serviço de gerenciamento central (SGC) com Otimização de tráfego global (OTG). Para usar este recurso, você deve realizar o upgrade para Túnel de conexão 12.1.

Temas

Organização deste guia

Capítulo 1 Introdução	Este capítulo fornece um resumo dos capítulos deste guia, bem como uma descrição das convenções usadas.
Capítulo 2 Serviço do túnel de conexão	Este capítulo fornece instruções sobre a instalação e o uso do Windows para executar o Serviço do Túnel de conexão (STC), assim como sobre o uso de uma linha de comando ou script para executar o STC.
Capítulo 3 Cliente do Túnel de conexão para o Windows	Este capítulo fornece informações relativas ao download, à instalação, configuração e operação do Cliente do Túnel de conexão do Secure Mobile Access (SMA).
Capítulo 4 Cliente Túnel de conexão para MacOS/Linux	Este capítulo fornece informações relativas ao download, à instalação, configuração e operação do Cliente do Túnel de conexão (TC) do SMA no MacOS e Linux.
Suporte SonicWall	Este capítulo fornece informações de contato do Suporte da SonicWall.

Convenções do guia

Convenção	Uso
Negrito	Destaca os nomes de caixas de diálogo, janelas, telas e parâmetros, os ícones e os botões.
`Código`	Usado para nomes de arquivos e texto ou valores que sejam inseridos na interface.
Itálico	Indica o nome de um manual técnico. Também indica ênfase em certas palavras em uma frase. Por vezes, indica a primeira ocorrência de um termo ou conceito significante.

2

Serviço do túnel de conexão

Sobre o Serviço do túnel de conexão

O cliente do Serviço do túnel de conexão é um componente do servidor do Windows da solução Secure Mobile Access (SMA 1000) da SonicWall que permite o acesso seguro e autorizado a aplicativos baseados na Web e de cliente/servidor e a compartilhamentos de arquivos do Windows.

Em um ambiente de servidor, você pode instalar e configurar um componente suplementar — STC — de forma que a conexão VPN seja automaticamente iniciada sem a intervenção do usuário: não é necessário qualquer login de usuário e não são exibidos ícones ou a interface do usuário.

Por exemplo, você pode desejar sincronizar dados entre um sistema remoto no campo e um servidor de arquivos protegido atrás da VPN em sedes corporativas. No sistema remoto — executando a plataforma Windows Server — o STC é configurado para ser executado em um horário específico, se conectar ao servidor de arquivos corporativo e sincronizar seu banco de dados com o banco de dados mestre nas sedes.

O STC é suportado no Windows Server 2008 R2 e superior.

Instalar o Serviço de Túnel de conexão

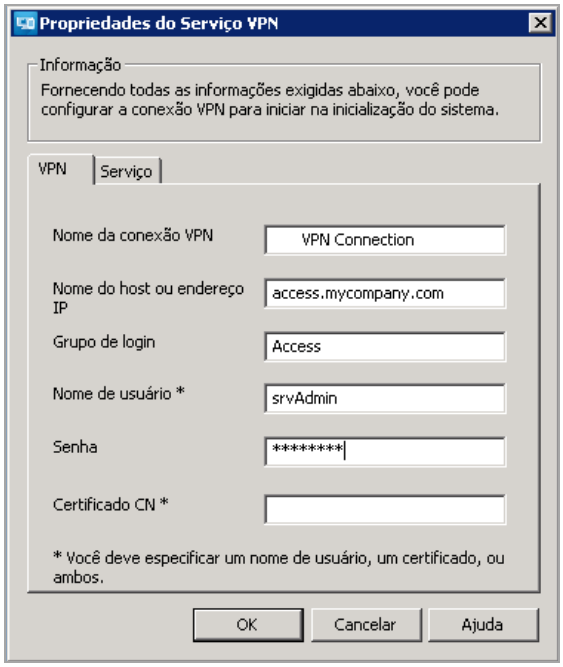
A utilização do Serviço de Túnel de conexão envolve a instalação do Túnel de conexão (TC) e do Serviço do túnel de conexão (STC).

Para instalar e configurar o Serviço de túnel de conexão:

1. Efetue login no Console de gerenciamento de equipamentos (CGE) no seu dispositivo da série SMA 1000 da SonicWall.
2. Navegue até a página **Configuração de agente** > **Download** .
3. Em **Pacotes de instalação do cliente**, baixe os pacotes de instalação de 32 ou 64 bits para o Túnel de conexão e o Serviço do túnel de conexão.
4. Instale o Túnel de conexão primeiro (`ngsetup_<xx>.exe` ou `ngsetup64_<xx>.exe`). Um atalho designado por **Conexão VPN da SonicWall** é criado na área de trabalho.

5 Instale o Serviço do túnel de conexão (`ctssetup_<xx>.exe` ou `ctssetup64_<xx>.exe`). Um atalho designado por **Opções do serviço VPN da SonicWall** é criado na área de trabalho.

6 Na área de trabalho, clique duas vezes no atalho **Opções do serviço VPN da SonicWall**. Como alternativa, clique duas vezes em **Opções do serviço VPN da SonicWall** no Painel de controle. A caixa de diálogo **Propriedades do serviço VPN da SonicWall** será exibida.



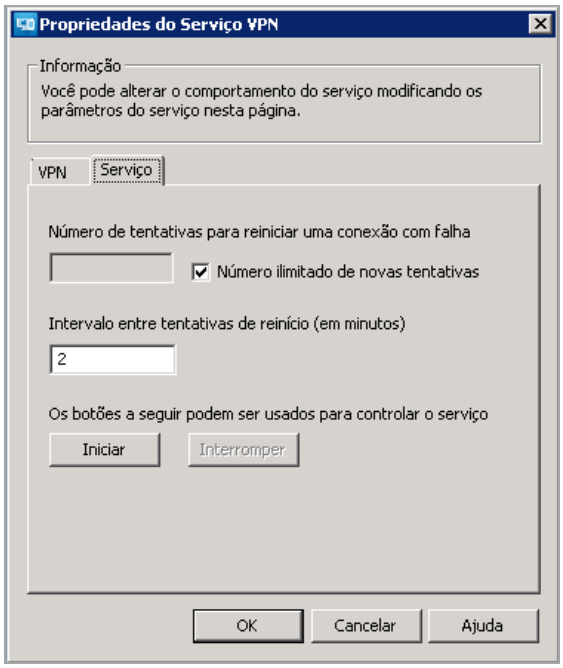
7 Na guia **VPN**, defina as seguintes configurações:

Nome da conexão VPN	Digite o nome do objeto de conexão do Cliente de conexão SonicWall exatamente como aparece na janela **Conexões de rede** do Windows (**Iniciar|Conectar a|Mostrar todas as conexões**). Por padrão, esta é a **Conexão VPN da SonicWall**.
Nome do host ou endereço IP	Digite o nome do host ou o endereço IP do equipamento da série SMA 1000 da SonicWall.
Grupo de login	Digite o nome do território usado por usuários neste grupo de login.
Nome de usuário e Senha	Digite as credenciais de um usuário neste **Grupo de login**. Você deve inserir um nome de usuário e senha ou um certificado CN. Em alguns casos de autenticação em cadeia, são necessários um nome de usuário e um certificado.
Certificado CN	O nome comum (CN) de um certificado identifica seu proprietário. Especifique o CN para o certificado associado a este território.

8 Na guia **Serviço**, defina as seguintes configurações:

Número de tentativas para reiniciar uma conexão com falha	Especifique quantas tentativas de reinicialização devem ser feitas se uma conexão inicial falhar.
Número ilimitado de novas tentativas	Selecione esta caixa de seleção para continuar tentando conectar continuamente até se conectar com sucesso.
Intervalo entre tentativas de reinício	Especifique a quantidade de tempo (em minutos) para aguardar entre as tentativas de reinicialização.

9 Clique no botão **Iniciar**. Os botões **Iniciar** e **Interromper** são usados para controlar o serviço.



10 Para confirmar que o Túnel de conexão foi iniciado, abra o atalho **Conexão VPN da SonicWall** na área de trabalho. Você deve ver a conexão estabelecida.

Como alternativa, você pode usar o comando `ipconfig` na linha de comando para confirmar que possui um endereço IP virtual para a Conexão VPN da SonicWall.

Importar o certificado do cliente

O certificado especificado para o STC deve estar localizado no repositório de certificados do **Computador local** do dispositivo do usuário; os certificados em um repositório do usuário não estão disponíveis para o serviço. O Microsoft Management Console (MMC) é uma ferramenta para gerenciamento de ferramentas administrativas, incluindo snap-ins e snap-ins de extensão.

Para importar um certificado para o armazenamento do** Computador local **do usuário:

1 Para abrir o Console de gerenciamento da Microsoft, clique no botão Iniciar do Windows e digite `mmc` no campo de texto.

2 Pressione **Enter**.

3 No menu **Arquivo**, escolha a opção para adicionar um snap-in.

4 Para adicionar um snap-in autônomo, selecione **Certificados** e, em seguida, clique no botão **Adicionar** >. Os snap-ins podem gerenciar certificados para diferentes contas.

5 Selecione **Conta do computador**.

6 Clique em **Next** (Avançar).

7 Selecione **Computador local**.

8 Clique em **Concluir**.

Agora, você deve ver **Certificados (Computador local)** na lista de snap-ins selecionados. O certificado deve agora ser copiado para um armazenamento de certificados.

9 No Console de Gerenciamento da Microsoft, clique com o botão direito do mouse em **Pessoal** > **Certificados** no painel de navegação esquerdo e, em seguida, selecione **Todas as tarefas > Importar**.

10 Especifique o arquivo de certificado que deseja importar, conjuntamente com sua senha.

11 Coloque o certificado em seu armazenamento **Pessoal**.

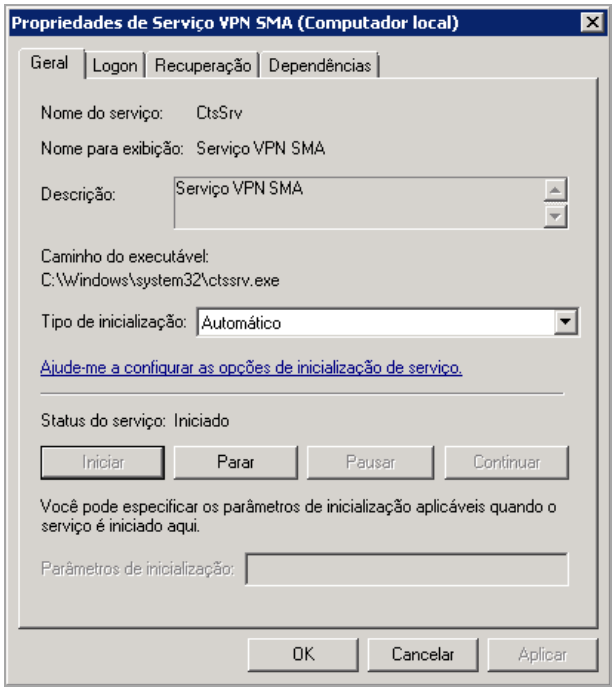
Usar os serviços do Windows para executar o STC

Você pode usar os Serviços do Windows para gerenciar o STC em um computador local ou remoto.

