AUTHORIZED DOCUMENTATION

Guia do Usuário do Endpoint Security Client 4.0

December 22, 2008

Novell®
ZENworks® Endpoint Security Management

4.0

www.novell.com

Informações Legais

A Novell, Inc. não faz representações ou garantias quanto ao conteúdo ou à utilização desta documentação e especificamente se isenta de quaisquer garantias de comerciabilidade expressas ou implícitas ou adequação a qualquer propósito específico. A Novell, Inc. reserva-se o direito de revisar esta publicação e fazer mudanças em seu conteúdo, a qualquer momento, sem a obrigação de notificar qualquer pessoa ou entidade sobre essas revisões ou mudanças.

Além disso, a Novell, Inc. não faz representações nem garantias com relação a qualquer software, e se isenta de quaisquer garantias de comerciabilidade expressas ou implícitas ou adequação a qualquer propósito específico. A Novell, Inc. reserva-se o direito de fazer mudanças em qualquer e em todas as partes do software Novell, a qualquer momento, sem a obrigação de notificar qualquer pessoa ou entidade sobre essas mudanças.

Quaisquer informações técnicas ou sobre produtos fornecidas de acordo com este Contrato estão sujeitas aos controles de exportação dos EUA e às leis comerciais de outros países. Você concorda em cumprir todos os regulamentos do controle de exportação e em obter as licenças ou a classificação necessárias para exportar, reexportar ou importar produtos finais. Você concorda em não exportar nem reexportar para entidades que constam nas listas de exclusão de exportação atual dos EUA ou para qualquer país embargado ou terrorista conforme especificado nas leis de exportação dos EUA. Você concorda em não usar produtos para fins proibidos relacionados a armas nucleares, biológicas e químicas ou mísseis. Consulte a página International Trade Services da Novell na Web (http://www.novell.com/info/exports/) para obter mais informações sobre como exportar softwares da Novell. A Novell não se responsabiliza pela falha em obter as aprovações necessárias para exportação.

A Novell, Inc. é titular de direitos de propriedade intelectual relativos à tecnologia incorporada no produto descrito neste documento. Especificamente e sem limitações, esses direitos de propriedade intelectual podem incluir uma ou mais das patentes dos EUA listadas na página de patentes legais da Novell na Web (http://www.novell.com/company/legal/patents/) e uma ou mais patentes adicionais ou aplicativos com patente pendente nos EUA e em outros países.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Documentação Online: Para acessar a documentação online mais recente para este e outros produtos da Novell, consulte a página de Documentação da Novell (http://www.novell.com/documentation).

Marcas registradas da Novell

Para conhecer as marcas registradas da Novell, consulte a lista de marcas registradas e marcas de serviço da Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiais de terceiros

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Índice

Sobre este guia

Este *Guia do Usuário do Novell® ZENworks® Endpoint Security Client 4.0* destina-se a informar o usuário final sobre o funcionamento do Endpoint Security Client 4.0 para Microsoft Windows* Vista* e Windows Server 2008*.

As informações deste guia estão organizadas da seguinte maneira:

Público

Esse guia pode ser enviado a todos os funcionários da empresa para ajudá-los a entender o Endpoint Security Client.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no GroupWise. Use o recurso Comentários do Usuário, localizado na parte inferior das páginas de documentação online, ou acesse o site de feedback de documentação da Novell (http://www.novell.com/documentation/feedback.html) para enviar seus comentários.

Documentação adicional

O ZENworks Endpoint Security Management é suportado por documentação adicional (nos formatos PDF e HTML), que pode ser utilizada para que você conheça e implemente o produto. Para obter mais informações, consulte o site de documentação do ZENworks Endpoint Security Management 3.5 na web (http://www.novell.com/documentation/zesm35).

Convenções da documentação

Na documentação da Novell, o símbolo de maior que (>) é usado para separar as ações de uma etapa e os itens de um caminho de referência cruzada.

Um símbolo de marca registrada (®, ™ etc.) indica uma marca registrada da Novell. Um asterisco (*) indica uma marca registrada de terceiros.

Quando for possível digitar um determinado nome de caminho com uma barra invertida em algumas plataformas ou com uma barra normal em outras, o nome do caminho será apresentado com uma barra invertida. Os usuários de plataformas que requerem barras normais, por exemplo, Linux*, devem usar essas barras conforme o necessário no software.

Introdução

1

O Novell® ZENworks® Endpoint Security Client 4.0 é uma versão cliente que suporta o Microsoft Windows Vista com Support Pack 1 executado no modo de 32 bits e o Windows Server 2008 executado no modo de 32 bits. O Endpoint Security Client 4.0 usa o ZENworks Endpoint Security Management 3.5 Server e o Console de Gerenciamento.

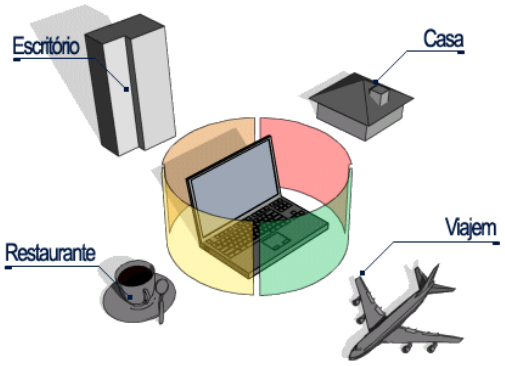
O Novell ZENworks Endpoint Security Management (ESM) tem o objetivo de proteger ativos de dados corporativos por meio de uma ferramenta de gerenciamento centralizado denominada ZENworks Security Client. O ZENworks Endpoint Security Client 4.0 é instalado nos computadores da empresa que executam o Windows Vista e o Windows Server 2008 e assegura o uso obrigatório de políticas de segurança criadas e enviadas por meio do sistema de distribuição e gerenciamento do ESM. Isso permite que empresas de grande e pequeno porte criem, implantem, apliquem e monitorem políticas de segurança de computador em computadores dentro e fora do perímetro de segurança corporativa.

