



Deep Freeze

ADVANCED System Integrity

Guia do Usuário



Last modified: Junho, 2015

© 1999 - 2015 Faronics Corporation. Todos os direitos reservados. Faronics, Deep Freeze, Faronics Core, Faronics Anti-Virus, Anti-Executable, Faronics Device Filter, Faronics Power Save, Faronics Insight, Faronics System Profiler, and WINSelect são marcas comerciais ou registradas da Faronics Corporation. Todos os outros nomes de empresas e produtos são marcas comerciais de seus respectivos proprietários.



Contents

Prefácio	7
Informações importantes	8
Sobre a Faronics	8
Documentação do produto	8
Suporte técnico	9
Informações de contato	9
Introdução	11
Visão geral do Deep Freeze	12
Requisitos de sistema	13
Arquivos do Deep Freeze Enterprise	14
Instalando o Deep Freeze	15
Visão geral da instalação	16
Instalando o Administrador de configuração do Deep Freeze e o Console corporativo	16
Customization Code	21
Reinicializando o Customization Code	21
Modo de ATUALIZAÇÃO	21
Senhas para uso único	23
Utilizando o administrador de configuração Deep Freeze	25
Acessando o administrador de configuração	26
Barra de ferramentas e menus	26
Guia Senhas	29
Guia Unidades	30
Unidades congeladas	30
ThawSpace	31
ThawSpace existente	32
Sempre descongelar discos rígidos externos	33
Guia Tarefas da estação de trabalho	35
Windows Update	36
Reiniciar	39
Desligar	40
Tempo de inatividade	41
Arquivo de lote	43
Período descongelado	45
Guia Windows Update	48
Guia Arquivo de lote	50
Guia Opções avançadas	52
Rede	52
Opções avançadas	53
Modo Furtivo	55
Licença	55
Criando o Programa de Instalação de Estação de Trabalho e a Seed da estação de trabalho	56
Usando o Console corporativo do Deep Freeze	59



Configuração do Deep Freeze 60	
Aplicando a Configuração do Deep Freeze	60
Editando a configuração do Deep Freeze	60
Excluindo a configuração do Deep Freeze	61
Exportando a configuração do Deep Freeze	61
Console corporativo do Deep Freeze	62
Iniciando o Console corporativo	62
Ativando o Console corporativo	62
Ícones de status	63
Exibir colunas	64
Seleção com base no status	65
Gerenciando a comunicação entre o Console e as estações de trabalho	66
Configurando o serviço local	66
Editando ou removendo uma conexão de serviço local	68
Consoles remotos	69
Configurando conexões ativadas por controle remoto	69
Conectando-se a um console remoto	70
Gerenciando o Deep Freeze com o Console	71
Atualizando o software Deep Freeze	72
Enviando mensagens a computadores	72
Destino instalando o Deep Freeze	72
Atualizando um arquivo de configuração do Deep Freeze	72
Executar Windows Update	73
Formatar ThawSpace	73
Licenciamento	75
Agendando tarefas do Deep Freeze	78
atribuindo computadores a tarefas agendadas	81
Executando uma tarefa imediatamente	82
Excluindo uma tarefa	82
Propriedades de tarefas agendadas	82
Gerenciando Rede e grupos	83
Adicionando um grupo	83
Construindo uma estrutura de grupo definida pelo usuário	85
Importando grupos do Active Directory	86
Histórico	87
Adicionando computadores a um grupo	88
Configurar ações personalizadas	90
Controlar com RDC	90
Execução remota	91
Enviar por push e instalar arquivo MSI	92
Excluindo, importando e exportando ações personalizadas	92
Enviar por push e iniciar	93
Inicialização remota	94
Personalizador de console	96
Desligamento do Console corporativo do Deep Freeze	98
Instalação do Deep Freeze na estação de trabalho	99
Instalação ou desinstalação assistida	99
Desinstalando o Deep Freeze na estação de trabalho via Console	100
Instalação ou desinstalação em segundo plano	101
Exemplo de linha de comando	101
Instalação ou desinstalação sem segundo plano usando um atalho	102



Instalação pela rede em vários computadores.	102
Instalando sobre versões existentes do Deep Freeze	102
Instalando usando processamento de imagem	103
Instalação de destino.	104
Verificar atualizações.	105
Gerenciando computadores Deep Freeze	107
Tela de logon	108
Iniciando o Deep Freeze em dispositivos com tela sensível ao toque	108
Guia Status	109
Status na próxima inicialização	109
Clonar	109
Licença	110
Guia Senha	111
Guia Rede	112
Guia ThawSpace.	113
Instalações, alterações e remoções permanentes de softwares.	114
Gerenciando o Anti-Virus	115
Visão geral do Anti-Virus	116
Configuração do Anti-Virus.	117
Criando a configuração do Anti-Virus	117
Aplicando a configuração do Anti-Virus.	142
Editando as configurações Anti-Virus	143
Excluindo a configuração do Anti-Virus.	143
Usando o Faronics Anti-Virus no Console corporativo.	144
Comandos Anti-Virus	144
Programação de tarefas Anti-Virus	152
Usando o Anti-Virus na estação de trabalho	153
Iniciando o Anti-Virus na estação de trabalho	153
Verificando a estação de trabalho	154
Verificando um arquivo ou pasta através do clique com o botão direito	156
Visualizar histórico de verificação	156
Visualizar e executar ação em arquivos em quarentena	157
Atualizando definições do Anti-Virus na estação de trabalho	158
Gerenciando o Anti-Virus na estação de trabalho através da bandeja do sistema	159
Verificar atualizações do Anti-Virus	160
Atualizar o Faronics Anti-Virus	161
Desinstalar o Anti-Virus do Console corporativo	162
Desativar o Faronics Anti-Virus no Console corporativo	163
Controle de linha de comando do Deep Freeze	165
Controle de linha de comando do Deep Freeze (DFC.EXE)	166
Valores de retorno do DFC	166
Sintaxe da linha de comando do Deep Freeze.	167
Sintaxe da linha de comando do Faronics Anti-Virus	170
Apêndice A Portas e protocolos	171
Apêndice B Exemplos de rede	173



Exemplo1 - Sub-rede única 174	
Exemplo 2 - Várias sub-redes, um serviço local.	176
Exemplo 3 - Várias portas, Console acessado remotamente	178
Exemplo 4 - Múltiplas sub-redes, múltiplos serviços locais	179
Apêndice C Solução de problemas para uma conexão de console remoto	181
Sem clientes no console	181
A porta está em Erro de uso ao iniciar o Console	182
Apêndice D Criando um Console corporativo personalizado do Deep Freeze	183
Apêndice E Arquivos de ação do Deep Freeze - Exemplo RDC	187
Arquivos de ação do Deep Freeze	187
Exemplo de arquivo de ação	187
Estrutura do arquivo de ação do Deep Freeze	189
Parâmetros do console	191



Prefácio

Este guia do usuário explica como instalar, configurar e utilizar o Deep Freeze Corporativo.

Tópicos

Informações importantes

Suporte técnico



Informações importantes

Esta seção contém informações importantes sobre seu produto Faronics.

Sobre a Faronics

A Faronics fornece soluções líderes de mercado que ajudam a gerenciar, simplificar e proteger os mais complexos ambientes de TI. Nossos produtos garantem 100% de disponibilidade de máquina e têm impactado significativamente a vida cotidiana de milhares de profissionais da área de tecnologia da informação. Alimentada por um foco centrado no mercado, as inovações tecnológicas da Faronics beneficiam instituições de ensino, instalações de centros de saúde, bibliotecas, organizações governamentais e corporações.

Documentação do produto

Os seguintes documentos formam o conjunto de documentação do Deep Freeze Enterprise:

- *Deep Freeze Enterprise Guia do usuário* — é o documento que você está lendo. Este documento explica como usar o produto.
- *Deep Freeze Enterprise Notas da versão* — esse documento lista os novos recursos, problemas conhecidos e problemas corrigidos.



Suporte técnico

Foram realizados todos os esforços para que este software fosse projetado visando a facilidade de uso e a eliminação de falhas. Se você encontrar algum problema, entre em contato com a equipe de suporte técnico.

E-mail: support@faronics.com

Telefone: 800-943-6422 ou +1-604-637-3333

Horas: das 7:00 às 17:00 (Hora do Pacífico)

Informações de contato

- Site: www.faronics.com
- E-mail: sales@faronics.com
- Telefone: 800-943-6422 ou +1-604-637-3333
- Fax: 800-943-6488 ou +1-604-637-8188
- Horas: das 7:00 às 17:00 (Hora do Pacífico)

Endereço:

Faronics Technologies USA Inc.
100, W. San Fernando Street, Suite 465
San Jose, CA, 95113
EUA

Faronics Corporation (matriz)
609 Granville Street, Suite 1400
Vancouver, BC V7Y 1G5
Canadá

Faronics Corporation (Europa)
Venture House, 2 Arlington Square, Downshire Way
Bracknell, RG12 1WA, Inglaterra





Introdução



O Deep Freeze protege os computadores que estão definidos para iniciar do disco rígido. Configure o CMOS para iniciar somente do disco rígido. O CMOS deve ser protegido por senha para impedir alterações não autorizadas. O Deep Freeze protege o Registro mestre de inicialização (MBR) quando o computador é Congelado.

Tópicos

Visão geral do Deep Freeze

Requisitos de sistema



Visão geral do Deep Freeze

O Faronics Deep Freeze ajuda a eliminar problemas de danos ao computador e paralisações no sistema, tornando as configurações do computador indestrutíveis. Uma vez instalado o Deep Freeze em um computador, quaisquer alterações feitas no computador — independentemente de ter sido feita involuntariamente ou com más intenções — jamais serão permanentes. O Deep Freeze fornece imunidade imediata para muitos dos problemas que assolam os computadores nos dias atuais — flutuações inevitáveis de configuração, desconfiguração acidental do sistema, atividade de software malicioso e degradação não intencional do sistema.

O Faronics Anti-Vírus agora pode ser gerenciado usando-se o Deep Freeze Enterprise (uma licença separada é necessária para o Faronics Anti-Vírus). O Faronics Anti-Vírus oferece proteção contra ameaças à segurança sem reduzir o desempenho do computador com longas verificações e uso de memória. Criado com tecnologia de próxima geração, o Faronics Anti-Virus oferece um poderoso antivírus, anti-rootkit e antispyware em um só software. Ele protege você contra as ameaças de malware altamente complexas de hoje, ao mesmo tempo proporcionando uma integração perfeita com o Deep Freeze.

A integração com o Deep Freeze com Faronics anti-virus assegura sua proteção e está atualizado da maneira mais simples possível, fornecendo recursos de implantação e gerenciamento através do Console Corporativo do Deep Freeze. Projetado para funcionar em conjunto perfeitamente, o Faronics Anti-Virus é atualizado mesmo enquanto as estações de trabalho estão congeladas, oferecendo o sistema de proteção mais abrangente.



Requisitos de sistema

- O Deep Freeze e o Faronics Anti-Virus têm suporte nos sistemas:
 - XP, Vista, Windows 7, Windows 8.1, Server 2003, 2008 e 2012
 - Windows 7 e 8 incorporado
 - O Deep Freeze requer que 10% do disco rígido seja deixado como espaço livre
 - As versões de 32 e 64 bit do Windows têm suporte
 - O Windows XP (32 e 64 bits) deve ter o Service Pack 2 ou posterior instalado
- A Faronics recomenda um mínimo de 256 MB de memória de sistema nos sistemas protegidos
- O Administrador de configuração do Deep Freeze e o Console corporativo têm suporte nos sistemas:
 - XP, Vista, Windows 7, Windows 8.1, Server 2003, 2008 e 2012
 - as versões de 32 e 64 bits são suportadas
 - O Windows XP (32 e 64 bits) deve ter o Service Pack 2 ou posterior instalado



Arquivos do Deep Freeze Enterprise

O Deep Freeze usa diferentes ícones coloridos para representar seus componentes. Os arquivos identificados por um ícone vermelho devem geralmente ser instalados somente em um computador administrativo.

Ícone	Definição
	Arquivo de instalação do Administrador de configuração do Deep Freeze Enterprise e do Console corporativo.
	O aplicativo Administrador de configuração é utilizado para criar arquivos de programa de instalação personalizados e pré-configurados para o computador e Seeds da estação de trabalho.
	O aplicativo de Console corporativo é utilizado para implantar, monitorar, gerenciar e manter de maneira centralizada as instalações do Deep Freeze.
	Um arquivo de instalação personalizado da estação de trabalho do Deep Freeze é criado no Administrador de configuração e implantado nas estações de trabalho da empresa. Este arquivo inclui a Seed da estação de trabalho. Se o arquivo de instalação da estação de trabalho do Deep Freeze for instalado, não será necessário instalar a Seed da estação de trabalho separadamente.
	A Seed da estação de trabalho permite a comunicação perfeita entre o Console corporativo e os computadores em uma rede. Quando a Seed da estação de trabalho é instalada em um computador, este passa a ser visível no Console corporativo. Uma vez que um computador fica visível no Console corporativo, diversas ações podem ser executadas remotamente sobre este computador, tais como reinicialização, desligamento ou despertar na LAN. O Deep Freeze também pode ser instalado remotamente em computadores visíveis, permitindo assim que ações relacionadas ao Deep Freeze sejam executadas em computadores remotos.



Instalando o Deep Freeze

Este capítulo descreve o processo de instalação do Deep Freeze.

Tópicos

[Visão geral da instalação](#)

[Customization Code](#)

[Senhas para uso único](#)



Visão geral da instalação

Instalando o Administrador de configuração do Deep Freeze e o Console corporativo

O Administrador de configuração destina-se a ser instalado somente no computador usado para administrar o Deep Freeze. O Administrador de configuração é usado para criar arquivos de instalação personalizados do Deep Freeze e Seeds da estação de trabalho. O Console corporativo do Deep Freeze é instalado automaticamente com o Administrador de configuração do Deep Freeze.



Se você estiver usando o Deep Freeze 6.5 (ou superior), você tem a opção de atualizar automaticamente o Console corporativo, o Administrador de configuração, e os arquivos de instalação/configuração do Deep Freeze (na pasta Instalar Programas) enquanto instala o Deep Freeze 8.1 (ou superior).

Execute as seguintes etapas para instalar o Administrador de configuração:

1. Clique duas vezes no arquivo *DFEnt.exe* para começar o processo de instalação. A seguinte tela será exibida:



2. Clique em *Avançar*. Leia e aceite o contrato de licença. Clique em *Avançar*.



Chave de licença do Deep Freeze Corporativo

Chave de licença

Usar versão de avaliação

[Comprar agora](#)

<Voltar Avançar > Cancelar

3. Insira a chave de licença no campo *Chave de licença* ou marque a caixa de seleção *Usar avaliação* para instalar no modo de Avaliação. Clique em *Avançar*.

Contrato de licença de usuário final

Licença do Deep Freeze Enterprise

Faronics Corporation
Copyright 1999 - 2014 Todos os direitos reservados.

Contrato de licença mestre

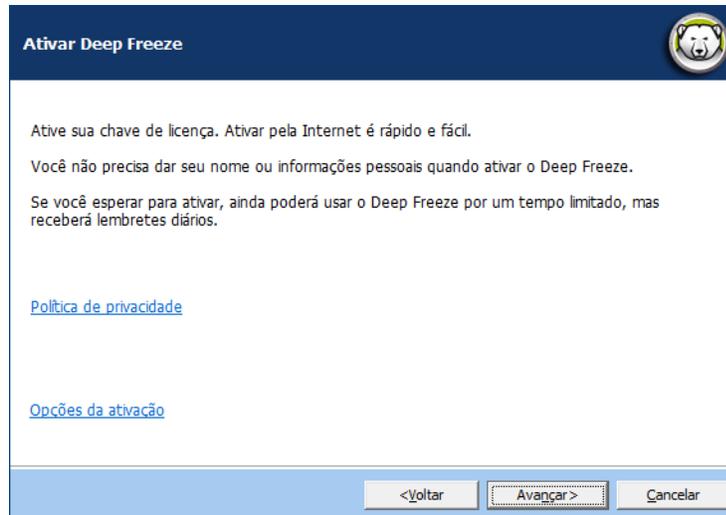
LEIA COM ATENÇÃO! Este é um contrato legal entre você (seja um indivíduo ou uma única entidade) e a Faronics Corporation ("Faronics"). Ele diz respeito ao Produto identificado abaixo, incluindo a versão do código de objeto do software do produto.

CASO NÃO CONCORDE COM OS TERMOS DESTES CONTRATO, não use o Produto, pois fazê-lo violaria leis nacionais e internacionais de direitos autorais e propriedade intelectual. Em vez disso, destrua o software ou contate-nos para providenciar a destinação adequada.

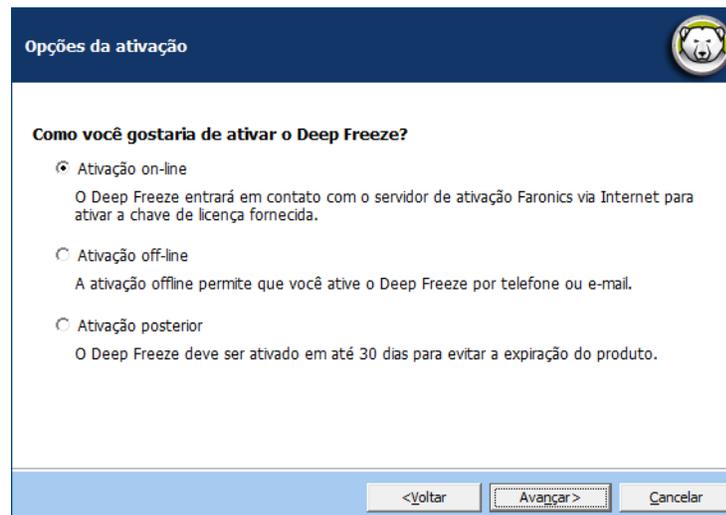
Aceito os termos do Contrato de licença.
 Não aceito os termos do Contrato de licença.

<Voltar Avançar > Cancelar

4. Insira a chave de licença no campo *Chave de licença* ou marque a caixa de seleção *Usar avaliação* para instalar no modo de Avaliação. Clique em *Avançar*.
5. Clique em *Avançar* para exibir opções de ativação. Clique em *Avançar* novamente para ativar a Licença do Deep Freeze via Internet. O computador deve estar conectado à Internet para Ativação online. A Licença Deep Freeze deve ser ativada em 30 dias após a instalação, caso isso não ocorra, você receberá lembretes constantes para ativar o produto. Durante a ativação, a Licença do Deep Freeze é autenticada na Faronics.



6. Alternativamente, clique em *Opções de ativação*. Três opções estão disponíveis:



- Selecione *Ativação online* para ativar a Licença do Deep Freeze online. Esta opção é a mesma da etapa 4. Clique em *Avançar* depois de selecionar esta opção. O Deep Freeze é ativado online clicando em *Avançar*.
 - Selecione *Ativação offline*. Esta opção permite ativar por telefone ou e-mail. Clique em *Avançar* após a ativação. A tela *Ativação offline* é exibida.
 - Selecione *Ativação posterior*. Esta opção permite ativar depois.
7. Se você tiver selecionado *Ativar offline*, envie a chave de licença e ID da instalação para o Suporte de Ativação Faronics via telefone ou e-mail. Quando tiver recebido o Código de ativação da Faronics, insira-o no campo *Código de ativação* e clique em *Avançar*. A Licença do Deep Freeze agora está ativada.



Ativação off-line

Entre em contato com o suporte de ativação Faronics em 604-637-8271 ou 1-800-943-6422 na América do Norte ou envie um e-mail para activation@faronics.com com os detalhes abaixo para solicitar um código de ativação para o Deep Freeze.

Chave de licença:
ID da instalação:

Código da ativação:

8. Quando o processo de instalação estiver concluído, a tela *Customization Code* será exibida.

Ativação bem-sucedida

Parabéns! Sua chave de licença foi ativada com sucesso.

9. Especifique o *Customization Code* e clique em *Avançar*. O *Customization Code* deve ter, no mínimo, oito caracteres. A instalação está concluída.



Um Customization Code é um identificador único que criptografa por completo o administrador de configuração, o Corporativo, os arquivos de instalação da estação de trabalho, o uso único e o controle de linha de comando do Deep Freeze.

Seu Customization Code, caso perdido ou esquecido, não poderá recuperado pela Faronics ou qualquer outro terceiro. É recomendável que você grave e armazene com segurança seu Customization Code.

Insira um Customization Code no campo abaixo. O código deve ter pelo menos oito caracteres de comprimento e pode conter combinação de caracteres alfanuméricos, incluindo espaços.

Insira um Customization Code:

Avançar >



Customization Code

O Customization Code é um identificador único que criptografa o administrador de configuração, o console corporativo, os arquivos de instalação do computador, o sistema de geração de senha para uso único e o controle de linha de comando do Deep Freeze. Este código não é uma senha que pode ser utilizada para acessar o Deep Freeze.

O Customization Code garante que administradores não autorizados não sejam capazes de acessar ou controlar determinado computador. Múltiplos administradores Deep Freeze que controlam o mesmo grupo de computadores devem utilizar o mesmo Customization Code.



O Customization Code deve ser gravado e armazenado com cuidado. A Faronics não pode recuperar um Customization Code perdido ou esquecido.

Reinicializando o Customization Code

Se outro administrador quiser criar os arquivos de instalação com o mesmo Administrador de configuração usando um Customization Code diferente, execute as seguintes etapas:

1. Execute o arquivo *DFInit.exe*.
2. Isso irá redefinir o Customization Code existente para o Administrador de configuração e o Console corporativo.
3. Insira um novo Customization Code.
4. Clique em *OK* para o novo Customization Code tornar-se ativo.

Modo de ATUALIZAÇÃO

O modo de Atualização pode ser usado para criar automaticamente versões atualizadas de arquivos existentes do Deep Freeze Enterprise através da execução de um comando de *Atualização* especial. Este comando executa duas tarefas:

- Atualiza versões anteriores do Console corporativo do Deep Freeze e do Administrador de configuração do Deep Freeze. (Encontrado no *Faronics > Deep Freeze 7 Enterprise*.)
- Atualiza todos os arquivos criados por usuários armazenados na pasta *Faronics > Deep Freeze 7 Enterprise > Instalar programas*.

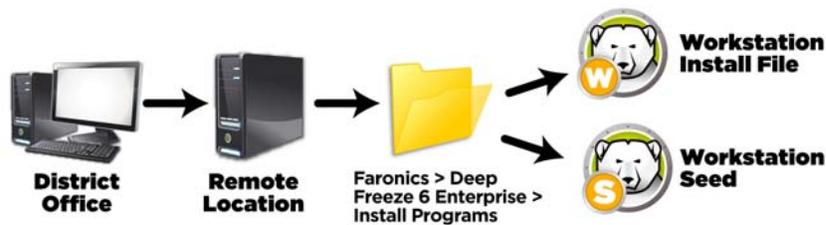
O benefício dessas atualizações é que uma série de arquivos pode ser atualizada para a versão mais recente enquanto retém seus dados de configuração (criados com uma versão mais antiga do Deep Freeze Enterprise).

O comando atualiza arquivos automaticamente criados por um administrador (*.exe*, *.rdx*) que estão presentes no diretório *Faronics > Deep Freeze 7 Enterprise > Instalar programas*, incluindo os seguintes subdiretórios:

- *Arquivos de instalação da estação de trabalho*
- *Arquivos da Seed da estação de trabalho*



No exemplo a seguir, o escritório do distrito recebeu uma nova versão do Administrador de configuração do Deep Freeze e pode automaticamente atualizar quaisquer arquivos de instalação de estação de trabalho do Deep Freeze e Seeds da estação de trabalho em um local remoto.



O comando de atualização não requer uma senha, mas requer um Customization Code. Use a seguinte sintaxe de comando:

```
\PathToFile\DFEnt.exe /update="Customization Code" c:\dfupdate.log
```

- *PathToFile* deve ser substituído pelo caminho real para o arquivo de instalação (*DFEnt.exe*)
- *DFEnt.exe* deve ser o nome real do arquivo de instalação (ele pode diferir se tiver sido baixado)
- O Customization Code deve estar em cotas se houver espaço nele
- O Customization Code deve corresponder ao Customization Code dos arquivos de instalação antigos

O arquivo de log fornece detalhes completos de quais arquivos, exatamente, foram atualizados.

O processo de atualização pode levar alguns minutos para ser concluído.

O modo de Atualização não atualiza a versão existente do Deep Freeze nos computadores. Os computadores devem ser atualizados usando-se o Console corporativo.



Senhas para uso único

O Sistema de geração de senhas para uso único é usado para gerar senhas temporárias para Deep Freeze que expiram à meia-noite no dia em que elas foram geradas.

A caixa de diálogo Senhas para uso único pode ser acessada de

- *Ferramentas*>*Senhas para uso único* no Console corporativo. Para obter mais informações, consulte [Usando o Console corporativo do Deep Freeze](#).
- *Arquivo*>*Senhas para uso único* no Administrador de configuração. Para obter mais informações, consulte [Utilizando o administrador de configuração Deep Freeze](#).

A Senha de Uso Único (OTP) pode ser útil se, por exemplo, uma senha do Deep Freeze for perdida ou se um arquivo de configuração tiver sido criado sem nenhuma senha definida. Um OTP também pode ser usado para fornecer acesso a um computador para um indivíduo que realiza deveres de manutenção sem exigir que ele saiba a senha permanente do Deep Freeze.

Para criar um OTP, execute estas etapas:

1. Selecione a opção *Senha válida para uso único somente* ou *Senha válida para vários usos*. Todas as OTPs expiram à meia-noite do dia em que foram criadas, independentemente do tipo.
2. Insira o Token do OTP do computador que exige o OTP no campo *Token*. O OTP Token para o computador está localizado na caixa de diálogo de logon, conforme mostrado a seguir.



3. Clique em *Gerar*.



A interface de linha de comando do Deep Freeze não tem suporte para o uso de Senhas de Uso Único.





Utilizando o administrador de configuração Deep Freeze

Tópicos

[Acessando o administrador de configuração](#)

[Guia Senhas](#)

[Guia Unidades](#)

[Guia Tarefas da estação de trabalho](#)

[Guia Windows Update](#)

[Guia Arquivo de lote](#)

[Guia Opções avançadas](#)

[Criando o Programa de Instalação de Estação de Trabalho e a Seed da estação de trabalho](#)



Acessando o administrador de configuração

Abra o administrador de configuração selecionando o seguinte caminho a partir do menu Iniciar:

Iniciar > Todos os programas > Faronics > Deep Freeze 7 Enterprise > Administrador Deep Freeze

O Administrador de configuração fornece diversas guias para configurar senhas, unidades congeladas, tarefas de estação de trabalho, atualizações do Windows, arquivos em lote e opções avançadas. Quando as configurações estiverem definidas, um arquivo de instalação na estação de trabalho poderá ser criado. O arquivo de instalação da estação de trabalho pode ser instalado nos computadores que precisam ser protegidos pelo Deep Freeze. O Administrador do Deep Freeze também pode ser acessado a partir do Console do Deep Freeze.

Barra de ferramentas e menus

Barra de ferramentas

A Barra de ferramentas está disponível na parte superior de cada guia do Administrador de configuração.

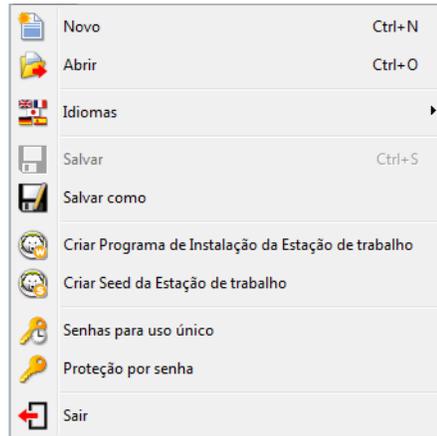


Ícone	Função
Novo	Apaga todas as definições de configurações existentes. Abre com as definições de configuração padrão.
Abrir	Abre qualquer .rdx salvo, arquivo de instalação da estação de trabalho ou arquivo da Seed da estação de trabalho.
Salvar	Salva um .rdx, arquivo de instalação da estação de trabalho ou arquivo da Seed da estação de trabalho. O nome do arquivo e o caminho são listados na parte inferior do Administrador de configuração na seção de status.
Salvar como	Salva as definições de da configuração como um arquivo .rdx.
Ajuda	Acessa o arquivo da ajuda do Deep Freeze.
Criar	<p><i>Criar arquivo de instalação da estação de trabalho</i> cria um instalador personalizado para instalação em estações de trabalho. As estações de trabalho ainda podem ser gerenciadas a partir do Console corporativo do Deep Freeze.</p> <p><i>Criar arquivo da Seed da estação de trabalho</i> cria uma seed que permite que o Console do Deep Freeze se comunique com estações de trabalho em toda a rede. Quando a seed é instalada nas estações de trabalho, o arquivo de instalação da estação de trabalho do Deep Freeze pode então ser implantado remotamente.</p>



Menu Arquivo

O menu *Arquivo* contém as mesmas opções que aquelas disponíveis na Barra de Ferramentas, com as adições da opção para escolher a partir dos idiomas disponíveis e *Proteção por senha*.



Proteção por senha

A Proteção por senha oferece uma camada adicional de segurança para o administrador.

Para proteger com senha o acesso ao Administrador de configuração, execute as seguintes etapas:

1. Abra o menu *Arquivo* e selecione *Proteção por senha*.
2. Marque a caixa de seleção *Proteger com senha*.
3. Insira e confirme a senha.
4. Clique em *OK* para definir a senha ou *Cancelar* para sair da caixa de diálogo sem definir uma senha.