Como usar os Serviços do Windows para configurar e executar o STC:

1 Na plataforma Windows Server executando o Serviço do túnel de conexão, execute os Serviços do Windows.

2 Abra a caixa de diálogo Propriedades do Serviço VPN da SonicWall (**Painel de controle > Ferramentas administrativas > Serviços > Serviço VPN SMA da SonicWall**).



3 Use essas configurações para controlar o serviço (iniciar, interromper, pausar, retomar ou desabilitar), configurar as ações de recuperação em caso de falha do serviço ou desativar o serviço para um determinado perfil de hardware.

4 Clique em **OK**.

Usar um comando ou script para executar o STC

Você pode usar o utilitário sc.exe do Windows para comunicar com o Controlador de serviço (services.exe) a partir do prompt de comando ou em um arquivo em lote. Isso permite que você automatize a inicialização e o desligamento do serviço VPN da SonicWall.

Em um ambiente onde você deseja que os usuários possam iniciar a conexão de VPN clicando em um atalho (e sem conhecer as credenciais), você também deve criar um atalho na área de trabalho que inicie um comando ou arquivo em lote. Por exemplo:

Para iniciar e interromper o Serviço de túnel de conexão em um computador remoto, use os seguintes comandos:

```
sc \\SERVERNAME start ctssrv
sc \\SERVERNAME stop ctssrv
```

Para iniciar ou interromper o Serviço de túnel de conexão a partir da linha de comando ou de um aplicativo de terceiro, utilize os seguintes comandos:

```
%windir%\system32\sc.exe start ctssrv
%windir%\system32\sc.exe stop ctssrv
```

Solução de problemas

Use o Visualizador de eventos do Windows (**Painel de controle > Ferramentas administrativas > Visualizador de eventos > Aplicativo**, onde a **Origem** é STC) para visualizar todas as informações, avisos ou mensagens de erro relacionados à execução do Serviço do túnel de conexão.

Para obter mensagens mais detalhadas, analise o log de serviço, o local padrão é: `ALLUSERSPROFILE%\Application Data\SonicWall`.

NOTA: Se o seu ambiente incluir um proxy HTTP de saída para acesso à internet, você deve usar um que não exija autenticação, caso contrário, verá a seguinte mensagem de erro no arquivo de log do STC (`ctssrv.log`): `O acesso direto à Internet não está disponível`.

NOTA: Você também deve configurar o STC para ser executado em uma conta de usuário do Windows com privilégios de administrador.

3

Cliente do Túnel de conexão para o Windows

Sobre o Túnel de conexão

O cliente do Túnel de conexão é um componente cliente do Windows da solução Túnel de conexão (SMA) que permite o acesso seguro e autorizado a aplicativos baseados na Web, de cliente/servidor e a compartilhamentos de arquivos do Windows.

O cliente do Túnel de conexão permite que você se conecte aos recursos de rede que são protegidos pelo equipamento da série SMA 1000 da SonicWall.

O Túnel de conexão é suportado no Windows 7 e superior e no Windows 10 Anniversary Update e superior. O Windows Vista não é suportado.

Recursos disponíveis do Túnel de conexão

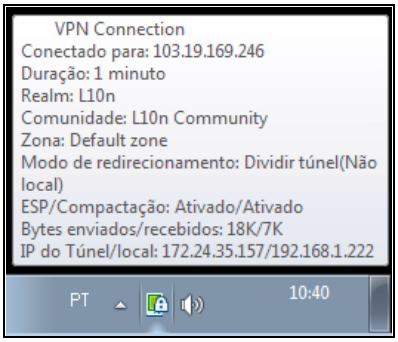
O Túnel de conexão permite que você acesse com segurança os seguintes tipos de recursos:

Tipos de recurso

Tipo de recurso	Descrição
Recursos cliente/servidor	Aplicativos cliente/servidor, aplicativos de cliente "thin" e serviços de terminal, como o Microsoft Outlook, Citrix e Windows Terminal Services.
Sites e aplicativos da Web	Conteúdo online e aplicativos baseados na Web que podem ser acessados por meio de um navegador, como o Microsoft Outlook Web Access, Domino Web Access e sites da Web em geral (como intranets).
Compartilhamentos de rede do Windows	Pastas e arquivos do Windows compartilhados por meio do Ambiente de rede do Windows e unidades mapeadas.

Como saber se o Túnel de conexão está em execução

Quando o Túnel de conexão está em execução e conectado à VPN, um ícone poderá ser exibido na área de notificação da barra de tarefas. Se você pausar o ícone com seu cursor, as informações de status da conexão serão exibidas:



Você pode configurar o Túnel de conexão para não exibir isso durante conexões ativas; para obter mais informações, consulte Definir as configurações do Túnel de conexão.

Você também pode verificar o estado da conexão VPN do Túnel de conexão na janela **Conexões de rede do Windows**.

Visualizar informações de status de conexão

Para visualizar as informações de status da conexão:

1. No menu **Iniciar**, clique em **Painel de controle**. Continue com as etapas seguintes dependendo do seu sistema operacional. Para exibir todas as conexões sem fio, com fio, discadas e de VPN disponíveis:
   a. Clique em **Rede e internet**.
   b. Clique em **Centro de rede e compartilhamento**.
   c. Clique no link **Conectar a uma rede**.
2. No menu **Visualizar**, clique em **Detalhes**.
3. Na seção **Discagem**, visualize as informações de status da conexão para a conexão do Túnel de conexão.

   ⓘ **NOTA:** Seu administrador pode ter personalizado o nome deste aplicativo.)

   Se o Túnel de conexão estiver enfrentando uma interrupção de rede temporária, será exibido um **círculo vermelho** com um **X** no ícone do Túnel de conexão na área de notificação da barra de tarefas. Se a conexão de rede for restabelecida, o círculo vermelho com o X desaparecerá e o ícone do Túnel de conexão retornará ao seu estado normal.

Executar o cliente do Túnel de conexão

Temas:

- Baixando o Túnel de conexão
- Iniciar o Túnel de conexão
- Especificar um grupo de login
- Processar certificados de servidor

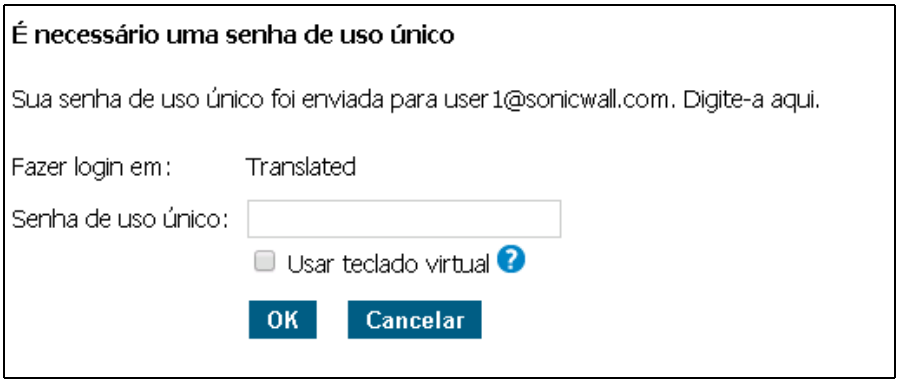
Baixando o Túnel de conexão

O Túnel de conexão pode ser baixado do menu WorkPlace. Você precisa ter privilégios de administrador para instalar o software.

Para baixar o Túnel de conexão:

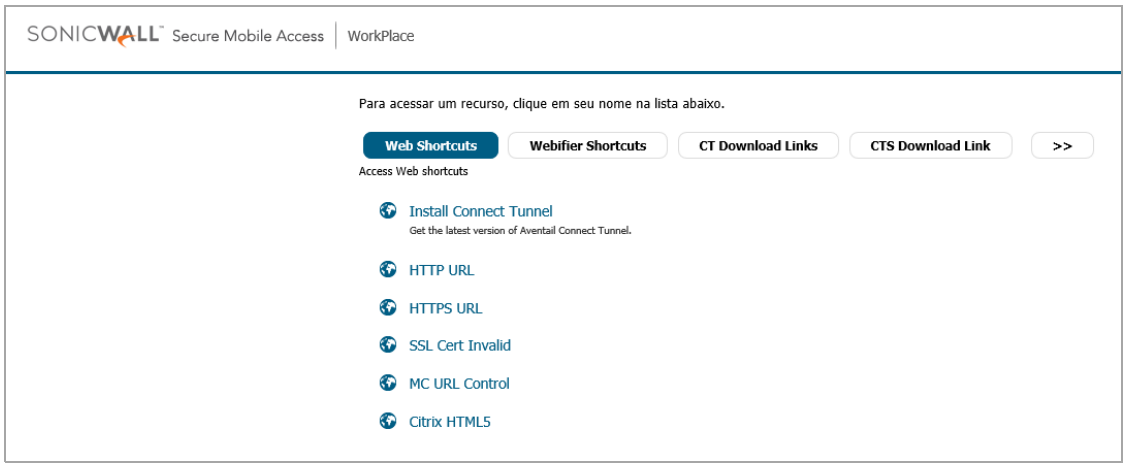
1 Faça login no WorkPlace.

Dependendo da sua configuração, você pode ter recebido uma senha de uso único de seu administrador, que permitirá que baixe o Túnel de conexão.



2 Insira a senha que foi enviada a você. O aplicativo do Workplace aparece e permite-lhe baixar o software.

3 No WorkPlace, clique na entrada para **Instalar o Túnel de conexão**.



4 Clique em **Instalar**. Quando a instalação estiver concluída, faça logout do Workplace.

Iniciar o Túnel de conexão

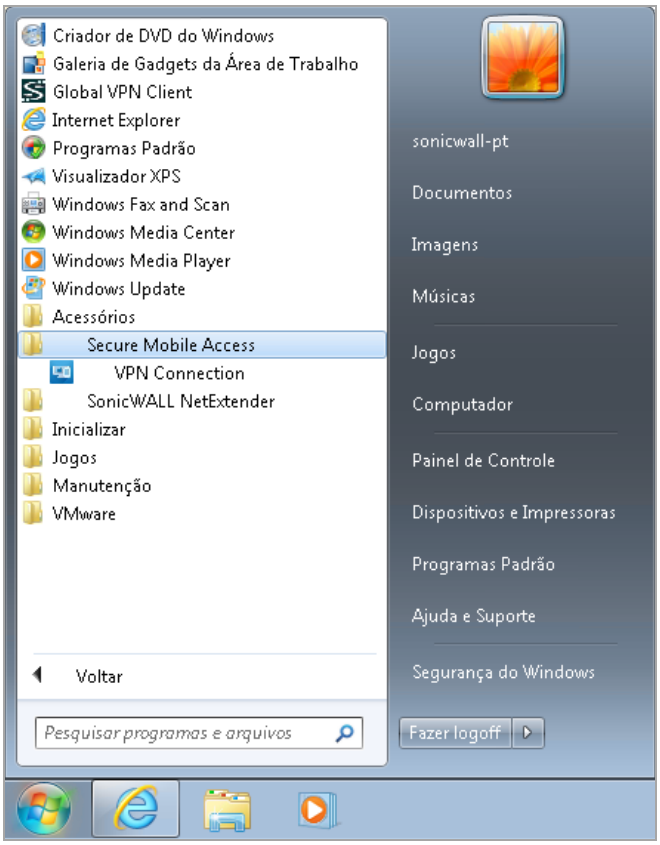
Para acessar os recursos de rede por meio do Túnel de conexão, você deve primeiro confirmar sua identidade. Isso garantirá que somente usuários autorizados possam acessar recursos de rede protegidos. As credenciais usadas para verificar sua identidade normalmente são compostas de um nome de usuário e uma senha (ou código de acesso).