As seções a seguir contêm informações adicionais:

1.1 Aplicação de Segurança em Computadores Móveis

A execução obrigatória da segurança ocorre tanto globalmente como em cada rede local. Cada local listado em uma política de segurança determina as permissões do usuário nesse ambiente de rede e as configurações de firewall que estão ativadas. As configurações de firewall determinam as portas do projeto de rede, os endereços de rede e os aplicativos que possuem acesso à rede e como o acesso é permitido.

Figura 1-1 *O ESM ajusta as configurações de segurança com base no ambiente de rede detectado*

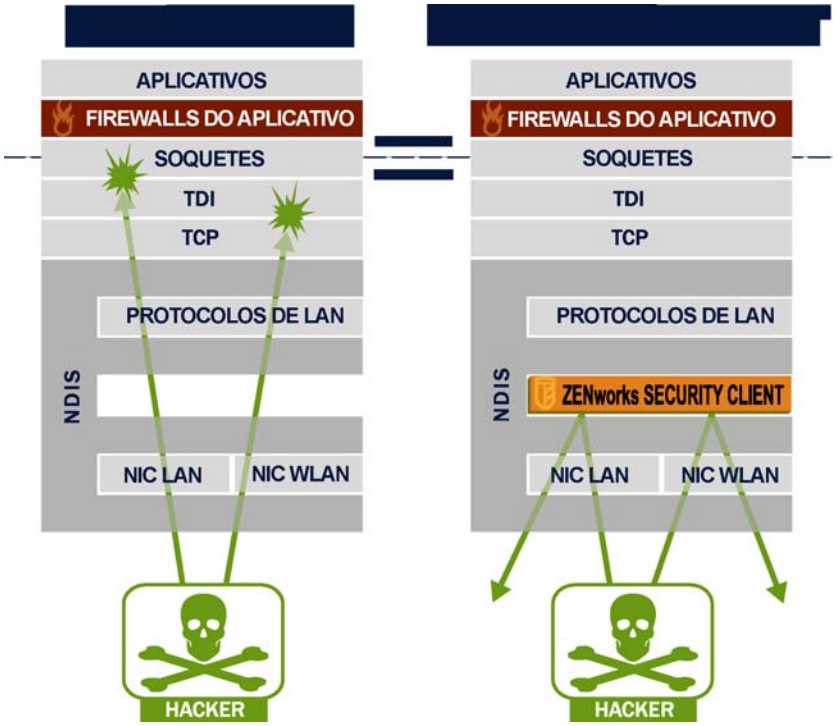


As operações normais do Endpoint Security Client 4.0 ficarão claras para o usuário depois que os ambientes de rede forem definidos. Ocasionalmente, as medidas de proteção do Endpoint Security Client 4.0 podem interromper a operação normal. Quando isso acontece, mensagens e hiperlinks são exibidos para notificar o usuário sobre a política de segurança e as etapas de proteção executadas, e para direcioná-lo às informações adicionais que o ajudarão a solucionar o problema.

1.2 Proteção de Firewall de Camada NDIS

Na proteção de dispositivos móveis, o ESM é superior às tecnologias típicas de firewall pessoal que operam no nível do aplicativo ou como um driver de gancho de firewall. O cliente de segurança do ESM é integrado ao driver de especificação de interface de driver de rede (NDIS) para cada placa de interface de rede (NIC), fornecendo proteção assim que o tráfego atinge o computador. As diferenças entre o ESM e os firewalls e os drivers de filtro da camada do aplicativo estão ilustradas na Figura 1-2, “Eficácia de um firewall de camada NDIS” na página 10.

Figura 1-2 *Eficácia de um firewall de camada NDIS*



As decisões de segurança e o desempenho do sistema são otimizados quando as implementações de segurança operam na camada mais baixa apropriada da pilha do protocolo. Com o Endpoint Security Client 4.0, o tráfego não solicitado é eliminado até atingir os níveis mais baixos da pilha do driver NDIS, graças à tecnologia de Bloqueio de Portas Adaptativo (inspeção do pacote com informações de estado). Essa abordagem oferece proteção contra ataques com base em protocolo, incluindo explorações de porta não autorizadas, ataques de Inundação SYN, entre outros.

Convém seguir todas as recomendações de manutenção e operação deste documento para garantir a proteção do ambiente de segurança do ponto de extremidade.

Visão geral do Endpoint Security Client 4.0

2

O ZENworks® Security Client protege computadores contra ataques de invasão de dados em casa, no trabalho e em viagens, utilizando a aplicação de políticas de segurança criadas pelo administrador do ESM (Endpoint Security Management) da empresa. As configurações de firewall atribuídas a locais individuais são automaticamente ajustadas quando usuários de laptops transitam entre a rede corporativa e suas redes domésticas, ou viajam e efetuam login em uma rede pública ou aberta.

Os níveis de segurança são aplicados nas diversas localidades do usuário e não exigem experiência ou conhecimentos sobre segurança de rede, configurações de portas, arquivos compartilhados ocultos ou outros detalhes técnicos. Para obter informações imediatas sobre quais locais e políticas estão disponíveis, basta passar o mouse sobre o ícone da barra de tarefas para visualizar a Dica de Ferramentas do Endpoint Security Client (consulte Figura 2-1).

Figura 2-1 *Dica de Ferramentas do Endpoint Security Client*

As seções a seguir contêm informações adicionais:

- Seção 2.1, “Terminologia do ESM” na página 11
- Seção 2.2, “Efetuando login no Endpoint Security Client 4.0” na página 12

2.1 Terminologia do ESM

Os termos a seguir são usados com freqüência nesta documentação:

Localizações: Os locais são definições simples que ajudam o usuário a identificar o ambiente de rede em que ele está inserido, fornecem configurações de segurança imediatas (definidas pelo administrador) e permitem que o usuário grave o ambiente de rede e mude as configurações de firewall aplicadas.