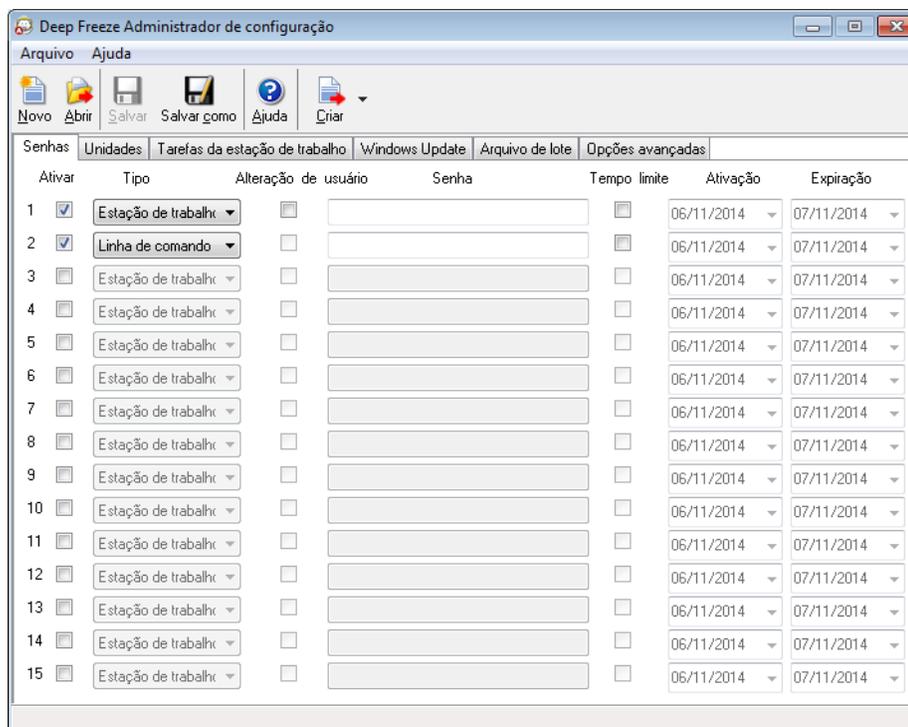


Armazene a senha em um local seguro. Se a senha for perdida, você não poderá recuperá-la. Você terá que reinstalar o Deep Freeze.



Guia Senhas

O Deep Freeze Enterprise permite ao administrador escolher até 15 senhas fixas.



Para criar uma senha, execute as seguintes etapas:

1. Selecione *Ativar* na linha apropriada.
2. A partir da lista suspensa *Tipo*, escolha o tipo preferido de senha. Estas opções estão disponíveis:
 - *Estação de trabalho*: designada para uso na estação de trabalho quando a *Tela de logon* é exibida.
 - *Linha de comando*: para uso com controles de linha de comando. A ferramenta de controle da linha de comando (*DFC.exe*) não funciona exceto se pelo menos uma senha de linha de comando estiver definida.
3. Opcional: Para senhas, marque a caixa de seleção *Alteração de usuário* para permitir que um usuário altere a senha no computador.
4. Insira a senha.



A senha inserida no campo *Senha* não está oculta.

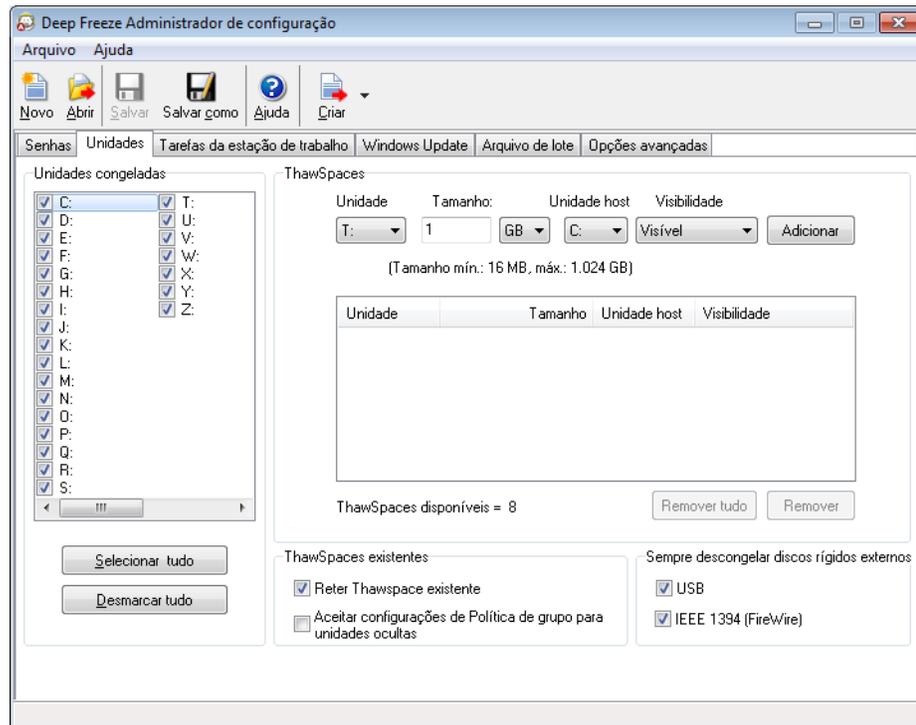
Não use a mesma senha para a linha de comando e a GUI.

5. Para definir uma senha para se tornar ativa e expirar em datas específicas, marque a caixa de seleção *Tempo limite* e use os calendários suspensos para especificar uma *Data de ativação* e *Data de vencimento*.



Guia Unidades

A guia Unidades é usada para selecionar quais unidades devem ser congeladas (protegidas pelo Deep Freeze) ou descongeladas (desprotegidas). Você também pode criar um ThawSpace — um espaço virtual hospedado em uma unidade local Congelada ou Descongelada, onde dados podem ser salvos permanentemente sem serem excluídos pelo Deep Freeze durante uma reinicialização.



Unidades congeladas

Por padrão, todas as unidades estão Congeladas. Para colocar uma unidade em um estado Descongelado, limpar a caixa da unidade preferida.

Embora somente unidades locais (unidades físicas ou partições) podem estar Congeladas, todas as letras das unidades são mostradas porque o arquivo de instalação pré-configurado pode ser instalado em vários computadores com várias configuração de hardware e software.

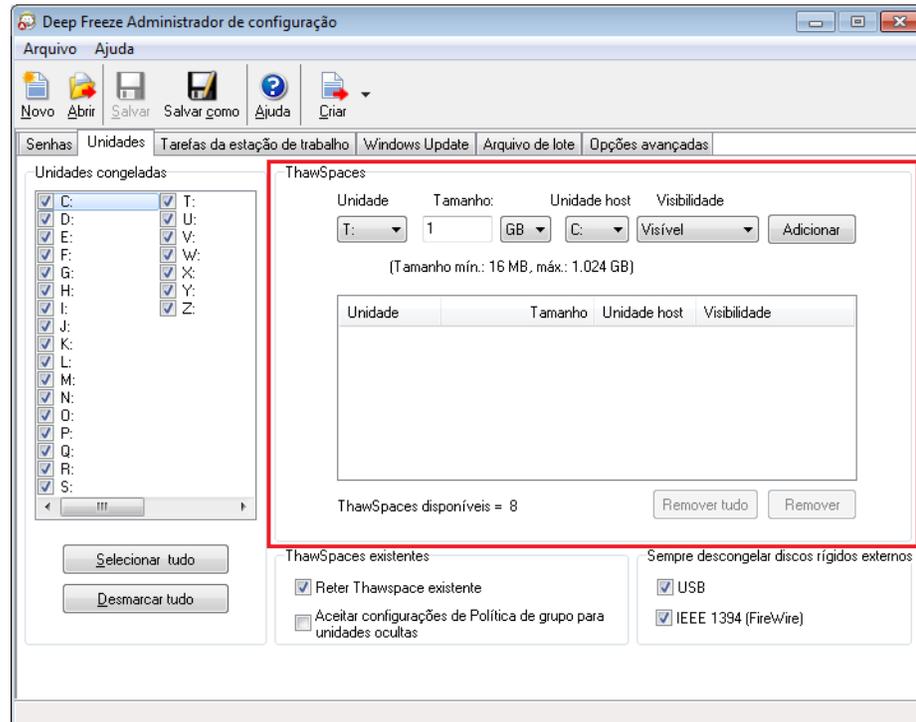
Exemplo

Na tela acima, a *D:* não está selecionada na lista Unidades congeladas. Portanto, todas as unidades exceto *D:* estão congeladas.



ThawSpace

O ThawSpace é um espaço virtual que pode ser usado para armazenar programas, salvar arquivos ou fazer alterações permanentes. Todos os arquivos armazenados no ThawSpace são retidos após uma reinicialização, mesmo que o computador esteja Congelado. Um ThawSpace pode ser criado em uma unidade que está configurada para estar Congelada ou Descongelada.



Para criar um ThawSpace único ou vários ThawSpaces, usando o Administrador de configuração, execute estas etapas:

1. **Selecione a *Letra da unidade*.** A letra padrão é *T:*. Porém, ela pode ser alterada para qualquer letra disponível. A próxima letra disponível é usada automaticamente se a letra da unidade selecionada já existe no computador quando o Deep Freeze está instalado.
 - Quando uma *Letra da unidade* é selecionada a partir do menu suspenso e usada para criar um ThawSpace, ela é removida do menu suspenso.
 - Quando um ThawSpace é removido, a *Letra da unidade* correspondente é adicionada de volta ao menu suspenso.
 - A *Letra da unidade* não pode ser a mesma que a da *Unidade host*.
2. **Inserir o *Tamanho*.** Esse o tamanho do ThawSpace. O tamanho máximo é de 1.024 GB e o tamanho mínimo é de 16 MB.
 - Se o computador não tiver espaço livre suficiente para acomodar o tamanho do ThawSpace selecionado, o tamanho do ThawSpace está ajustado para abaixo para assegurar o funcionamento adequado do computador.
 - Se você selecionar o Tamanho menor que 16 MB, o ThawSpace é configurado para 16 MB.
 - Se você selecionar o Tamanho maior que 1.024 GB (1TB), o ThawSpace é configurado para 1.024 GB (1TB).



3. Selecionar a unidade de armazenamento do ThawSpace em *MB* ou *GB*.
4. Selecionar a *Letra Host*.
 - A *Unidade Host* é a unidade onde o ThawSpace é criado.
 - O armazenamento necessário para o ThawSpace é usado a partir do armazenamento disponível na *Unidade Host*.
5. Selecionar *Visível* ou *Oculto* a partir do menu suspenso *Visibilidade*.
 - Se selecionar *Visível*, a unidade será visível no Windows Explorer.
 - Se selecionar *Oculto*, a unidade não será visível no Windows Explorer.
 - Porém, a unidade oculta pode ser acessada ao digitar a letra da unidade em *Início>Execução*.
6. Clique em *Adicionar* para adicionar o ThawSpace.

Remover um ThawSpace

Para remover um ThawSpace, selecione o ThawSpace e clique em *Remover*. O ThawSpace é removido e agora a letra da unidade é adicionada de volta ao menu suspenso *Letra da Unidade*. Clique em *Remover tudo* para remover todos os ThawSpaces.



Antes de remover um ThawSpace, remova qualquer perfis de redirecionamento ou Links simbólicos.

Ao remover um ThawSpace também serão removidos os dados armazenados nele.

Um ThawSpace não está protegido pelo Deep Freeze. Implante opções de proteção de dados padrão como procedimentos do Anti-Virus e de backup.

Exemplo

Na tela acima, um *ThawSpace* de 16 MB é criado na *Unidade host C:* e o ThawSpace é designado com a letra de unidade *T:*. O ThawSpace *T:* é definido como *Visível* e pode ser acessado via o Windows Explorer.



É recomendado atribuir letras de unidade para o final do alfabeto (X, Y, Z), a fim de evitar a reassignação automática quando uma unidade removível for desconectada.

ThawSpace existente

A caixa *Reter ThawSpace existente* é selecionada por padrão para evitar que ThawSpaces criados durante instalações anteriores sejam excluídos.

Uma caixa de diálogo sempre é exibida perguntando se o ThawSpace deverá ser retido ou excluído na Desinstalação atendida, independente de se *Reter ThawSpace existente* foi selecionado. Esta opção não é exibida se a desinstalação é executada através do Console Corporativo.

A opção *Seguir configurações de política de grupo para unidades ocultas* garante que as configurações de Política de grupo para unidades ocultas não entrem em conflito com as configurações do Deep Freeze para unidades ocultas.



Configurações de Políticas de grupo para unidades ocultas são específicas do usuário. Configurações do Deep Freeze para unidades ocultas são globais se a opção *Seguir configurações de política de grupo para unidades ocultas* estiver desativada.



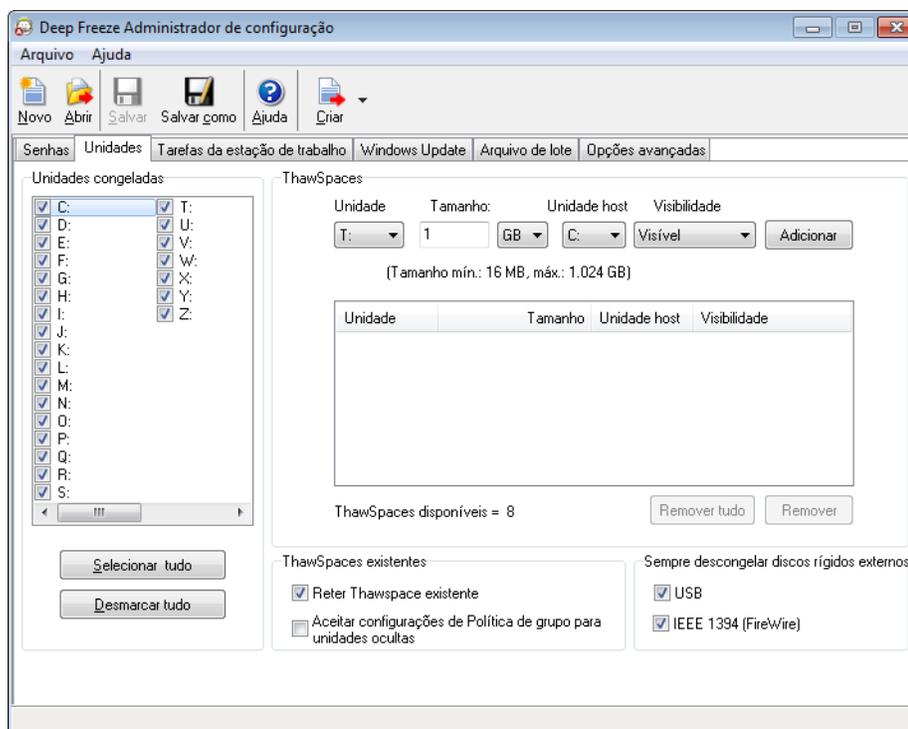
Se não houver nenhuma Política de grupo para unidades ocultas, recomenda-se desativar esta opção.

Sempre descongelar discos rígidos externos

O painel *Sempre descongelar discos rígidos externos* tem duas caixas de seleção, *USB* e *IEEE 1394 (FireWire)* e ambas as caixas de seleção são marcadas por padrão. Isso assegura que os discos rígidos USB ou os discos rígidos IEEE 1394 (FireWire) sejam sempre descongelados.

Se as caixas de seleção dos discos rígidos externos USB e/ou IEEE 1394 (FireWire) foram desmarcadas, a unidade será *Congelada* ou *Descongelada* de acordo com a letra que cada unidade monta na seção Unidades congeladas.

As unidades de rede e unidades de mídia removível (floppy, chaves de memória, CD-RW, etc.) não são afetadas pelo Deep Freeze e, portanto, não podem ser congeladas.



Exemplo

Na tela acima, as unidades *E:* e *F:* são selecionadas no painel *Unidades congeladas*.

Vamos supor que *E:* corresponde a um disco rígido USB e *F:* corresponde a um disco rígido IEEE 1394 (FireWire).



As caixas de seleção *USB* e *IEEE 1394 (FireWire)* são marcadas no painel *Sempre descongelar discos rígidos externos*, os discos rígidos externos deveriam ser *Descongelados*.

A caixa de seleção *USB* está marcada. A caixa de seleção *IEEE 1394 (FireWire)* está desmarcada. Neste exemplo, a unidade *USB (D:)* seria descongelada e a unidade *IEEE 1394 (FireWire) (F:)* seria congelada.



Tarefas da estação de trabalho vs. Tarefas agendadas: Se a comunicação entre o Console corporativo e o computador de destino falhar, as Tarefas da estação de trabalho ainda serão executadas uma vez que elas existem no computador de destino.

As tarefas agendadas através do Assistente de tarefas agendadas no Console corporativo do Deep Freeze existem no Console corporativo e não nos computadores de destino. Portanto, uma conectividade contínua entre o Console corporativo e o computador de destino é necessária para as Tarefas agendadas serem executadas. Para obter mais informações, consulte a seção [Agendando tarefas do Deep Freeze](#).



A sobreposição de tarefas não pode ser criada na guia Tarefas da estação de trabalho. Será exibida uma mensagem, se uma tarefa recém-criada sobrepujar uma tarefa existente.



Uma mensagem pode ser exibida para o usuário por um máximo de 5 minutos. Deve haver uma falha de no mínimo 5 minutos entre quaisquer duas tarefas.



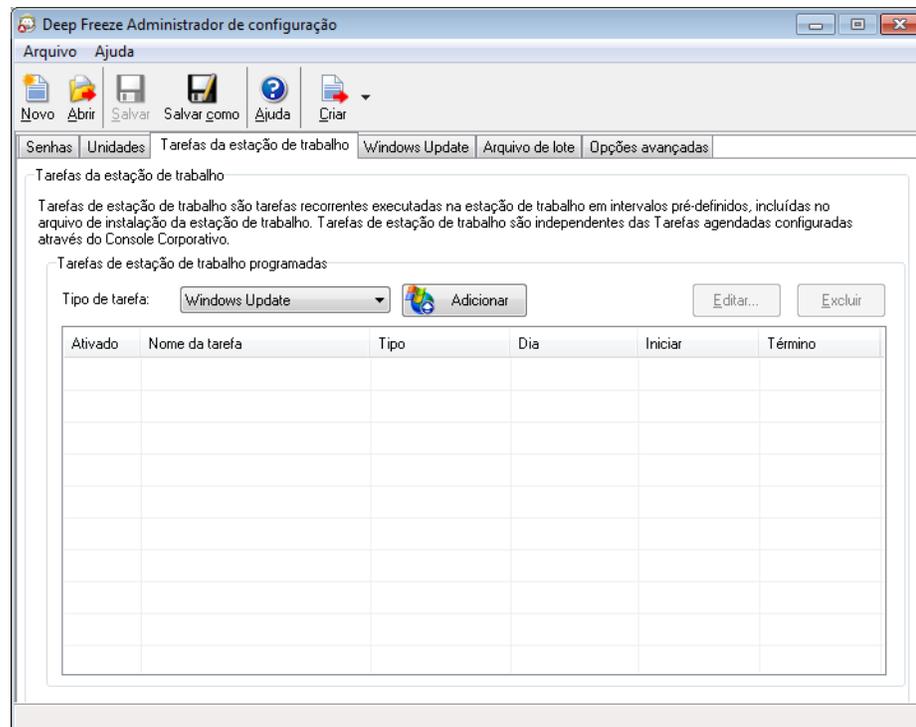
Uma tarefa da estação de trabalho é disparada somente quando o Deep Freeze está no estado Congelado.

Windows Update

As tarefas do Windows Update são agendadas para baixar atualizações do Windows na estação de trabalho. As atualizações do Windows podem ser baixadas mesmo quando a estação de trabalho está em um estado Congelado. Uma tarefa de atualização do Windows tem uma hora de início e uma hora de término. Após o download das atualizações do Windows, a estação de trabalho é reiniciada em um estado Descongelado para aplicar.

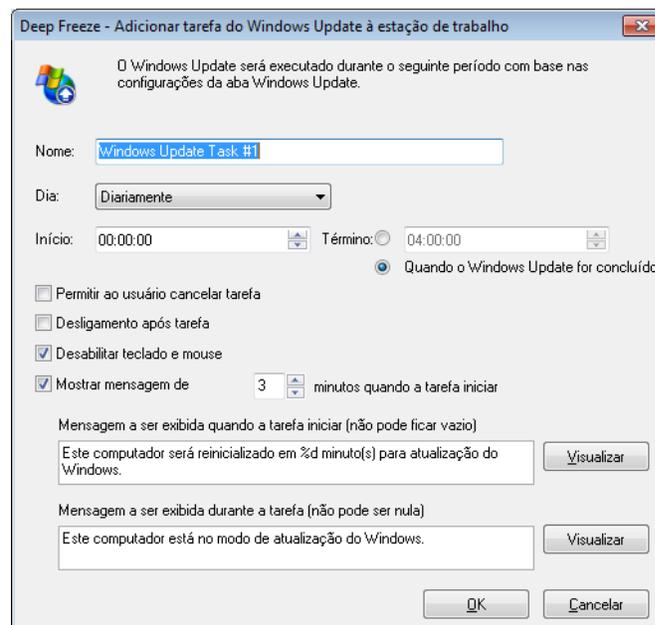


As atualizações do Windows também podem ser aplicadas manualmente na estação de trabalho selecionando-se a estação de trabalho e via o comando *Executar Windows Update* a partir do menu de contexto no Console do Deep Freeze. Para obter mais informações, consulte [Gerenciando o Deep Freeze com o Console](#).



A tarefa de atualização do Windows pode ser agendada executando-se as tarefas a seguir:

1. Selecione *Windows Update* na lista suspensa *Tipo de tarefa* e clique em *Adicionar*.
2. As opções a seguir são exibidas:



- *Nome* - especifique um nome para a tarefa.
- *Dia* - selecione o dia ou especifique se a tarefa irá ocorrer em dias úteis ou nos finais de semana.



- *Início* - selecione a hora de início.
 - *Início* - selecione a hora de término. O intervalo mínimo é de 15 minutos. Alternativamente, você pode selecionar *Quando o Windows Update for concluído*. Se a Tarefa Windows Update não for concluída em 6 horas, o Deep Freeze irá encerrar a tarefa educadamente.
 - *Permitir ao usuário cancelar tarefa* - marque a caixa de seleção se o usuário tiver permissão para cancelar a tarefa antes do seu início.
 - *Desligamento após tarefa* - marque a caixa de seleção para desligar o computador após a tarefa.
 - *Desativar teclado e mouse* - marque a caixa de seleção para desativar o teclado e o mouse durante a tarefa.
 - *Mostrar mensagem* - marque a caixa de seleção para exibir uma mensagem no computador *Antes e Durante* a tarefa. Especifique o intervalo de tempo em minutos e insira uma breve mensagem a ser exibida antes do início da tarefa.
3. Clique em Ok. Você será conduzido para a [Guia Windows Update](#) para definir as configurações adicionais se elas não tiverem sido configuradas anteriormente.



A mensagem *Este computador será reinicializado em %d para atualização do Windows* é exibida no campo *Mensagem a ser exibida antes da tarefa*. Esta mensagem pode ser editada. Adicione a palavra *minutos* à mensagem após *%d* para incluir a palavra minutos como parte da mensagem.



Ao agendar a tarefa de atualização do Windows selecione a opção *Quando o Windows Update for concluído*. Revise os boletins de segurança da Microsoft no site da Technet (<http://technet.microsoft.com/en-us/security/bulletin>) para considerar o período apropriado com base nas atualizações críticas e de segurança que estão sendo lançadas.



Se você não estiver usando o WSUS, o processo de atualização do Windows do Deep Freeze só irá aplicar atualizações de intervenção não-usuário críticas e de segurança. Se você estiver usando o WSUS, todas as atualizações do WSUS aprovadas serão aplicadas.

Alternativamente, para aplicar outras atualizações disponíveis visite o site Catálogo do Microsoft Update (<http://catalog.update.microsoft.com>) para obter downloads em KB que podem ser aplicados usando-se uma tarefa de estação de trabalho de arquivo de lote do Deep Freeze. As tarefas de arquivo de lote também podem ser usadas para aplicar outras atualizações de software de terceiros.



As configurações da guia Windows Update do Deep Freeze substituem as configurações do Windows Update da estação de trabalho.

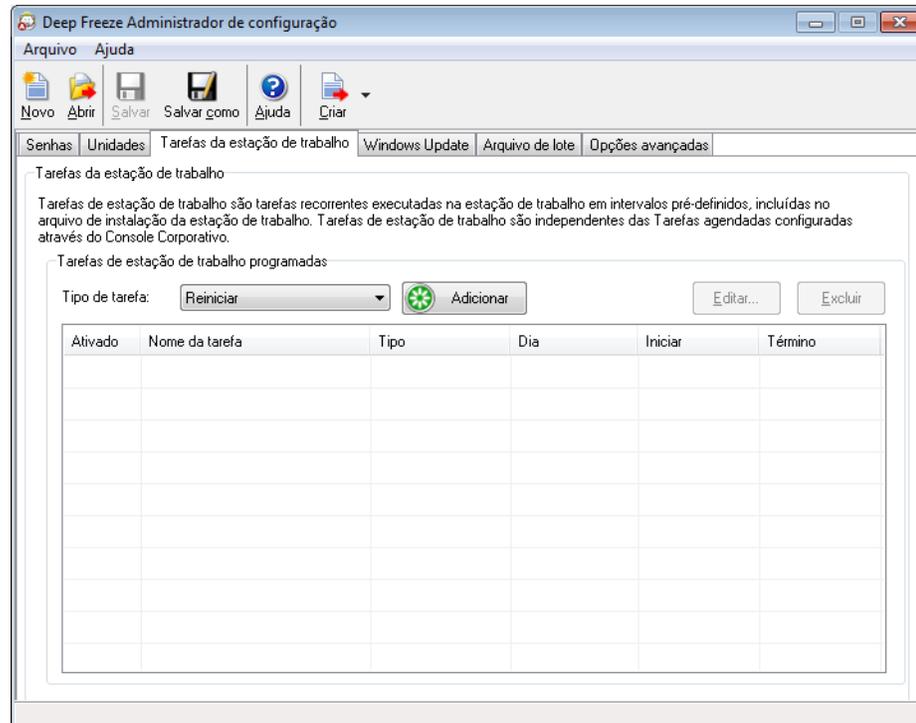


Exemplo

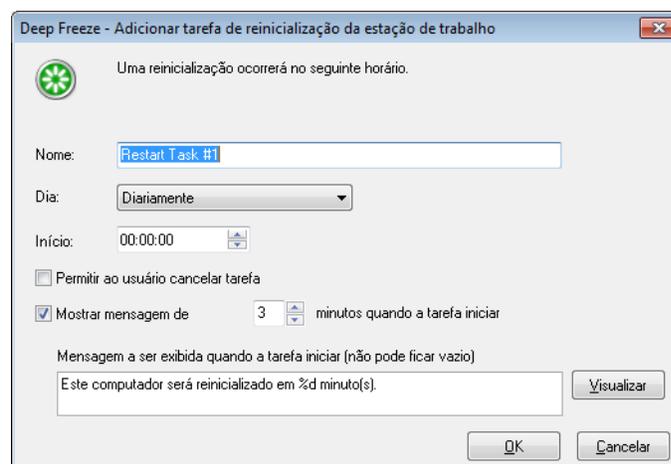
Na tela acima, uma tarefa do Windows Update foi criada para realizar atualizações do Windows no computador diariamente às 12h00 e encerrar quando o *Windows Update* estiver concluído. A tarefa é configurada para exibir uma mensagem para o usuário antes do Windows Update. O teclado e o mouse são desativados.

Reiniciar

A tarefa Reiniciar pode ser agendada executando-se as tarefas a seguir:



1. Selecione *Reiniciar* na lista suspensa *Tipo de tarefa* e clique em *Adicionar*.
2. As opções a seguir são exibidas:





- *Nome* - especifique um nome para a tarefa.
 - *Dia* - selecione o dia ou especifique se a tarefa irá ocorrer em dias úteis ou nos finais de semana.
 - *Início* - selecione a hora de início.
 - *Permitir ao usuário cancelar tarefa* - marque a caixa de seleção se o usuário tiver permissão para cancelar a tarefa antes do seu início.
 - *Mostrar mensagem* - marque a caixa de seleção para exibir uma mensagem no computador antes do início da tarefa. Especifique o intervalo de tempo em minutos e insira uma breve mensagem a ser exibida antes do início da tarefa.
3. Clique em Ok.



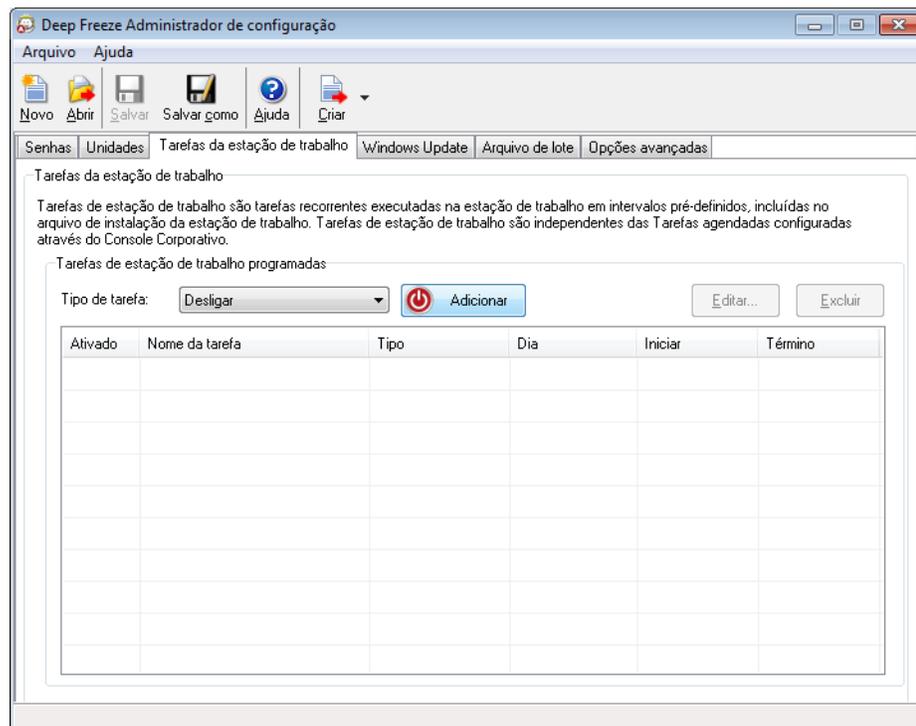
A mensagem *Este computador será reinicializado em %d segundos* é exibida no campo *Mensagem a ser exibida antes da tarefa*. Esta mensagem pode ser editada. Adicione a palavra *minutos* à mensagem após *%d* para incluir a palavra minutos como parte da mensagem.

Exemplo

Na tela acima, uma Tarefa de estação de trabalho foi criada para reiniciar o computador diariamente às 12h00. A tarefa é configurada para exibir uma mensagem para o usuário 1 minuto antes da reinicialização.

Desligar

A tarefa Desligar pode ser agendada executando-se as tarefas a seguir:





1. Selecione *Desligar* na lista suspensa *Tipo de tarefa* e clique em *Adicionar*.
2. As opções a seguir são exibidas:

- *Nome* - especifique um nome para a tarefa.
 - *Dia* - selecione o dia ou especifique se a tarefa irá ocorrer em dias úteis ou nos finais de semana.
 - *Início* - selecione *Hora de início*.
 - *Permitir ao usuário cancelar tarefa* - marque a caixa de seleção se o usuário tiver permissão para cancelar a tarefa antes do seu início.
 - *Mostrar mensagem* - marque a caixa de seleção para exibir uma mensagem no computador antes do início da tarefa. Especifique o intervalo de tempo em minutos e insira uma breve mensagem a ser exibida antes da execução da tarefa.
3. Clique em Ok.