Dependendo dos recursos, você também pode precisar inserir uma senha única e/ou aceitar uma Política de uso aceitável.

Para iniciar o Túnel de conexão:

1 Para:

- No Windows 7, clique em **Iniciar > Todos os programas > SonicWall Secure Mobile Access > Conexão VPN da SonicWall**.

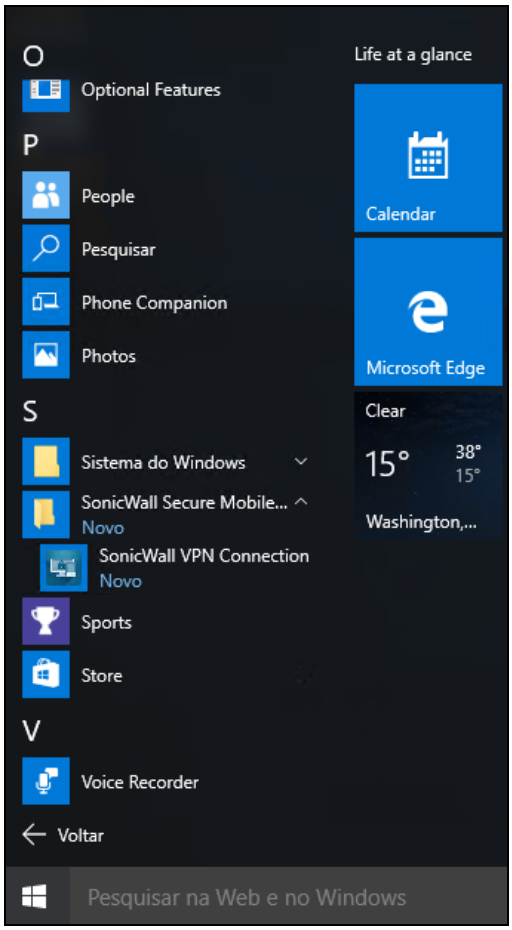


- Para o Windows 8.x e superior:

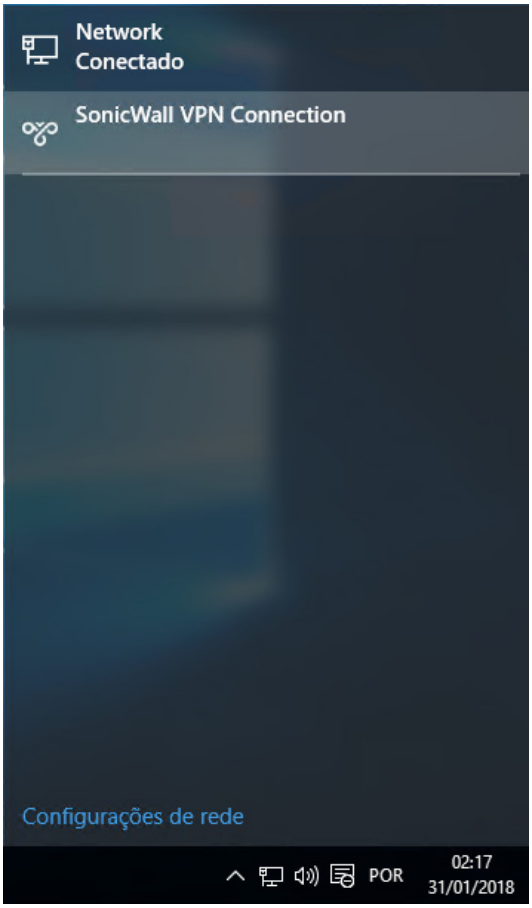
  1) Clique no botão **Iniciar** e, em seguida, selecione uma das seguintes opções:

ⓘ **NOTA:** Seu administrador pode ter personalizado o nome deste aplicativo.

- **Todos os programas > Conexão VPN da SonicWall**, clique em **Conexões** e selecione a conexão do Túnel de conexão que deseja usar.

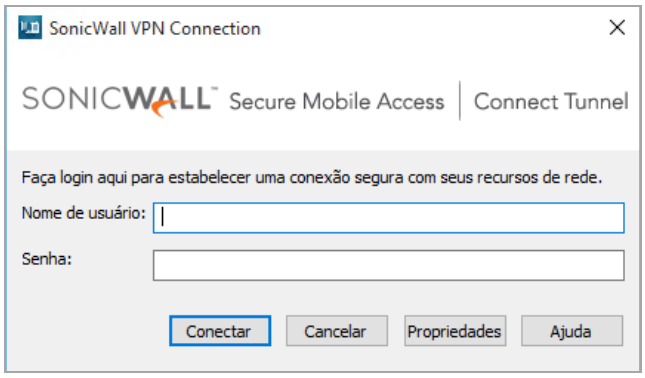


- **Rede > Conexão VPN da SonicWall**.



2) Clique no botão **Conectar**.

2 Você verá uma tela de login inicial.



3 Insira suas credenciais de autenticação. Dependendo da forma como seu administrador configurou o Túnel de conexão, você pode ver uma combinação dos seguintes prompts:

- Digite seu nome de usuário no campo **Nome de usuário**.
- No campo **Senha** ou **Código de acesso**, digite sua senha ou código de acesso. (As senhas podem diferenciar maiúsculas de minúsculas. Certifique-se de que as teclas Caps Lock ou Num Lock não estejam ativadas.)
- Insira uma senha de uso único que foi enviada a você por seu administrador.

- Se um certificado de cliente for necessário para autenticação, a lista **Certificado** exibe os certificados em seu dispositivo que correspondem ao certificado de autoridade (CA) usado pelo servidor de autenticação. Frequentemente, haverá somente um listado.

4 Se uma Política de uso aceitável for exibida, clique em **Aceitar** para aceitá-la.

5 Clique em **Conectar**.

O ícone do Túnel de conexão é exibido na área de notificação da barra de tarefas, indicando que o Túnel de conexão está sendo executado e está conectado à VPN.

Seu login pode não ser exatamente igual ao mostrado acima. Seu administrador poderia enviar a você um login que permita que se conecte a uma rede específica.

NOTA: Na caixa de diálogo de login do Túnel de conexão, você pode clicar em **Propriedades** para exibir a caixa de diálogo **Propriedades do Túnel de conexão**, onde você pode iniciar uma conexão diferente ou alterar as preferências do programa. Para obter mais informações, consulte Definir as configurações do Túnel de conexão.

Especificar um grupo de login

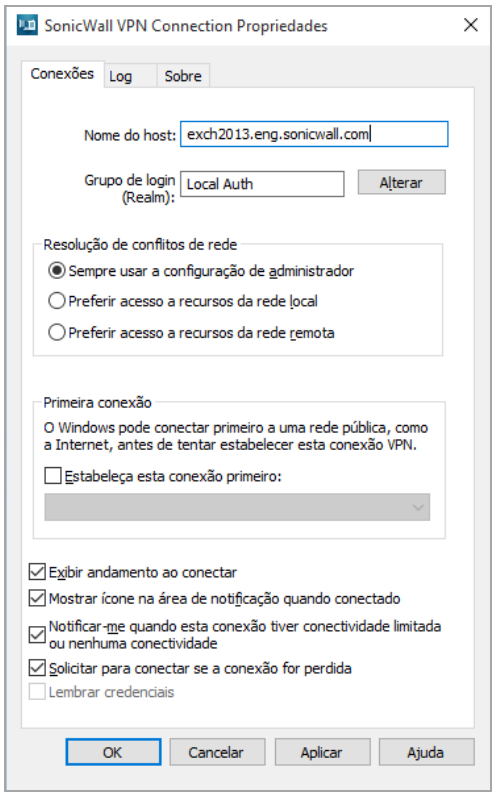
O Túnel de conexão permite que você faça login em diferentes grupos, se necessário (por exemplo, se alternar entre fazer login no grupo “Vendas” e no grupo “Marketing”). Você pode precisar fornecer credenciais de autenticação diferentes para cada grupo de login.

Você deve especificar um grupo de login todas as vezes que iniciar uma conexão com sua VPN. Esta opção está disponível somente quando o Túnel de conexão estiver offline (isto é, quando não conectado à sua VPN). Você não precisa de privilégios administrativos para alterar um nome de host ou grupo de login.

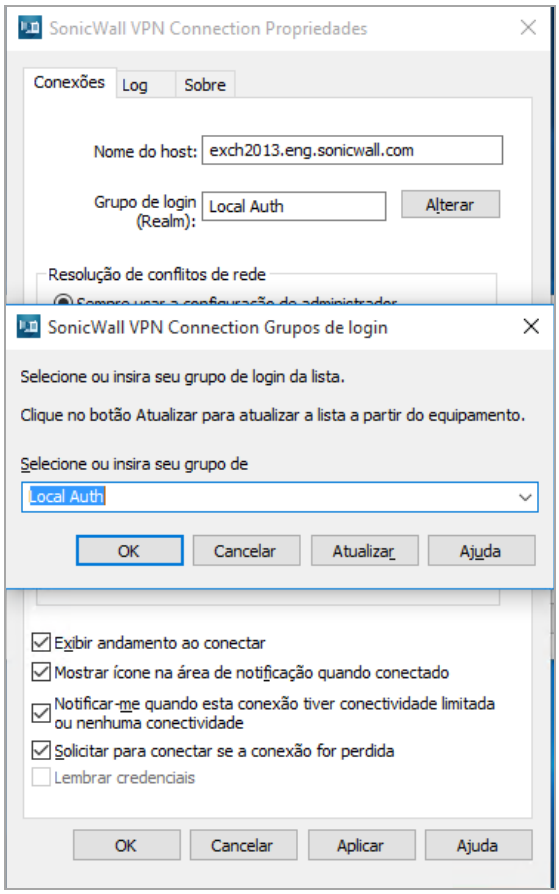
Para especificar o grupo de login:

1 Na caixa de diálogo de login da **Conexão Secure Mobile Access VPN**, clique em **Propriedades**.

2 À direita do campo **Grupo de login**, clique em **Alterar**.



A caixa de diálogo **Grupos de login da Conexão Secure Mobile Access VPN** é apresentada e exibe a lista atual de grupos de login.



3 No campo **Selecione ou insira seu grupo de login**, selecione ou digite o nome do grupo de login no qual você deseja fazer login.

Se o grupo de login não for exibido na lista, clique em **Atualizar** para atualizar a lista de grupos de login disponíveis.