Cada local recebe configurações de segurança exclusivas, negando acesso a determinados hardwares e funcionalidades em ambientes de rede mais hostis e permitindo um acesso mais amplo em ambientes confiáveis. As localizações definem as seguintes informações:

- A freqüência com que o Endpoint Security Client verifica uma atualização de política neste local
- As permissões de gerenciamento de localização concedidas a um usuário
- As configurações de firewall que serão usadas neste local
- O hardware de comunicação que terá permissão para conectar

- Em que nível os usuários terão permissão para usar dispositivos de armazenamento removíveis (como mini-unidades e cartões de memória) e unidades de CD/DVD-RW
- Todos os ambientes de rede que podem ajudar a definir o local

Configurações de Firewall: As configurações de firewall controlam a conectividade de todas as portas de rede (1-65535), pacotes de rede (ICMP, ARP, etc.), endereços de rede (IP ou MAC), e os aplicativos de rede (compartilhamento de arquivo, software de mensagem instantânea, etc.) que têm permissão para obter uma conexão de rede quando a configuração é aplicada. Três configurações de firewall são incluídas como padrão no ESM e podem ser implementadas em um local. O Administrador do ESM também pode criar configurações de firewall específicas que não podem ser listadas aqui.

- **Tudo Adaptável:** Essa configuração de firewall define todas as portas de rede com informações de estado (todo tráfego de entrada na rede não solicitado é bloqueado e todo o tráfego de rede de saída é permitido). Pacotes 802.1x e ARP são permitidos, e todos os aplicativos da rede têm permissão para uma conexão de rede.
- **Tudo Aberto:** Essa configuração de firewall define todas as portas de rede como abertas (todo tráfego de rede é permitido). Todos os tipos de pacotes são permitidos. Todos os aplicativos de rede podem ter uma conexão de rede.
- **Tudo Fechado:** Essa configuração de firewall fecha todas as portas do projeto de rede e restringe todos os tipos de pacote.

Adaptadores: Consulta três adaptadores de comunicação normalmente encontrados em um ponto de extremidade:

- Adaptadores com Fio (conexões LAN)
- Adaptadores Wi-Fi (placas Wi-Fi PCMCIA e rádios Wi-Fi incorporados)

Também consulta outros hardwares de comunicação que podem estar incluídos em um computador, como infravermelho, Bluetooth*, Firewire* e portas paralelas e seriais.

Dispositivos de Armazenamento: Consulta dispositivos de armazenamento externos que podem representar uma ameaça à segurança quando dados são copiados, ou introduzidos, nesses dispositivos em um ponto de extremidade. Mini-unidades USB, placas de memória Flash e placas de memória SCSI PCMCIA, junto com as tradicionais unidades Zip*, unidades de disquete e unidades de CDR externas, bem como as unidades de CD/DVD instaladas (incluindo CD-ROM, CD-R/RW, DVD, DVD R/RW), podem ser todas bloqueadas, permitidas ou exibidas como Somente Leitura em um único local.

Ambientes de Rede: Um ambiente de rede é a coleção de serviços de rede e endereços de serviço necessários para identificar uma localização de rede.

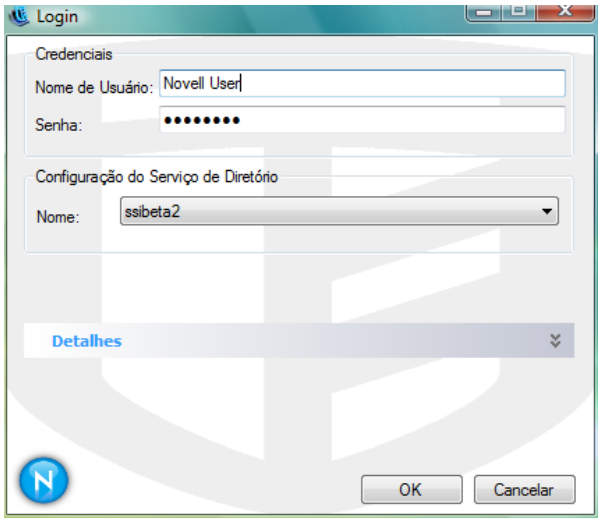
2.2 Efetuando login no Endpoint Security Client 4.0

Se você for membro do domínio do Active Directory corporativo, o Endpoint Security Client 4.0 usará seu nome de usuário e sua senha do Windows* para efetuar seu login no Serviço de Distribuição de Política (nenhuma janela popup será exibida). Se você for membro de uma árvore do Novell eDirectory, o Endpoint Security Client 4.0 solicitará seu nome de usuário e sua senha da árvore (consulte Figura 2-2).

Observa o: Com o Novell eDirectory, o usuário receberá uma janela popup de login após a instalação do Endpoint Security Client 4.0. Isso permite que você forneça seu nome de usuário e sua senha para a árvore.

Se você não for membro do domínio que hospeda o Serviço de Distribuição de Política, o Endpoint Security Client 4.0 solicitará seu nome de usuário e sua senha desse domínio (consulte Figura 2-2).

Figura 2-2 *Login do Endpoint Security Client 4.0*



Digite o seu nome de usuário e senha para o domínio ou para a árvore do eDirectory e clique em *OK*.

O Nome de Configuração de Serviço do Diretório deve corresponder aos serviços de diretório nos quais você está se autenticando. Utilize o menu suspenso para verificar se você tem mais de um serviço disponível.

Observa o: Não será necessário efetuar login no Endpoint Security Client quando ele estiver sendo executado como um programa independente. O Administrador do ESM tem um método diferente de distribuir políticas a usuários independentes.

Usando o Endpoint Security Client 4.0

3

As seções a seguir contêm informações adicionais sobre ações que você pode executar com o aplicativo de usuário final do Novell® ZENworks® Endpoint Security, o Endpoint Security Client 4.0:

Observa o: As ações listadas acima podem ser restringidas pelo administrador em qualquer localização.

3.1 Movimentando-se entre ambientes de rede

Cada rede utilizada por um usuário final pode exigir medidas de segurança diferentes. O Endpoint Security Client 4.0 fornece segurança e proteção em locais identificados por conexões de rede disponíveis. O Endpoint Security Client 4.0 detecta os parâmetros de ambiente de rede e muda para o local apropriado, aplicando os níveis de proteção necessários de acordo com a política de segurança atual.

As informações de ambiente de rede são armazenadas ou predefinidas em um local. Isso permite que o Endpoint Security Client 4.0 mude automaticamente para um local quando os parâmetros de ambiente são detectados.