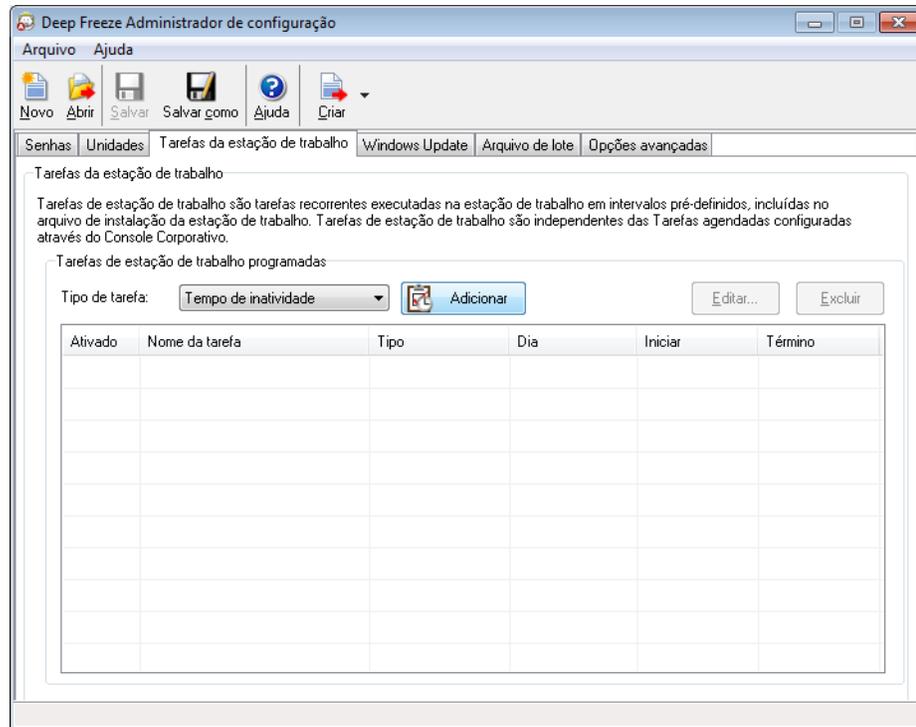
A mensagem *Este computador será desligado em %d segundos* é exibida no campo *Mensagem a ser exibida antes da tarefa*. Esta mensagem pode ser editada. Adicione a palavra *minutos* à mensagem após *%d* para incluir a palavra minutos como parte da mensagem.

Exemplo

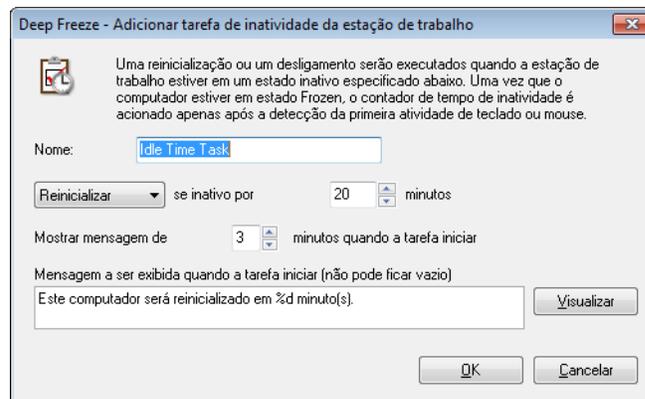
Na tela acima, uma Tarefa de estação de trabalho foi criada para desligar o computador diariamente às 12h00. A tarefa é configurada para exibir uma mensagem para o usuário 1 minuto antes da tarefa de desligamento.

Tempo de inatividade

A tarefa de Tempo de inatividade pode ser agendada executando-se as tarefas a seguir:



1. Selecione *Tempo de inatividade* na lista suspensa *Tipo de tarefa* e clique em *Adicionar*.
2. As opções a seguir são exibidas:



- *Nome* - especifique um nome para a tarefa.
- *Reiniciar* ou *Desligar* - selecione *Reiniciar* ou *Desligar* e especifique o tempo de inatividade em minutos após os quais a tarefa deverá ser executada.
- *Mostrar mensagem* - marque a caixa de seleção para exibir uma mensagem. Especifique o intervalo de tempo em minutos e insira uma breve mensagem.



Após o computador ter sido iniciado, o contador de tempo de inatividade é acionado apenas após a detecção da primeira atividade de teclado ou mouse. Durante uma sessão de área de trabalho remota, o tempo de inatividade do computador controlador é usado para ativar a tarefa.



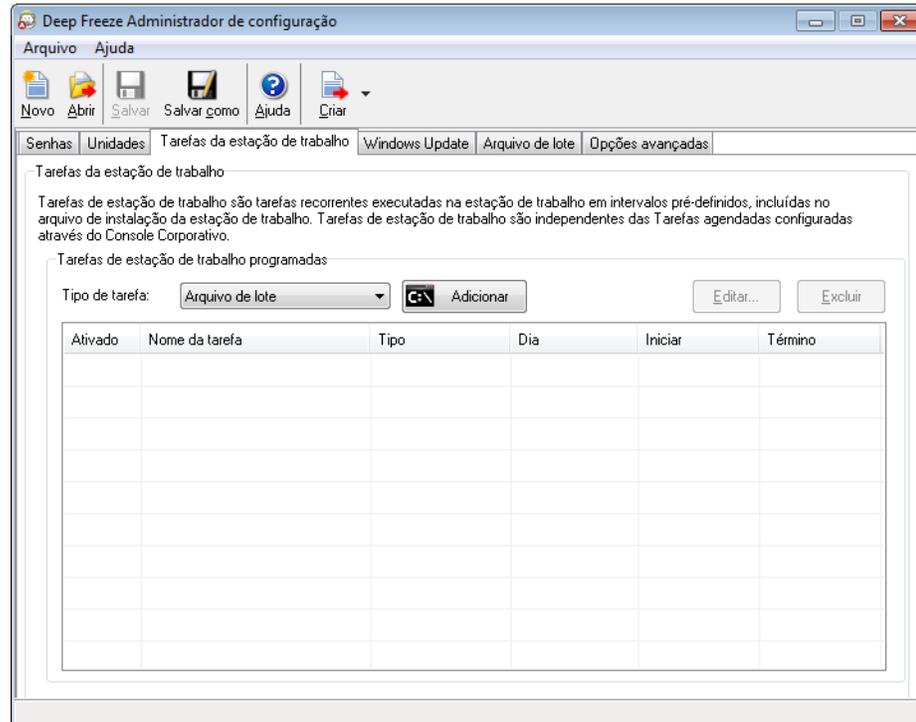
3. Clique em Ok.

Exemplo

Na tela acima, a tarefa Tempo de inatividade é definida para *Reiniciar* quando o computador está inativo por 1 minuto. A mensagem é exibida para o usuário por 1 minuto após o tempo de inatividade ter decorrido. O computador será reiniciado, exceto se o usuário cancelar a tarefa na caixa de diálogo da mensagem exibida.

Arquivo de lote

As tarefas de arquivo de lote são agendadas para execução de arquivos em lote na estação de trabalho. Uma tarefa de arquivo de lote tem uma hora de início e uma hora de término. Durante este período, o arquivo de lote é executado na estação de trabalho. Você deve definir configurações adicionais na guia Arquivo de lote para que a tarefa de arquivo de lote funcione. Você pode configurar para desligar a estação de trabalho após a tarefa do arquivo de lote ter sido concluída. As estações de trabalho serão reiniciadas *Congeladas* depois de o arquivo de lote ter sido executado.



A tarefa Arquivo de lote pode ser agendada executando-se as tarefas a seguir:

1. Selecione *Arquivo de lote* na lista suspensa *Tipo de tarefa* e clique em *Adicionar*.
2. As opções a seguir são exibidas:



Deep Freeze - Adicionar tarefa Arquivo de lote à estação de trabalho

A tarefa do arquivo de lote será executada durante o seguinte período, com base nas configurações da aba Arquivo de lote.

Nome:

Dia:

Início: Término:

Permitir ao usuário cancelar tarefa

Desligamento após tarefa

Desabilitar teclado e mouse

Mostrar mensagem de minutos quando a tarefa iniciar

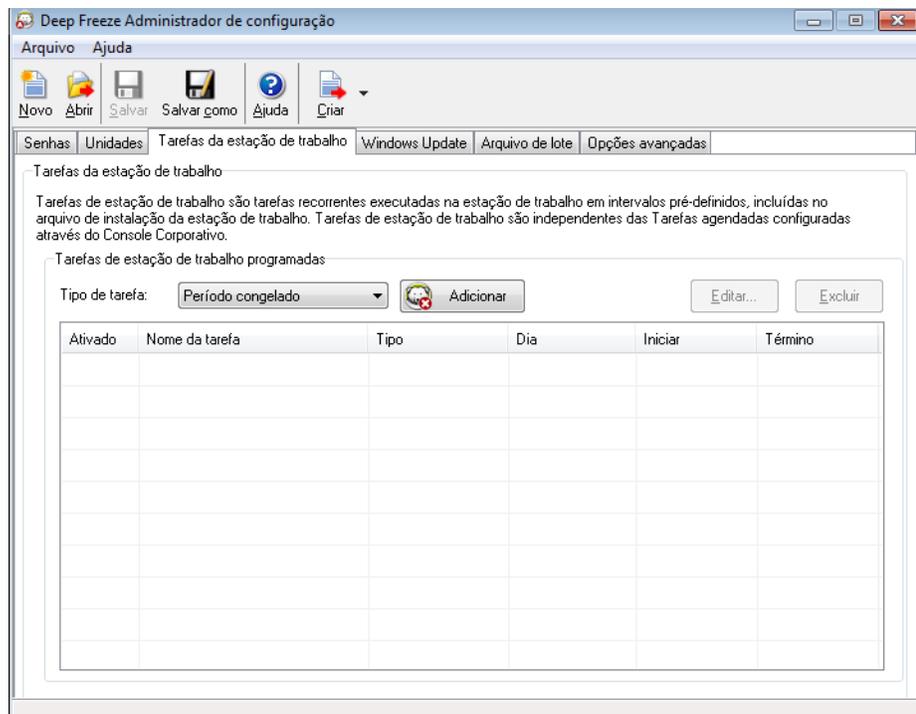
Mensagem a ser exibida quando a tarefa iniciar (não pode ficar vazio)

Mensagem a ser exibida durante a tarefa (não pode ser nula)

- *Nome* - especifique um nome para a tarefa.
 - *Dia* - selecione o dia ou especifique se a tarefa irá ocorrer em dias úteis ou nos finais de semana.
 - *Início* - selecione a hora de início.
 - *Início* - selecione a hora de término. O intervalo mínimo é de 15 minutos.
 - *Permitir ao usuário cancelar tarefa* - marque a caixa de seleção se o usuário tiver permissão para cancelar a tarefa antes do seu início.
 - *Desligamento após tarefa* - marque a caixa de seleção para desligar o computador após a tarefa.
 - *Desativar teclado e mouse* - marque a caixa de seleção para desativar o teclado e o mouse durante a tarefa.
 - *Mostrar mensagem* - marque a caixa de seleção para exibir uma mensagem no computador *Antes* e *Durante* a tarefa. Especifique o intervalo de tempo em minutos e insira uma breve mensagem a ser exibida antes do início da tarefa.
3. Clique em Ok.
 4. Vá para [Guia Arquivo de lote](#) para definir configurações adicionais.



A mensagem *Este computador será reinicializado em %d para arquivo em lotes* é exibida no campo *Mensagem a ser exibida antes da tarefa*. Esta mensagem pode ser editada. Adicione a palavra *minutos* à mensagem após *%d* para incluir a palavra minutos como parte da mensagem.



- *Nome* - especifique um nome para a tarefa.
 - *Dia* - selecione o dia ou especifique se a tarefa irá ocorrer em dias úteis ou nos finais de semana.
 - *Início* - selecione a hora de início.
 - *Início* - selecione a hora de término. O intervalo mínimo é de 15 minutos.
 - *Permitir ao usuário cancelar tarefa* - marque a caixa de seleção se o usuário tiver permissão para cancelar a tarefa antes do seu início.
 - *Desligamento após tarefa* - marque a caixa de seleção para desligar o computador após a tarefa.
 - *Desativar teclado e mouse* - marque a caixa de seleção para desativar o teclado e o mouse durante a tarefa.
 - *Mostrar mensagem* - marque a caixa de seleção para exibir uma mensagem no computador *Antes e Durante* a tarefa. Especifique o intervalo de tempo em minutos e insira uma breve mensagem a ser exibida antes do início da tarefa.
3. Clique em Ok.



A mensagem *Este computador será reinicializado em %d para Manutenção* é exibida no campo *Mensagem a ser exibida antes da tarefa*. Esta mensagem pode ser editada. Adicione a palavra *minutos* à mensagem após *%d* para incluir a palavra minutos como parte da mensagem.

Exemplo

Programas Anti-Virus requerem atualizações de definição de vírus para proteger o sistema. As definições de vírus podem ser atualizadas durante um Período congelado.



Na tela acima, uma tarefa de Período congelado foi criada diariamente entre 12h00 h e 12h15. O usuário não tem permissão para cancelar a tarefa antes de seu início. O computador será desligado após o período de manutenção. O teclado e o mouse são desativados durante o período de manutenção. A tarefa é configurada para exibir uma mensagem para o usuário 5 minutos antes do início da tarefa. A mensagem a seguir será exibida no computador às 11:55 AM, *O computador será reinicializado em 5 minutos para entrar em um Período congelado.*

Para garantir que as definições de vírus serão aplicadas permanentemente, agende a atualização da definição de vírus para seu programa Anti-Vírus de forma que ele inicie *após* o Deep Freeze ter iniciado com êxito a tarefa do Período descongelado e *termine* antes que o Deep Freeze termine a tarefa do Período descongelado. Isso irá assegurar que as definições de vírus baixadas e atualizadas pelo programa Anti-Virus fiquem permanentemente no sistema. Conseqüentemente, o sistema está totalmente protegido pelo Anti-Virus e o Deep Freeze.



Faronics Anti-Virus: O Faronics Anti-Virus funciona com o Deep Freeze e não requer uma tarefa de Período descongelado para atualização das definições de vírus. O Faronics Anti-Virus pode atualizar definições de vírus mesmo quando os computadores gerenciados pelo Deep Freeze estão em um estado *Congelado*.

Outros programas antivírus: Todos os outros programas antivírus requerem o agendamento de uma tarefa de Período descongelado para atualizar definições de vírus. Consulte o guia do usuário do seu programa antivírus para obter informações sobre como as definições de vírus são baixadas. Alternativamente, as definições de vírus podem ser aplicadas quando os computadores gerenciados pelo Deep Freeze estão em um estado *Descongelado*. Você também pode agendar uma instalação *sem intervenção do usuário* das suas definições de vírus através de uma tarefa de arquivo de lote.

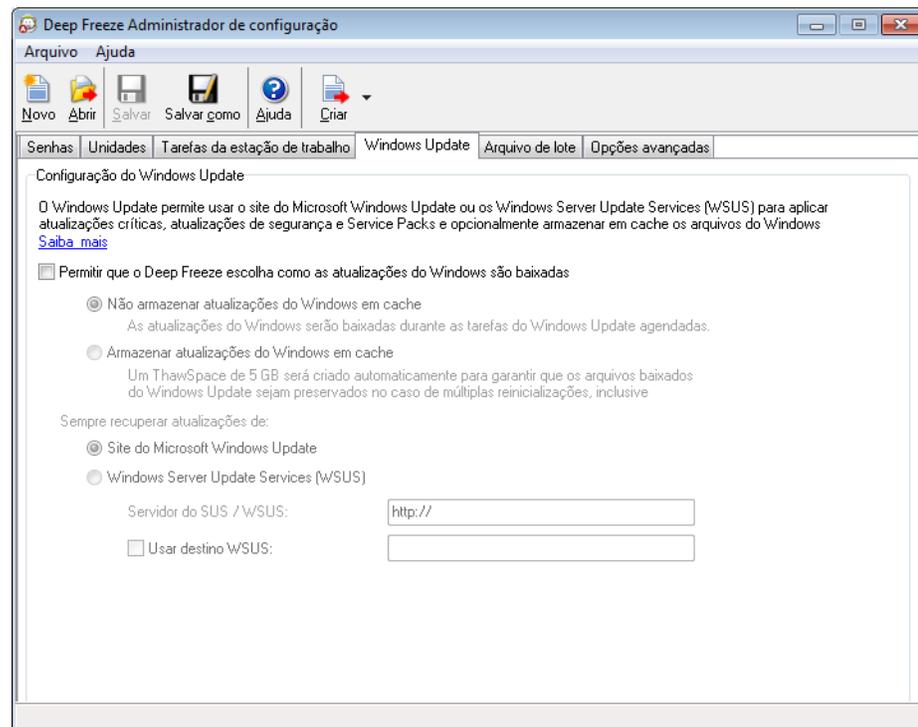


Guia Windows Update

A guia Windows Update permite a você personalizar configurações para Windows Update. Ao criar pela primeira vez uma tarefa do Windows Update, você receberá uma opção para modificar as configurações padrão na guia Windows Update. Modificar as configurações padrão não é mandatório. O Windows Update será realizado mesmo com as configurações padrão. As configurações na guia Windows Update serão aplicadas a todas as tarefas do Windows Update.



As configurações da guia Windows Update do Deep Freeze substituem as configurações do Windows Update da estação de trabalho.



As configurações na guia Windows Update podem ser personalizadas da seguinte maneira:

Permitir que o Deep Freeze escolha como as atualizações do Windows são baixadas: — marque esta caixa de seleção para permitir que o Deep Freeze escolha como as atualizações do Windows são baixadas. Estas opções estão disponíveis:

- Selecione as opções de download das atualizações do Windows.
 - *Não armazenar atualizações do Windows em cache* — selecione esta opção para baixar atualizações do Windows somente durante a tarefa do Windows Update.
 - *Armazenar atualizações do Windows em cache* — selecione esta opção para baixar quando a estação de trabalho estiver em um estado Congelado ou Descongelado e instalar durante a tarefa do Windows Update. Esta opção cria um ThawSpace de 4 GB e as Atualizações do



Windows são armazenadas no ThawSpace para garantir que os arquivos do Windows Update sejam preservados entre múltiplas reinicializações.

- Sempre recuperar atualizações de:
 - *Site do Microsoft Windows Update* — selecione esta opção para baixar atualizações diretamente do site do Microsoft Windows Update.
 - *Windows Server Update Services (WSUS)* — selecione esta opção para baixar do servidor do WSUS. Especifique o *Servidor do SUS/WSUS*. Opcionalmente, selecione *Usar destino WSUS* especifique o destino. O cliente Microsoft SUS e o servidor do SUS/WSUS podem ser baixados em: <http://www.microsoft.com/wsus>.



Um arquivo de log é criado para cada estação de trabalho individual e está armazenado localmente na estação de trabalho.

O nome padrão do arquivo de log do Windows Update do Deep Freeze é *DFWuLogfile.log* e ele pode ser encontrado em:

C:\Arquivos de programa\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (sistemas de 32 bits) e C:\Arquivos de programa (x86)\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (sistemas de 64 bits).

- Você não pode alterar o nome ou o local do arquivo de log.
- O arquivo de log do Deep Freeze e o arquivo de log do Windows Update (em `c:\windows\windowsupdate.log`) são muito úteis para solução de problemas das atualizações do Windows.
- X é um valor incremental dependendo de quantas vezes você tiver instalado o Deep Freeze na estação de trabalho.

Entre em contato com o suporte técnico da Faronics para obter ajuda na solução de problemas com o DFWuLogfile.log (em <http://support.faronics.com>).

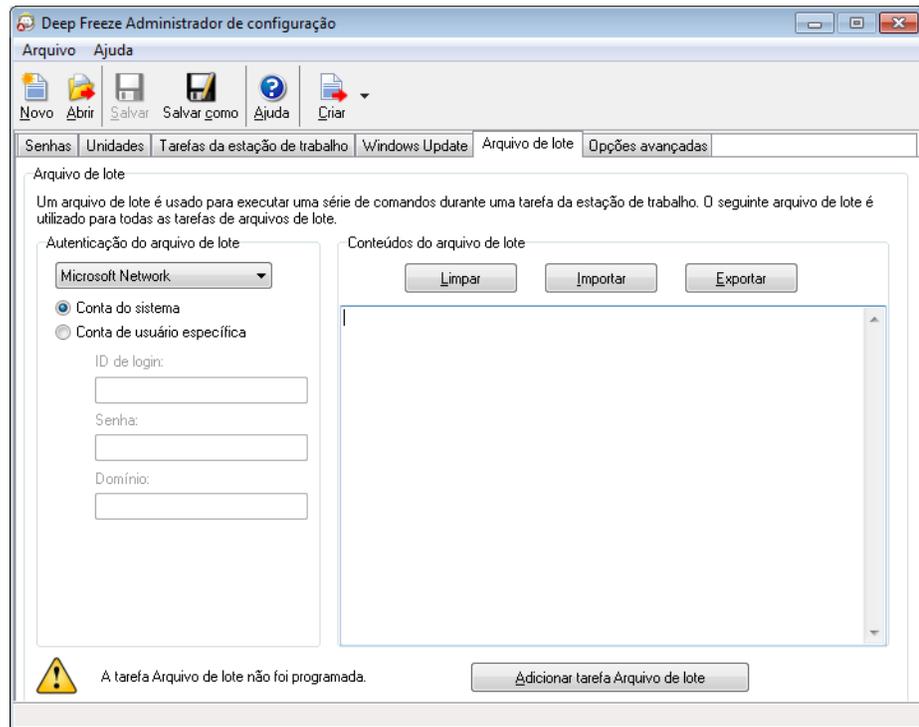
Entre em contato com o Suporte da Microsoft para solução de problemas de erros do Windows Update. (Veja <http://support.microsoft.com/kb/906602>)

Veja também Microsoft KB 902093 *Como ler o arquivo de log do Windows Update* encontrado em: <http://support.microsoft.com/kb/902093/> ou visite <http://support.microsoft.com>.



Guia Arquivo de lote

A guia Arquivos de lote permite personalizar as configurações para a tarefa Arquivo de lote. Quando você agenda uma tarefa Arquivo de lote da guia Tarefas da estação de trabalho, você deve definir as configurações na guia Arquivo de lote.



Configure as seguintes opções:

- Autenticação do arquivo de lote

Selecione Microsoft Network e selecione se a conta a ser usada é uma conta Sistema ou uma Conta de usuário especificada. Se você tiver selecionado Conta de usuário especificada, indique identificação de logon, senha e domínio. Para Rede Novell, selecione Novell, especifique a identificação de logon, senha, árvore, contexto e servidor.



A configuração padrão que usa a autenticação Microsoft Network/conta Sistema deve ser testada antes de usar credenciais alternativas. Usar esta conta de nível de máquina frequentemente é suficiente para concluir a tarefa. O uso de uma conta de usuário especificada pode ser necessário se o arquivo de lote exigir acesso a recursos seguros.

- Conteúdos do arquivo de lote



Insira um arquivo de lote personalizado para ser executado durante a tarefa Arquivo de lote. O mesmo arquivo de lote se aplica a todas as tarefas Arquivo de lote. As seguintes opções estão disponíveis ao executar arquivos de lote personalizados:

- Para limpar o arquivo de lote atual, clique em *Limpar*.
- Para carregar um arquivo existente, clique em *Importar* e navegue até o local do arquivo.
- Para salvar o conteúdo do campo, clique em *Exportar* e navegue até o local preferido para salvar.

O arquivo de lote pode ser qualquer comando ou série de comandos que o processador de comandos puder executar. Você pode executar scripts aleatórios que requerem o uso de um mecanismo de script de terceiros chamando o script a partir do arquivo de lote como se ele estivesse sendo executado a partir da linha de comando.

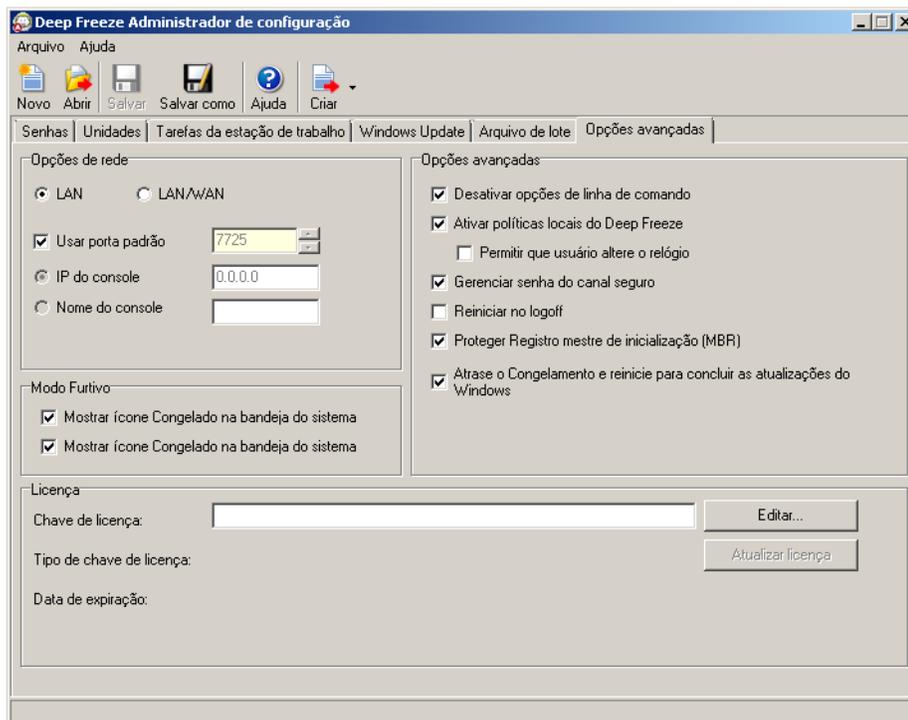


Arquivos de lote permitem usar VB scripts, PowerShell scripts, Ninite e outras soluções de terceiros. Entre em contato com seu fornecedor de software ou consulte o guia do usuário da sua solução de terceiros para saber mais sobre soluções de script que incluem opções *sem intervenção do usuário*.



Guia Opções avançadas

A guia Opções avançadas é usada para configurar as configurações de rede usadas pelos computadores para comunicação com o Console, configurar diversas opções de segurança e administrar chaves de licença.



Rede

A comunicação entre o Console corporativo do Deep Freeze e os computadores com o Deep Freeze instalado pode usar dois modos diferentes: Modo LAN ou Modo LAN/WAN.

- **LAN:** Selecione LAN para configurar o Deep Freeze para comunicar-se dentro de uma rede local (LAN). O modo LAN é um modo de autoconfiguração que requer somente um número de porta. A porta padrão é 7725. O número da porta pode ser alterado se ela estiver em conflito com outros programas na LAN. No modo LAN, o computador de destino do Deep Freeze e o Console corporativo encontram um ao outro através de transmissões UDP. Essas transmissões só ocorrem quando o computador ou o Console corporativo são iniciados, assegurando que existam pouco tráfego de rede associado à comunicação com o computador de destino e o Console.
- **LAN/WAN:** Selecione LAN/WAN para configurar o Deep Freeze para comunicar-se em uma LAN e em uma WAN (rede de longa distância). A LAN/WAN pode ser usada em um ambiente de LAN ou WAN e pela Internet. Este modo usa um endereço IP ou o nome do computador, junto com um número de porta, para permitir a comunicação entre o Console corporativo e os computadores gerenciados.

Os seguintes dois métodos estão disponíveis para identificar o Console:



- especifique o IP do Console, que deve ser estático
- especifique o Nome do Console, neste caso o IP pode ser dinâmico (se a resolução do nome DNS válido estiver disponível como parte da infraestrutura de domínio).

Quando o Console corporativo está por trás de um firewall ou de um roteador NAT (conversão de endereços de rede), o firewall ou o roteador devem estar configurados para permitir que o tráfego passe através do Console corporativo. Dependendo do firewall ou roteador, pode ser necessário configurar os computadores com o endereço IP do firewall para que o tráfego possa ser transmitido.



O Deep Freeze configura automaticamente as exceções necessárias no Windows Firewall. Não é necessário configurar manualmente o Windows Firewall.

Para obter mais informações sobre a configuração e o uso do Deep Freeze em um ambiente de rede específico, consulte [Apêndice B](#) ou entre em contato com o suporte técnico.

Se um número de porta diferente do padrão de 7725 (registrada para o Deep Freeze) for usado, deve-se ter cuidado para assegurar que não existam conflitos com aplicativos já em execução na rede. Portas amplamente conhecidas (0-1023) devem ser evitadas e quaisquer Portas Registradas (1024-49151) deve ser verificadas quanto a conflitos antes da implantação.



Recomenda-se usar portas no intervalo não alocado acima de 49152. Usando a segmentação de portas, você pode isolar um laboratório ou prédio por número de porta configurando o número de porta das estações de trabalho e no Console corporativo do Deep Freeze. Usando este método, você pode fornecer funções de gerenciamento para um conjunto específico de estações de trabalho e não para toda a organização. As exceções de porta UDP e TCP dessas portas serão necessárias. Para obter mais informações, consulte [Exemplo 3 - Várias portas, Console acessado remotamente](#).

Uma lista completa das portas atribuídas a diversos aplicativos pode ser encontrada no site Internet Assigned Numbers Authority em <http://www.iana.org/assignments/port-numbers>.

Opções avançadas

- *Desative opções da linha de comando* - essa opção fica selecionada por padrão. Desmarcar essa caixa permite personalização adicional do programa de instalação do Deep Freeze quando usar o Sistema de instalação em segundo plano. Selecionar esta opção evita que as escolhas de configurações pré-existentes sejam alteradas durante a instalação.
- *Ativar políticas locais do Deep Freeze* - para melhorar a segurança, o Deep Freeze remove os seguintes privilégios locais: Programas de depuração, modificações de firmware e alterações de tempo do sistema; limpe estas opções para usar os privilégio existentes.
- *Permitir que o usuário altere o relógio* - Selecione esta opção para permitir aos usuários Congelados ajustar o relógio do sistema. Ative esse recurso durante o Horário de Verão para permitir que o Windows atualize o horário automaticamente a cada temporada.
- *Gerenciar senha do canal seguro* — A senha do canal seguro é um recurso de todos os sistemas operacionais no Windows e somente é aplicável se o sistema está executando o Windows Server Domain Environment. A senha do canal seguro é usada para comunicações seguras entre o servidor e as estações de trabalho. A senha de canal seguro é alterada automaticamente com base nas configurações do sistema operacional. Enquanto usa o Deep Freeze, a senha de canal seguro recém alterada foi perdida na reinicialização. A opção *Gerenciar senha do canal seguro* evita essa situação. O recurso Gerenciar senha do canal seguro do Deep Freeze altera o



valor da Política de grupo *Idade máxima da senha da conta da máquina* com base no estado do Deep Freeze (*Congelado* ou *Descongelado*).