Dependendo da forma como seu administrador configurou o Túnel de conexão, alguns grupos de login podem não ser exibidos na lista; contudo, você ainda pode fazer login em um grupo de login “oculto” (se estiver autorizado para tal) digitando seu nome em **Selecione ou insira seu grupo de login**.

4 Clique em **OK**.

Processar certificados de servidor

Algumas configurações de VPN exigem que você aceite um certificado de servidor antes de poder obter acesso a um recurso de rede protegido. Um certificado de servidor é essencialmente uma assinatura digital que confirma a identidade do servidor.

Se você acessar um recurso de rede que usa um certificado de servidor, o Túnel de conexão poderá exibir o certificado. O Túnel de conexão exibirá um aviso de certificação apenas se o certificado do equipamento VPN não for de uma fonte confiável. Você deve então confirmar que o certificado do servidor é de uma fonte confiável antes de aceitá-lo. Caso contrário, o processo de login irá continuar sem qualquer prompt.

NOTA: O Túnel de conexão irá processar/avisar apenas relativamente aos certificados da VPN durante o processo de login, mas não dos recursos. Os aplicativos usados para acessar recursos, tais como o Internet Explorer, devem tratar de todos os certificados associados aos recursos.

Porque qualquer pessoa pode emitir um certificado, você deve aceitar certificados somente de fontes confiáveis, dado que as informações que você recebe podem ser inválidas. Você não precisa de privilégios administrativos para processar certificados do servidor. Se você tiver dúvidas se deve ou não aceitar um certificado, fale com seu administrador.

Para processar um certificado de servidor:

1. Quando um certificado de fonte confiável for exibido, certifique-se de que o certificado esteja associado ao servidor correto.
2. Aceitar ou rejeitar o certificado:
   - Se você clicar em **Rejeitar**, sua conexão não será estabelecida.
   - Se você clicar em **Aceitar**, o certificado é aceito como válido e o processo de login continuará.

   Da mesma forma, você pode ser solicitado a aceitar um acordo de licença ou Política de uso aceitável.

Sair do Túnel de conexão

Encerrar o Túnel de conexão irá encerrar sua sessão VPN e desconectá-lo da rede remota.

Para sair do Túnel de conexão:

1. Na área de notificação da barra de tarefas, clique com o botão direito no ícone do Túnel de conexão.
2. Clique em **Desconectar**.

Definir as configurações do Túnel de conexão

Esta seção descreve como visualizar e definir as configurações do cliente do Túnel de conexão. Você precisa ter privilégios de administrador em seu computador para alterar essas configurações.

Temas:

Visualizar as configurações atuais do Túnel de conexão

Para visualizar as configurações atuais do Túnel de conexão:

1. No menu **Iniciar**, clique em **Painel de controle**. Continue com as etapas seguintes dependendo do seu sistema operacional. Para exibir todas as conexões sem fio, com fio, discadas e de VPN disponíveis:
   a. Clique em **Rede e internet**.
   b. Clique em **Centro de rede e compartilhamento**.

c Clique no link **Conectar a uma rede**.

2 Na seção **Discagem**, clique com o botão direito do mouse no nome da conexão Túnel de conexão (seu administrador pode ter personalizado o nome deste aplicativo) e, em seguida, clique em **Propriedades**. A caixa de diálogo **Propriedades do** Túnel de conexão é exibida.

3 Verifique as informações nas guias **Conexão** e **Sobre**:

- Clique na guia **Conexões** para visualizar as configurações de conexão atuais.
- Clique na guia **Sobre** para visualizar as informações básicas sobre o aplicativo.
- Clique em **Informações do arquivo** na guia **Sobre** para obter informações mais detalhadas.

Definir configurações gerais

Esta seção descreve como definir as configurações gerais do Túnel de conexão.

Para definir as configurações gerais do *Túnel de conexão:*

1 No menu **Iniciar**, clique em **Painel de controle**. Continue com as etapas seguintes dependendo do seu sistema operacional. Para exibir todas as conexões sem fio, com fio, discadas e de VPN disponíveis:

a Clique em **Rede e internet**.

b Clique em **Centro de rede e compartilhamento**.

c Clique no link **Conectar a uma rede**.

2 Na seção **Discagem**, clique com o botão direito do mouse no nome da conexão Túnel de conexão.

ⓘ **NOTA:** Seu administrador pode ter personalizado o nome deste aplicativo.)

3 Clique em **Propriedades**. A caixa de diálogo **Propriedades do** Túnel de conexão é exibida.

4 Clique na guia **Conexões** e defina as configurações da Conexão conforme necessário. Para exibir:

- Uma barra de status durante o processo de conexão, marque a caixa de seleção **Exibir andamento ao conectar**.
- O ícone do Túnel de conexão na área de notificação da barra de tarefas durante as conexões ativas, marque a caixa de seleção **Mostrar ícone na área de notificação quando conectado**.
- Uma notificação se a conexão de rede estiver enfrentando conectividade limitada ou nenhuma conectividade, marque a caixa de seleção **Notificar-me quando esta conexão tiver conectividade limitada ou nenhuma conectividade**.
- Um prompt para estabelecer uma nova conexão se a conectividade de rede for perdida, marque a caixa de seleção **Solicitar para conectar se a conexão for perdida**.

5 Clique em **OK**.

Conectar a outra VPN

Para especificar o nome de host ou endereço IP da VPN:

1 No menu **Iniciar**, clique em **Painel de controle**. Continue com as etapas seguintes dependendo do seu sistema operacional. Para exibir todas as conexões sem fio, com fio, discadas e de VPN disponíveis:

a Clique em **Rede e internet**.

b Clique em **Centro de rede e compartilhamento**.

c Clique no link **Conectar a uma rede**.

2 Na seção **Discagem**, clique com o botão direito do mouse no nome da conexão Túnel de conexão.

NOTA: Seu administrador pode ter personalizado o nome deste aplicativo.)

3 Clique em **Propriedades**. A caixa de diálogo **Propriedades do Túnel de conexão** é exibida.

4 Clique na guia **Conexões** e, em seguida, no campo **Nome do host ou endereço IP da VPN**, digite o nome do host ou o endereço IP da VPN à qual deseja se conectar.

5 Clique em **OK**.

Configurar conexões

Clicar no botão **Propriedades** no menu de login leva você à guia **Conexões**, que contém a lista de conexões e suas propriedades associadas, juntamente com as operações para modificar, adicionar e excluir conexões.

A lista da guia **Conexões** mostra todas as conexões configuradas para a máquina cliente. A seleção de um item da lista preenche todos os campos de dados na seção **Propriedades** para as guias **Conexão** e **Log**.

Conexão padrão é uma conexão que você pode usar para modificar e/ou conectar a um equipamento para puxar a lista de conexões definidas pelo administrador.

A seção **Propriedades** está oculta para as conexões definidas pelo Administrador do AMC, visível para **Conexão padrão**.

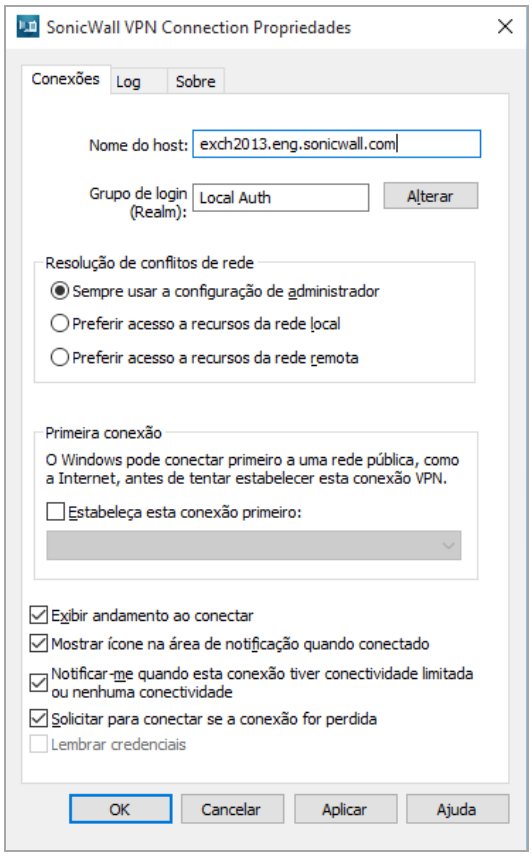
A guia **Conexões** contém os parâmetros gerais para a conexão selecionada.

Nome da conexão mostra um nome amigável para a conexão, usado na lista de exibição de conexões. Esta opção está desativada para a **Conexão padrão**.

Configurar uma conexão padrão

O login em seu Túnel de conexão pode ter a opção para conexões padrão. Neste caso, a **Conexão padrão** está disponível na lista **Conexões**.

Se a **Conexão padrão** estiver selecionada, clicar no botão **Propriedades** faz com que a caixa de diálogo **Propriedades de conexão** seja exibida.



A guia **Conexões** exibe informações sobre o nome do host e o grupo de login (Território). Se quiser alterar os grupos de login, clicar em **Alterar** permitirá que você selecione uma opção em uma lista dos grupos de login atuais. Se nenhum outro grupo estiver disponível, clique em **Cancelar** para retornar à caixa de diálogo **Conexão**.

A seção **Resolução de conflitos de rede** permite que você escolha qual tipo de resolução de conflito de rede deve ser executado. Se a Resolução de conflito de rede for controlada pelo administrador por meio de configurações da comunidade, esta seção não estará disponível.

A seção **Primeira conexão** permite que você estabeleça uma conexão de Internet antes de estabelecer uma conexão VPN. Isso é mais comumente usado ao estabelecer conexões executando discagem sobre VPN. Para usar esta opção, marque a caixa de seleção Estabelecer esta conexão de e, em seguida, selecione uma opção na lista suspensa de conexões.

Exibir andamento ao conectar é uma opção que controla se as mensagens de sequência de login devem ser exibidas ou não enquanto a conexão está sendo estabelecida. Isso inclui, entre outras coisas: Autenticação, Verificações de EPC e Estabelecimento da VPN.

Mostrar ícone na área de notificação é uma opção que permite que você especifique se o ícone da Conexão Secure Mobile Access VPN (cabeça de cavaleiro) é ou não exibido na bandeja do sistema do Windows.

Notificar-me quando esta conexão tiver conectividade limitada ou nenhuma conectividade é uma opção que permite que você veja mensagens sobre possíveis problemas de conexão (lentidão, perda de pacotes etc.) que podem ocorrer quando o Túnel de conexão estiver em execução.

Solicitar para conectar se a conexão cair ou for perdida é uma opção que controla se a caixa de diálogo de login da **Conexão** Secure Mobile Access **VPN** aparece novamente ou não se a conexão cair ou for perdida por qualquer motivo.

Ao terminar de fazer suas escolhas, clique em **OK**. O Túnel de conexão salva a configuração atual e fecha a caixa de diálogo **Propriedades de conexão**.

Estabelecer uma conexão de rede inicial

Em alguns casos, você pode precisar estabelecer uma conexão de rede antes de poder conectar à VPN; isso é normalmente necessário somente se você usar uma conexão de discagem para conectar à Internet.

Esta seção descreve como configurar uma conexão que deve ser estabelecida antes de você conectar à VPN.