- **Ambientes Armazenados:** Definido pelo usuário (consulte Seção 3.2.1, “Gravando um Ambiente de Rede” na página 16).
- **Ambiente Predefinido:** Definido pelo Administrador do ESM na empresa, utilizando uma política de segurança publicada.

Quando o usuário entra em um novo ambiente de rede, o cliente compara o ambiente detectado com todos os valores armazenados e predefinidos na política de segurança. Se uma correspondência for encontrada, o Endpoint Security Client 4.0 ativará o local atribuído. Quando o ambiente detectado não puder ser identificado como um ambiente armazenado ou predefinido, o cliente ativa o local Desconhecido padrão.

A localização Desconhecida tem estas predefinições:

- Mudar Localizações = Permitido
- Mudar Configurações de Firewall = Não permitido

- Gravar Localização = Não permitido
- Atualizar Política = Permitido
- Configurações de Firewall padrão = Tudo Aberto

Por padrão, todos os tipos de adaptador (com fio, Wi-Fi e modem) têm permissão no local Desconhecido. Isso permite que o computador interaja perifericamente com seu ambiente de rede e tente associar uma política de local, conforme descrito acima.

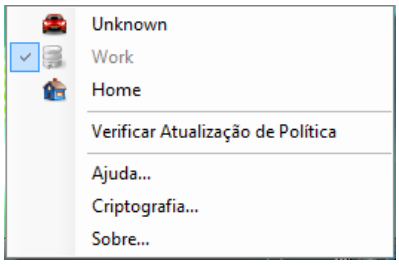
3.2 Mudando Localizações

Na inicialização, o Endpoint Security Client 4.0 muda para o local Desconhecido. Em seguida, ele tenta detectar o ambiente de rede atual e mudar o local automaticamente. Se o ambiente de rede não for reconhecido ou não tiver sido predefinido, será necessário mudar o local manualmente.

Caso não consiga executar as etapas a seguir, talvez o seu administrador do ZENworks Endpoint Security tenha impedido que você mudasse o local manualmente.

Para mudar um local:

1. Clique o botão direito do mouse no ícone do *Endpoint Security Client 4.0* na barra de tarefas para exibir um menu de opções.



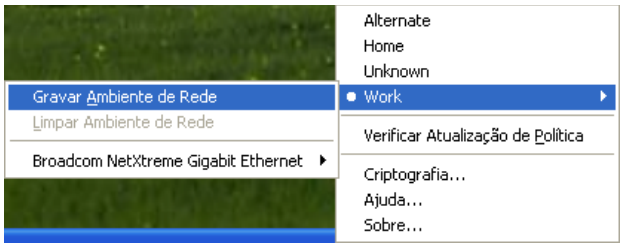
2. Clique no local apropriado.

3.2.1 Gravando um Ambiente de Rede

É necessário que um ambiente de rede esteja predefinido na política de segurança ou seja gravado pelo usuário final para que o Endpoint Security Client 4.0 possa mudar os locais automaticamente. A gravação de um ambiente de rede grava os parâmetros de rede do local atual e permite que o Endpoint Security Client 4.0 mude automaticamente para esse local na próxima vez que o usuário entrar no ambiente de rede. Quando aplicado a um ambiente de rede Wi-Fi, o Endpoint Security Client 4.0 usará o LockOn™ para o único ponto de acesso selecionado.

Para gravar um ambiente:

1. Clique o botão direito do mouse no ícone do *Endpoint Security Client 4.0* na barra de tarefas para exibir o menu.
2. Clique no local para o qual deseja mudar.
3. Clique o botão direito do mouse no ícone do *Endpoint Security Client 4.0*, passe o mouse sobre o local atual para exibir o submenu e clique em Gravar Ambiente de Rede para gravar o ambiente.



Se esse ambiente de rede tiver sido gravado em um local anterior, o Endpoint Security Client 4.0 perguntará se o usuário deseja gravar o novo local. Selecione *Sim* para gravar o ambiente no local atual e limpar o ambiente do seu local anterior, ou *Não* para deixar o ambiente no local anterior.

Observa o: A função *Gravar Ambiente de Rede* pode ser restringida pelo Administrador do ESM em qualquer local.

Ambientes de rede adicionais também podem ser gravados em um local. Por exemplo, se uma localização definida como Aeroporto fizer parte da política atual, cada aeroporto visitado pelo usuário móvel poderá ser gravado como um ambiente de rede dessa localização. Dessa forma, sempre que um usuário móvel retornar a um ambiente de aeroporto gravado, o Endpoint Security Client 4.0 mudará automaticamente para o local Aeroporto.

3.2.2 Gravando um Ambiente Wi-Fi

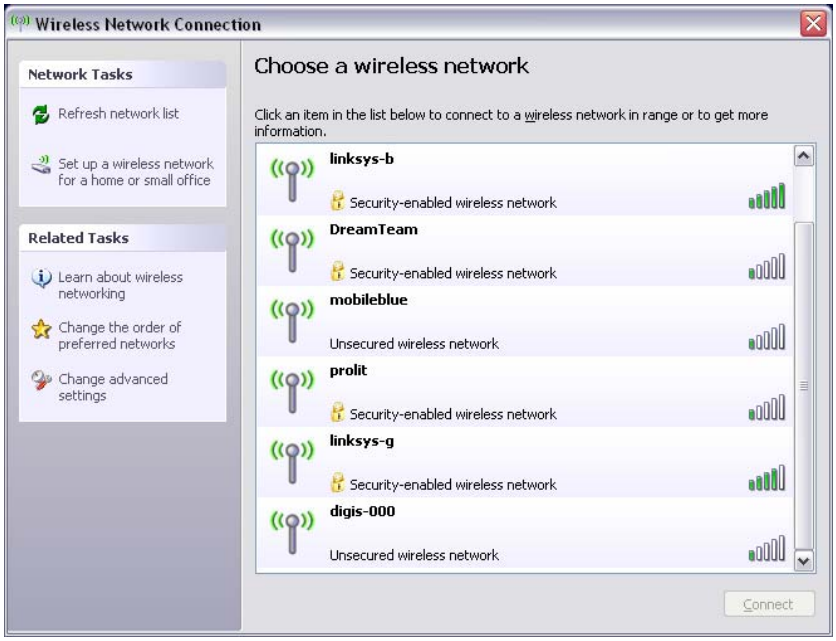
Quando um usuário ativa seu adaptador Wi-Fi, é possível que haja dúzias de pontos de acesso disponíveis. Um adaptador Wi-Fi pode rastrear um único ponto de acesso no início, mas se houver vários pontos de acesso próximos ao adaptador, o ponto de acesso associado pode ser descartado e o gerenciador de conexões sem fio pode solicitar que o adaptador mude para o ponto de acesso com o sinal mais forte. Quando isso acontece, a atividade da rede atual é paralisada, o que geralmente obriga o usuário a reenviar alguns pacotes e a reconectar a VPN à rede corporativa.