- Selecione a opção *Gerenciar senha do canal seguro* se deseja o Deep Freeze para gerenciar a Senha do canal seguro.

Quando a estação de trabalho está Congelada: A estação de trabalho não alterará a Senha do canal seguro. Isso assegura que as comunicações seguras entre o servidor e a estação de trabalho sempre são mantidas.

Quando a estação de trabalho está Descongelada: A estação de trabalho alterará a Senha de canal seguro e sincronizará a senha com o servidor.

- Não selecione a opção *Gerenciar senha do canal seguro* se não deseja que o Deep Freeze gerencie a Senha do canal seguro.

Quando a estação de trabalho está Congelada: Quando a Senha do canal seguro é alterada e sincronizada com o servidor, ela é redefinida para a senha antiga na inicialização.

Quando a estação de trabalho está Descongelada: Se a estação de trabalho está *Descongelada* no dia a Senha do canal seguro é alterada, a senha nova tem efeito e a estação de trabalho é sincronizada com o servidor.



O recurso Gerenciar a Senha de canal seguro do Deep Freeze que sempre substitui a Política de grupo *Idade máxima da senha da conta da máquina*.

Configurar a seguinte Política de grupo do recurso Senha do canal seguro para trabalhar:

Controlador de Domínio: Recuse alteração da senha da conta da máquina para Não Definido

- *Reiniciar no logoff* - Selecione esta caixa para *Reiniciar* automaticamente o computador quando ele é desligado. Se esta opção é selecionada, o computador é reinicializado quando um usuário se desconecta em um estado *Congelado*.
- *Proteger Registro mestre de inicialização (MBR)* - marque esta caixa de seleção caso deseje que o Deep Freeze proteja o Registro mestre de inicialização. Se esta opção estiver selecionada, as alterações ao Registro mestre de inicialização são revertidas na inicialização quando o computador estiver no estado *Congelado*.
- *Atrasar reinicialização Frozen para concluir tarefas do Windows* - selecione esta opção para atrasar a reinicialização em um estado *Frozen* se a configuração ou a instalação de atualizações do Windows estiverem pendentes durante uma tarefa Windows Update. Se você selecionar esta opção e executar atualizações do Windows (por meios diferentes do Deep Freeze), reinicializar em estado *Frozen* garantirá que toda instalação e configuração de atualizações do Windows esteja concluída antes de reinicializar em estado *Frozen*.



Se você selecionar *Atrasar reinicialização Frozen para concluir atualizações do Windows* e instalar o Deep Freeze, o instalador verificará se todas as atualizações do Windows foram concluídas. Se as atualizações do Windows não foram concluídas, a instalação do Deep Freeze não continuará. Conclua as atualizações do Windows e tente instalar o Deep Freeze novamente.

Se você desabilitar *Atrasar reinicialização Frozen para concluir atualizações do Windows* e instalar o Deep Freeze, certifique-se de que todas as atualizações do Windows foram concluídas manualmente. Desabilitar esta opção pode resultar no travamento do computador em um ciclo de reinicialização para atualizações incompletas do Windows.

Exemplo

Em um ambiente de domínio Windows usando o Windows Server 2008 R2 que gerencia múltiplas estações de trabalho, a Senha de canal seguro é usada para comunicação segura entre o servidor e as estações de trabalho.

No Administrador de Configuração do Deep Freeze, vá para a guia *Opções avançadas* e selecione *Gerenciar senha do canal seguro*. Crie o arquivo de instalação da estação de trabalho e implante-o na estação de trabalho.

Configurar a seguinte Política de grupo do recurso Senha do canal seguro para trabalhar:

Controlador de Domínio: Recuse alteração da senha da conta da máquina para Não Definido

Membro de Domínio: Desabilitar alterações da senha da conta da máquina para Desabilitado

Quando a estação de trabalho está congelada, a Senha de canal seguro não é alterada. Quando a estação de trabalho está descongelada, a Senha do canal seguro é alterada na estação de trabalho e sincronizada com o servidor.

Modo Furtivo

- *Mostrar o ícone Congelado na bandeja do sistema* - Selecione esta opção para exibir o ícone para indicar que o Deep Freeze está instalado e o computador está Congelado.
- *Mostrar o ícone Descongelado na bandeja do sistema* - Selecione esta opção para exibir o ícone para indicar que o Deep Freeze está instalado e o computador está Descongelado.

Se as opções para mostrar um ícone do Deep Freeze na bandeja do sistema estiverem desmarcadas, o atalho de teclado CTRL+ALT+SHIFT+F6 deverá ser usado para acessar a caixa de diálogo de logon.

Licença

- *Chave de licença* - Clique em *Editar* e insira a chave de licença.
- *Tipo de chave de licença* - o tipo de chave de licença é exibido. Este campo é exibido se esta for uma versão de avaliação ou uma versão completa.
- *Data de expiração* - A *Data de expiração* do Deep Freeze é exibida.



A chave de licença pode ser atualizada das seguintes maneiras:

- através do arquivo de instalação da estação de trabalho - a chave da licença é atualizada no Administrador de configuração e um arquivo de instalação da estação de trabalho é criado. A chave de licença agora faz parte do arquivo de instalação da estação de trabalho.
- Através do Console corporativo - a chave de licença pode ser atualizada diretamente na Console corporativa. Quando a chave de licença é atualizada no Console corporativo, ela é automaticamente atualizada em todos os computadores conectados. Para obter mais informações sobre a atualização diretamente através do Console corporativo, consulte a seção *Licenciamento*.
- Manualmente em cada computador - a chave de licença pode ser atualizada manualmente em cada computador. Para obter mais informações, consulte a seção *Guia Status*.



Ao baixar atualizações da versão do Deep Freeze Enterprise de www.faronicslabs.com lembre-se de que você irá precisar copiar e colar a mais nova chave de licença de sua conta para uso na instalação. A Faronics atualiza a chave de licença a cada revisão do software. Sua conta no Faronics Labs será atualizada com a nova chave de licença em cada versão.



Criando o Programa de Instalação de Estação de Trabalho e a Seed da estação de trabalho

Para criar arquivos personalizados de programa de instalação do Deep Freeze com todas as opções que foram configuradas nas seções anteriores, clique no botão *Criar* na barra de ferramentas do Administrador de configuração e selecione *Criar Programa de Instalação da Estação de Trabalho*.



O nome de arquivo padrão deste programa é *DFWks.exe*. Recomendamos que você mantenha o nome padrão, mas em implantações maiores você deve incluir sufixo com informações relacionadas à sua configuração, como: *DFwks_10gbThawSpace.exe* ou *DFWks_NoMaintenance.exe* ou *DFwks_Wed-5pmUpdates.exe* para ajudar na organização e identificação das funções do instalador. A mesma recomendação se aplica a arquivos de configuração *Deep Freeze (.rdx)* também.

Então, este arquivo pode ser utilizado para instalar o Deep Freeze nos computadores utilizando:

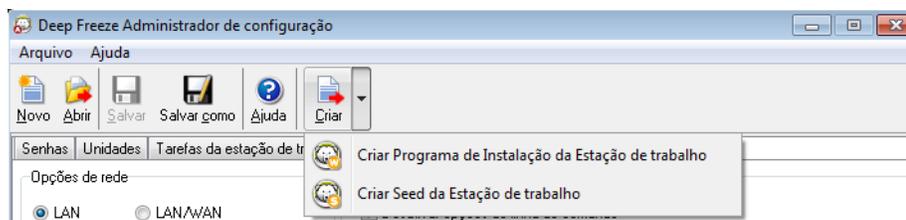
- Instalação assistida (instalação baseada nas entradas do usuário)
- Sistema de instalação em segundo plano — instalação que não informa o andamento ao usuário e nem exibe mensagens durante a sua execução). Para obter mais informações sobre o comando de Instalação em segundo plano, consulte Instalação ou desinstalação em segundo plano, página 101.
- Instalação de destino — Através do Console corporativo do Deep Freeze para estações de trabalho que já contém uma Seed ou versões anteriores do Deep Freeze que foram criadas com o mesmo Customization Code.

Para criar uma Seed da estação de trabalho, clique no botão *Criar* na barra de ferramentas do Administrador de configuração e selecione *Criar arquivo da Seed da estação de trabalho*. A Seed da estação de trabalho é um programa leve que permite aos administradores instalar e controlar remotamente os computadores a partir do Console corporativo. A Seed da estação de trabalho pode ser instalada como parte de uma imagem mestra e depois implantada via um software de imagem. Todos os computadores da LAN com a Seed da estação de trabalho instalada são exibidos no Console corporativo. O nome de arquivo padrão para este programa é *DFWksSeed.exe*.

Todos os arquivos são salvos na pasta *Deep Freeze Enterprise/Instalar programas* por padrão. Um local diferente pode ser escolhido e o nome do arquivo pode ser alterado se necessário. Recomenda-se que seja usada uma convenção de nomenclatura se você estiver criando múltiplos arquivos de instalação personalizados.



Os arquivos *DFwks.exe*, *DFwksseed.exe* e *depfrz.rdx* podem ser criados e implantados de forma intercambiável para qualquer computador Deep Freeze que usa o mesmo Customization Code. A Seed do Deep Freeze pode ser usada como um modelo/espaco reservado para assegurar que seus elementos básicos como senhas, configuração de rede ou tarefas de estação de trabalho padronizadas sejam todas consistentes. A seed não irá usar nenhuma das definições de configuração, mas as reterá no arquivo. Para usar o arquivo como um modelo basta abrir o arquivo *DFwksseed.exe* usando o Administrador de configuração e fazer quaisquer alterações necessárias. Depois, para criar a instalação da estação de trabalho, clique em *Criar > Criar arquivo de instalação da estação de trabalho*.



Recomenda-se restringir o uso do Administrador de configuração em ambientes maiores por motivos de segurança; Isso pode ser feito protegendo-se o Administrador do Deep Freeze com senha ou alternativamente, tornando-o indisponível através da remoção do arquivo DFAdmin.exe da pasta `c:\program files\faronics\Deep Freeze 7 Enterprise`. Este arquivo pode ser movido para a estação de trabalho do Administrador de domínio e excluído do Console corporativo comum do Deep Freeze. Ele pode ser restaurado copiando-o de outra instalação da mesma versão e autorizando o uso da senha OTP ou através da reinstalação ou atualização do Deep Freeze Enterprise usando-se o mesmo Customization Code.



Usando o Console corporativo do Deep Freeze

Este capítulo descreve o uso do Console corporativo do Deep Freeze.

Tópicos

[Configuração do Deep Freeze](#)

[Console corporativo do Deep Freeze](#)

[Gerenciando a comunicação entre o Console e as estações de trabalho](#)

[Consoles remotos](#)

[Conectando-se a um console remoto](#)

[Gerenciando o Deep Freeze com o Console](#)

[Licenciamento](#)

[Agendando tarefas do Deep Freeze](#)

[atribuindo computadores a tarefas agendadas](#)

[Gerenciando Rede e grupos](#)

[Histórico](#)

[Adicionando computadores a um grupo](#)

[Configurar ações personalizadas](#)

[Personalizador de console](#)

[Desligamento do Console corporativo do Deep Freeze](#)

[Instalação do Deep Freeze na estação de trabalho](#)

[Desinstalando o Deep Freeze na estação de trabalho via Console](#)

[Instalação ou desinstalação em segundo plano](#)

[Verificar atualizações](#)

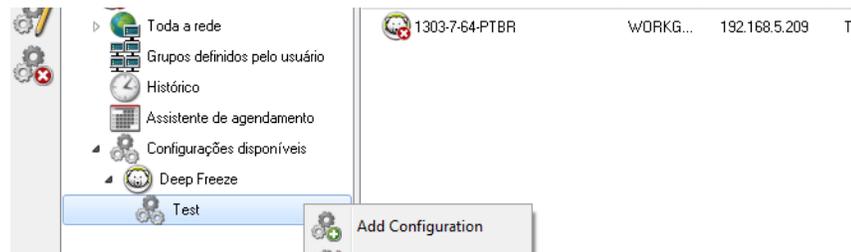


Configuração do Deep Freeze

Uma configuração do Deep Freeze é um grupo de definições que determinam o comportamento do Deep Freeze na estação de trabalho. As configurações do Deep Freeze podem ser criadas e aplicadas através do Console do Deep Freeze.

Conclua as etapas a seguir para criar uma configuração do Deep Freeze:

1. Inicie o Console do Deep Freeze
2. Vá para *Rede e grupos* > *Configurações disponíveis* > *Deep Freeze*.
3. Clique com o botão direito e selecione *Criar nova configuração*.



4. Selecione ou especifique as configurações de cada guia conforme descrito em [Utilizando o administrador de configuração Deep Freeze](#).
5. Clique em *Ok*.
6. Especifique o nome da configuração e clique em *OK*.

Aplicando a Configuração do Deep Freeze

Quando a configuração é criada, ela pode ser aplicada a múltiplas estações de trabalho.

Conclua as etapas a seguir para aplicar a configuração do Deep Freeze:

1. Vá para o painel *Estações de trabalho*.
2. Selecione uma ou mais estações de trabalho.
3. Clique com o botão direito e selecione *Atualizar configuração* > *Deep Freeze* > *[Nome da configuração]*.

A configuração será aplicada às estações de trabalho selecionadas.

Editando a configuração do Deep Freeze

Conclua as etapas a seguir para editar a configuração do Deep Freeze:

1. Vá para o painel *Redes e grupos* no Console corporativo.
2. Selecione *Configurações disponíveis* > *Deep Freeze* > *[Nome da configuração]*.
3. Clique com o botão direito na configuração selecionada e selecione *Editar configuração selecionada*.
4. Edite as configurações conforme necessário.
5. Clique em *Ok*.



Excluindo a configuração do Deep Freeze

Conclua as etapas a seguir para excluir a configuração do Deep Freeze:

1. Vá para o painel Redes e grupos no Console corporativo.
2. Selecione *Configurações disponíveis* > *Deep Freeze* > *[Nome da configuração]*.
3. Clique com o botão direito na configuração selecionada e selecione *Excluir configuração selecionada*.
4. Clique em *Ok*.

Exportando a configuração do Deep Freeze

Conclua as etapas a seguir para exportar a configuração do Deep Freeze:

1. Vá para o painel Redes e grupos no Console corporativo.
2. Selecione *Configurações disponíveis* > *Deep Freeze* > *[Nome da configuração]*.
3. Clique com o botão direito na configuração selecionada e selecione *Exportar como*. Há três opções:
 - Selecione Instalador de estação de trabalho. Especifique um nome e clique em *Salvar*.
 - Selecione Seed da estação de trabalho. Especifique um nome e clique em *Salvar*.
 - Selecione Arquivo de configuração. Especifique um nome e clique em *Salvar*.



Console corporativo do Deep Freeze

O Console corporativo do Deep Freeze exibe o status de todas as estações de trabalho congeladas, descongeladas e computadores de destino da rede e permite que o administrador execute tarefas específicas nestes computadores. Informações de status detalhadas estão disponíveis com relatórios seletivos ou de grupo.

O Console corporativo permite aos administradores executar remotamente as seguintes tarefas:

- Imediatamente instalar computadores de destino
- Seletivamente congelar, descongelar ou descongelar bloquear um ou mais computadores
- Bloquear ou desbloquear computadores selecionados
- Reiniciar ou desligar computadores
- Parar manutenção agendada
- Ligar computadores equipados com uma placa de rede Wake-on-LAN
- Atualizar o software Deep Freeze
- Agendar tarefas diretamente do Console
- Enviar mensagens aos computadores.
- Importar grupos e contêineres do Active Directory
- Gerar senhas para uso único
- Agendar ações
- Personalizar o Console corporativo
- Atualizar a chave de licença

O Console corporativo só será capaz de ativar um computador do estado de desligado se este estiver devidamente configurado para ser ativado ao receber um pacote Wake-on-LAN.

Iniciando o Console corporativo

O Console corporativo é instalado com o Administrador de configuração do Deep Freeze. Abra o Console selecionando o seguinte caminho no menu Iniciar:

Iniciar > Todos os programas > Faronics > Deep Freeze 7 Enterprise > Console do Deep Freeze

Ativando o Console corporativo

Como um recurso de segurança do Deep Freeze Enterprise o recurso OTP impede o uso não autorizado do Console corporativo do Deep Freeze. Quando o arquivo *DFConsole.exe* é copiado para um novo computador, o Console deve ser ativado. Quando ele é executado pela primeira vez no novo computador, uma caixa de diálogo é exibida com um Token OTP.

O administrador de rede insere este token no Sistema de geração OTP do Administrador de configuração. Um OTP é gerado. Insira na caixa de diálogo e o Console será executado.



O computador no qual o Console corporativo está instalado não deve ter uma instalação da Seed da estação de trabalho (usando a mesma porta) nem uma instalação do Deep Freeze completo.

Ícones de status

O Console corporativo exibe o status dos computadores na rede de área local com os seguintes ícones ao lado ou acima do nome do computador, dependendo da visualização selecionada:

Ícone	Definição
	Destino: Os computadores que têm a Seed da estação de trabalho do Deep Freeze instalada, mas não têm o Deep Freeze instalado; o Deep Freeze só pode ser remotamente instalado em computadores com este ícone.
	Computadores com o Deep Freeze instalado em um estado congelado
	Computadores com o Deep Freeze instalado em um estado descongelado
	Computadores com o Deep Freeze instalado em um estado descongelado bloqueado
	Computadores que estão atualmente desligados
	Computadores que estão atualmente no Maintenance Mode
	Computadores cuja comunicação com o Console foi interrompida
	Computadores que estão bloqueados



Exibir colunas

O console corporativo do Deep Freeze oferece a capacidade de especificar colunas a que são exibidas no painel Estações de trabalho. Siga estas etapas para exibir as colunas desejadas:

1. Vá para *Exibir* > *Colunas*.
2. Selecione as colunas seguintes para exibição:
 - Configuração
 - Data da configuração
 - Data de expiração
 - Arquivo de instalação
 - Endereço IP
 - Status da licença
 - Nome de login
 - Endereço MAC
 - Sistema operacional
 - Porta
 - Status
 - Versão
 - Grupo de trabalho
 - Anti-Virus



Seleção com base no status

Você pode selecionar as estações de trabalho com base no status do Deep Freeze nas estações de trabalho gerenciadas. A seleção com base no status pode ser feita por meio do menu *Selecionar* no console corporativo do Deep Freeze. O menu Selecionar tem as seguintes opções:

- Selecionar todas as congeladas: seleciona todas as estações de trabalho no estado Congelado. Estações de trabalho Congeladas e Bloqueadas também são selecionadas.
- Selecionar todas as descongeladas: seleciona todas as estações de trabalho no estado Descongelado. Estações de trabalho Descongeladas e Bloqueadas também são selecionadas.
- Selecionar todos de Destino: seleciona todos os computadores de destino nos quais o Deep Freeze possa estar instalado.
- Selecionar tudo: seleciona todas as estações de trabalho.

As opções de seleção seguintes também estão disponíveis no painel Status:

- Congeladas: seleciona as estações de trabalho no estado Congelado. Estações de trabalho Congeladas e Bloqueadas também são selecionadas.
- Descongeladas: seleciona as estações de trabalho no estado Descongelado. Estações de trabalho Descongeladas e Bloqueadas também são selecionadas.
- Destino: seleciona todos os computadores de destino nos quais o Deep Freeze possa estar instalado.
- Histórico: exibe o histórico.
- Total: seleciona todas as estações de trabalho.

O painel de status no console corporativo do Deep Freeze também pode ser usado para selecionar e exibir a contagem de estação de trabalho em um estado específico.

Rede e grupos		Estações de trabalho					
[localhost:7725]		Estações de trabalho	Grupo de...	Endereço IP	Status	Confi...	Data da c...
Toda a rede		1303-7-64-E5	WORKG...	192.168.5.207	Congelada	DFWks	Não dis
Grupos definidos pelo usuário		1303-7-64-PTBR	WORKG...	192.168.5.209	Thawed	Test	Não dis
Histórico							
Assistente de agendamento							
Configurações disponíveis							
Deep Freeze							

Congelada	1	
Thawed	1	
Destino	0	
Histórico	0	
Total	2	



Gerenciando a comunicação entre o Console e as estações de trabalho

Existem dois tipos de conexões do Console para a estação de trabalho e do Console para Console:

1. Conexões locais — conexões que só podem ser acessadas pelo console corporativo que as hospeda.
2. Conexões ativadas por controle remoto — conexões que podem ser acessadas pelo console que as hospedas, bem como por outros consoles conectados remotamente.



O Serviço de servidor do Deep Freeze 6.5 não irá atualizar automaticamente o Serviço de servidor do Deep Freeze 6.4 ou anterior. Ambos os serviços podem ser instalados no mesmo computador, mas somente um serviço poderá ser executado por vez.

Um computador pode perder a comunicação com o Console por qualquer um dos seguintes motivos:

- O computador é desligado manualmente ou é desligado sem aviso
- A rede está experimentando tráfego pesado ou falhas
- As configurações de rede do computador são alteradas para apontar para um novo console

Na maioria dos casos, a comunicação com o computador é restabelecida quando o computador é ligado ou quando as condições que estão causando a interrupção nas comunicações são corrigidas. Pode levar diversos minutos para o computador responder ao Console e restabelecer a comunicação. Se a comunicação não puder ser restabelecida, entre em contato com o [Suporte técnico](#) para obter as etapas para solução de problemas.

Configurando o serviço local

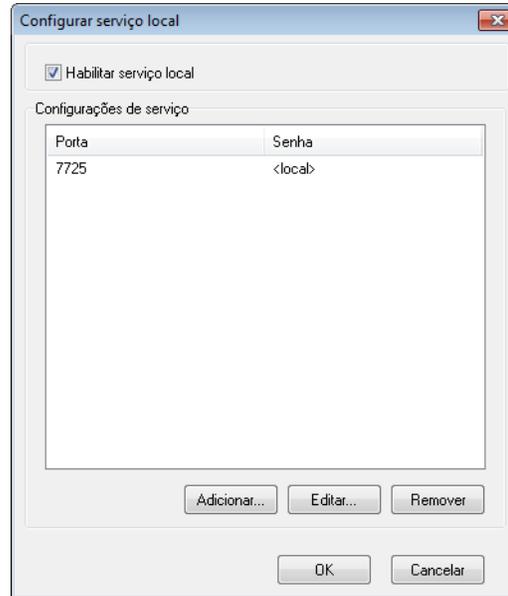
O serviço local é um serviço que estabelece e mantém conexões com os computadores.

Ativando o serviço local

Por padrão, o serviço local será instalado e ativado quando o Console é executado pela primeira vez.

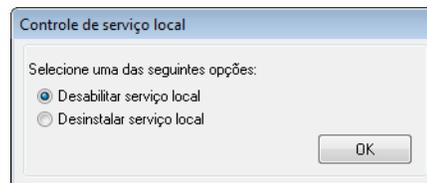
Para ativar o serviço local novamente se ele tiver sido desativado (e/ou desinstalado)

1. Selecione *Ferramentas > Configuração de rede*.
2. Marque a caixa de seleção *Habilitar serviço local* para ativá-lo.



Desativando o serviço local

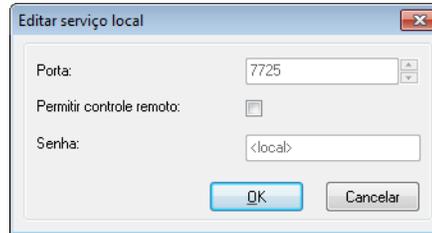
Desmarcar a caixa de seleção *Habilitar serviço local* e clicar em *OK* exibe a opção para desativar ou desinstalar o serviço local.



Adicionando uma conexão de serviço local

1. Para adicionar uma conexão de serviço local, selecione *Ferramentas > Configuração de rede*.
2. Para adicionar uma conexão selecione Adicionar e especifique o número da porta (7725 neste caso).
3. Para ativar o Console para ser controlado remotamente, marque a caixa de seleção *Permitir controle remoto* e especifique uma senha.

Depois de selecionar *Adicionar*, uma conexão que atende a porta 7725 será criada na lista de conexões do serviço local e também no painel da rede do Console.



Editando ou removendo uma conexão de serviço local

Quando uma conexão de serviço local tiver sido adicionada, ela pode ser editada ou removida através das opções *Ferramentas > Configuração de rede*.

Para editar uma conexão de serviço local execute as seguintes etapas:

1. Assegure-se de que a opção *Habilitar serviço local* esteja selecionada.
2. Selecione uma porta da lista de conexões do serviço local e clique em *Editar*.
3. A caixa de diálogo *Editar* é exibida e permite que a porta seja controlada remotamente e protegida por senha.
4. Para remover uma porta do serviço local, destaque a porta e clique em *Remover*. Isso não exclui a entrada do painel *Rede e grupos* no Console corporativo. Isso simplesmente remove-a da lista de conexões do serviço local.
5. Para remover a entrada do painel de rede no Console, selecione-a e clique no ícone *Remover* localizado na barra lateral.



Consoles remotos

Um Console remoto é um Console que hospeda uma ou mais conexões que permitem que outros Consoles se conectem. As conexões existentes devem ser editadas para permitir que elas sejam acessadas remotamente.

Configurando conexões ativadas por controle remoto

Para permitir que uma conexão seja acessada remotamente realize as seguintes etapas:

1. Abra *Ferramentas > Configuração de rede*.
2. Marque a caixa de seleção *Habilitar serviço local*.
3. Selecione uma porta da lista e clique em *Editar*.
4. Assegure-se de que *Permitir controle remoto* esteja selecionada.
5. Especificar uma senha.
6. Clique em *Ok*.



Conectando-se a um console remoto

Quando um console remoto tiver sido estabelecido pelo console host ele pode ser acessado por outros consoles a partir de uma máquina diferente.

1. Selecione o ícone *Conectar ao console remoto* na barra lateral ou clicando com o botão direito no item de rede. Ao selecionar, a caixa de diálogo *Conectar ao console remoto* aparece:

The screenshot shows a dialog box titled "Conectar ao console remoto". It has a close button (X) in the top right corner. The fields are: "Nome do console remoto" with a placeholder "[0.0.0.0:1]"; "IP do console remoto" with a placeholder "0.0.0.0"; "Nº da porta" with a value of "1" and up/down arrow buttons; and "Senha" with an empty text box. At the bottom, there are two buttons: "Conectar" and "Cancelar".

2. Na caixa de diálogo *Conectar ao console remoto*, especifique os detalhes da conexão como *Nome do console remoto*, *IP do console remoto*, *Número de porta* e *Senha*. Estas informações são fornecidas pelo administrador do console host. Quando inseridas, estas informações podem ser recuperadas clicando-se com o botão direito do mouse em uma porta no painel *Redes e grupos* e selecionando-se *Propriedades*.



Se a conexão com um console remoto tiver sido interrompida, ela pode ser reconectada clicando-se no ícone *Reconectar ao console remoto* na barra lateral ou clicando-se em uma entrada no painel *Redes e grupos*.



Gerenciando o Deep Freeze com o Console

O Console corporativo contém uma barra de ferramentas na parte superior da tela que permite o acesso rápido às funções do Console.

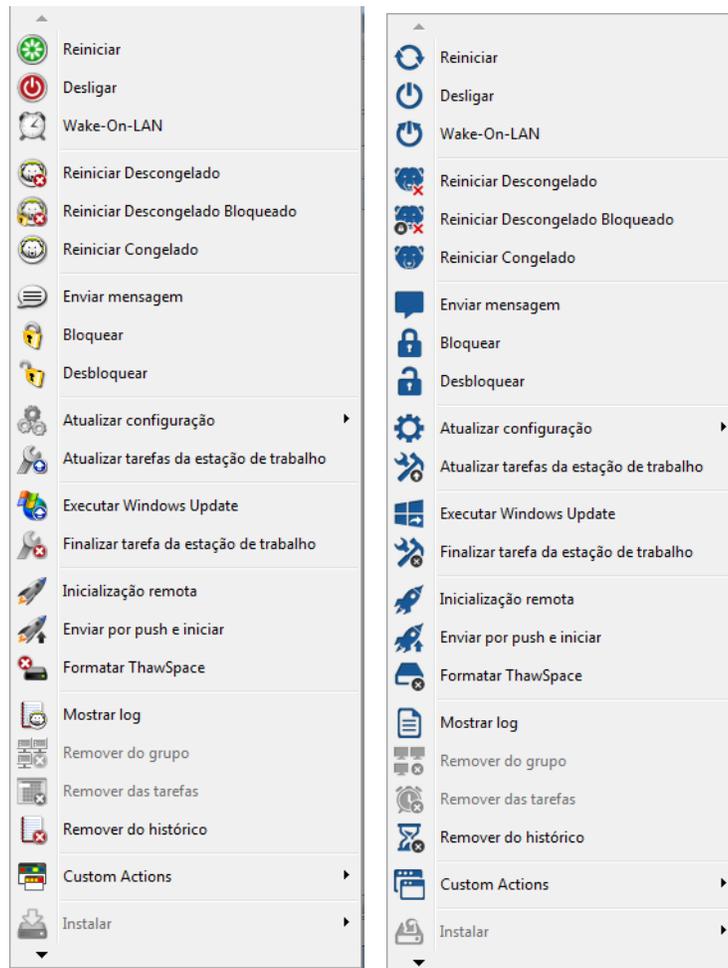
Vá para *Exibir > Aparência clássica* para exibir os ícones no formato Windows clássico.



Vá para *Exibir > Aparência moderna* para exibir os ícones no formato Windows moderno.



Esses comandos também podem ser acessados usando o menu contextual, conforme mostrado a seguir, que aparece clicando-se com o botão direito em um ou mais computadores. Quando uma ação particular é escolhida, o computador selecionado realiza a ação e os ícones de status são atualizados de forma correspondente. Se vários computadores forem selecionados, a ação só será aplicada nos computadores aplicáveis. Por exemplo, se você selecionar computadores que estejam Descongelados e Congelados, e aplicar a ação Reinicializar descongelado, somente os computadores Congelados serão Descongelados. A ação não será aplicada nos computadores já Descongelados.





Ícones específicos são desativados se o computador selecionado não suporta aquela ação. Por exemplo, um computador que tem um ícone *Destino*, não irá mostrar a opção para ser Descongelado ou Congelado, porque o programa ainda não está instalado.