Para configurar uma primeira conexão:

1. No menu **Iniciar**, clique em **Painel de controle**. Continue com as etapas seguintes dependendo do seu sistema operacional. Para exibir todas as conexões sem fio, com fio, discadas e de VPN disponíveis:
    a. Clique em **Rede e internet**.
    b. Clique em **Centro de rede e compartilhamento**.
    c. Clique no link **Conectar a uma rede**.
2. Na seção **Discagem**, clique com o botão direito do mouse no nome da conexão Túnel de conexão.

    NOTA: Seu administrador pode ter personalizado o nome deste aplicativo.)
3. Clique em **Propriedades**. A caixa de diálogo **Propriedades do Túnel de conexão** é exibida.
4. Clique na guia **Conexões** e, em seguida, em **Primeira conexão**, selecione a caixa de seleção **Estabelecer esta conexão primeiro**.
5. Na lista, selecione a conexão que deve ser estabelecida primeiro e, em seguida, clique em **OK**.

Atualizar o software do Túnel de conexão

Seu administrador de rede pode emitir atualizações de software quando uma nova versão do software Túnel de conexão for disponibilizada ou quando seus requisitos de rede mudarem. Seu administrador determina se disponibilizará as atualizações de software para você e quando.

Se o seu administrador tiver habilitado a atualização de software do Túnel de conexão, um alerta será exibido durante o processo de login sempre que uma atualização do Túnel de conexão estiver pronta para download.

Para fazer o download e instalar uma atualização de software:

- Durante o login, se a caixa de diálogo **Atualização de software do Túnel de conexão** for exibida e indicar que uma atualização de software está disponível, as opções disponíveis dependem de como seu administrador configurou a atualização do software:
    - Clique em **Atualizar** para fazer o download e instalar imediatamente a atualização de software. Se você selecionar esta opção, a atualização de software será instalada e, depois, o processo de login continuará.
    - Clique em **Lembre-me mais tarde** para adiar a atualização de software e continuar com o login. Se você selecionar esta opção, o Túnel de conexão irá informá-lo novamente (uma vez por dia) até que faça o download e instale a atualização clicando em **Atualizar**. Dependendo de como seu administrador configurou o Túnel de conexão, esta opção pode estar indisponível.
    - Clique em **Cancelar** para cancelar a atualização de software e o processo de login.

Solução de problemas

Esta seção descreve como solucionar problemas básicos de cliente do Túnel de conexão. Se você estiver tendo problemas para conectar à sua VPN ou acessar recursos da rede local ou remota, veja se o seu problema é resolvido por meio do seguinte. Se o problema continuar, entre em contato com seu administrador de sistema.

Temas:

Não é possível conectar

Veja alguns itens a serem verificados se estiver tendo problemas para conectar à sua VPN:

- Certifique-se de que o Túnel de conexão esteja em execução e ativamente conectado à rede. Para obter mais informações, consulte Como saber se o Túnel de conexão está em execução.
- Verifique na caixa de diálogo **Propriedades do** Túnel de conexão que você está iniciando uma conexão com o nome de host ou endereço IP corretos. Para obter mais informações, consulte Conectar a outra VPN.
- Verifique na caixa de diálogo **Propriedades do** Túnel de conexão que você está iniciando uma conexão com o grupo de login correto. Para obter mais informações, consulte Especificar um grupo de login.
- Se estiver usando um firewall pessoal, você pode precisar configurar o firewall para poder acessar sua VPN. Para fazer isso, configure o firewall para permitir que o tráfego de `ngvpnmgr.exe` acesse a Internet e adicione o nome de host ou endereço IP da VPN como um host ou zona confiável.
- A autenticação pode exigir que você tenha um certificado de cliente específico em seu dispositivo. Se você fizer alterações aos certificados instalados em seu computador entre tentativas de login, atualize a lista apresentada durante o login clicando em **Atualizar**.

Não é possível acessar os recursos ou a Internet

Seu dispositivo pode ter sido classificado na zona de segurança incorreta:

- Seu administrador pode solicitar que você confirme a zona de segurança na qual você foi classificado. Se as zonas de segurança foram configuradas, você poderá visualizar sua zona atual pausando o ícone do Túnel de conexão na área de notificação da barra de tarefas com seu cursor.

Quando o equipamento recebe solicitações de recursos ou acesso à Internet de clientes, elas poderão ser manipuladas de algumas formas diferentes. Seu administrador faz esta escolha de configuração no AMC:

- No modo *dividir túnel*, somente o tráfego destinado a recursos que foram especificados no AMC é redirecionado para o equipamento, e todo o outro tráfego é enviado normalmente. Em outras palavras, seu administrador define uma lista de recursos que são mantidos em segurança porque eles estão acessíveis somente por meio do equipamento, mas você tem acesso aberto a qualquer coisa que não esteja claramente especificada na lista de recursos (por exemplo, outros sites da Internet).
- No modo *redirecionar tudo*, que é a abordagem mais segura (e limitada), todo o tráfego é redirecionado por meio do equipamento: você não pode acessar nada que não esteja na lista de recursos permitidos.
- Seu administrador pode optar por conceder a você acesso a impressoras locais e compartilhamentos de arquivos, independentemente do modo de túnel.

Se estiver tendo problemas para acessar recursos, seu administrador pode instruí-lo a fazer uma alteração na caixa de diálogo **Propriedades** da Conexão Secure Mobile Access VPN na guia **Conexões**. As opções de **Resolução de conflitos de rede** estão disponíveis somente quando seu administrador configurou você para o modo dividir túnel. Se você precisar fazer uma alteração de configuração, ela deve ser feita enquanto o Túnel de conexão está desconectado.

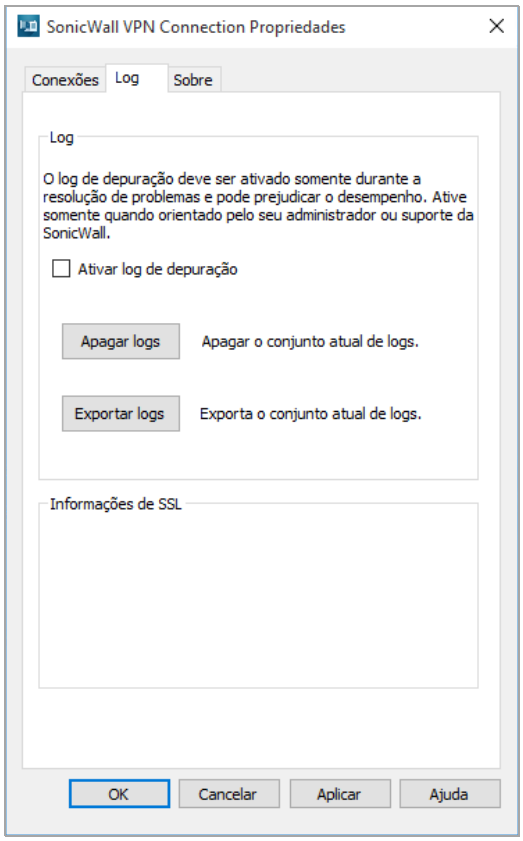
Por exemplo, você tem um recurso de host — um Servidor Web — com um endereço de `192.168.230.1`. Você está em uma viagem de negócios e a impressora que deseja usar está em uma rede local em um centro de conferências e ela usa este mesmo endereço. Você está usando um território que está configurado para o modo dividir túnel e seu administrador optou por conceder a você acesso a impressoras locais e compartilhamentos de arquivo. Para permitir que você imprima no centro de conferências, seu administrador poderá instruí-lo a abrir a caixa de diálogo **Propriedades** da Conexão Secure Mobile Access VPN, clicar na guia **Conexões** e, em seguida, clicar em **Preferir acesso a recursos da rede local** para sua sessão.

Trabalhar com logs

Você pode precisar responder à solicitação de um administrador para habilitar logs de depuração, reproduzir um problema ou baixar logs por outro motivo.

1 Para ativar o log, clique no botão **Propriedades**.

2 Clique na guia **Log**.



3 Apague o log existente clicando em **Apagar logs** e, em seguida, clique em **Aplicar**.

4 Marque a caixa de seleção para **Ativar log de depuração** e clique em **OK**. Deixe o log ser executado pelo período especificado. O log receberá um nome de acordo com a fórmula:

```
ngutil-YYYYMMDD_at_HHMMSS.txt
```

5 Quando você quiser exportar o log, retorne à guia **Configurações**, clique em **Exportar logs** e, em seguida, clique em **OK**.

Cliente Túnel de conexão para MacOS/Linux

Sobre o Túnel de conexão

O Túnel de conexão do SonicWall Secure Mobile Access com Smart Tunneling é um componente cliente da solução Secure Mobile Access VPN (Rede virtual privada), que permite o acesso seguro e autorizado a aplicativos baseados na Web e de cliente/servidor e o compartilhamento de arquivos. Esta seção descreve o Túnel de conexão para os sistemas operacionais MacOS e Linux e contém as seguintes seções:

Com o Túnel de conexão, você pode se conectar a recursos de rede que são protegidos pela Secure Mobile Access VPN e acessar os seguintes tipos de recursos:

- **Recursos cliente/servidor:** Aplicativos cliente/servidor, aplicativos de cliente "thin" e serviços de terminal.
- **Sites e aplicativos da Web:** Conteúdo online e aplicativos baseados na Web que podem ser acessados por meio de um navegador.
- **Compartilhamentos de rede:** Pastas e arquivos compartilhados e unidades mapeadas.

O Túnel de conexão nas plataformas MacOS e Linux suporta IPv6, o qual é preferido quando IPv4 e IPv6 estiverem disponíveis.

Requisitos do sistema

Este aplicativo cliente exige JVM (Java Virtual Machine) e é destinado para uso em computadores Linux de 32 bits e 64 bits e computadores PPC/IA-32 e PPC/IA-64 com base em Apple Macintosh.

Iniciar o Túnel de conexão

Para acessar os recursos de rede por meio do Túnel de conexão, sua identidade deve ser verificada primeiro. Isso garantirá que somente usuários autorizados possam acessar recursos de rede protegidos. As credenciais usadas para verificar sua identidade normalmente são compostas de um nome de usuário e uma senha ou um código de acesso.

Temas:

- Túnel de conexão no MacOS
- Túnel de conexão no Linux
- Especificar um grupo de login
- Conectar a outra VPN
- Sair do Túnel de conexão

Túnel de conexão no MacOS

Para iniciar o Túnel de conexão no MacOS:

1. No Finder, clique duas vezes em **Aplicativos** e, em seguida, clique duas vezes no ícone do Túnel de conexão. A caixa de diálogo de login do **Túnel de conexão** é exibida.
2. Na lista **Configuração**, selecione uma configuração VPN e clique em **Conectar**.

   Se não houver configurações salvas, você deve criar uma; consulte Editar configurações do Túnel de conexão para obter mais informações.
3. Se você acessar um recurso de rede que usa um certificado de servidor autoassinado ou inválido, o Túnel de conexão exibirá o certificado. Confirme que o certificado do servidor é de uma fonte confiável antes de aceitá-lo.