Se um ponto de acesso for gravado como parâmetro de ambiente de rede em um local, o adaptador rastreará esse ponto de acesso e não perderá a conexão até que ele saia fisicamente do alcance ponto de acesso. Ao retornar ao ponto de acesso, o adaptador será associado automaticamente a ele, o local mudará, e todos os demais pontos de acesso não ficarão mais visíveis no software de gerenciamento de conexões sem fio.

Para gravar um ambiente Wi-Fi:

1 Abra o software de gerenciamento de conexões e selecione o ponto de acesso desejado.

Observa o: O software de gerenciamento de conexões poderá ser substituído pelo local quando a política de segurança do ESM estiver definida para gerenciar sua conectividade sem fio.



2 Especifique todas as informações de segurança necessárias (WEP ou outra chave de segurança) e clique em *Conectar*.

3 Conclua as etapas descritas em Seção 3.2.1, “Gravando um Ambiente de Rede” na página 16 para gravar esse ambiente.

3.2.3 Removendo um ambiente gravado

Para remover um ambiente de rede gravado de um local:

1 Clique o botão direito do mouse no ícone do *Endpoint Security Client* na barra de tarefas para exibir o menu.

2 Mude para a localização apropriada.

3 Clique o botão direito do mouse no ícone do *Endpoint Security Client* e selecione o local atual para exibir o submenu.

4 Clique em *Limpar Ambiente de Rede* para limpar o ambiente.

Observa o: Isso limpará todos os ambientes de rede gravados nesse local.

3.3 Criptografia de Dados

Quando ativado pela política, o Endpoint Security Client 4.0 gerencia a criptografia dos arquivos colocados em um diretório específico no ponto de extremidade e colocados em dispositivos de armazenamento removíveis.

As instruções a seguir ajudarão você a usar o ZENworks Endpoint Security no ponto de extremidade.

- Seção 3.3.1, “Gerenciando Arquivos em Volumes que Não São do Sistema” na página 19
- Seção 3.3.2, “Gerenciando Arquivos no Armazenamento Removível” na página 19

3.3.1 Gerenciando Arquivos em Volumes que Não São do Sistema

Discos fixos são definidos como todas as unidades de volume que não são do sistema e estão instaladas no computador, bem como todas as partições de uma unidade de disco rígido. Cada disco fixo no ponto de extremidade tem uma pasta “Safe Harbor” (por padrão a pasta se chama `Arquivos Criptografados`) e existe em cada volume que não é do sistema ou unidade fora do diretório raiz. Todos os arquivos colocados nessa pasta serão criptografados com a chave de criptografia atual. Somente usuários autorizados no computador poderão descriptografar esses arquivos.

Ao gravar um arquivo, selecione a pasta Safe Harbor nas pastas disponíveis da unidade desejada.

3.3.2 Gerenciando Arquivos no Armazenamento Removível

Armazenamento removível é definido como qualquer dispositivo de armazenamento "conectado" ao computador. Isso inclui (entre outros): mini-unidades USB, placas de memória Flash e placas de memória PCMCIA, além das tradicionais unidades Zip, unidades de disquete e unidades de CDR externas, câmeras digitais com capacidade de armazenamento e MP3 players.

Quando o ZENworks Endpoint Security for executado, os arquivos armazenados nesses dispositivos serão criptografados à medida que forem acessados pelo sistema operacional ou pelo usuário. Os arquivos copiados no dispositivo serão criptografados imediatamente. Quando um dispositivo de armazenamento removível for conectado a um computador não gerenciado pelo sistema do ZENworks Endpoint Security, os arquivos permanecerão criptografados e não poderão ser descriptografados.

A criptografia do armazenamento removível ocorrerá quando o dispositivo for inserido (consulte “E se eu não quiser o dispositivo criptografado?” na página 20). Contudo, os arquivos adicionados a um dispositivo de armazenamento removível criptografado em outro computador não serão criptografados, e a criptografia deverá ser feita manualmente.

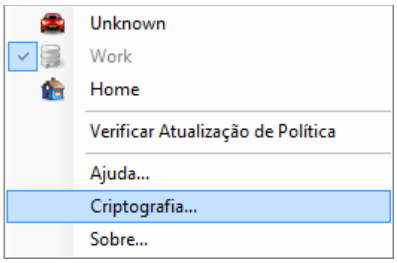
As seções a seguir contêm mais informações:

- “Criptografando arquivos” na página 19
- “E se eu não quiser o dispositivo criptografado?” na página 20
- “Usando a Pasta Arquivos Compartilhados” na página 21
- “Alterando a senha dos arquivos da pasta Arquivos Compartilhados” na página 22