Atualizando o software Deep Freeze

Para atualizar computadores Deep Freeze (onde o Deep Freeze 7.7 ou posterior está instalado) com uma nova versão do Deep Freeze, execute as seguintes etapas:

1. No Console corporativo, selecione os computadores a serem atualizados. Os computadores podem estar em um estado Congelado ou Descongelado.
2. Clique com o botão direito e selecione *Atualizar Deep Freeze* no menu contextual.
3. Os computadores selecionados são atualizados para a nova versão do software Deep Freeze, mas reterão todas as configurações da versão atual. Os computadores serão reinicializados duas vezes para concluir a atualização.

Enviando mensagens a computadores

Para enviar uma mensagem a um ou mais computadores, execute as seguintes etapas:

1. Selecione os computadores para onde será enviada uma mensagem.
2. Clique com o botão direito e selecione *Enviar mensagem* no menu contextual.
3. Digite a mensagem na caixa de diálogo que aparece e clique em *Enviar*. É exibida uma caixa de diálogo que pede a confirmação para enviar a mensagem para os computadores selecionados.
4. Clique em *OK* para enviar ou *Cancelar* para fechar a caixa de diálogo sem enviar a mensagem.

Destino instalando o Deep Freeze

Execute as seguintes etapas para instalar remotamente uma instalação de estação de trabalho completa em qualquer computador que tenha a Seed da estação de trabalho instalada.

1. Clique com o botão direito em um ou mais computadores e selecione *Instalar*. Uma caixa de diálogo é exibida, e pergunta se a instalação deve continuar. Clique em *Ok*.
2. É exibida uma caixa de diálogo para selecionar o arquivo a ser instalado no computador remoto.
3. Selecione o arquivo de instalação a ser usado e clique em *Abrir*.
4. O computador instala o Deep Freeze e reinicia.
5. Quando a instalação for concluída, o Console corporativo refletirá a alteração no status do computador, e exibirá que ele está *Congelado*.

Atualizando um arquivo de configuração do Deep Freeze

Execute as etapas a seguir para atualizar a configuração em ou em diversos computadores com as configurações de um arquivo *.rdx* existente. (Um arquivo *.rdx* é um arquivo que contém as condições especificadas no Administrador de configuração Deep Freeze).



1. Clique com o botão direito do mouse nos computadores e selecione *Atualizar com arquivo RDX*.
2. Aparece uma mensagem solicitando que um arquivo *.rdx* existente seja localizado.
3. Clique em *Ok*. Uma caixa de diálogo *Abrir arquivo* padrão é exibida para selecionar um arquivo *.rdx*.
4. Localize um arquivo e clique em *Abrir* para atualizar a configuração nos computadores selecionados com as configurações no arquivo *.rdx*. Clique em *Cancelar* para cancelar a atualização da configuração.

Executar Windows Update

As atualizações do Windows podem ser aplicadas sob demanda clicando-se com o botão direito do mouse no menu de contexto.

Execute as etapas a seguir para executar atualizações do Windows na estação de trabalho.

1. Clique com o botão direito do mouse nos computadores e selecione *Executar Windows Update*.
2. Clique em *Ok*.

As atualizações do Windows são aplicadas nas estações de trabalho selecionadas. As configurações definidas na guia *Guia Windows Update* são usadas.

Além de aplicar atualizações do Windows sob demanda a partir do clique com o botão direito do mouse no menu de contexto, você também pode agendar a tarefa de atualizações do Windows. Para obter mais informações, consulte *Agendando tarefas do Deep Freeze* para saber como agendar uma tarefa de atualizações do Windows.



Se as opções de rede na nova configuração tiverem alterado, os computadores podem perder comunicação com o Console corporativo existente. Se a comunicação com os computadores estiver perdida, verifique as configurações de rede nos computadores atualizados para assegurar que os números de portas e/ou o endereço IP do Console não foram alterados.



As alterações nas senhas entram em vigor imediatamente. Todas as outras alterações entram em vigor após cada computador ser reiniciado. Unidades ThawSpace e/ou Congeladas não podem ser alteradas através da atualização do arquivo de configuração.

Formatar ThawSpace

O console corporativo do Deep Freeze oferece a capacidade de formatar todos os ThawSpaces remotamente em estações de trabalho gerenciadas.

Siga estas etapas para formatar o ThawSpaces:

1. Selecione uma ou várias estações de trabalho.
2. Clique com o botão direito do mouse e selecione *Formatar ThawSpace*. Como alternativa, você pode clicar no ícone *Formatar ThawSpace* na barra de ferramentas.
3. Um aviso *Todos os ThawSpaces serão formatos nos computadores selecionados* é exibido.
4. Selecione *Deseja prosseguir?* para confirmar.
5. Clique em *Ok*.



O comando Formatar ThawSpace exclui todos os dados em ThawSpaces. Os dados não podem ser recuperados depois de excluídos. Faça backup de arquivos importantes antes de formatar o ThawSpace.



Licenciamento

A chave de licença pode ser atualizada via Console corporativo.

Para atualizar a chave de licença, execute as etapas a seguir:

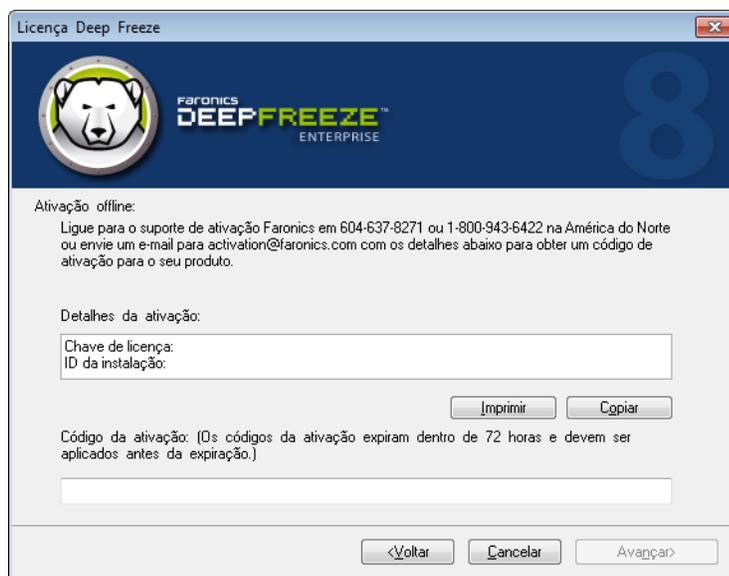
1. Iniciando o *Console corporativo*.
2. Vá para *Ferramentas > Licenciamento*.
3. A caixa de diálogo *Licença Deep Freeze* é exibida.



4. Clique em *Editar* e insira a chave de licença no campo *Chave de licença*.
5. Clique em *Atualizar licença*. Isso irá converter o Deep Freeze da versão de *Avaliação* para uma versão *Licenciada*. O campo *Tipo de chave de licença* exibe a *Chave de licença*. A *Data de expiração* exibe a data e a hora em que a licença expira.
6. Clique em *Ativação online* para ativar a Licença Deep Freeze via Internet. O computador deve estar conectado à Internet para Ativação online. A Licença Deep Freeze deve ser ativada dentro de 30 dias da instalação, caso contrário o Deep Freeze irá parar de funcionar. Durante a ativação, a Licença do Deep Freeze é autenticada na Faronics.
7. Alternativamente, clique em *Opções de ativação*. Duas opções estão disponíveis:



- Selecione *Ativação online* para ativar a Licença do Deep Freeze online. Esta opção é a mesma da etapa 1. Clique em *Avançar* depois de selecionar esta opção. O Deep Freeze é ativado online clicando em *Avançar*.
 - Selecione *Ativação offline*. Esta opção permite ativar por telefone ou e-mail. Clique em *Avançar* após a ativação. A tela *Ativação offline* é exibida.
8. Envie os *Detalhes da ativação* para o Suporte de Ativação Faronics via telefone ou e-mail. Quando tiver recebido o Código de ativação da Faronics, insira-o no campo *Código de ativação* e clique em *Avançar*. A Licença do Deep Freeze agora está ativada.



A chave de licença é automaticamente atualizada em todos os computadores que se comunicam com o Console corporativo. Se um computador estiver offline (desligado ou desconectado da rede), a chave de licença será atualizada quando o computador se comunicar com o Console corporativo da próxima vez.





Agendando tarefas do Deep Freeze

Para agendar uma tarefa do Deep Freeze no Console corporativo usando o Assistente de tarefas agendadas, execute as seguintes etapas:

1. Abra o *Assistente de tarefas agendadas* de uma das seguintes maneiras:
 - clique em *Assistente de agendamento* no painel *Redes e grupos* e clique no ícone *Adicionar tarefa*
 - clique com o botão direito do mouse em *Assistente de agendamento* no painel *Redes e grupos* e escolha *Adicionar tarefa*

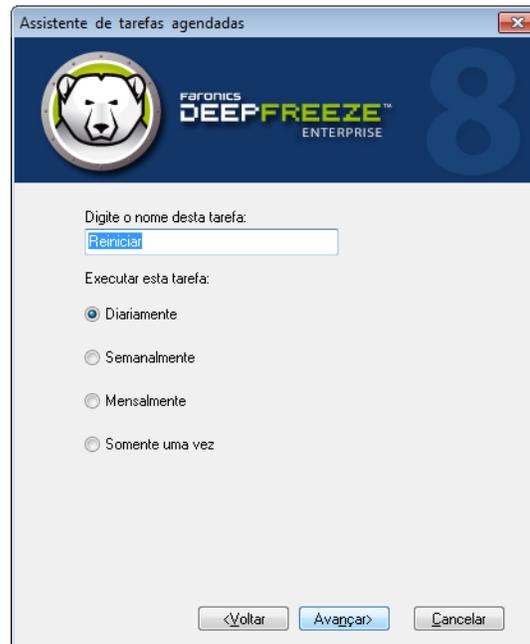
A tela a seguir é exibida:



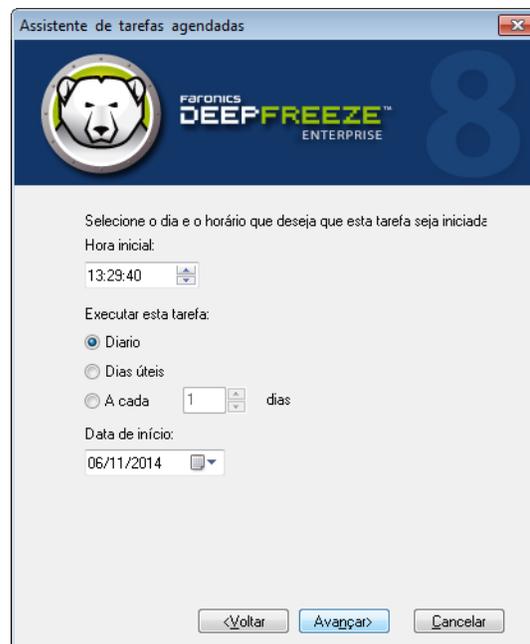
2. Clique duas vezes na tarefa preferida ou selecione a tarefa e clique em *Avançar*. As tarefas a seguir estão disponíveis para o Deep Freeze:
 - Reiniciar
 - Desligar
 - Wake-On-LAN
 - Reiniciar Congelado
 - Reiniciar Descongelado
 - Reiniciar Descongelado Bloqueado
 - Enviar mensagem
 - Executar Atualizações do Windows



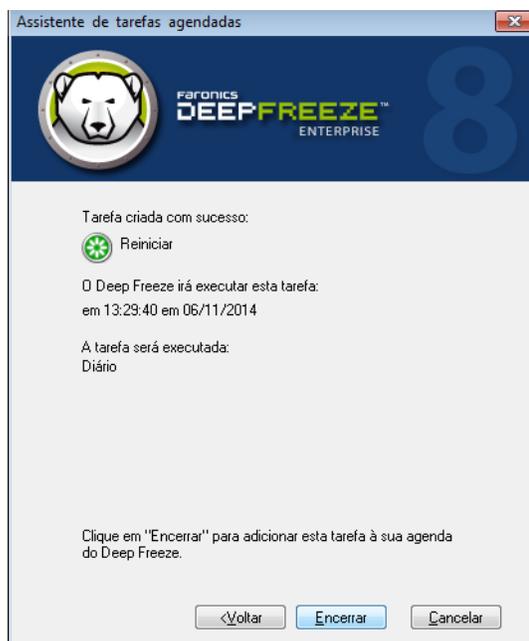
3. Na tela a seguir, insira um nome para a tarefa e escolha a agenda de execução de tarefa preferida: Diariamente, semanalmente, mensalmente ou somente uma vez. Os nomes das tarefas devem ser exclusivos. Duas tarefas não pode ter o mesmo nome. Clique em *Avançar*.



4. Dependendo da escolha da execução de tarefas, as opções de configuração de data e hora que se seguem irão variar. Clique em *Avançar*.



5. Clique em *Concluir* quando a configuração estiver concluída.

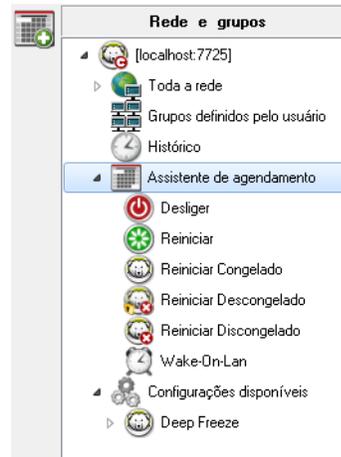


A hora inicial padrão de uma tarefa é cinco minutos a partir da hora atual.



atribuindo computadores a tarefas agendadas

Depois do agendamento de uma tarefa, ela será exibida no *Assistente de agendamento* no painel *Redes e grupos* do Console.



Para atribuir computadores a uma tarefa, selecione os computadores preferidos no painel *Estações de trabalho* no Console e arraste-os para a tarefa preferida. Ou arraste um grupo para a tarefa.

Para ver quais computadores estão atribuídos a uma tarefa específica, clique na tarefa. Os computadores atribuídos aparecem no painel *Estações de trabalho*.

Para excluir um computador de uma tarefa, clique no computador e pressione *Excluir*.

Para excluir um computador de uma tarefa, clique com o botão direito do mouse no computador e selecione *Remover da tarefa*.



Executando uma tarefa imediatamente

Para executar uma tarefa imediatamente, clique com o botão direito do mouse e selecione *Executar tarefa*.

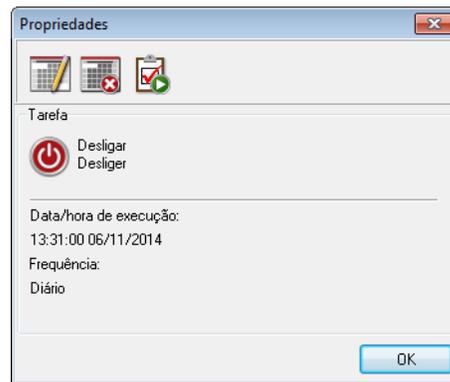
Excluindo uma tarefa

Para excluir uma tarefa, clique na tarefa e pressione *Excluir*.

Propriedades de tarefas agendadas

Para ver as propriedades de uma tarefa, clique com o botão direito no nome da tarefa e selecione *Visualizar propriedades*.

A seguinte tela será exibida:



As propriedades de uma tarefa não podem ser alteradas após ela ter sido criada. Somente os computadores que irão executar a tarefa podem ser alterados adicionando ou excluindo-se computadores.



As tarefas agendadas ainda serão executadas mesmo que o Console corporativo seja fechado, desde que o serviço local esteja ativado e as conexões de rede não sejam desligadas ao sair do Console corporativo.



Gerenciando Rede e grupos

O Console corporativo automaticamente organiza computadores por seus grupos de trabalho ou domínio. Clique no grupo de trabalho ou domínio adequado para visualizar os computadores naquele grupo de trabalho ou domínio.

O Console corporativo pode ser usado para definir os grupos específicos, a fim de organizar computadores.

Adicionando um grupo

A caixa de diálogo Adicionar grupo permite configurar vários filtros para classificar as estações de trabalho em grupos diferentes. Esse filtro atualiza automaticamente a lista de estações de trabalho com base nas alterações dos parâmetros selecionados.

Siga estas etapas para adicionar um grupo com um Filtro:

1. clique com o botão direito do mouse em *Grupos definidos pelo usuário* no painel *Rede e grupos*.
2. Selecione *Adicionar grupo*. A caixa de diálogo Adicionar grupo é exibida:

3. Especifique o *Nome do grupo*.
4. Selecione *Coluna*.
5. Selecione *Comparação*.
6. Selecione *Opção E/Ou* se estiver adicionando outro filtro.
7. Especifique *Valor* ou *Expressão regular*.
8. Clique em *Adicionar*.

A tabela seguinte mostra a Coluna, Comparação, Opção e Valores.

Selecionar Coluna	Selecionar Comparação	Selecionar Opção	Especificar Valor ou Expressão regular
Estações de trabalho	Igual a	e	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .
	Não é igual a	Ou	
	Expressão regular		



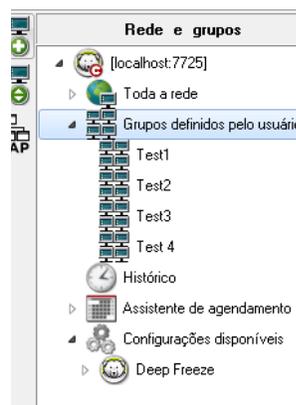
Selecionar Coluna	Selecionar Comparação	Selecionar Opção	Especificar Valor ou Expressão regular
Grupo de trabalho	Igual a Não é igual a Expressão regular	e Ou	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .
Endereço IP	Igual a Maior que Maior ou igual a Menor que Menor ou igual a Expressão regular	e Ou	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .
Status	Igual a Não é igual a Expressão regular	e Ou	Congelado Congelado e bloqueado Descongelado Descongelado e bloqueado Aplicando Windows Update Aplicando arquivo de lote Período descongelado Modo de manutenção Licença expirada Seed da estação de trabalho Desconhecido
Configuração	Igual a Não é igual a Expressão regular	e Ou	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .
Data da configuração	Igual a Maior que Maior ou igual a Menor que Menor ou igual a Expressão regular	e Ou	Especifique a <i>Data</i> .
Arquivo de instalação	Igual a Não é igual a Expressão regular	e Ou	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .



Selecionar Coluna	Selecionar Comparação	Selecionar Opção	Especificar Valor ou Expressão regular
Versão	Igual a	e	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .
	Maior que	Ou	
	Maior ou igual a		
	Menor que		
	Menor ou igual a		
Expressão regular			
	Igual a	e	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .
	Não é igual a	Ou	
Expressão regular			
Endereço MAC	Igual a	e	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .
	Não é igual a	Ou	
	Expressão regular		
Nome de login	Igual a	e	Especifique o <i>Valor</i> ou a <i>Expressão regular</i> .
	Não é igual a	Ou	
	Expressão regular		

Construindo uma estrutura de grupo definida pelo usuário

Após a adição de um grupo, um ou mais subgrupos podem ser adicionados abaixo dele, e subgrupos adicionais podem ser adicionados indefinidamente como uma maneira de diferenciar entre ambientes, como no exemplo mostrado a seguir:





Importando grupos do Active Directory

Se a estrutura de grupo já tiver sido designada dentro do Active Directory, aquela estrutura pode ser importadas diretamente no Console corporativo. Execute estas etapas para importar do Active Directory:

1. Selecione *Ferramentas* > *Importar grupos do Active Directory* ou clique no ícone *LDAP* localizado na barra lateral.
2. A caixa de diálogo a seguir será exibida. Selecione a guia *Microsoft* ou a guia *Novell*.

The screenshot shows a dialog box titled "Parâmetros do Servidor LDAP". It has two tabs: "Microsoft" and "Novell". The "Microsoft" tab is active. The dialog contains the following fields and controls:

- Servidor LDAP: Text input field.
- Domínio: Text input field.
- ID de login: Text input field.
- Senha: Password input field.
- Login anônimo: Checked checkbox.
- Buttons: "Conectar" and "Cancelar".

3. Insira as informações do servidor LDAP do local da importação. A opção para logon anônimo também está disponível. Se esta caixa de seleção não estiver marcada, um nome de usuário e uma senha serão necessários.
4. Clique em *Conectar*. A hierarquia do *Active Directory* é exibida. Selecione as entradas necessárias e clique em *Importar*.



Histórico

O Console corporativo armazena o histórico dos computadores de destino.

Se um computador estiver desconectado de uma rede, desligado ou estiver sendo reiniciado, um sinal de exclamação (!) será exibido no Console corporativo para o determinado computador. Se o computador voltar a estar online, o sinal de exclamação desaparecerá.

Se o computador permanecer offline (por exemplo, se o computador estava permanentemente desconectado da rede), ou se o computador estiver desligado, o sinal de exclamação continuará ativo.

No Console corporativo, vá para *Arquivo > Sair*. Selecione a opção *Fechar o Console do Deep Freeze e desligar conexões de rede* e clique em *OK*. Quando você reabrir o Console corporativo, os computadores com o sinal de exclamação (!) irão aparecer no Histórico. Se o computador estiver desligado e estiver equipado com o hardware Wake-On-LAN, clique com o botão direito no computador no Histórico e selecione *Wake-On-LAN* para ativar o computador.

Opções do Histórico:

- Para visualizar o histórico, clique em *Histórico* no painel *Redes e grupos*.
- Para excluir os computadores do Histórico, selecione os computadores, clique com o botão direito do mouse e selecione *Remover do Histórico* no menu de contexto.
- Para ativar o computador usando o recurso Wake-ON-LAN, selecione os computadores, clique com o botão direito e selecione *Wake-ON-LAN* no menu de contexto.



Adicionando computadores a um grupo

É possível adicionar computadores a um grupo arrastando-os do painel *Estações de trabalho* para o grupo desejado ou usando-se um filtro automático definido durante a criação dos grupos.

A filtragem automática permite que os computadores sejam adicionados automaticamente a grupos definidos por usuários. Os computadores são adicionados com base no nome do computador.

Curingas (*, ?) podem ser usado para adicionar computadores com base em um segmento específico do nome.

Exemplo: *Lab1-** adiciona todos os computadores com nomes que começam com *Lab1-* .

Ordenando grupos alfabeticamente

Para classificar os grupos alfabeticamente, clique com o botão direito em *Grupos definidos pelo usuário* e selecione *Ordenar grupos alfabeticamente*.

Removendo estações de trabalho do grupo definido pelo usuário

Para remover um computador de um grupo, clique com o botão direito do mouse no computador em *Grupos definidos pelo usuário* e selecione *Remover do grupo*.

Importando ou exportando grupos para arquivo

Para importar grupos de um arquivo ou exportar grupos para um arquivo, escolha a opção preferida do menu *Ferramentas*.



Visualizando o arquivo de log do Console

O Console corporativo mantém um log dos status e histórico das atividades de todos os computadores conectados. O log armazena informações dos 7 dias anteriores. As informações mais antigas do que 7 dias são automaticamente excluídas do log.

Estação de trab...	Domínio	Hora	Status	Endereço IP	Endereço MAC	Applied Command	Arquivo de
1303-7-64-PTBR	WORKGROUP	quinta-feira novembro 0...	Thawed	192.168.5.209	080027b18a36		Test.exe
1303-7-64-PTBR	WORKGROUP	quinta-feira novembro 0...		192.168.5.209	080027b18a36		
1303-7-64-PTBR	WORKGROUP	quinta-feira novembro 0...	Thawed	192.168.5.209	080027b18a36		Test.exe
1303-7-64-PTBR	WORKGROUP	quinta-feira novembro 0...	Thawed	192.168.5.209	080027b18a36	Licença atualizada	Test.exe
1303-7-64-PTBR	WORKGROUP	quinta-feira novembro 0...		192.168.5.209	080027b18a36		
1303-7-64-PTBR	WORKGROUP	quinta-feira novembro 0...	Thawed	192.168.5.209	080027b18a36		Test.exe
1303-7-64-PTBR	WORKGROUP	quinta-feira novembro 0...	Thawed	192.168.5.209	080027b18a36	Licença atualizada	Test.exe

- Para visualizar o arquivo de log de um ou de vários computadores, clique com o botão direito do mouse nos computadores e selecione *Mostrar log*.
- Para ordenar o arquivo de log, clique em um título que desejar. Estas colunas estão disponíveis:
 - Estação de trabalho
 - Domínio
 - Hora
 - Status
 - Endereço IP
 - Endereço MAC
 - Comando aplicado (Frozen, Thawed, Restart, Shutdown)
 - Arquivo de instalação
- Para exportar o arquivo de log, clique em Exportar como e selecione Texto ou CSV. Especifique o nome do arquivo e clique em OK.

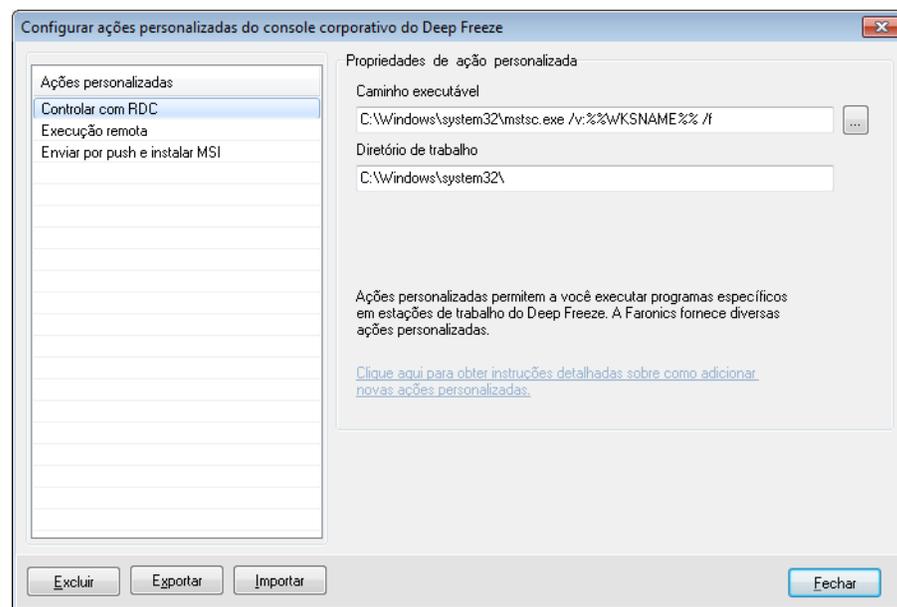


Configurar ações personalizadas

O Deep Freeze fornece as seguintes ações personalizadas que podem ser acessadas via o menu *Ações*. Ações adicionais podem ser criadas para atender a necessidades específicas. O Deep Freeze oferece três ações padrão. As ações personalizadas adicionais podem ser configuradas importando-se o arquivo *.xml* apropriado no Console do Deep Freeze. Para obter mais informações sobre Ações personalizadas, a estrutura do arquivo de ação personalizada e detalhes sobre diversos parâmetros, consulte o [Apêndice E](#).

Controlar com RDC

Isso permite a conexão com o computador através do Microsoft Remote Desktop Protocol. A Conexão de área de trabalho remota já deve estar ativada nas máquinas de destino.

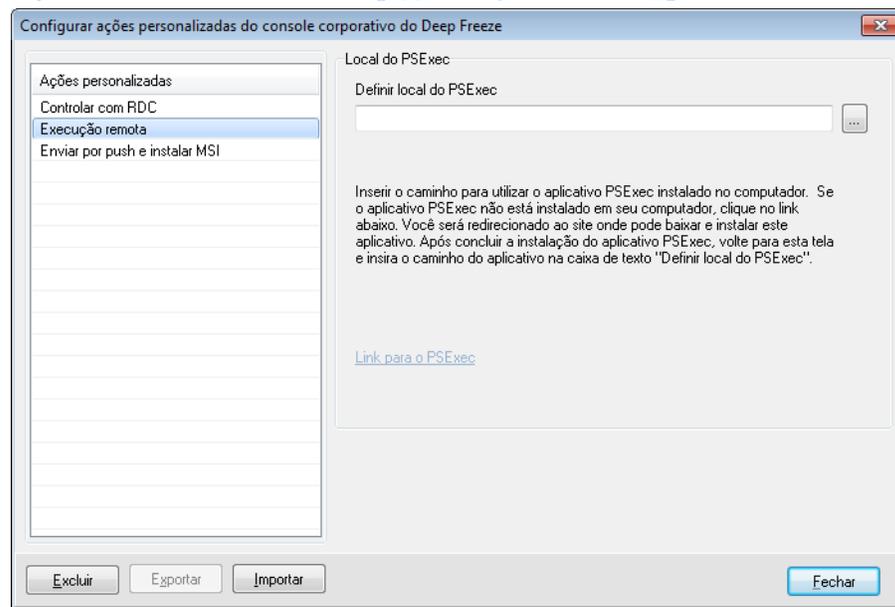


1. Vá para o menu *Ação > Ações personalizadas*.
2. Selecione *Controlar com RDC*.
3. Insira o *Caminho executável* ou navegue para selecionar o local.
4. Insira o *Diretório de trabalho*.
5. Clique em *Aplicar*.



Execução remota

A Execução remota permite remotamente executar um arquivo executável em um computador. O PsExec é uma ferramenta que pode ser usada para executar remotamente um arquivo executável em um computador. O PsExec deve ser baixado e instalado no computador. Para obter mais informações sobre o PsExec, visite <http://www.faronics.com/pstools>.



Configurar

1. Vá para *Ação > Ações personalizadas*.
2. Selecione *Execução remota*.
3. Insira o *Local do PSEXec* ou navegue para selecionar o local.
4. O *Caminho executável* e o *Diretório de trabalho* são adicionados automaticamente. O *Arquivo executável* e o *Diretório de trabalho* podem ser modificados depois.
5. Clique em *Fechar*.

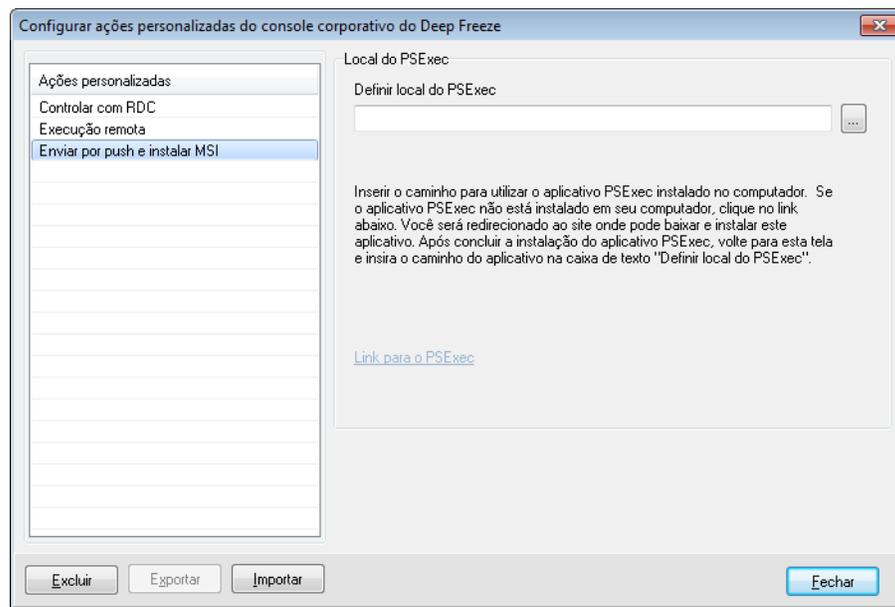
Executar

1. Selecione os computadores no painel *Estações de trabalho*.
2. Selecione *Ação > Execução remota*.
3. A caixa de diálogo *Execução remota* é exibida.
4. Digite o *Nome de usuário*, a *Senha* e o *Comando*.
5. Clique em *Ok*.