   NOTA: Visto que qualquer pessoa pode emitir um certificado, você deve aceitar certificados somente de fontes confiáveis, dado que as informações que você recebe podem ser inválidas. Se você tiver dúvidas se deve ou não aceitar um certificado, fale com seu administrador.
4. Na seleção do **Grupo de login**, escolha seu Grupo de login e, em seguida, clique em **OK**.
5. No campo **Nome de usuário**, insira seu nome de usuário.
6. No campo **Senha** ou **Código de acesso**, digite sua senha ou código de acesso. (As senhas podem diferenciar maiúsculas de minúsculas: certifique-se de que as teclas Caps Lock e Num Lock não estejam ativadas.)
7. Clique em **OK**. Uma mensagem na caixa de diálogo de login indica o status da conexão VPN.

   DICA: Na caixa de diálogo de login do Túnel de conexão, você pode iniciar uma conexão a uma lista.

   DICA: No diretório **Aplicativos**, você pode arrastar o ícone do Túnel de conexão até o painel de controle para um acesso mais fácil

Túnel de conexão no Linux

Para iniciar o Túnel de conexão na plataforma Linux:

1. Após o Túnel de conexão ser instalado, você pode executar `startctui` a partir de qualquer lugar. Você também pode iniciar o Túnel de conexão clicando duas vezes no ícone do Túnel de conexão na área de trabalho. A caixa de diálogo de login do **Túnel de conexão** é exibida.
2. Na lista **Configuração**, selecione uma configuração VPN e clique em **Conectar**. Se não houver configurações salvas, você deve criar uma; consulte Criar uma nova configuração para obter mais informações.
3. Se você acessar um recurso de rede que usa um certificado de servidor autoassinado ou inválido, o Túnel de conexão exibirá o certificado. Confirme que o certificado do servidor é de uma fonte confiável antes de aceitá-lo. Como qualquer pessoa pode emitir um certificado, você deve aceitar certificados somente

de fontes confiáveis. Caso contrário, as informações que recebe podem ser inválidas. Se você tiver dúvidas se deve aceitar um certificado, fale com seu administrador.

4 Na seleção do **Grupo de login**, escolha seu Grupo de login e clique em **OK**.

5 No campo **Nome de usuário**, insira seu nome de usuário.

6 No campo **Senha** ou **Código de acesso**, digite sua senha ou código de acesso. (As senhas podem diferenciar maiúsculas de minúsculas: certifique-se de que as teclas Caps Lock e Num Lock não estejam ativadas.)

7 Clique em **OK**. Uma mensagem na caixa de diálogo de login indica o status da conexão VPN.

DICA: Na caixa de diálogo de login do Túnel de conexão, você pode iniciar uma conexão com outra VPN ou grupo de login escolhendo uma configuração diferente na lista **Configuração**.

Especificar um grupo de login

O Túnel de conexão permite que você faça login em diferentes grupos de login; por exemplo, você pode alternar entre fazer login nos grupos “Vendas” e “Marketing”. Você pode precisar fornecer credenciais de autenticação diferentes para cada grupo de login.

Você deve especificar um grupo de login todas as vezes que iniciar uma conexão com sua VPN. Esta opção está disponível somente quando o Túnel de conexão estiver offline, isto é, quando não estiver conectado à sua VPN.

Para especificar o grupo de login

1 Na caixa de diálogo de login do Túnel de conexão, escolha uma **Configuração** e clique em **Editar**.

2 Na caixa de diálogo **Editar configuração**, clique em **Esquecer seleção** e escolha **Salvar**.

3 Escolha a **Configuração** salva e clique em **Conectar**.

4 Selecione o novo Grupo de login e clique em **OK**.

Conectar a outra VPN

Para especificar outra VPN para conectar, o Túnel de conexão deve estar offline (ou seja, não conectado à sua VPN – **Status: Desconectado**).

Para especificar o nome de host ou endereço IP da VPN:

1 Na caixa de diálogo de login do Túnel de conexão, clique em **Adicionar configuração**.

2 Insira um nome para a configuração no campo **Nome**.

3 No campo **Servidor**, digite o nome do host ou o endereço IP da VPN à qual deseja se conectar.

4 Clique em **OK**. A caixa de diálogo de login é exibida.

Como saber se o Túnel de conexão está em execução

Quando o Túnel de conexão está em execução e conectado à VPN, é exibida uma caixa de diálogo de status de conexão. Esta caixa de diálogo contém informações básicas de conexão, incluindo o nome da configuração que você está usando no momento e o nome de host ou endereço IP da VPN à qual você está conectado. Você pode minimizar esta caixa de diálogo em sistemas Linux. Contudo, fechar esta caixa de diálogo encerrará sua conexão de rede e fechará o Túnel de conexão.

Sair do Túnel de conexão

Para encerrar sua sessão de VPN e desconectar da rede remota, clique em **Desconectar** na caixa de login do **Túnel de conexão.**

Gerenciar configurações

Para simplificar o processo de login, você pode definir uma ou mais configurações de VPN. Se, por exemplo, você algumas vezes conectar a outro grupo de login ou VPN, pode salvar essas configurações usando nomes diferentes.

Temas:

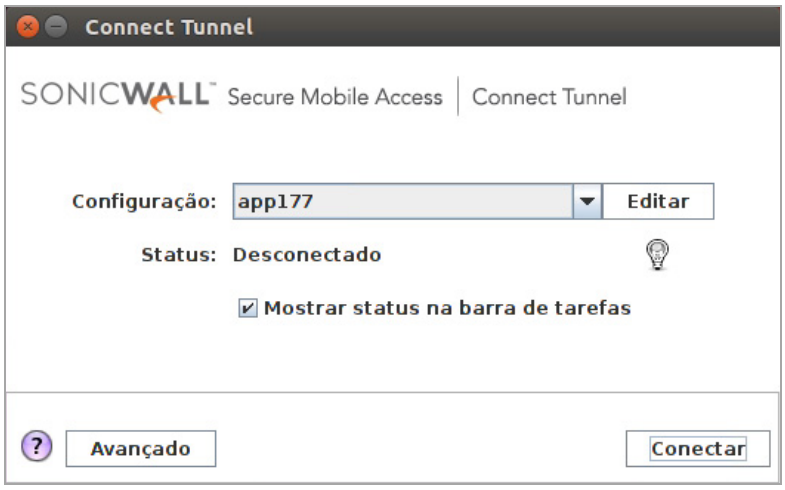
- Visualizar configurações do Túnel de conexão
- Editar configurações do Túnel de conexão
- Excluir uma configuração
- Criar uma nova configuração
- Selecionar o botão Avançado
- Opções avançadas
- Armazenamento em cache de credenciais/Detecção de rede segura

Visualizar configurações do Túnel de conexão

NOTA: O Túnel de conexão deve estar offline, ou seja, não conectado à sua VPN (**Status: Desconectado**).

Para visualizar suas configurações:

1 Na caixa de diálogo de login do Túnel de conexão, selecione a configuração na lista **Configuração**.



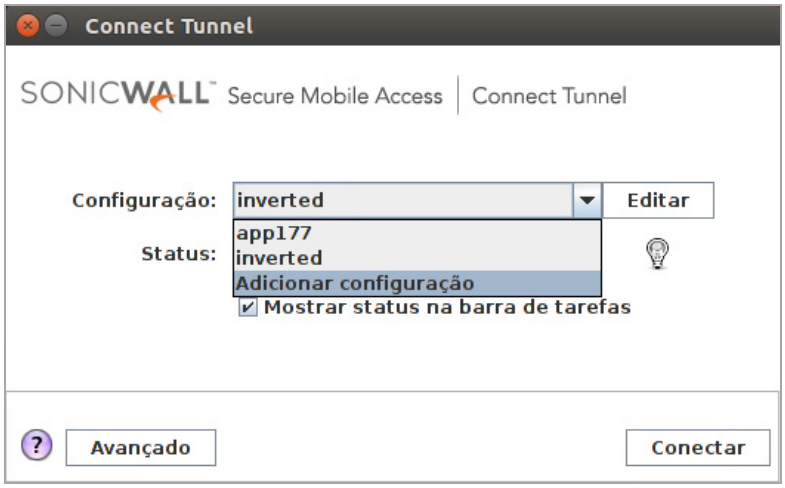
2 Clique em **Editar**. A partir daqui, você pode visualizar as suas definições de configuração após selecionar a configuração desejada.

Editar configurações do Túnel de conexão

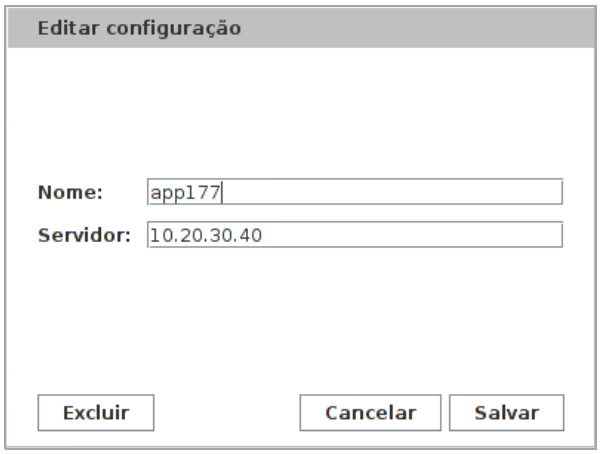
NOTA: O Túnel de conexão deve estar offline, ou seja, não conectado à sua VPN (**Status**: desconectado).

Para editar suas configurações:

1 Na caixa de diálogo de login do Túnel de conexão, selecione a configuração no menu suspenso **Configuração**.



2 Clique em **Editar** para editar a configuração. A caixa de diálogo **Editar configuração** é exibida.



3 Edite o campo **Nome** ou **Servidor**, conforme necessário.

4 Clique em **Salvar** para salvar suas alterações.

Excluir uma configuração

NOTA: O Túnel de conexão deve estar offline, ou seja, não conectado à sua VPN (**Status: Desconectado**).

Para excluir uma configuração:

1 Na caixa de diálogo de login do Túnel de conexão, selecione a configuração na lista **Configuração** e clique em **Editar**.

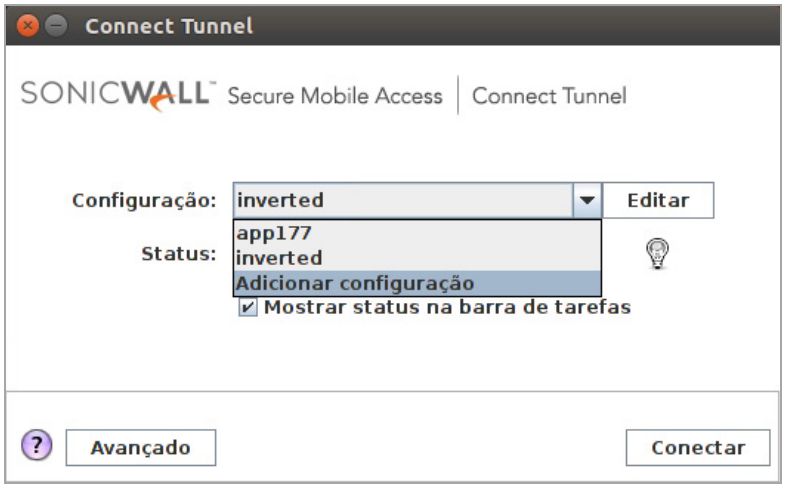
2 Clique em **Excluir** para excluir a configuração.