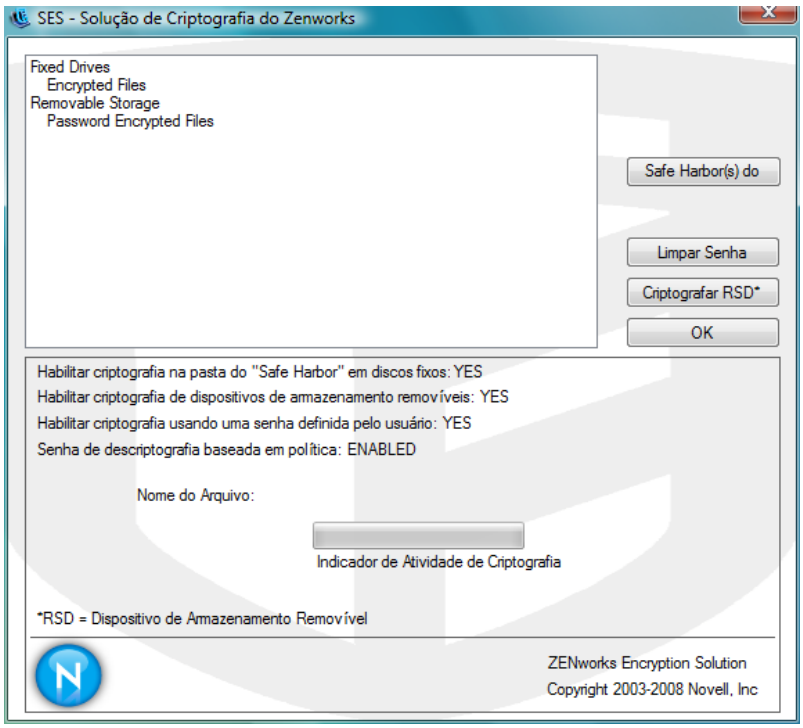
Criptografando arquivos

Para criptografar arquivos adicionados em um dispositivo de armazenamento removível:

1. Conecte o dispositivo de armazenamento à porta apropriada em seu computador.
2. Clique o botão direito do mouse no ícone do *Endpoint Security Client* na barra de tarefas.
3. Selecione *Criptografia* no menu.



4 Clique em *Criptografar RSD*. Essa operação criptografa todos os arquivos no dispositivo de armazenamento removível com a chave de criptografia atual.

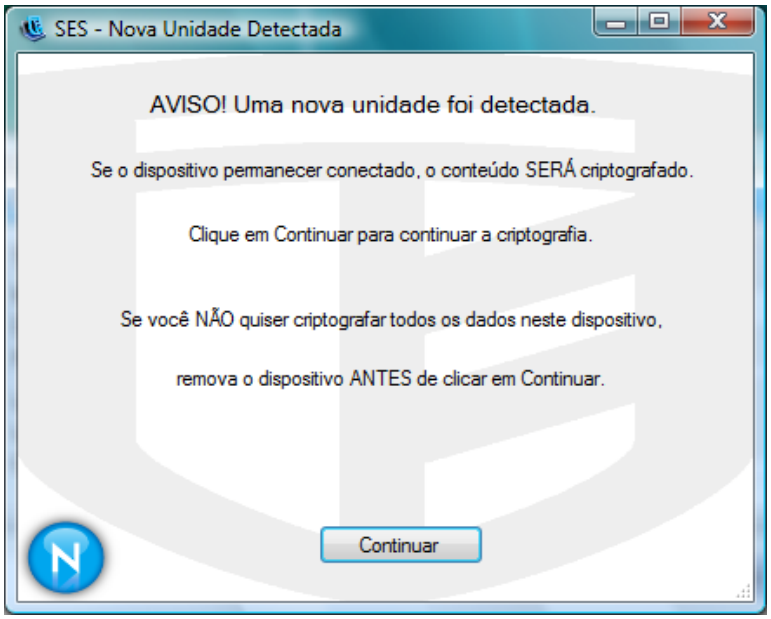


O tempo necessário para criptografar os arquivos dependerá da quantidade de dados armazenados no dispositivo.

E se eu não quiser o dispositivo criptografado?

Quando um dispositivo de armazenamento removível for inserido, o Endpoint Security Client perguntará se você deseja que a unidade seja criptografada ou se prefere removê-la e não criptografar todos os arquivos.

Figura 3-1 *Aviso de Criptografia quando um Novo Dispositivo é Inserido*



Aviso: Para impedir a criptografia, remova a unidade antes de clicar em *Continuar*. Clique em *Continuar* para criptografar a unidade ou para fechar a janela depois de removê-la.

Usando a Pasta Arquivos Compartilhados

Quando disponibilizada pela política, a pasta `Arquivos Compartilhados` é criada em todos os dispositivos de armazenamento removíveis conectados ao computador que está executando o ZENworks Endpoint Security. Os arquivos dessa pasta podem ser acessados pelos usuários de outros grupos de política, usando uma senha criada pelo usuário. Os usuários que não estiverem executando o ZENworks Endpoint Security podem acessar esses arquivos com o utilitário ZENworks File Decryption. Entre em contato com o Suporte da Novell para obter mais informações sobre o utilitário ZENworks File Decryption.

Observa o: As senhas são removidas a cada reinicialização. Uma senha será solicitada para acessar os arquivos adicionados à pasta `Arquivos Compartilhados` depois da reinicialização.

Para usar a pasta `Arquivos Compartilhados`:

1. Mova ou grave um arquivo na pasta `Arquivos Compartilhados`.
2. Quando a senha for solicitada, insira-a e confirme-a.
3. Insira uma dica para a senha.

Os usuários do ZENworks Endpoint Security não gerenciados pela política poderão acessar esses arquivos inserindo as senhas. Os usuários não gerenciados pelo ZENworks Endpoint Security precisarão do utilitário ZENworks File Decryption e da senha para acessar os arquivos.

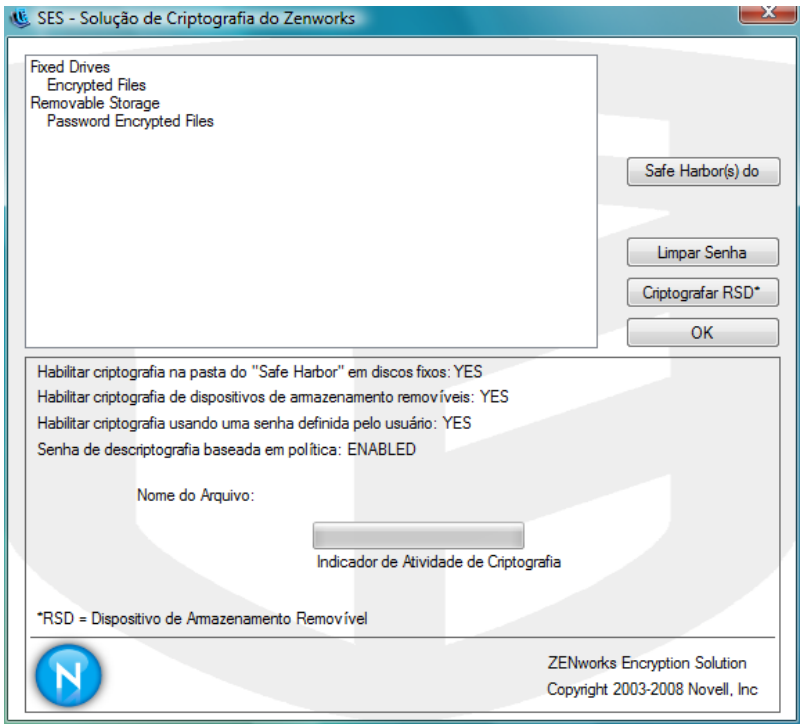
Alterando a senha dos arquivos da pasta Arquivos Compartilhados