Enviar por push e instalar arquivo MSI

A opção *Enviar por push e instalar arquivo MSI* permite enviar por push e instalar um arquivo *.msi* em um computador através do Console corporativo.



Configurar

1. Vá para *Ação > Ações personalizadas*.
2. Selecione *Enviar por push e instalar arquivo MSI*.
3. Insira o *Local do PSEXec* ou navegue para selecionar o local.
4. O *Caminho executável* e o *Diretório de trabalho* são adicionados automaticamente. O *Arquivo executável* e o *Diretório de trabalho* podem ser modificados depois.
5. Clique em *Fechar*.

Executar

1. Selecione os computadores no painel *Estações de trabalho*.
2. Selecione *Ação > Enviar por push e instalar arquivo MSI*.
3. A caixa de diálogo *Enviar por push e instalar arquivo MSI* é exibida.
4. Insira o *Nome do usuário*, *Senha*, *Nome do arquivo* e *Letra da unidade*.
5. Clique em *Ok*.

Excluindo, importando e exportando ações personalizadas

Excluindo ações personalizadas

Para excluir ações personalizadas, execute estas etapas:



1. Vá para o menu *Ação > Ações personalizadas*.
2. Selecione a ação personalizada a ser excluída.
3. Clique em *Excluir*.

Importando ações personalizadas

Para importar ações personalizadas, execute as seguintes etapas:

1. Vá para o menu *Ação > Ações personalizadas*.
2. Clique em *Importar*.
3. Navegue e selecione o arquivo *.xml* a ser importado.
4. Clique em *Abrir* para importar o arquivo.

Exportando ações personalizadas

Para exportar ações personalizadas, execute as seguintes etapas:

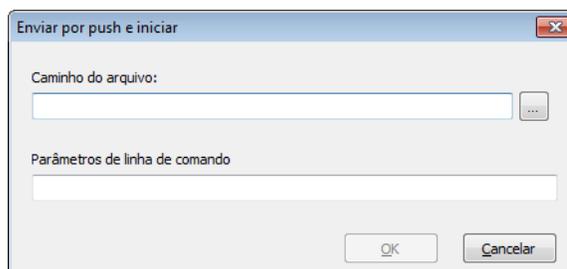
1. Vá para o menu *Ação > Ações personalizadas*.
2. Selecione a ação personalizada a ser exportada.
3. Clique em *Exportar*.
4. A caixa de diálogo Exportar ação personalizada para arquivo é exibida.
5. Especifique um *Nome de arquivo* e clique em *Salvar*.

Enviar por push e iniciar

Você pode enviar por push e iniciar arquivos em estações de trabalho gerenciadas.

Conclua os arquivos seguintes para enviar por push e iniciar arquivos em estações de trabalho gerenciadas:

1. Selecione uma ou mais estações de trabalho no painel Estação de trabalho.
2. Clique com o botão direito do mouse e selecione *Ações > Enviar por push e executar*. Aparecerá a caixa de diálogo Enviar por push e iniciar.



3. Procure o caminho de arquivo para selecionar ou especifique o caminho de arquivo.
 - *Nome de arquivo e caminho*: especifique o nome de arquivo e o caminho no qual o arquivo está disponível no computador do console. Como alternativa, você pode procurar o executável para selecionar. Tipos de arquivo compatíveis são *.exe* (executáveis) e *.msi* (instaladores MSI).



Arquivos MSI são executados em modo de instalação por padrão. Por exemplo, se o executável MyApplication.exe esteve disponível em C:/AppFolder, especifique *C:/AppFolder/MyApplication*.

4. Especifique os parâmetros de linha de comando com variáveis de ambiente (opcional):
 - *Argumentos*: especifique os argumentos que você deseja aplicar com este executável. Por exemplo, se o executável for executado do prompt de comando com o comando *C:\AppFolder\MyApplication -o logFile.log*, especifique *-o logFile.log* para argumentos. Para arquivos .msi, especifique os argumentos que você normalmente especificaria ao iniciar um arquivo .msi com o MSIEEXEC. Se você não especificar nenhum argumento para um arquivo .msi, o Deep Freeze acrescentará "/i" (instalar) automaticamente. O Deep Freeze também substitui qualquer opção de exibição por /qn, (em modo silencioso, sem IU).
5. Clique em OK.

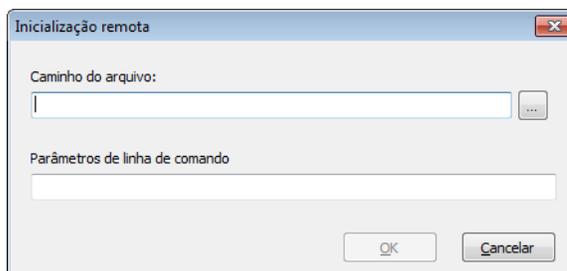
O arquivo é enviado por push para a estação de trabalho selecionada e iniciado remotamente nas estações de trabalho selecionadas.

Inicialização remota

Você pode iniciar arquivos de execução remotamente em estações de trabalho gerenciadas.

Conclua os arquivos seguintes para executar arquivos remotamente em estações de trabalho gerenciadas:

1. Selecione uma ou mais estações de trabalho no painel Estação de trabalho.
2. Clique com o botão direito do mouse e selecione *Ações > Execução remota*. A caixa de diálogo Execução remota é exibida:



3. Procure o caminho de arquivo para selecionar ou especifique o caminho de arquivo.
 - *Nome de arquivo e caminho*: especifique o nome de arquivo e o caminho no qual o arquivo está disponível no computador do console. Como alternativa, você pode procurar o executável para selecionar. Tipos de arquivo compatíveis são .exe (executáveis) e .msi (instaladores MSI). Instaladores MSI são executados em modo de instalação por padrão. Por exemplo, se o executável MyApplication.exe estiver disponível em C:/AppFolder, especifique *C:/AppFolder/MyApplication*.
4. Especifique os parâmetros de linha de comando com variáveis de ambiente (opcional):
 - *Argumentos*: especifique os argumentos que você deseja aplicar com este executável. Por exemplo, se o executável for executado do prompt de comando com o comando *C:\AppFolder\MyApplication -o logFile.log*, especifique *-o logFile.log* para argumentos. Para arquivos .msi, especifique os argumentos que você normalmente especificaria ao iniciar um arquivo .msi com o MSIEEXEC. Se você não especificar nenhum argumento para um arquivo



.msi, o Deep Freeze acrescentará "/i" (instalar) automaticamente. O Deep Freeze também substitui qualquer opção de exibição por /qn, (em quieto, sem IU).

5. Clique em OK.

O arquivo é executado remotamente nas estações de trabalho selecionadas.



Personalizador de console

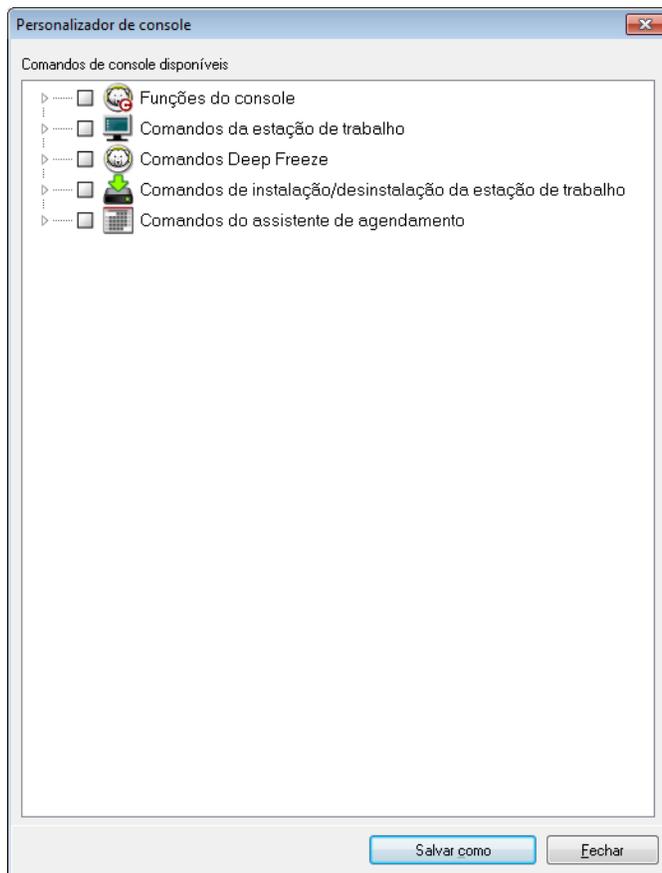
O Personalizador de console permite especificar quais recursos e comandos você quer que estejam disponíveis no Console, e salvar o resultado como um novo console que pode ser distribuído em sua organização.

As configurações disponíveis estão agrupadas em categorias (as funções do Console, comandos da Estação de trabalho, comandos do Deep Freeze, comandos de instalação/desinstalação da estação de trabalho e comandos do assistente de agendamento). Clique no ícone mais (+) na extrema esquerda de cada categoria para exibir a lista completa das configurações disponíveis naquela categoria.

Selecione ou desmarque as caixas de seleção individuais conforme necessário. Alternativamente, selecione ou desmarque as categorias inteiras de uma vez. As configurações não selecionadas não estarão disponíveis no novo Console corporativo que você criar. Para ver um exemplo de como usar o Personalizador de console em um cenário prático, consulte o [Apêndice D](#).

Executes as seguintes etapas para criar consoles com funcionalidade limitada:

1. Selecione *Ferramentas > Personalizador de console*.
2. O Personalizador de console é exibido.



3. Selecione os recursos a serem exibidos no novo Console.
4. Clique em *Salvar como* para salvar o Console. Especifique um nome para o arquivo.



5. Quando você clicar duas vezes no arquivo `.exe` recém-criado, o Console com a funcionalidade limitada será iniciado.



Desligamento do Console corporativo do Deep Freeze

Para desligar o Console do Deep Freeze selecione *Arquivo > Sair* ou clique no botão Fechar janela. Ao sair, você pode escolher:

- Minimizar o Console para a bandeja do sistema.

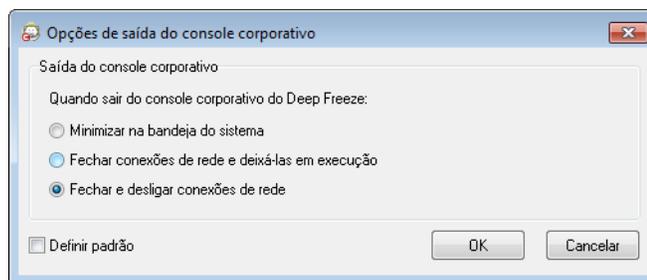
Isso não interrompe o Console e mantém as conexões ativas. O ícone do Console do Deep Freeze é exibido na bandeja do sistema. As tarefas agendadas ainda serão executadas. Para reabrir o Console corporativo do Deep Freeze, clique com o botão direito em seu ícone localizado na barra de tarefas e selecione *Restaurar Console do DF6*.

- Fechar o Console do Deep Freeze e deixar as conexões de rede em execução

Isso fecha o Console, mas mantém as conexões com os computadores ativas. As tarefas agendadas ainda serão executadas.

- Fechar o Console do Deep Freeze e desligar conexões de rede.

Isso interrompe os processos do Console, fecha as conexões (incluindo o serviço local), e as tarefas agendadas não irão começar a ser executadas. Entretanto, as tarefas agendadas que começaram a ser executadas irão continuar.



A caixa de diálogo não será exibida em futuras saídas quando a opção *Definir padrão* tiver sido selecionada. Para sair dessas configurações selecione *Ferramentas > Opções de saída*.



Instalação do Deep Freeze na estação de trabalho

Depois de um arquivo de programa de instalação personalizada ter sido criado usando-se o Administrador de configuração, o Deep Freeze pode ser implantado em computadores que usam uma instalação assistida, uma instalação de destino, o Sistema de instalação em segundo plano ou como parte de um processo de imagem.

Todos os utilitários de fundo e software antivírus devem ser desativados e todos os aplicativos devem ser fechados antes da instalação. Esses programas podem interferir com a instalação, o que poderia resultar no funcionamento incorreto do Deep Freeze.

O computador reinicia após qualquer tipo de instalação ser concluída. O Deep Freeze deve estar em um estado Descongelado para qualquer tipo de desinstalação ser bem-sucedida.

Qualquer ThawSpace existente será excluído durante uma desinstalação se:

- a opção para reter um ThawSpace existente não tiver sido verificada no Administrador de configuração
- o ThawSpace não tiver sido criado com o Deep Freeze Enterprise Versão 5 ou posterior

Instalação ou desinstalação assistida

Para instalar ou desinstalar o Deep Freeze, execute estas etapas:

1. Execute o arquivo do programa de instalação (*DFWks.exe*) no computador. A seguinte tela será exibida:
2. Clique em *Instalar* para iniciar a instalação. Siga as etapas apresentadas, depois leia e aceite o contrato de licença. O Deep Freeze é instalado e o computador é reiniciado.



Clique em *Desinstalar* para desinstalar o Deep Freeze. A opção Desinstalar só pode ser clicada se o Deep Freeze tiver sido instalado anteriormente e o computador estiver atualmente Descongelado. Se houver um ThawSpace existente, o Deep Freeze exibirá uma caixa de diálogo perguntando se ele deve ser retido ou excluído.



Se o disco rígido estiver muito fragmentado, não será possível criar ThawSpaces. Uma mensagem é exibida solicitando que você anule a instalação ou instale o Deep Freeze sem os ThawSpaces.



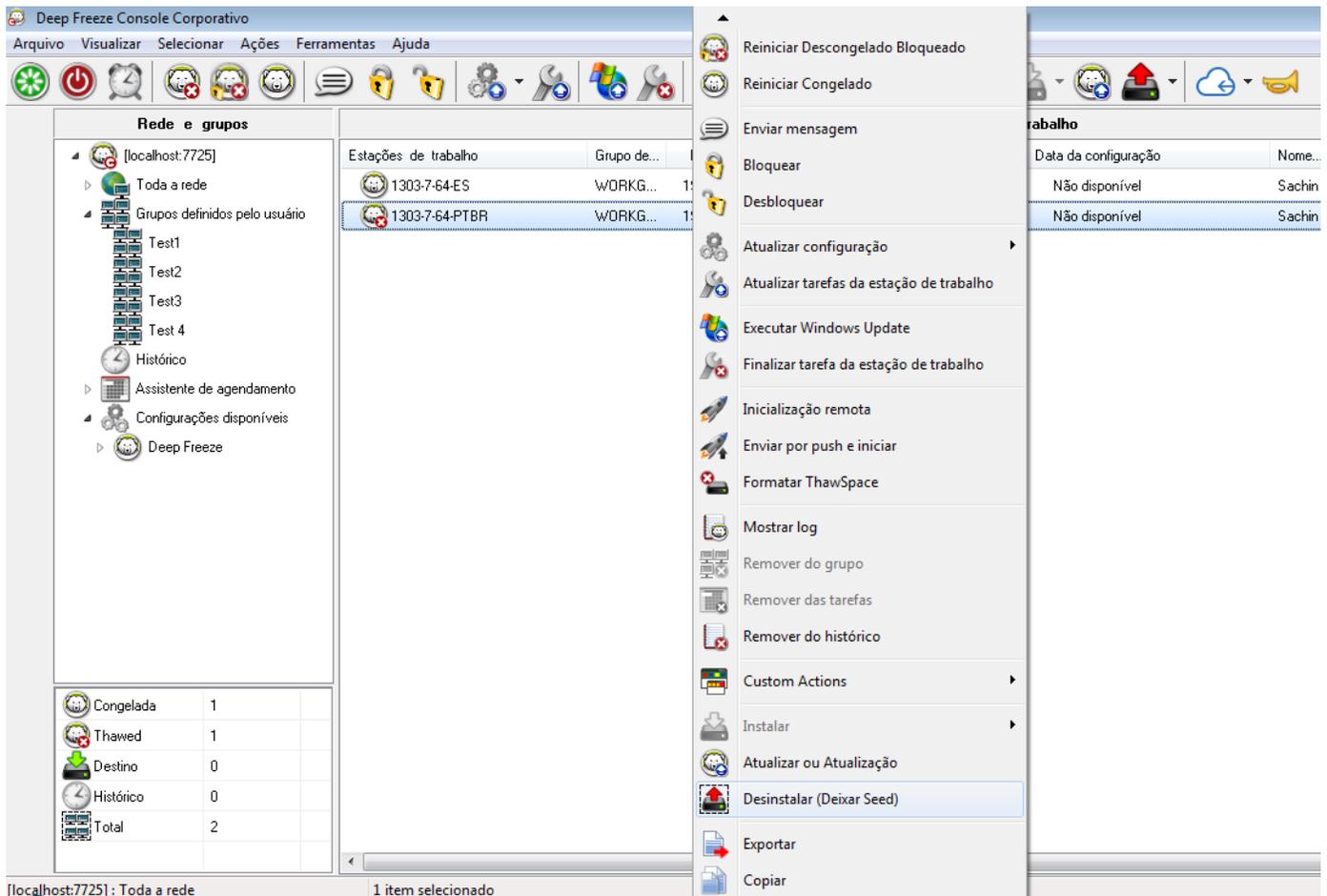
Se você selecionar *Atrasar reinicialização Frozen para concluir atualizações do Windows* (Guia Opções avançadas no Administrador de Configuração) e instalar o Deep Freeze, o instalador verificará se todas as atualizações do Windows foram concluídas. Se as atualizações do Windows não foram concluídas, a instalação do Deep Freeze não continuará. Conclua as atualizações do Windows e tente instalar o Deep Freeze novamente.

Se você desabilitar *Atrasar reinicialização Frozen para concluir atualizações do Windows* e instalar o Deep Freeze, certifique-se de que todas as atualizações do Windows foram concluídas sem usar o Deep Freeze. Desabilitar esta opção pode resultar no travamento do computador em um ciclo de reinicialização para atualizações incompletas do Windows.



Desinstalando o Deep Freeze na estação de trabalho via Console

O Console corporativo pode ser usado para desinstalar o Deep Freeze completamente ou para desinstalar o Deep Freeze, mas deixar a Seed da estação de trabalho. Um computador deve estar em um estado Descongelado para desinstalar o programa.



Para desinstalar o Deep Freeze em um computador e deixar a Seed da estação de trabalho, clique com o botão direito nas estações de trabalho congeladas e selecione *Desinstalar (Deixar Seed)*, conforme mostrado acima. Ou clique no ícone na barra de ferramentas.

Para desinstalar completamente o Deep Freeze e a Seed da estação de trabalho, selecione os computadores a serem desinstalados e clique no ícone *Desinstalar* na barra de ferramentas.



O computador deve estar no modo Descongelado antes de o Deep Freeze ser desinstalado. O Console corporativo solicita confirmação. Quando a desinstalação estiver confirmada, o Deep Freeze será desinstalado e o computador reiniciado.



Instalação ou desinstalação em segundo plano

O Deep Freeze pode ser rapidamente instalado em vários computadores através de uma rede usando o Sistema de instalação em segundo plano. Qualquer utilitário de implantação que permite a execução de uma linha de comando em um computador remoto pode implementar o Sistema de instalação em segundo plano. Após a conclusão da Instalação em segundo plano, o computador é reiniciado imediatamente. A linha de comando tem as seguintes opções:

Sintaxe	Descrição
<code>[/Install]</code>	Instala o Deep Freeze usando o arquivo de instalação
<code>[/Install /Seed]</code>	Instala somente o arquivo Seed da estação de trabalho especificado
<code>[/Install /Thawed]</code>	Instale o Deep Freeze usando o arquivo de instalação e inicie-o no estado Descongelado.
<code>[/Uninstall]</code>	Desinstala o Deep Freeze
<code>[/Uninstall /Seed]</code>	Desinstala o Deep Freeze e deixa a Seed da estação de trabalho instalada
<code>[/PW=password]</code>	Define uma senha durante a instalação*
<code>[/AllowTimeChange]</code>	Permite que o relógio do sistema seja alterado*
<code>[/Freeze=C,D,...]</code>	Congela apenas as unidades listadas (descongela todas as outras)*
<code>[/Thaw=C,D,...]</code>	Descongela apenas as unidades listadas (congela todas as outras)*
<code>[/USB]</code>	Isenta discos rígidos USB externos de proteção
<code>[/FireWire]</code>	Isenta discos rígidos FireWire externos de proteção

Exemplo de linha de comando

```
DFWks.exe /Install /Freeze=C /PW=password
```

No exemplo acima, o arquivo do programa de instalação do Deep Freeze é nomeado *DFWks.exe*. Somente a unidade C: será congelada. Quaisquer outras unidades no computador serão descongeladas. Se o computador tiver somente uma unidade C:, unidade C:, a chave `[/Freeze]` pode ser omitida. Uma senha (senha) será criada. Após executar o comando, o Deep Freeze será instalado e o computador reinicializará congelado e pronto para uso.

O Sistema de instalação em segundo plano não funciona sem a chave `[/Install]` ou `[/Uninstall]`. O Deep Freeze deve estar em um estado descongelado antes que `[/Uninstall]` possa ser usada.



Para executar as opções de configuração da linha de comando, Desativar opções da linha de comando na guia Opções avançadas deve estar desmarcada.



* Essas opções estão desativadas por padrão.

Instalação ou desinstalação sem segundo plano usando um atalho

O Deep Freeze pode ser instalado diretamente em um computador sem ter que usar a caixa de diálogo de instalação executando-se estas etapas.

1. Localize o arquivo do programa de instalação do Deep Freeze (*DFWks.exe*) no computador de destino.
2. Clique com o botão direito no ícone e escolha *Criar atalho*.
3. Clique com o botão direito no atalho e escolha *Propriedades*.
4. Edite o caminho do campo Destino digitando `/install` ou `/uninstall` ao final do caminho.

Exemplo de destino de atalho:

```
C:\Documents and Settings\DFWks.exe /install
```

Clicar duas vezes no novo atalho resulta na instalação ou desinstalação imediata do Deep Freeze, seguida de uma reinicialização do computador.

O Deep Freeze deve estar em um estado descongelado antes que `/uninstall` possa ser usada.



Se o disco rígido estiver muito fragmentado, não será possível criar ThawSpaces. A instalação é anulada.

Instalação pela rede em vários computadores

O Sistema de instalação em segundo plano também pode ser usado para instalar o Deep Freeze em vários computadores através de uma rede. Se as estações de trabalho da rede usam scripts de logon, os scripts podem ser usados para instalar automaticamente o Deep Freeze em todas as estações de trabalho em rede. Todas as estações de trabalho serão reinicializadas congeladas e prontas para uso após a conclusão da instalação.

Use as seguintes sintaxes de linha de comando para criar um arquivo de log de relatório de erros de instalação:

```
\\Server Name\Share Name\DFWks.exe /Install >> my.log
```

Instalando sobre versões existentes do Deep Freeze

Exceto se o recurso Atualizar o software Deep Freeze estiver em uso (para Deep Freeze 6.5 e posterior), todas as versões do Deep Freeze devem ser desinstaladas antes de executar qualquer nova instalação do Deep Freeze.

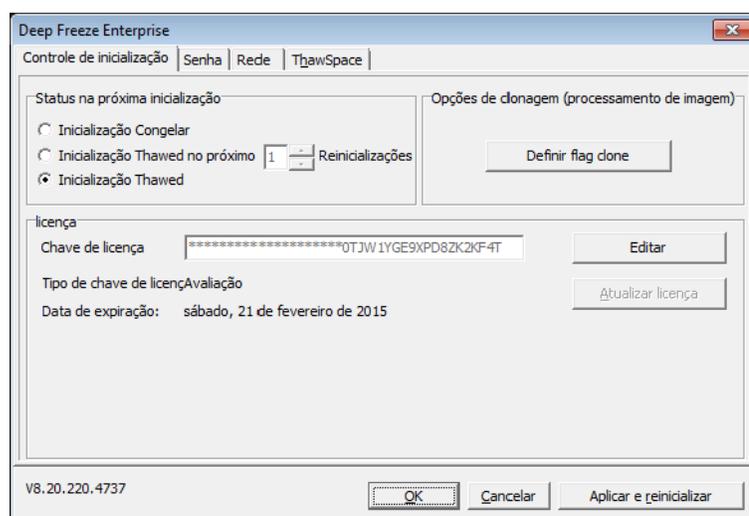


Instalando usando processamento de imagem

O Deep Freeze foi projetado para funcionar com todos os principais softwares de gerenciamento de área de trabalho e de imagem. Use a Instalação assistida ou a Instalação em segundo plano para instalar o Deep Freeze em uma imagem mestra.

O Deep Freeze deve ser preparado para implantação antes da finalização de uma imagem mestra. Para preparar a imagem mestra para implantação, execute estas etapas:

1. Reinicie o computador em um estado *Descongelado*.
2. Inicie o Deep Freeze usando o atalho do teclado *CTRL+SHIFT+ALT+F6*. Alternativamente, pressione *SHIFT* e clique duas vezes no ícone do Deep Freeze na Bandeja do sistema.
3. Insira a senha e clique em *OK*.
4. Clique em *Definir sinalizador clone* na guia *Controle da inicialização*.
5. A mensagem *Sinalizador definido com sucesso. Deseja reinicializar seu computador agora?* é exibida. Clique em *Sim* para reinicializar o computador imediatamente. Clique em *Não* para reinicializar o computador mais tarde.



O comando Definir sinalizador clone é importante durante o processamento de imagem, pois ele inicia os computadores em um estado Descongelado se o Deep Freeze não puder ler seu arquivo de configuração depois que a imagem é instalada com sucesso.

Se o sinalizador clone não for definido, e se o Deep Freeze não puder ler seu arquivo de configuração, todas as unidades são Congeladas depois que a imagem é instalada com sucesso.



Se você estiver usando o Sysprep, certifique-se de definir o sinalizador clone depois de preparar o sistema para processamento de imagem, e logo antes de iniciar o Sysprep.

Após o processamento da imagem, os computadores exigem uma reinicialização adicional para que o Deep Freeze detecte corretamente as alterações na configuração do disco. Se os computadores tiverem o processamento de imagem em um modo autônomo, deverão ser realizadas etapas para assegurar que os computadores sejam reinicializados para permitir a atualização da configuração.



Para retornar ao estado Congelado após a conclusão do processamento de imagem, defina o Deep Freeze para Inicialização congelado nos próximos n número de reinicializações (na imagem mestra) para que após o número n de reinicializações o computador esteja automaticamente congelado. Alternativamente, use o Controle de linha de comando do Deep Freeze para congelar os computadores selecionados.

Instalação de destino

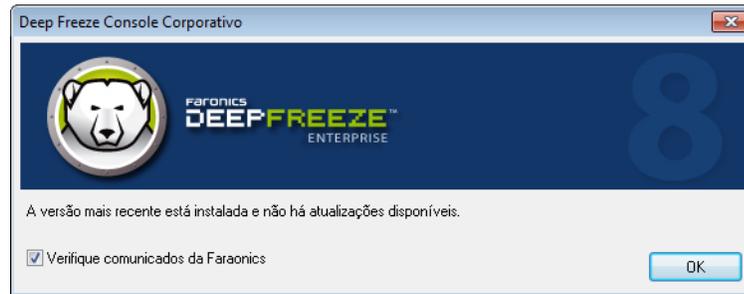
O Deep Freeze também pode ser implantado usando-se uma Instalação de destino a partir do Console corporativo.



Verificar atualizações

O Deep Freeze permite verificar se há versões mais novas disponíveis.

Vá para *Ajuda > Verificar atualizações*. Isso verifica se há versões mais novas do Deep Freeze disponíveis.



Se houver uma nova versão disponível, clique em *Baixar a versão mais recente* para atualizar o Deep Freeze.





Gerenciando computadores Deep Freeze

Este capítulo descreve o gerenciamento de computadores onde o Deep Freeze está instalado.

Tópicos

Tela de logon

Guia Status

Guia Senha

Guia Rede

Guia ThawSpace

Instalações, alterações e remoções permanentes de softwares



Tela de logon

Use uma das seguintes maneiras para acessar o Deep Freeze em um computador.

1. Se o ícone do Deep Freeze estiver exibido na bandeja do sistema, mantenha pressionada a tecla SHIFT e clique duas vezes no ícone do Deep Freeze. Se o Deep Freeze estiver em execução no modo Furtivo e se o ícone do Deep Freeze não estiver exibido, o atalho do teclado CTRL+ALT+SHIFT+F6 deve ser usado para acessar a caixa de diálogo de logon.



2. Insira a senha do administrador e clique em OK para fazer logon no Deep Freeze.

Como um recurso de segurança adicional, o Deep Freeze impede ataques de força bruta reiniciando automaticamente o computador após 10 tentativas de logon malsucedidas.

Iniciando o Deep Freeze em dispositivos com tela sensível ao toque

Você pode usar Ctrl+Alt+Shift+6 ou Ctrl+Alt+Shift+F6 para iniciar o Deep Freeze em dispositivos com tela sensível ao toque. No entanto, você deve habilitar todo o teclado antes de usar o atalho. Você também pode tocar e manter pressionado na bandeja do sistema para iniciar o menu de contexto do Deep Freeze.