Criar uma nova configuração

NOTA: O Túnel de conexão deve estar offline, ou seja, não conectado à sua VPN (**Status: Desconectado**).

Para criar uma nova configuração:

1 Na caixa de diálogo de login do Túnel de conexão, selecione **Adicionar configuração** na lista **Configuração**.



2 Atribua um nome à nova configuração (por exemplo, *Conectar de casa*).

Este é o nome que você verá na lista **Configuração** quando fizer login, portanto, especifique um nome que descreva sua função da melhor forma.

3 No campo **Servidor**, insira o nome do host ou o endereço IP para a VPN.

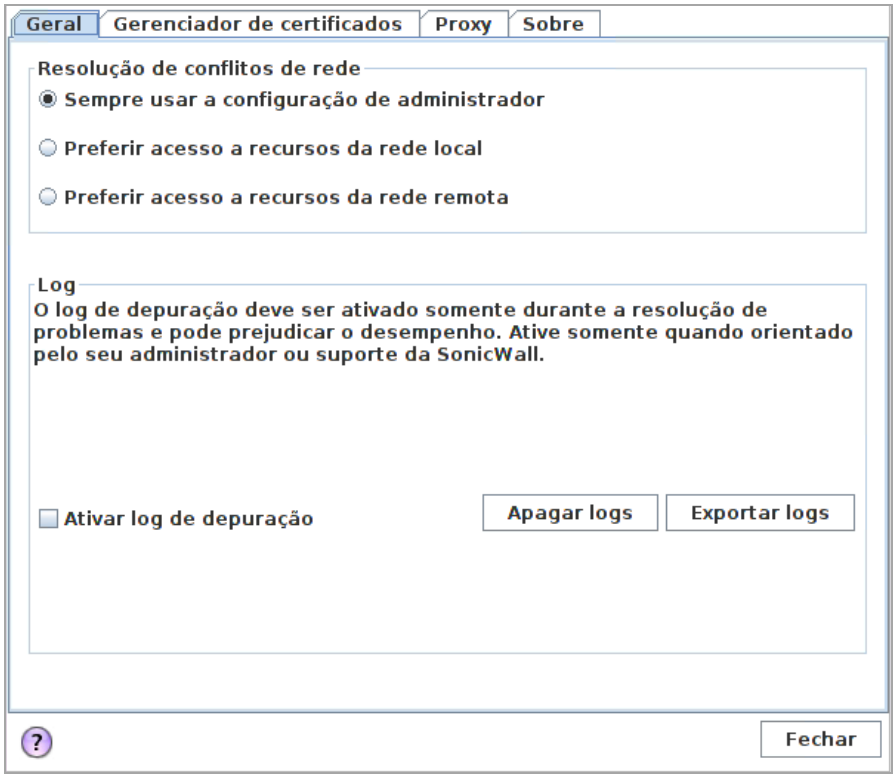
4 Clique em **Salvar** para salvar suas alterações.

Selecionar o botão Avançado

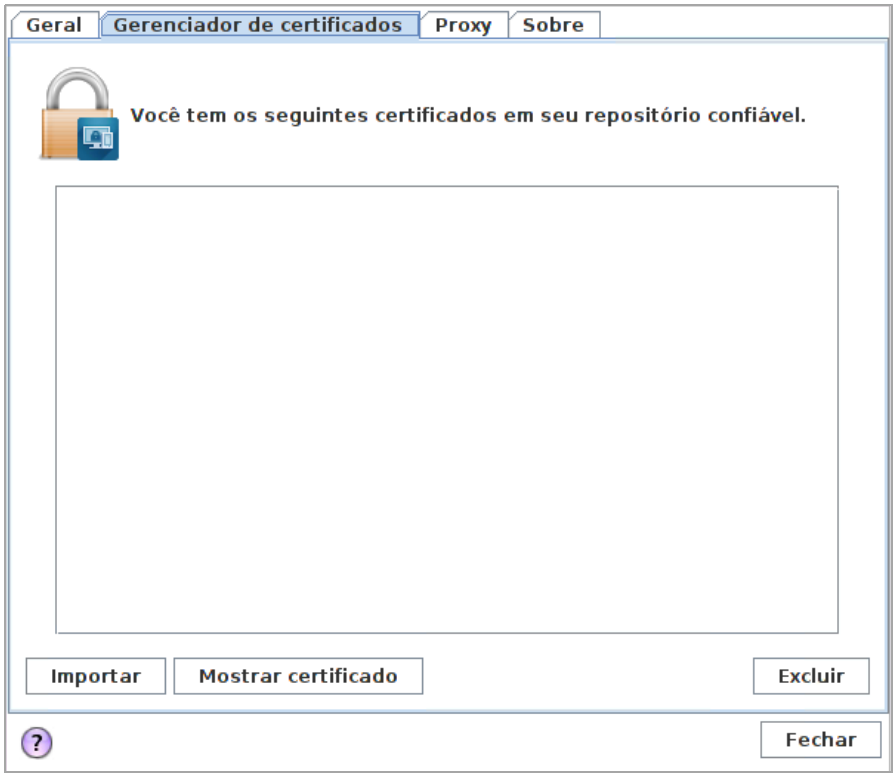
NOTA: O Túnel de conexão deve estar offline, ou seja, não conectado à sua VPN (**Status: Desconectado**).

Estas guias aparecem ao clicar em **Avançado: Geral, Gerenciador de certificados, Proxy,** e **Sobre.**

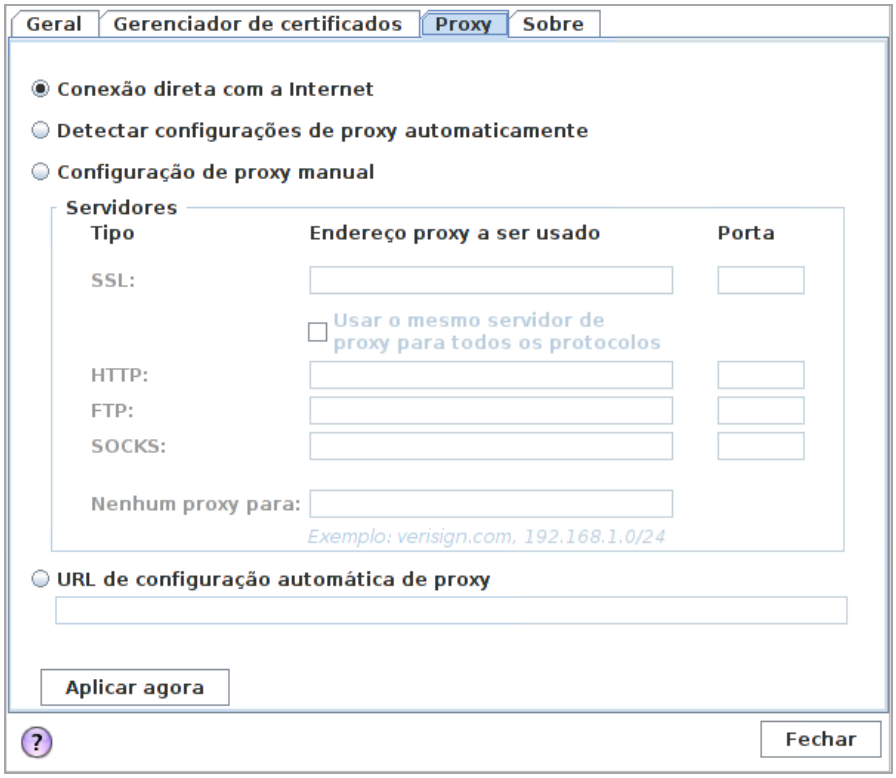
Geral



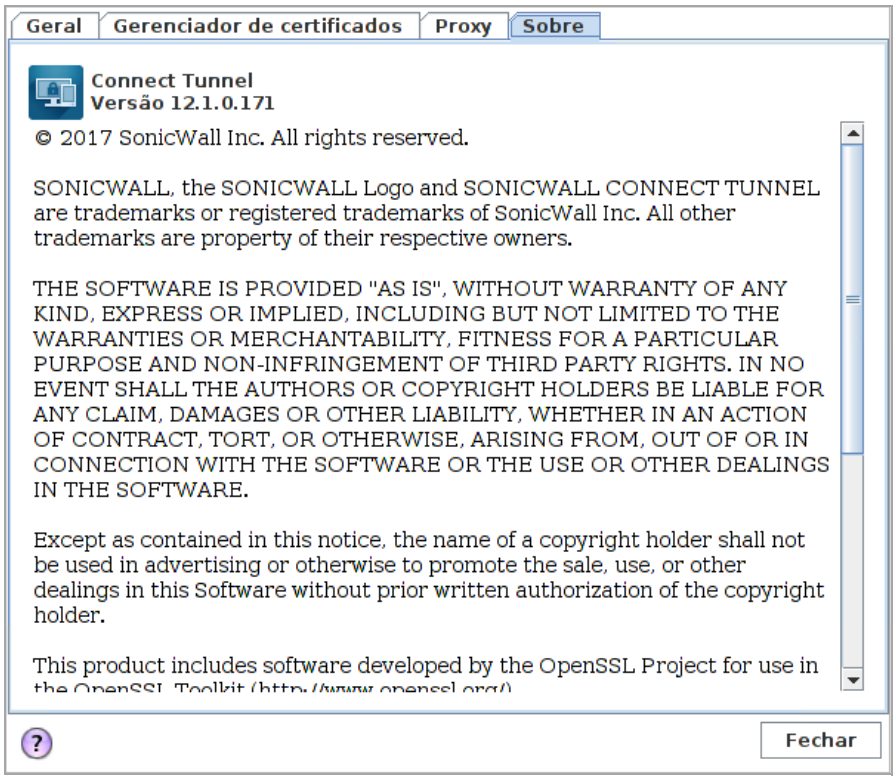
Gerenciador de certificados



Proxy


Geral
Gerenciador de certificados
Proxy
Sobre
Conexão direta com a Internet
Detectar configurações de proxy automaticamente
Configuração de proxy manual
Servidores
Tipo
Endereço proxy a ser usado
Porta
SSL:
Usar o mesmo servidor de proxy para todos os protocolos
HTTP:
FTP:
SOCKS:
Nenhum proxy para:
Exemplo: verisign.com, 192.168.1.0/24
URL de configuração automática de proxy
Aplicar agora
Fechar

Sobre


Geral
Gerenciador de certificados
Proxy
Sobre
Connect Tunnel
Versão 12.1.0.171
© 2017 SonicWall Inc. All rights reserved.
SONICWALL, the SONICWALL Logo and SONICWALL CONNECT TUNNEL are trademarks or registered trademarks of SonicWall Inc. All other trademarks are property of their respective owners.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use, or other dealings in this Software without prior written authorization of the copyright holder.
This product includes software developed by the OpenSSL Project for use in
Fechar

Opções avançadas

Quando o equipamento recebe solicitações de recursos ou acesso à Internet de clientes, elas poderão ser manipuladas de algumas formas diferentes. Seu administrador faz esta escolha de configuração no Console de Gerenciamento de Equipamentos (AMC):

- No modo Dividir túnel, somente o tráfego destinado a recursos que foram especificados no AMC é redirecionado para o equipamento. Todo o outro tráfego é enviado normalmente.