Você pode usar o controle Criptografia para mudar senhas de arquivos adicionados à pasta `Arquivos Compartilhados`.

Observa o: Essa operação não muda nenhuma senha existente, somente as senhas para arquivos futuros.

Para mudar a senha:

1. Conecte o dispositivo de armazenamento à porta apropriada em seu computador.
2. Clique o botão direito do mouse no ícone do *Endpoint Security Client* na barra de tarefas.
3. Selecione *Criptografia* no menu.
4. Clique em *Limpar Senha*.



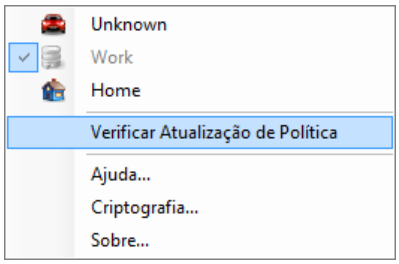
5. Arraste um arquivo para a pasta `Arquivos Compartilhados` e digite a nova senha e a dica.

A partir de agora, todos os novos arquivos adicionados à pasta usarão a nova senha de acesso.

3.4 Atualizando políticas

Novas políticas de segurança são lançadas para usuários gerenciados conforme são publicadas. O Endpoint Security Client recebe atualizações automaticamente em intervalos determinados pelo administrador do ESM. Contudo, o usuário gerenciado pode verificar as atualizações de política sempre que a política autorizar.

1. Clique o botão direito do mouse no ícone do *Endpoint Security Client* na barra de tarefas para exibir o menu.
2. Clique em *Verificar Atualização de Política*.

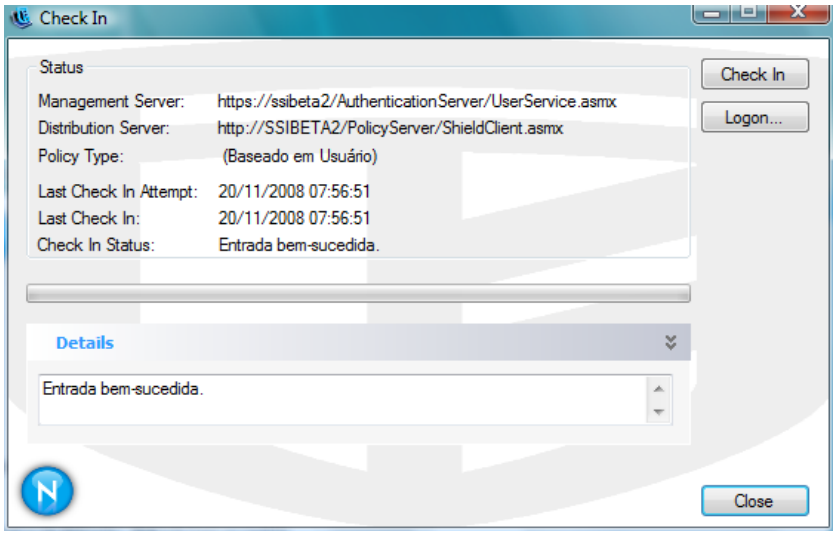


Observa o: Os recursos de atualização automática e verificação de atualização de política não ficam disponíveis quando o Endpoint Security Client é executado como um programa independente. O Administrador do ESM usa um método diferente para distribuir atualizações de política para esses usuários.

O Endpoint Security Client avisa quando a política é atualizada.

Você poderá verificar atualizações manualmente se o administrador do ZENworks Endpoint Security permitir o uso desse recurso.

1. Clique o botão direito do mouse no ícone do *Endpoint Security Client* na barra de tarefas para exibir o menu. Em seguida, clique em *Sobre* ou clique duas vezes no ícone do *Endpoint Security Client*.
2. Clique em *Registrar Entrada*.



Se você não tiver os direitos para executar um registro de entrada, o botão *Registro de Entrada* estará indisponível.

A janela Registro de Entrada exibe o estado atual do processo de registro de entrada. Ela exibe os servidores de gerenciamento e distribuição (se este for um cliente gerenciado), o tipo de política, a última tentativa de executar o registro de entrada e a última vez que ele foi concluído com êxito e o status do registro de entrada.

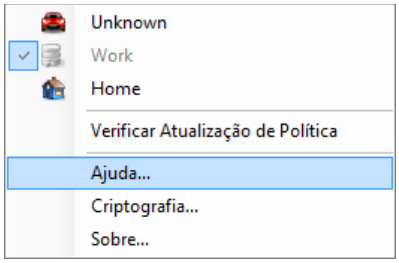
3 Para executar um registro de entrada manualmente, clique no botão *Registro de Entrada Manual*. As informações na janela Registro de Entrada são atualizadas da forma apropriada.

O botão *Login* permite que você efetue login no Serviço de Distribuição de Políticas. Para obter detalhes, consulte o Seção 2.2, “Efetuando login no Endpoint Security Client 4.0” na página 12.