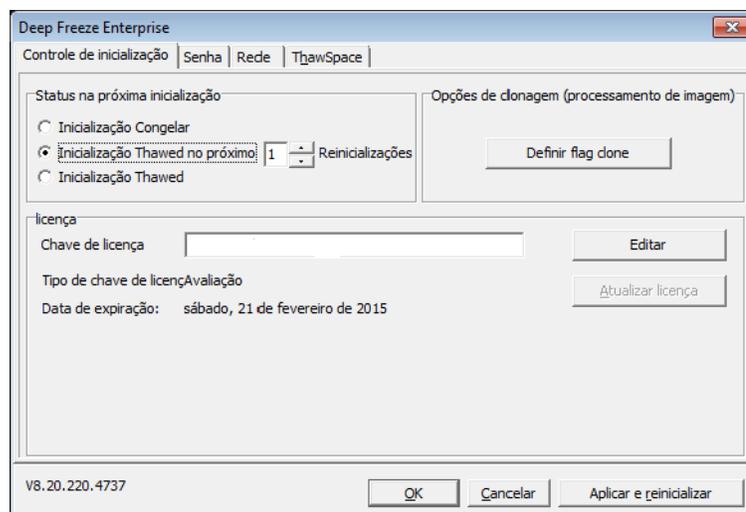


Guia Status

A guia *Status* exibe as seguintes opções:

Status na próxima inicialização

A guia *Status* é usada para definir o modo no qual o Deep Freeze estará após a próxima inicialização



Escolha uma das seguintes opções:

- *Inicialização congelado*
para assegurar que o computador esteja congelado na próxima vez em que ele for reinicializado
- *Inicialização descongelado na próxima*
para assegurar que o computador esteja descongelado a cada vez que for reinicializado pelo número especificado de próximas reinicializações. Quando aquele número de reinicializações tiver sido excedido, o computador será reinicializado congelado.
- *Inicialização descongelado*
para assegurar que o computador esteja descongelado na próxima vez em que ele for reinicializado

Selecione o botão de opções próximo à escolha desejada e clique em *OK* para salvar quaisquer alterações. Clicar em *Aplicar e Reinicializar* irá salvar quaisquer alterações e reinicializar o computador imediatamente.

Clonar

O painel *Clonar* é usado para preparar imagens mestras para o processo de implantação. Para obter mais informações, consulte a seção [Instalando usando processamento de imagem](#).



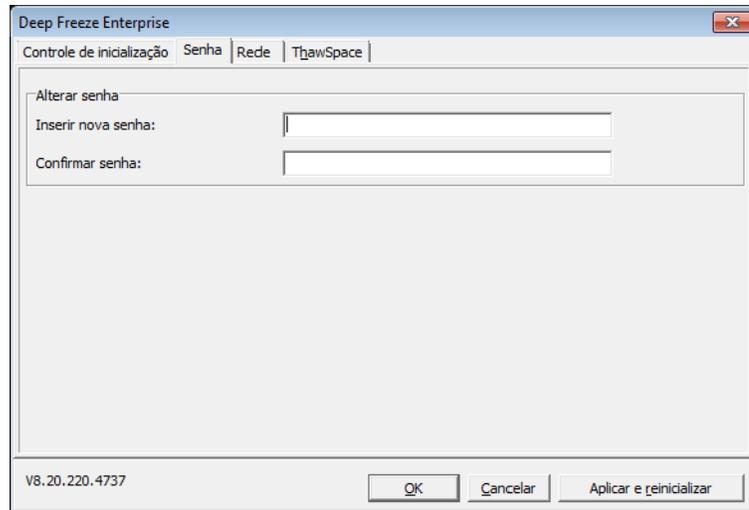
Licença

Insira a chave de licença no campo *Chave de licença*. Se nenhuma chave de licença for inserida, o Deep Freeze expira em 30 dias após a instalação.



Guia Senha

A guia *Senha* permite alterar a senha.

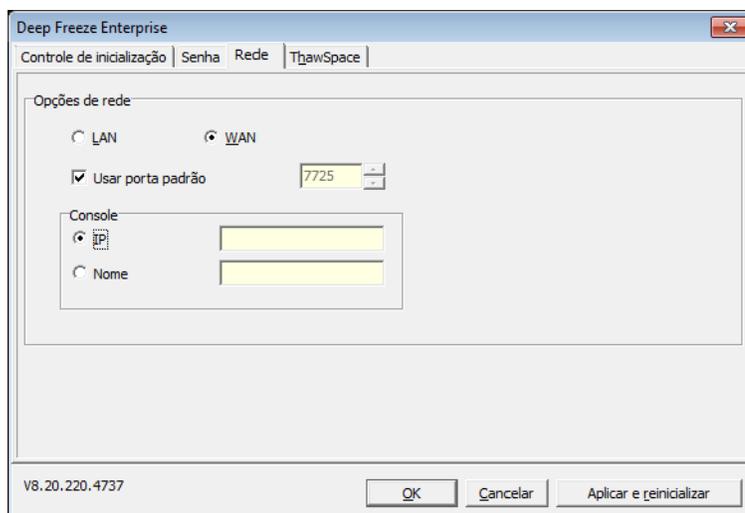


1. Especifique uma nova senha no campo *Inserir nova senha*.
2. Confirme a nova senha reinsertando a mesma senha no campo *Confirmar senha*.
3. Clique em Ok.
4. A senha é alterada e uma caixa de diálogo de confirmação é exibida.



Guia Rede

A guia *Rede* pode ser usada para configurar as opções de rede em um computador.



Para escolher o método de comunicação por *LAN* ou *WAN*, clique na opção preferida.

O número de porta padrão pode ser alterado desmarcando-se a caixa de seleção *Usar porta padrão* e inserindo-se o número da porta necessário.

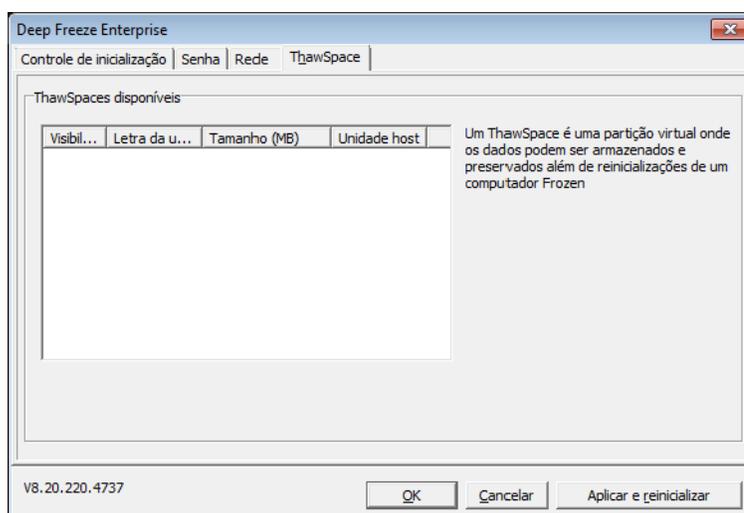
Para obter mais informações sobre a configuração da rede, consulte [Apêndice B](#).



Guia ThawSpace

O *ThawSpace* é uma partição virtual em um computador que pode ser usada para armazenar programas, salvar arquivos ou fazer alterações permanentes. Todos os arquivos armazenados no ThawSpace são salvos após uma reinicialização, mesmo que o computador esteja Congelado.

O ThawSpace só está disponível se ele tiver sido definido para ser criado no Administrador de Configuração do Deep Freeze.



Após a desinstalação do Deep Freeze, todos os ThawSpaces tornam-se visíveis. Quando o Deep Freeze é reinstalado, os ThawSpaces estão *Visíveis* ou *Ocultos* de acordo com as configurações originais na guia ThawSpace.

Qualquer ThawSpace existente é excluído durante uma desinstalação se quaisquer dos seguintes se aplicar:

- a opção para reter um ThawSpace existente não foi selecionada no *Administrador de configuração*
- o ThawSpace não tiver sido criado com o Deep Freeze Versão 5 ou posterior



Instalações, alterações e remoções permanentes de softwares

Os computadores devem estar descongelados para que quaisquer alterações permanentes entrem em vigor. A instalação de software frequentemente requer uma ou mais reinicializações para conclusão da instalação.

O Deep Freeze ajuda os administradores a superar desafios com a manutenção da configuração de seus computadores em um ambiente de produção. O Deep Freeze protege computadores de alterações não autorizadas, vírus e malware, que podem deixar os computadores em um estado não funcional. O Deep Freeze também fornece recursos para reter dados do usuário enquanto protege o computador.

Para obter mais informações sobre como implementar o Deep Freeze e assegurar que os dados do usuário sejam retidos, consulte *Deep Freeze - Retendo dados de usuário disponíveis* em <http://www.faronics.com/library>



Gerenciando o Anti-Virus

Este capítulo descreve a instalação e o uso do Anti-Virus com o Console corporativo.

Tópicos

Visão geral do Anti-Virus

Ativar o Anti-Virus no Console corporativo

Instalar o Cliente Anti-Virus na estação de trabalho

Configuração do Anti-Virus

Usando o Faronics Anti-Virus no Console corporativo

Programação de tarefas Anti-Virus

Usando o Anti-Virus na estação de trabalho

Verificar atualizações do Anti-Virus

Atualizar o Faronics Anti-Virus

Desinstalar o Anti-Virus do Console corporativo

Desativar o Faronics Anti-Virus no Console corporativo



Visão geral do Anti-Virus

O Anti-Virus pode ser instalado e usado via Console corporativo. O uso do Anti-Virus é opcional. O Deep Freeze Enterprise também pode ser usado independentemente sem o uso do Anti-Virus.

As seções a seguir são explicadas:

- Ativar o Anti-Virus no Console corporativo
- Instalar o Cliente Anti-Virus na estação de trabalho
- Configuração do antivírus
- Usando o Anti-Virus a partir do Console corporativo
- Agendando tarefas Anti-Virus
- Usando o Cliente Anti-Virus na estação de trabalho
- Verificar atualizações
- Atualizar o Faronics Anti-Virus
- Desinstalar o Cliente Anti-Virus da estação de trabalho
- Desativar o Anti-Virus no Console corporativo



Ativar o Anti-Virus no Console corporativo

O Anti-Virus agora é parte do Console corporativo e pode ser ativado internamente. É necessário adquirir uma licença separada para o Anti-Virus.

Siga estas etapas para ativar o Faronics Anti-Virus:

1. Inicie o Console Corporativo do Deep Freeze
2. Vá para *Ferramentas > Licenciamento > Licença do Faronics Anti-Virus*.
3. Marque a caixa de seleção *Gostaria de usar o Console do Deep Freeze para gerenciar o Faronics Anti-Virus*.
4. Clique em *Editar*.
5. Insira a chave de licença e clique em *Atualizar licença*.
6. Clique em *Fechar*. Os arquivos do instalador do Anti-Virus foram baixados. As colunas do Anti-Virus são exibidas no painel na estação do trabalho. O subnó do Anti-Virus é adicionado em *Configuração disponível* no painel Rede e grupos.



Instalar o Cliente Anti-Virus na estação de trabalho

Antes da instalação do Anti-Virus na estação de trabalho, assegure-se que o arquivo de instalação da estação de trabalho do Deep Freeze ou a Seed do Deep Freeze foi implementado na estação de trabalho que esta esteja no estado Descongelado.

Execute estas etapas para instalar o Anti-Virus na estação de trabalho:

1. Selecione uma estação de trabalho (ou várias estações de trabalho) a partir do painel *Estações de trabalho* > guia *Anti-Virus*.
2. Clique no ícone do Anti-Virus na barra de menus e selecione *Instalar Faronics Anti-Virus*.
3. Marque a caixa de seleção *Remover quaisquer produtos antivírus incompatíveis antes de instalar o Faronics Anti-Virus* para remover programas antivírus existentes.
4. Clique em *OK* para confirmar a ação.

A estação de trabalho é reinicializada e o cliente Anti-Virus é instalado nas estações de trabalho.

As opções do Anti-Virus estão ativadas na guia Anti-Virus.



Configuração do Anti-Virus

A configuração do Anti-Virus contém todas as configurações de como o Anti-Virus é executado nas estações de trabalho. A configuração contém a ação realizada pelo programa, a agenda, servidores proxy, relatórios de erro e as funcionalidades permitidas ao usuário nas estações de trabalho. As seções a seguir explicam como uma configuração Anti-Virus é criada e aplicada.

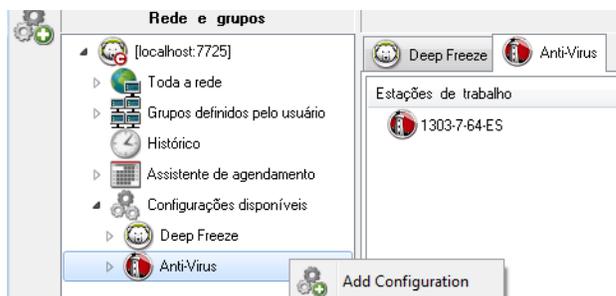


O Anti-Virus tem uma configuração *Padrão*. A política Padrão contém a configuração mais próxima ao ideal para gerenciamento do Anti-Virus.

Criando a configuração do Anti-Virus

Execute estas etapas para criar uma nova configuração do Anti-Virus:

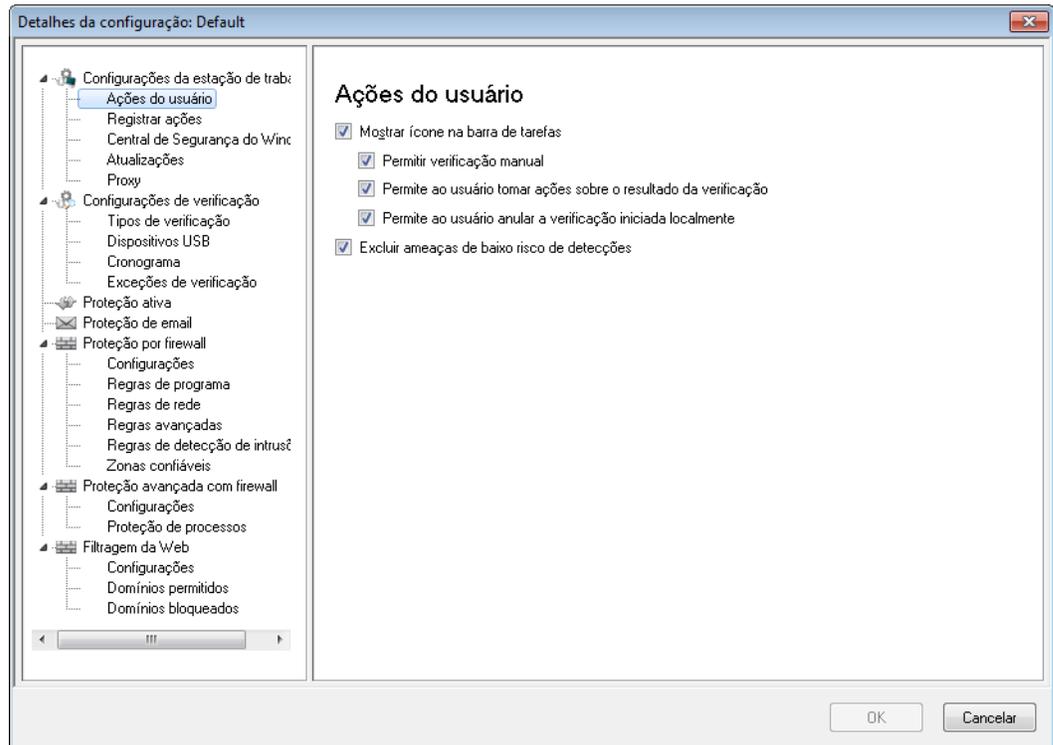
1. Iniciar o Console corporativo.
2. No painel *Rede e grupos*, vá para *Configurações disponíveis > Anti-Virus*.
3. Clique com o botão direito e selecione *Criar nova configuração*.



4. Especifique as configurações no nó *Configurações da estação de trabalho*:



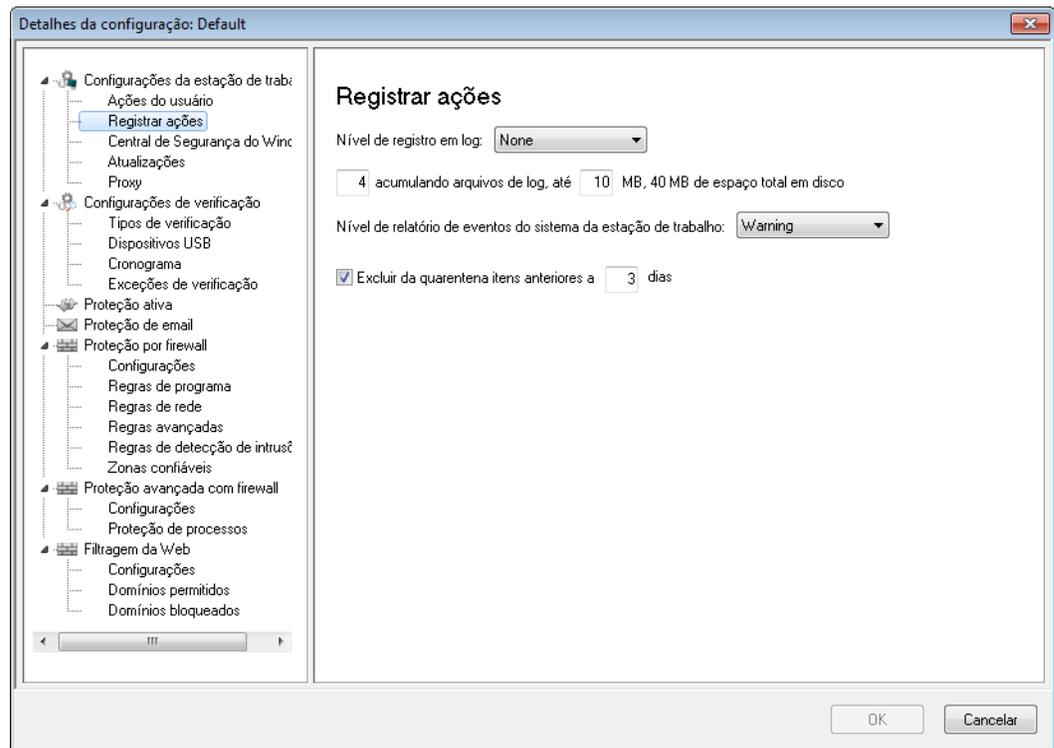
- Nó *Configurações da estação de trabalho* painel > *Ações do usuário*



- *Mostrar ícone na barra de tarefas* - marque a caixa de seleção para que o ícone do Faronics Anti-Virus seja exibido na barra de tarefas das estações de trabalho. Se esta caixa ficar desmarcada, o Faronics Anti-Virus será ocultado do usuário.
- *Permitir verificação manual* - marque a caixa de seleção para permitir que os usuários possam iniciar manualmente a verificação do Faronics Anti-Virus nas estações de trabalho.
- *Permitir que o usuário execute ações sobre resultados da verificação* - marque a caixa de seleção para permitir que o usuário da estação de trabalho execute uma ação sobre os resultados da verificação.
- *Permitir que o usuário anule verificação iniciada localmente* - marque a caixa de seleção para permitir que os usuários cancelem as verificações iniciadas localmente na estação de trabalho.
- *Excluir ameaças de baixo risco de detecções* - marque essa caixa de seleção para excluir ameaças de baixo risco das detecções. As ameaças de baixo risco são aquelas que não têm impacto negativo sobre o sistema, como os cookies.



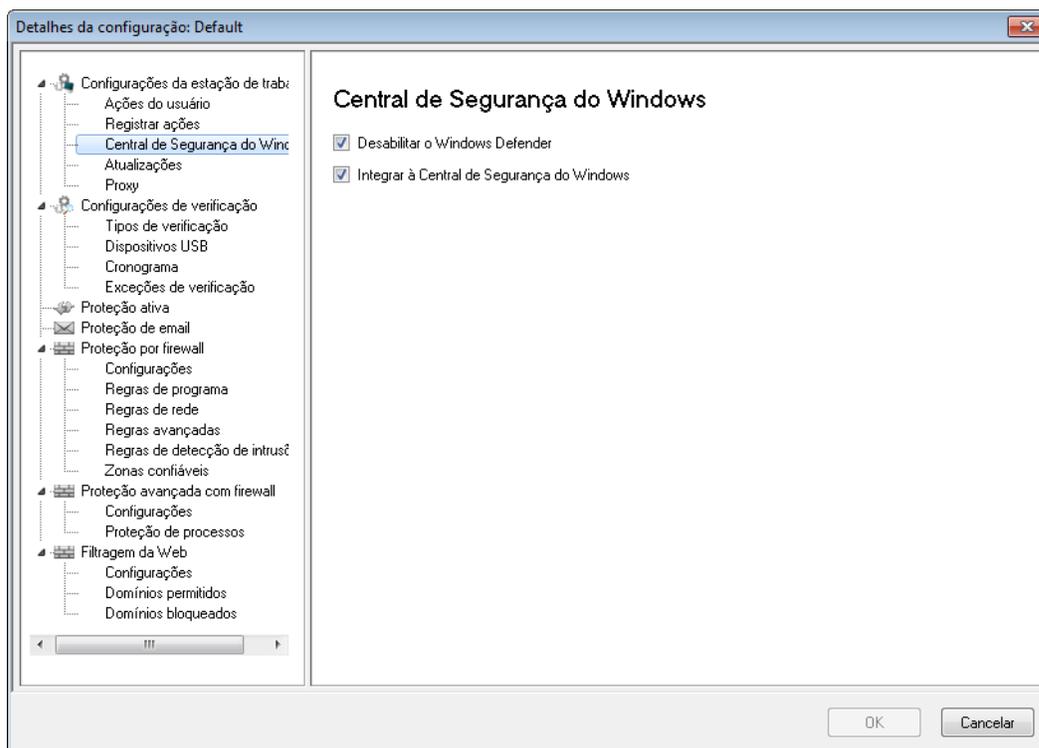
- Nó *Configurações da estação de trabalho* > *Registrar ações*



- *Nível de registro em log* - selecione o nível. Escolha *Nenhum* para não fazer registros. Selecione *Erro* para registrar mensagens de erro. Selecione *Rastrear* para rastrear. Escolha *Detalhado* para ter registros detalhados.
- *Número de arquivos de registro em log* - especifique o número de arquivos. As informações de registro são armazenadas em série nos arquivos. Por exemplo, se houver 3 arquivos A, B e C, o Faronics Anti-Virus primeiro gravará os registros em A. Quando A estiver cheio, passará para B e finalmente para C. Quando C estiver cheio, os dados do arquivo A serão apagados para dar lugar aos novos dados de registro.
- *Tamanho do arquivo* - defina o tamanho de cada arquivo em MB.
- *Nível de relatório de eventos do sistema da estação de trabalho*: selecione Nenhum, Erro, Aviso ou Informações.
- *Excluir da quarentena itens anteriores a* - especifique o número de dias durante os quais os itens serão mantidos em quarentena. O padrão é 3 dias.



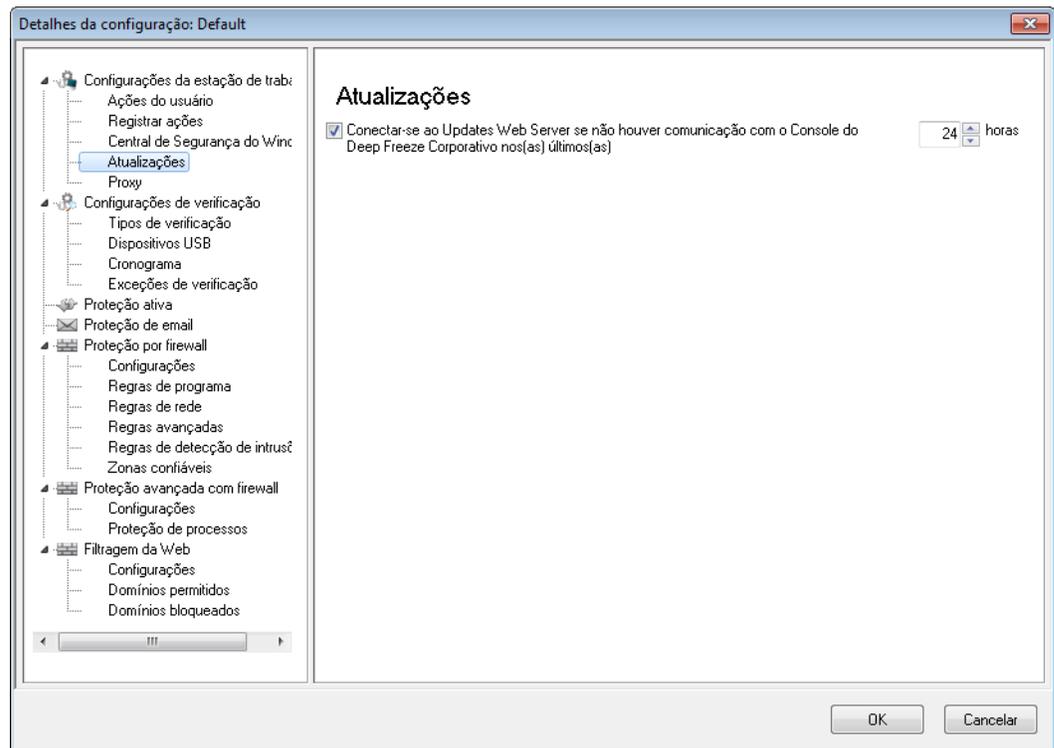
- Nó *Configurações da estação de trabalho* painel > *Central de Segurança do Windows*



- *Desativar Windows Defender* - marque essa caixa para desabilitar o Windows Defender. Isso evita possíveis conflitos entre o Faronics Anti-Virus e o Windows Defender. A execução de vários programas antivírus ou antispyware pode gerar conflitos, pois um programa pode confundir outro com uma ameaça. A demanda de trabalho e memória também pode aumentar, sobrecarregando o processador. Mas se quiser manter o Windows Defender em execução, você pode não desativá-lo.
- *Integrar à Central de Segurança do Windows* - marque para integrar o Faronics Anti-Virus à Central de Segurança do Windows. A Central de Segurança do Windows notificara na bandeja do sistema se o Faronics Anti-Virus está ativo ou inativo.



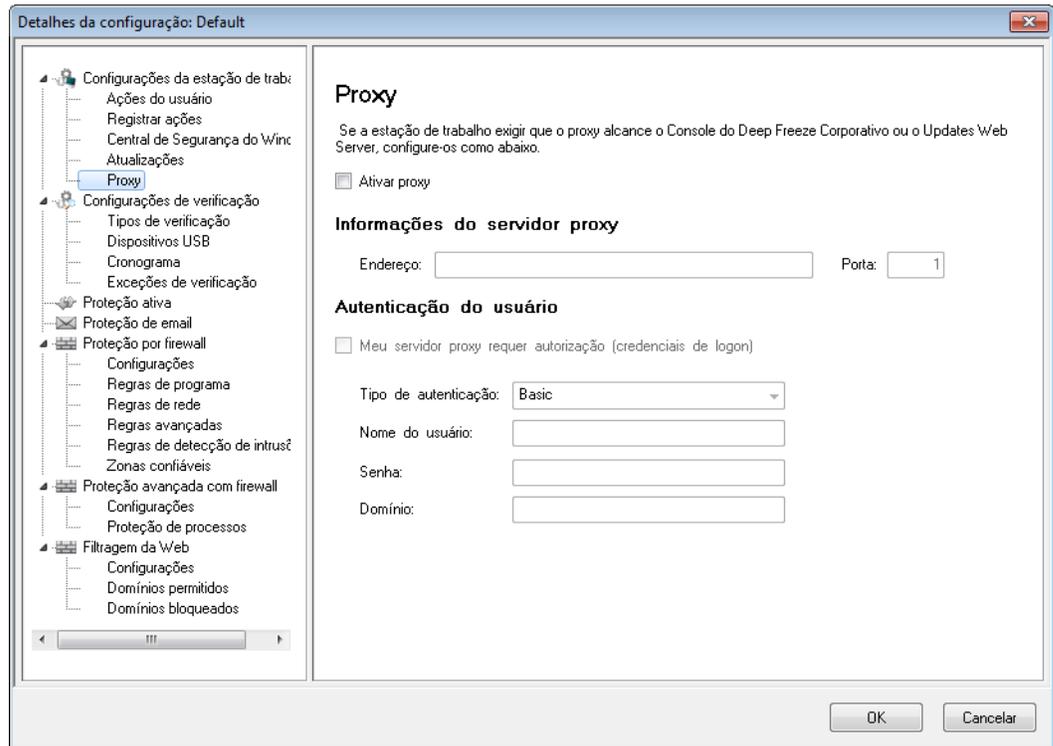
- *Nó Configurações da estação de trabalho > painel Atualizações*



- *Verificar atualizações a cada x horas*: marque a caixa de seleção para conectar-se ao Updates Web Server e baixar definições de vírus.



- *Nó Configurações da estação de trabalho > painel Proxy*

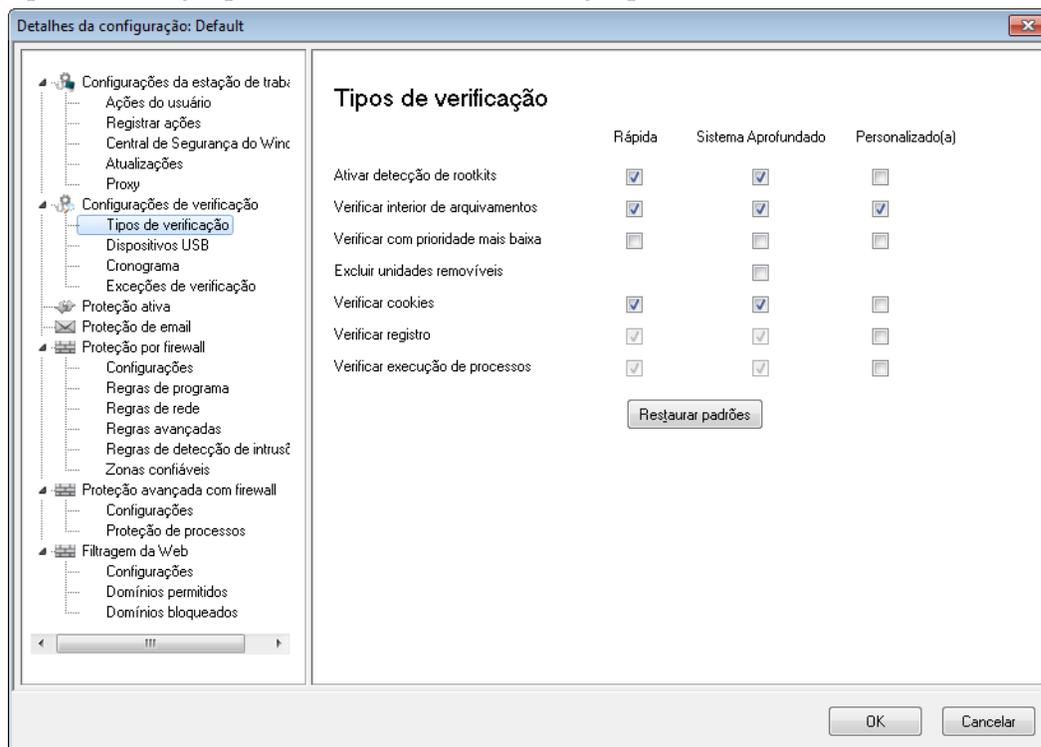


- *Ativar proxy* - selecione essa caixa se as estações de trabalho exigirem um proxy para se conectar ao Updates Web Server. Especifique o *Endereço* e a *Porta*.
- *Meu servidor proxy requer autorização (credenciais de logon)* - se o servidor exigir autenticação, especifique valores para os seguintes campos:
- *Tipo de autenticação* - selecione o tipo de autenticação.
 - *Nome de usuário* - especifique o nome de usuário.
 - *Senha* - especifique uma senha.
 - *Domínio* - defina o domínio.