  Em outras palavras, seu administrador define uma lista de recursos que são mantidos em segurança porque estão acessíveis somente por meio do equipamento, mas você tem acesso aberto a qualquer coisa que não esteja claramente especificada na lista de recursos (por exemplo, outros sites da Internet).
- No modo redirecionar tudo, que é a abordagem mais segura (e limitada), todo o tráfego é redirecionado por meio do equipamento. Você não pode acessar nada que não esteja na lista de recursos permitidos.
- Seu administrador pode optar por conceder a você acesso a impressoras locais e compartilhamentos de arquivos, independentemente do modo de túnel.

Se estiver tendo problemas para acessar recursos, seu administrador pode instruí-lo a fazer uma alteração nas configurações **Avançadas**. As opções de **Resolução de conflitos de rede** estão disponíveis somente quando seu administrador tive sido configurado para o modo dividir túnel especificamente para esta configuração de VPN. Se você precisar fazer uma alteração de configuração, ela deve ser feita enquanto o Túnel de conexão está desconectado.

Por exemplo, digamos que você tem um recurso de host — um Servidor Web — com um endereço de `192.168.230.1`. Você está em uma viagem de negócios e a impressora que deseja usar está em uma rede local em um centro de conferências e ela usa este mesmo endereço. Você está usando um território que está configurado para o modo dividir túnel e seu administrador optou por conceder a você acesso a impressoras locais e compartilhamentos de arquivo. Para permitir que você imprima no centro de conferências, seu administrador pode instruí-lo a abrir as configurações **Avançadas** clicar em **Preferir acesso a recursos da rede local** e, em seguida, clicar em **Atualizar**.

Armazenamento em cache de credenciais/Detecção de rede segura

Se o seu administrador autorizou a política de armazenamento em cache de credenciais, você pode ativar ou desativá-la por meio da caixa de seleção **Lembrar credencial** na caixa de diálogo **Opções do Túnel de conexão**. Se estiver ativada (selecionada) no Linux, a política funciona enquanto o Túnel de conexão estiver em execução. Contudo, no MacOS, as informações são armazenadas no conjunto de chaves e persistem nas reinicializações.

Se a Detecção de rede segura estiver ativada, o Túnel de conexão é colocado em um de três estados ao conectar a um equipamento pela primeira vez:

- **Conectado**: a máquina não está em um local seguro e precisa de uma conexão VPN para acessar recursos.
- **Ocioso**: a máquina está em uma rede segura e não precisa da conexão VPN para acessar recursos.
- **Desconectar/Erro**: A conexão foi perdida e desconectada devido a eventos da rede externa (por exemplo, mudança de rede, queda do sinal do wi-fi).

Processar certificados de servidor

Algumas configurações de VPN exigem que você aceite um certificado de servidor antes de poder obter acesso a um recurso de rede protegido. Um certificado de servidor é essencialmente uma assinatura digital que confirma a identidade do servidor.

Se você acessar um recurso de rede que usa um certificado de servidor, o Túnel de conexão poderá exibir o certificado. Confirme que o certificado do servidor é de uma fonte confiável antes de aceitá-lo.

NOTA: Visto que qualquer pessoa pode emitir um certificado, você deve aceitar certificados somente de fontes confiáveis, dado que as informações que você recebe podem ser inválidas. Se você tiver dúvidas se deve ou não aceitar um certificado, fale com seu administrador.

Definir configurações do Servidor Proxy (Somente Linux)

Para usuários de Linux, alguns recursos de rede podem exigir que o tráfego passe por um servidor de proxy da Internet, que fornece acesso de sua rede local à Internet. Seu administrador determina se um servidor proxy é necessário, mas você pode ocasionalmente precisar especificar as configurações para ele.

Em vários casos, o Túnel de conexão pode detectar automaticamente suas configurações do servidor proxy de internet. Entretanto, se as configurações não puderem ser detectadas automaticamente, você deve especificá-las manualmente.

Esta seção descreve como especificar as configurações do servidor proxy de saída. Esta opção está disponível somente quando o Túnel de conexão estiver offline (ou seja, quando não estiver conectado à sua VPN) e somente na versão Linux do programa.

Para definir as configurações do servidor proxy de saída (Linux):

1. Na caixa de diálogo de login do Túnel de conexão, clique em **Avançado**.
2. Clique na guia **Proxy**.
3. Clique em uma das seguintes opções:
    a. **Conexão direta com a Internet:** permite uma conexão direta com a Internet, sem redirecionamento do servidor proxy de saída.
    b. **Detectar configurações de proxy automaticamente:** Configura o cliente para detectar e usar as configurações do servidor proxy de saída conforme definido em sua rede remota.
    c. **Configuração de proxy manual:** permite que você especifique manualmente as configurações do servidor proxy. No campo **SSL**, digite o nome do host ou o endereço IP do servidor proxy de internet. No campo **Porta**, digite o número da porta na qual o servidor está escutando. Selecione **Usar o mesmo servidor de proxy para todos os protocolos** para usar o servidor **SSL** especificado para todo o tráfego ou especificar outros servidores proxy e seus números de porta para tráfego de HTTP, FTP ou SOCKS. Como alternativa, no campo **Nenhum proxy para**, você pode especificar nomes de host ou endereços IP que não deseja que sejam redirecionados por meio de um servidor proxy.
    d. **URL de configuração automática de proxy:** Configura o cliente para recuperar um arquivo de configuração automática de proxy (`.pac`) que especifica as configurações do servidor proxy. No campo, digite o URL do servidor que hospeda o arquivo `.pac`.
4. Clique em **OK**. A caixa de diálogo de login é exibida..

Solução de problemas

Esta seção descreve como solucionar problemas básicos de cliente do Túnel de conexão. Se você estiver tendo problemas para conectar à sua VPN ou acessar recursos da rede local ou remota, veja se o seu problema é resolvido por meio do seguinte. Se o problema continuar, entre em contato com seu administrador de sistema.

Temas:

- Não é possível conectar
- Não é possível acessar os recursos ou a Internet

Não é possível conectar

Veja alguns itens a serem verificados se estiver tendo problemas para conectar à sua VPN:

- Certifique-se de que o Túnel de conexão esteja em execução e ativamente conectado à rede. Para obter mais informações, consulte Como saber se o Túnel de conexão está em execução.
- Verifique na caixa de diálogo **Propriedades do** Túnel de conexão que você está iniciando uma conexão com o nome de host ou endereço IP corretos. Para obter mais informações, consulte Iniciar o Túnel de conexão.
- Verifique na caixa de diálogo **Propriedades do** Túnel de conexão que você está iniciando uma conexão com o grupo de login correto. Para mais informações, consulte Como saber se o Túnel de conexão está em execução.
- Se estiver usando um firewall pessoal, você pode precisar configurá-lo para poder acessar sua VPN. Para fazer isso, configure o firewall para permitir tráfego para o nome de host ou endereço IP da VPN na porta 443.

Não é possível acessar os recursos ou a Internet

- Seu dispositivo pode ter sido classificado na zona de segurança incorreta.
- Seu administrador pode solicitar que você confirme a zona de segurança na qual você foi classificado. Se as zonas de segurança foram configuradas, você poderá visualizar sua zona atual pausando o ícone do Túnel de conexão na área de notificação da barra de tarefas com seu cursor.
- Quando o equipamento recebe solicitações de recursos ou acesso à Internet de clientes, elas poderão ser manipuladas de algumas formas diferentes. Seu administrador faz esta escolha de configuração no AMC:
- No modo Dividir túnel, somente o tráfego destinado a recursos que foram especificados no AMC é redirecionado para o equipamento, e todo o outro tráfego é enviado normalmente. Em outras palavras, seu administrador define uma lista de recursos que são mantidos em segurança porque estão acessíveis somente por meio do equipamento, mas você tem acesso aberto a qualquer coisa que não esteja claramente especificada na lista de recursos (por exemplo, outros sites da Internet).
- No modo redirecionar tudo, que é a abordagem mais segura (e limitada), todo o tráfego é redirecionado por meio do equipamento: você não pode acessar nada que não esteja na lista de recursos permitidos.
- Seu administrador pode optar por conceder a você acesso a impressoras locais e compartilhamentos de arquivos, independentemente do modo de túnel.

Se estiver tendo problemas em acessar recursos, seu administrador pode instruí-lo a fazer uma alteração na caixa de diálogo **Propriedades do Túnel de conexão**, na guia **Avançado**. As opções de **Resolução de conflitos de rede** estão disponíveis somente quando seu administrador configurou você para o modo dividir túnel. Se você precisar fazer uma alteração de configuração, ela deve ser feita enquanto o Túnel de conexão está desconectado.

Por exemplo, você tem um recurso de host — um Servidor Web — com um endereço de `192.168.230.1`. Você está em uma viagem de negócios e a impressora que deseja usar está em uma rede local em um centro de conferências e ela usa este mesmo endereço. Você está usando um território que está configurado para o modo dividir túnel e seu administrador optou por conceder a você acesso a impressoras locais e compartilhamentos de arquivo. Para permitir que você imprima no centro de conferências, seu administrador poderá instruí-lo a abrir a caixa de diálogo **Propriedades do Túnel de conexão**, clicar na guia **Avançado** e, em seguida, clicar em **Preferir acesso a recursos da rede local** para sua sessão.

A

Suporte SonicWall

O suporte técnico está disponível para clientes que tiverem comprado produtos da SonicWall com um contrato de manutenção válido e para clientes com versões de avaliação.

O Portal de suporte fornece ferramentas de autoajuda que você pode usar para solucionar problemas com rapidez e de forma independente, 24 horas por dia, 365 dias por ano. Acesse o portal de suporte em https://www.sonicwall.com/pt-br/support.

O Portal de suporte permite:

- Visualizar artigos da base de conhecimentos e documentação técnica
- Visualizar tutoriais em vídeo
- Acessar o MySonicWall
- Saber mais sobre os serviços profissionais da SonicWall
- Revisar informações sobre garantia e serviços de suporte da SonicWall
- Registrar-se para treinamento e certificação
- Solicitar suporte técnico ou atendimento ao cliente

Para entrar em contato com o suporte da SonicWall, visite https://www.sonicwall.com/pt-br/support/contact-support.

Sobre este documento

Legenda

AVISO: O ícone AVISO indica risco de danos ao equipamento, ferimentos ou morte.

CUIDADO: O ícone CUIDADO indica um possível dano ao hardware ou perda de dados se as instruções não forem seguidas.

IMPORTANTE, NOTA, DICA, DISPOSITIVOS MÓVEIS ou VÍDEO: Um ícone de informação indica informações de suporte.

Túnel de conexão Guia do usuário
Atualizado – Janeiro de 2018
Versão de software - 12.1
232-004180-00, Rev. A