3.5 Visualizando a Ajuda

1 Clique o botão direito do mouse no ícone do *Endpoint Security Client* na barra de tarefas para exibir o menu.

2 Clique em *Ajuda*.



3.6 Anulando uma senha

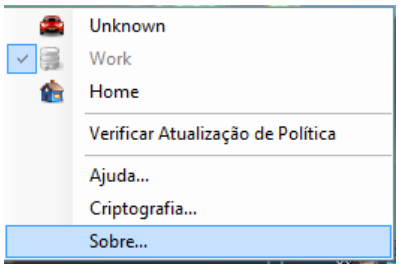
As interrupções na produtividade do usuário resultantes de restrições de conectividade, software ou thumb drives provavelmente são causadas pela política de segurança imposta pelo Endpoint Security Client 4.0. A mudança de local ou as configurações de firewall normalmente anulam essas restrições e restauram a funcionalidade interrompida. Contudo, em alguns casos, a restrição pode ser implementada de forma a afetar todos os locais e configurações de firewall. Quando isso ocorre, é necessário cancelar temporariamente as restrições para permitir a produtividade.

O Endpoint Security Client 4.0 possui um recurso chamado Substituição de Senha. Esse recurso desabilita temporariamente a política de segurança atual para permitir a execução da atividade necessária. O Administrador de Segurança só distribuirá uma chave de senha de uso único quando necessário e deverá ser informado sobre quaisquer problemas ocorridos com uma política de segurança. Depois que o tempo limite da chave de senha expirar (definido pelo administrador), a política de segurança que protege o ponto de extremidade será restaurada. A reinicialização do ponto de extremidade também restaura as configurações de segurança.

Para ativar a substituição de senha:

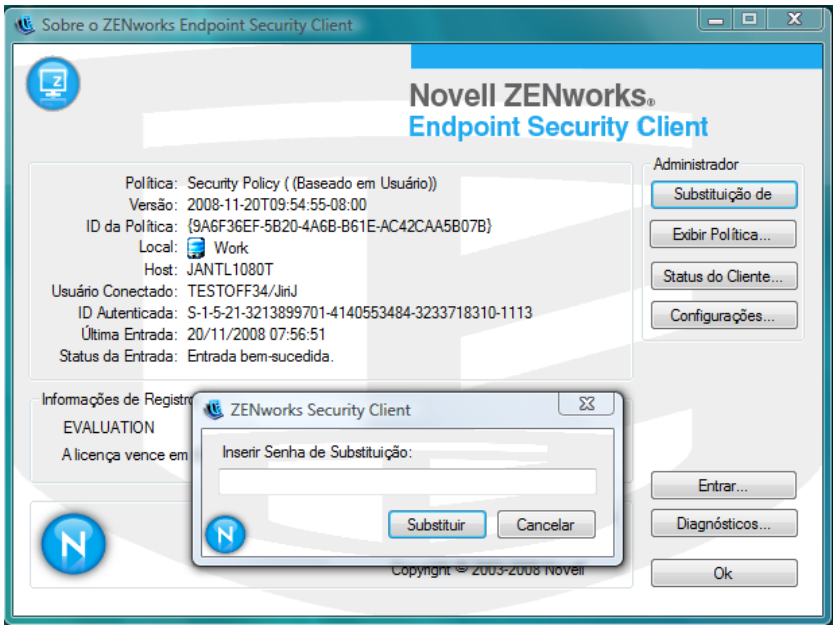
1 Entre em contato com o Administrador do ESM de sua empresa para obter a chave de senha

2 Clique o botão direito do mouse no ícone do *Endpoint Security Client* na barra de tarefas para exibir o menu. Em seguida, clique em *Sobre* ou clique duas vezes no ícone do *Endpoint Security Client*.



3 Clique em *Substituição de Senha* para exibir a janela de senha.

Observa o: Se o botão *Substituição de Senha* não for exibido nessa tela, isso significa que a sua política atual não possui uma substituição de senha.



4 Digite a chave de senha fornecida pelo Administrador do ZENworks Endpoint Security.

5 Clique em *OK*. A política atual será substituída por uma padrão, a política Tudo Aberto pelo tempo designado.

Clicar em *Carregar Política* (que substitui o botão *Substituição de Senha*) na janela *Sobre*, restaura a política anterior. Se o administrador tiver atualizado a política para solucionar problemas existentes, você poderá usar a opção *Verificar Atualização de Política* para fazer download da nova política imediatamente.

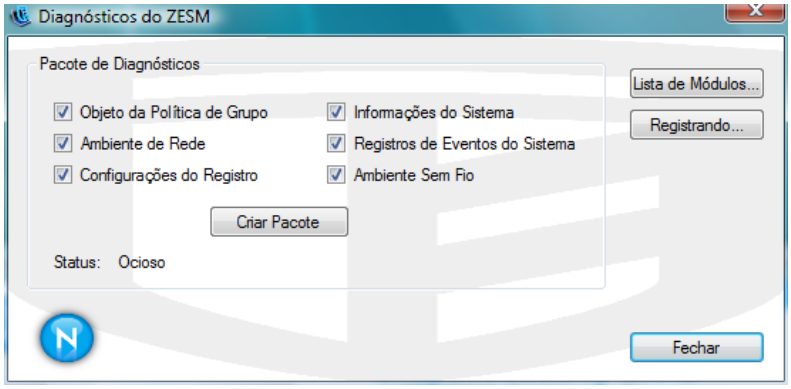
Aviso: Os serviços de criptografia não são substituídos.

3.7 Diagnóstico

A Novell fornece ferramentas de diagnóstico para permitir que o administrador solucione problemas do Endpoint Security Client. Seu administrador do ZENworks Security Client orientará você no processo de diagnóstico. Entre em contato com o Suporte da Novell se tiver mais perguntas.

Você será solicitado a fornecer um pacote de diagnósticos. O seu administrador do ZENworks Endpoint Security o informará sobre o que incluir no pacote. Para criar um pacote de diagnósticos:

1. Clique o botão direito do mouse no ícone do *Endpoint Security Client* na barra de tarefas para exibir o menu. Em seguida, clique em *Sobre* ou clique duas vezes no ícone do *Endpoint Security Client*.
2. Clique no botão *Diagnósticos*.



3. Marque tudo no painel Pacote de Diagnósticos ou apenas os itens que o seu administrador do ZENworks Endpoint Security solicitar, e clique em *Criar Pacote*.

   O cliente do ZENworks Endpoint Security cria um arquivo `zesmdiagnostics*.enc` na sua área de trabalho. Você poderá enviar esse arquivo para o administrador do ZENworks Endpoint Security.