5. Especifique configurações no nó *Verificando*:

- Nó *Verificando* > painel *Configurações de verificação* - selecione o seguinte para Verificação rápida, verificação profunda do sistema e Verificação personalizada.



O Faronics Anti-Virus oferece três tipos de verificações:

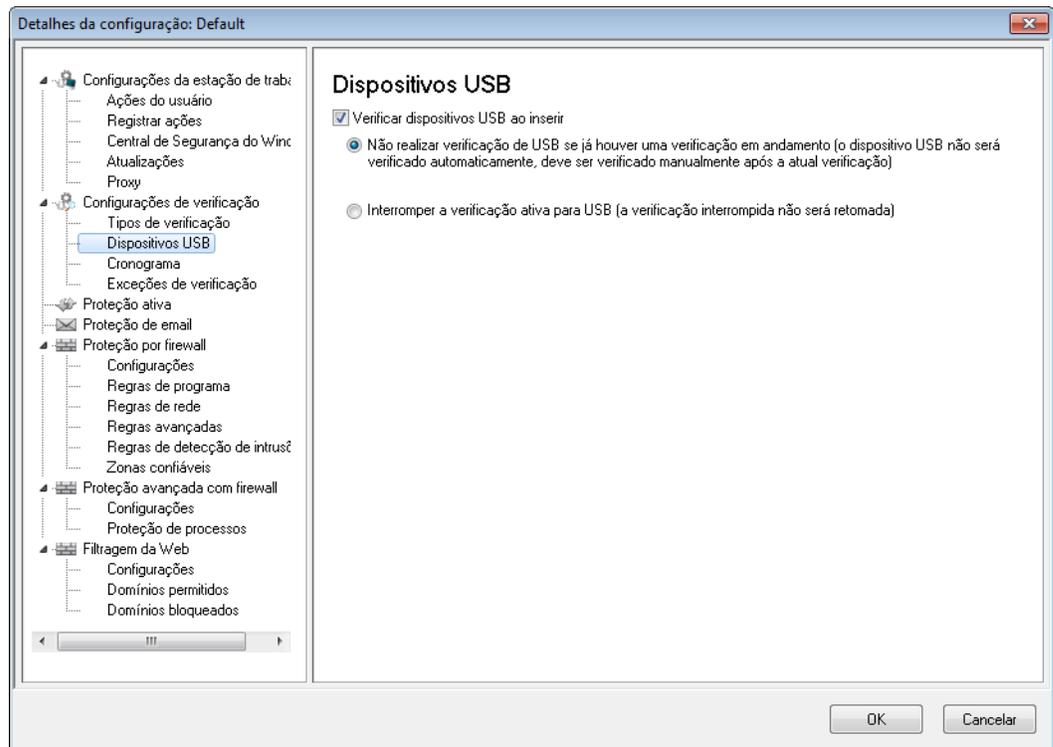
- *Verificação rápida* - verifica as áreas mais comumente afetadas do computador. Tem duração mais curta do que a Verificação profunda do sistema. A Verificação rápida também usa menos memória do que a Verificação profunda do sistema.
- *Verificação profunda do sistema* - verificação minuciosa de todas as áreas do computador. O tempo gasto na verificação depende o tamanho do disco rígido.
- *Verificação personalizada* - realiza uma verificação com base nas seleções feitas na caixa de diálogo *Detalhes da configuração*.

Para cada um dos tipos, selecione as seguintes opções (algumas podem estar esmaecidas, dependendo do tipo de verificação).

- *Ativar detecção de rootkits* - detecta se o computador foi infestado por rootkits.
- *Verificar interior de arquivamentos* - verifica o conteúdo de arquivos zip. Selecione para que a verificação inclua arquivos compactados, como .RAR e .ZIP. Se for encontrado um arquivo infectado, o arquivo .RAR será posto em quarentena. Se um arquivo .ZIP contiver um arquivo infectado, este será posto em quarentena e substituído por um arquivo .TXT, com texto dizendo que ele estava infectado e foi para quarentena.
- *Verificar com prioridade mais baixa* - o Faronics Anti-Virus funcionará com prioridade mais baixa, permitindo que se trabalhe com outros programas sem afetar o desempenho. Marque essa opção para verificações programadas em horários de uso normal do computador.
- *Excluir unidades removíveis* (por exemplo, USB): exclui as unidades removíveis do processo de verificação. Nenhum disco rígido externo, unidade USB, etc. serão verificados.
- *Verificar cookies*: os cookies salvos na estação serão verificados.



- *Verificar registro*: o registro é incluído.
- *Verificar execução de processos*: inclui todos os processos em execução.
- *Nó Verificação*> painel *Dispositivos USB* : defina as configurações a seguir.



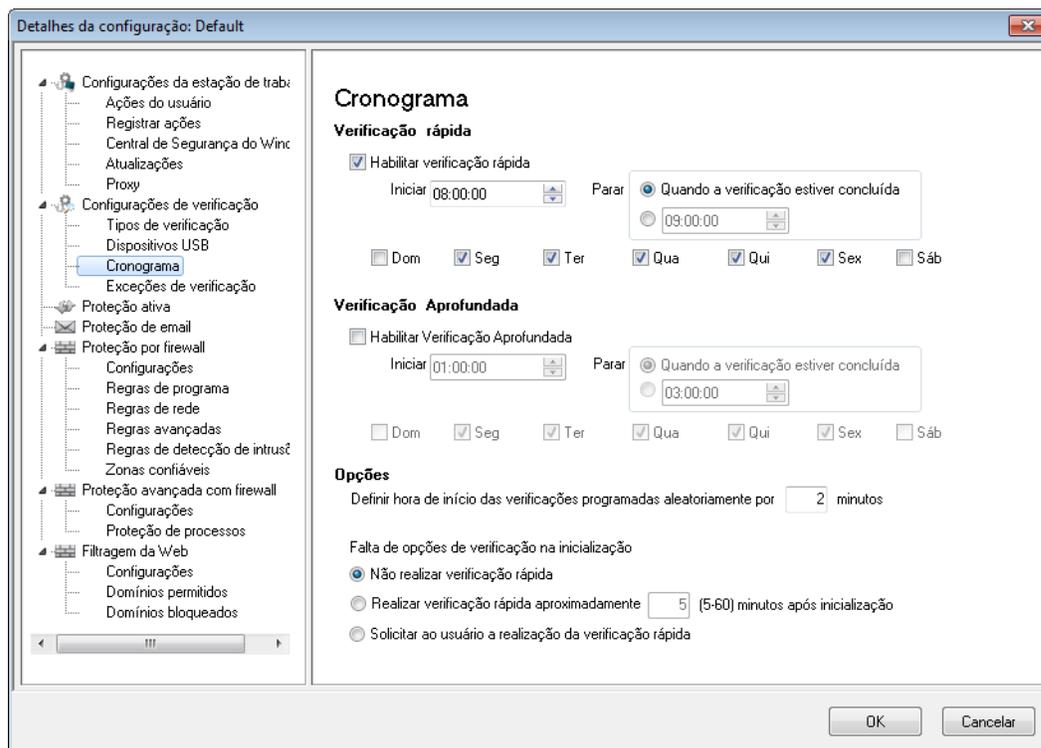
- *Verificar unidades USB ao inserir*: marque essa caixa para verificar dispositivos USB quando forem inseridos e selecione uma das opções a seguir.
 - *Não realizar verificação de USB se já houver uma verificação em andamento*: garante que a verificação não será interrompida quando se insere uma unidade USB. O dispositivo USB deverá ser verificado manualmente após a verificação em andamento.
 - *Interromper verificação ativa para verificar USB*: a verificação em andamento será interrompida ao se inserir uma unidade USB. Depois de interrompida, a verificação não é retomada automaticamente e deve ser reiniciada manualmente.



Se a caixa de seleção *Permitir verificação manual* da guia *Configurações da estação de trabalho* painel >*Ações do usuário* estiver marcada, o dispositivo USB será verificado automaticamente. Se *Permitir verificação manual* não estiver marcada, a verificação da unidade USB não será automática.



- Nó *Verificação* painel > *Programar*: defina as configurações a seguir.



Verificação rápida:

- *Permitir verificação rápida*: marque para permitir a verificação rápida.
- *Início* - especifique a hora de início.
- *Término* - especifique a hora de término. A duração máxima entre a hora de *Início* e de *Término* é de 23,59 horas. A verificação terminará se todos os arquivos tiverem sido verificados antes da hora de *Término*. Se a verificação não estiver concluída antes da hora de *Término*, a verificação será anulada na hora de *Término*. Você pode ainda selecionar *Quando a verificação estiver concluída* para garantir sua conclusão.
- *Dias*: selecione os dias em que ocorrerá a verificação rápida.

Verificação profunda:

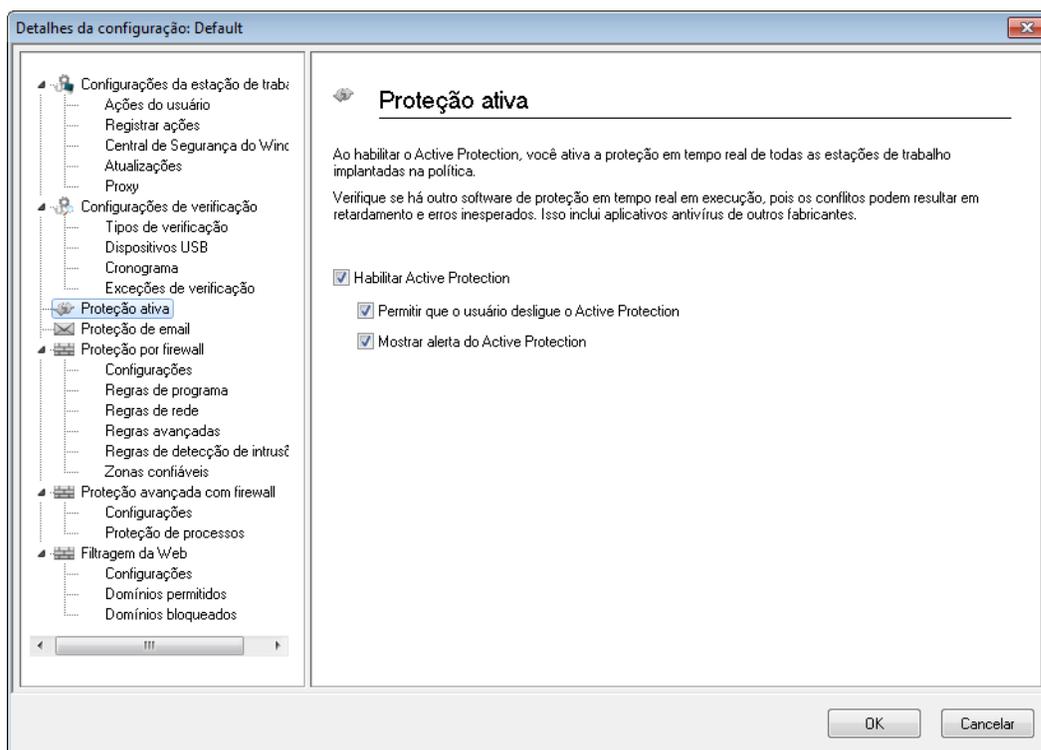
- *Permitir verificação profunda* - marque para permitir a verificação profunda.
- *Início* - especifique a hora de início.
- *Término* - especifique a hora de término. A duração máxima entre a hora de *Início* e de *Término* é de 23,59 horas. A verificação terminará se todos os arquivos tiverem sido verificados antes da hora de *Término*. Se a verificação não estiver concluída antes da hora de *Término*, a verificação será anulada na hora de *Término*. Você pode ainda selecionar *Quando a verificação estiver concluída* para garantir sua conclusão.
- *Dias*: selecione os dias em que ocorrerá a verificação profunda.

Opções:

- *Definir horas de início de verificações programadas aleatoriamente por x minutos*: defina quantos minutos. O início das verificações programadas será aleatório, reduzindo o impacto no tráfego da rede.



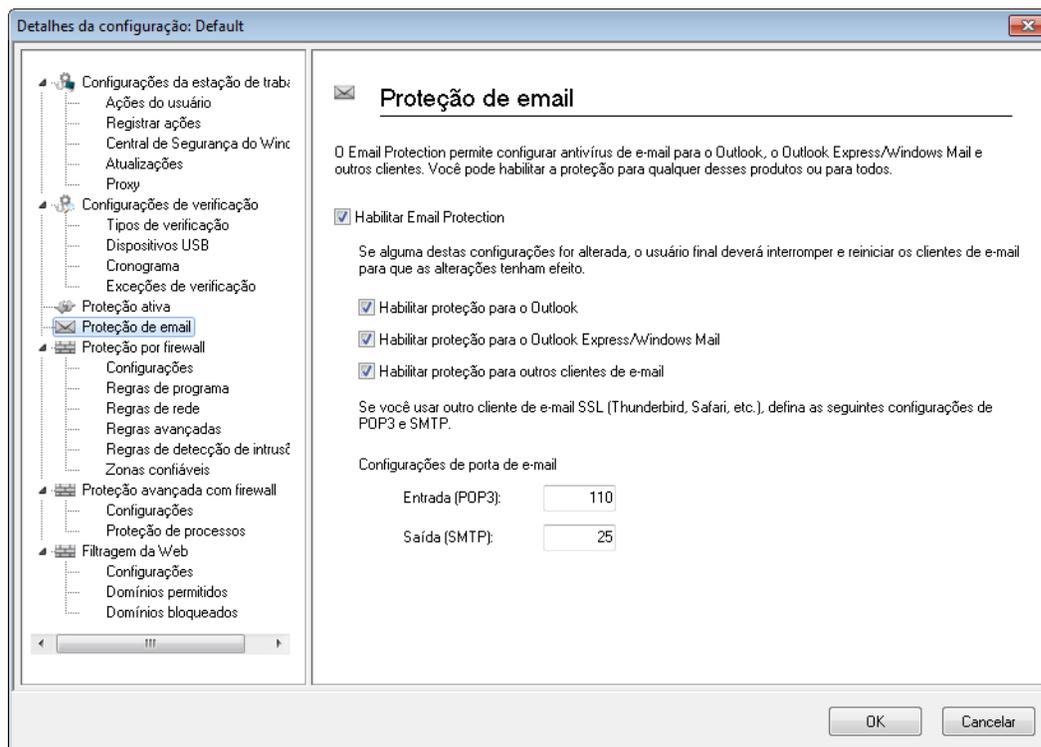
7. Defina as configurações no painel *Active Protection*.



- **Ativar Active Protection:** marque para ativar a proteção em tempo real. O Active Protection é a verificação em tempo real do Faronics Anti-Virus, realizada em segundo plano sem impacto sobre o desempenho do sistema. Se houver risco de infecção imediata por vírus na Internet, marque essa opção.
- **Permitir que o usuário desligue o Active Protection:** marque para que o usuário possa desativar o Active Protection. Se o usuário usar softwares que possam ser confundidos com vírus (macros avançadas no Microsoft Office ou arquivos em lote complexos, por exemplo), selecione essa opção.
- **Mostrar alerta do Active Protection:** marque para exibir um alerta ao detectar uma ameaça durante o Active Protection. Não marque essa caixa se não quiser que o alerta seja mostrado.



8. Defina as configurações no painel *Email Protection*.



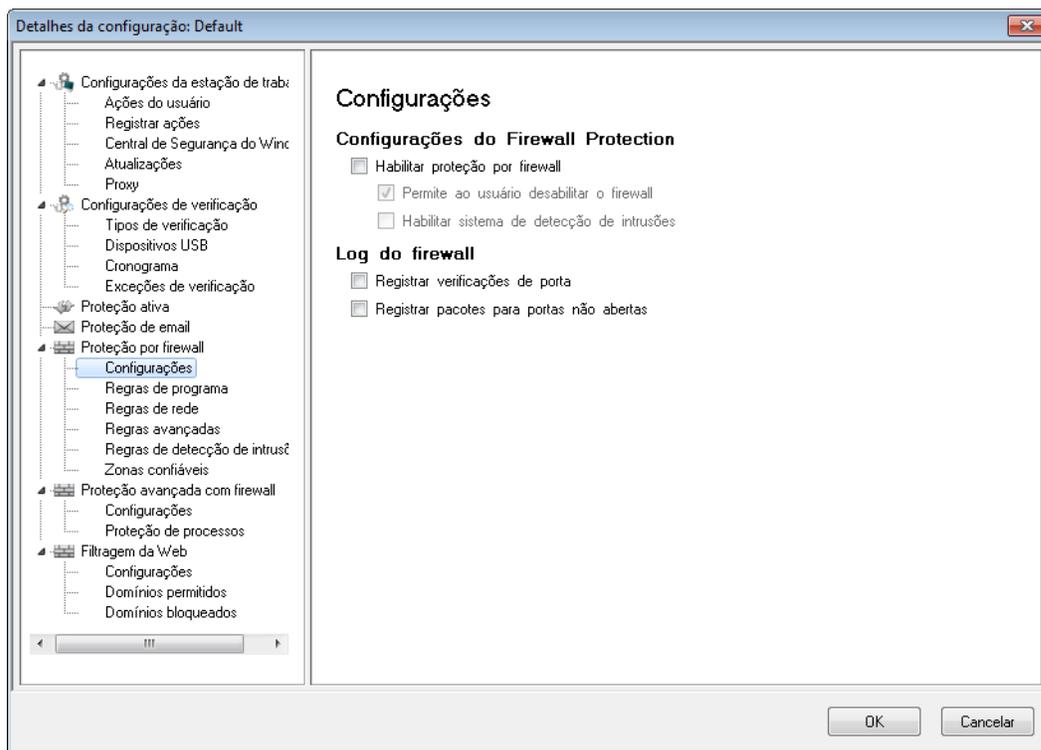
- **Ativar *Email Protection*** - marque essa caixa para ativar o Email Protection. Com *Ativar Email Protection* selecionada, as opções serão ativadas.
 - **Ativar *proteção para Outlook***: marque a caixa para habilitar a proteção para o Outlook. O Faronics Anti-Virus verificará todos os e-mails enviados e recebidos no programa.
 - **Ativar *proteção para Outlook Express/Windows Mail***: marque para habilitar a proteção para o Outlook Express e o Windows Mail. O Faronics Anti-Virus verificará todos os e-mails enviados e recebidos nos programas.
 - **Ativar *proteção para outros clientes de e-mail***: defina as configurações de porta de Entrada (POP3) e Saída (SMTP) de e-mail. O Faronics Anti-Virus verificará todas as mensagens no programa de e-mail usando as definições de *Entrada* e *Saída*.



9. Especifique configurações no nó *Firewall Protection*.

O Firewall Protection oferece proteção bidirecional, garantindo o tráfego de entrada e de saída. Você pode criar regras personalizadas para proteger a rede. Pode também *Permitir* ou *Bloquear* a comunicação e ainda definir o firewall como *Solicitar*.

- *Nó Firewall*> painel *Configurações*



Configurações do Firewall Protection:

- *Ativar proteção básica do firewall*: marque a caixa de seleção para habilitar a proteção do firewall.
- *Permitir que o usuário desative o firewall*: essa caixa fica habilitada com *Ativar proteção básica do firewall* marcada. Com essa opção selecionada, o usuário pode desativar o firewall na estação de trabalho.
- *Habilitar sistema de detecção de intrusões*: selecione essa opção para ativar o Sistema de detecção de intrusões.

Log do firewall:

- *Registrar pacotes para portas não abertas*: marque a caixa de seleção para registrar os pacotes de dados enviados a portas não abertas. Esses dados servem para analisar tentativas de comunicação com portas não abertas na rede.
- *Registrar verificações de porta*: marque a caixa de seleção para registrar todas as tentativas de verificar portas na sua rede. Os dados dessas verificações serão armazenados no arquivo de log.



- Nó *Firewall Protection* > painel *Regras de programa*

Regras de programa definem a ação tomada pelo firewall sobre a atividade de rede para um aplicativo. Regras de programa têm prioridade sobre as regras padrão. As regras padrão podem ser editadas, mas não excluídas.

Regras de programa

Regras de programa definem a ação tomada pelo firewall sobre a atividade de rede para um aplicativo. Regras de programa têm prioridade sobre as regras padrão. As regras padrão podem ser editadas, mas não excluídas.

Adicionar Editar Excluir

Nome	Programa	Entrada da ...	Saída da zo...	Entrada na ...	Saída da zo...
Faronics Event Re...	FaronicsEvent...	Permitir	Permitir	Permitir	Permitir
Faronics Core Serv...	FaronicsCoreS...	Permitir	Permitir	Permitir	Permitir
Faronics Anti-Virus ...	%INSTALL_DI...	Permitir	Permitir	Permitir	Permitir
Faronics Anti-Virus ...	%INSTALL_DI...	Permitir	Permitir	Permitir	Permitir
Faronics Anti-Virus ...	%INSTALL_DI...	Permitir	Permitir	Permitir	Permitir
Faronics Core Agent	FaronicsCoreA...	Permitir	Permitir	Permitir	Permitir
Faronics Enterprise...	EnterpriseWor...	Permitir	Permitir	Permitir	Permitir
SBAMSvc.EXE	%INSTALL_DI...	Bloquear	Permitir	Bloquear	Permitir
SBPIMSvc.EXE	%INSTALL_DI...	Bloquear	Permitir	Bloquear	Permitir
Internet Explorer	%PROGRAMF...	Permitir	Permitir	Bloquear	Permitir
lsass.exe	%WINDIR%\\s...	Bloquear	Permitir	Bloquear	Permitir
services.exe	%WINDIR%\\s...	Bloquear	Permitir	Bloquear	Permitir
winlogon.exe	%WINDIR%\\s...	Bloquear	Permitir	Bloquear	Permitir
svchost.exe	%WINDIR%\\s...	Bloquear	Permitir	Bloquear	Permitir
Deep Freeze Service	DFServ.exe	Permitir	Permitir	Permitir	Permitir
Deep Freeze Admin	DFAdmin.exe	Permitir	Permitir	Permitir	Permitir
Deep Freeze Cons...	DFConsole.exe	Permitir	Permitir	Permitir	Permitir
Deep Freeze Serv...	DFSserverCons...	Permitir	Permitir	Permitir	Permitir
Deep Freeze Serv...	DFSserverServi...	Permitir	Permitir	Permitir	Permitir

OK Cancelar



Clique em *Adicionar* para acrescentar uma regra de programa. Defina ou selecione as opções e clique em *OK*. Os parâmetros a seguir serão exibidos.

Adicionar uma regra

Uma regra de programa dá permissões a um programa específico. As regras de programa têm prevalência sobre as configurações da regra [Qualquer outro aplicativo].

Nome:

Programa:

Exemplo: C:\Caminho\Programa.exe

%Arquivosdeprogramas%\navegador\navegador.exe

Entrada da zona confiável: Permitir

Saída da zona confiável: Permitir

Entrada na zona não confiável: Permitir

Saída da zona não confiável: Permitir

[O que é uma zona?](#)

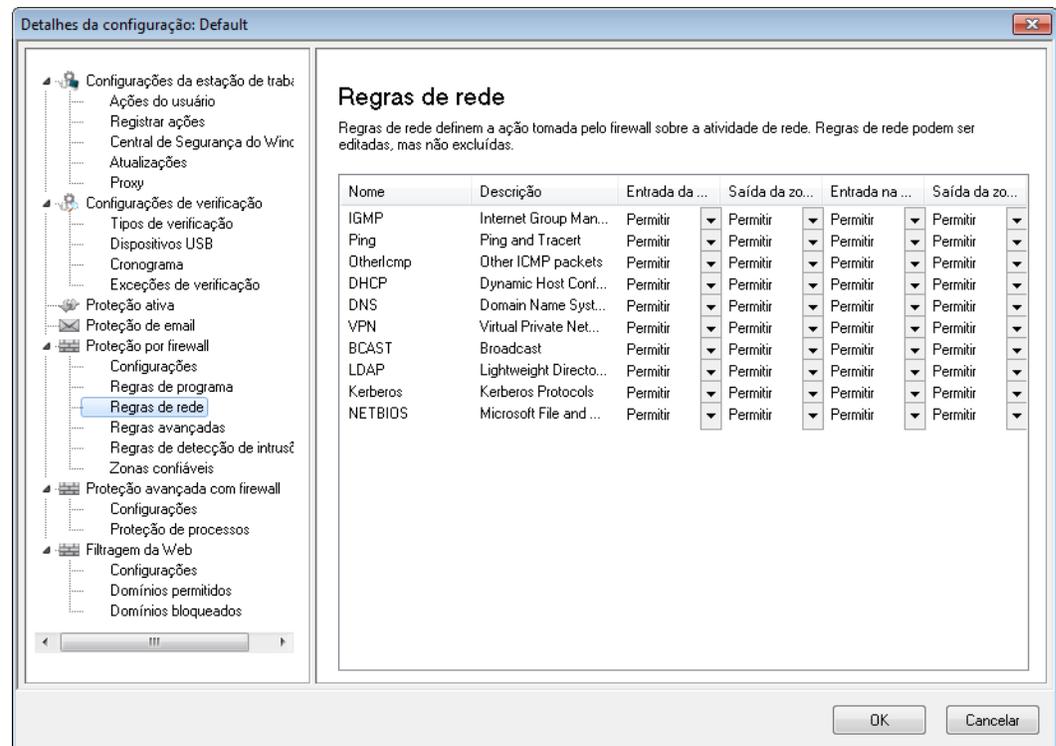
OK Cancelar

- *Nome*: o nome da regra.
- *Programa*: nome do programa, inclusive caminho completo e extensão.
- *Entrada na zona confiável*: a ação a ser executada para a comunicação de entrada no programa em uma zona confiável (*Permitir*, *Bloquear* ou *Solicitar*).
- *Saída da zona confiável*: a ação a ser executada para a comunicação que sai do programa em uma zona confiável (*Permitir*, *Bloquear* ou *Solicitar*).
- *Entrada na zona não confiável*: a ação a ser executada para a comunicação de entrada no programa em uma zona não confiável (*Permitir*, *Bloquear* ou *Solicitar*).
- *Saída da zona não confiável*: a ação a ser executada para a comunicação que sai do programa em uma zona não confiável (*Permitir*, *Bloquear* ou *Solicitar*).



- Nó *Firewall Protection* > painel *Regra de rede*

Regras de rede definem a ação tomada pelo firewall sobre a atividade de rede. Regras de rede podem ser editadas, mas não excluídas.



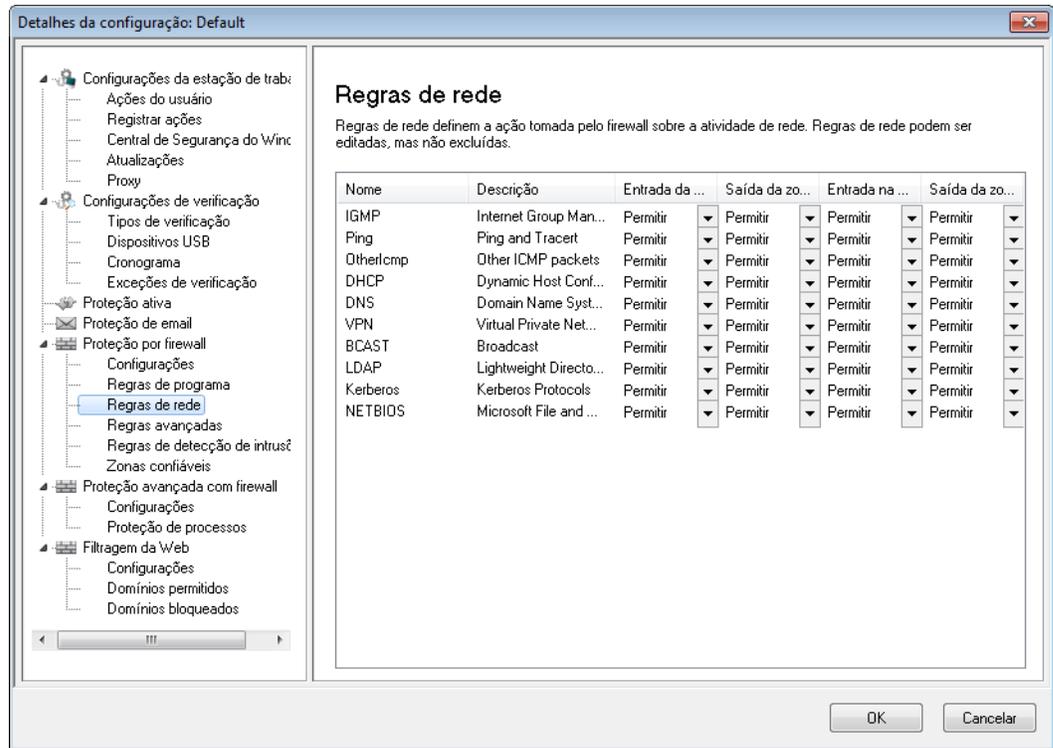
Os parâmetros a seguir serão exibidos.

- *Nome*: nome do protocolo.
- *Descrição*: descrição do protocolo.
- *Entrada na zona confiável*: a ação a ser executada para a comunicação de entrada no protocolo em uma zona confiável (*Permitir*, *Bloquear* ou *Solicitar*).
- *Saída da zona confiável*: a ação a ser executada para a comunicação que sai do protocolo em uma zona confiável (*Permitir*, *Bloquear* ou *Solicitar*).
- *Entrada na zona não confiável*: a ação a ser executada para a comunicação de entrada no protocolo em uma zona não confiável (*Permitir*, *Bloquear* ou *Solicitar*).
- *Saída da zona não confiável*: a ação a ser executada para a comunicação que sai do protocolo em uma zona não confiável (*Permitir*, *Bloquear* ou *Solicitar*).



- *Nó Firewall Protection* > painel *Regras avançadas*

Regras avançadas definem a ação tomada pelo firewall para determinado aplicativo, porta ou protocolo. Pode incluir um único protocolo, porta local ou remota e direção de tráfego ou uma combinação desses. Você pode adicionar, editar e excluir uma regra avançada.



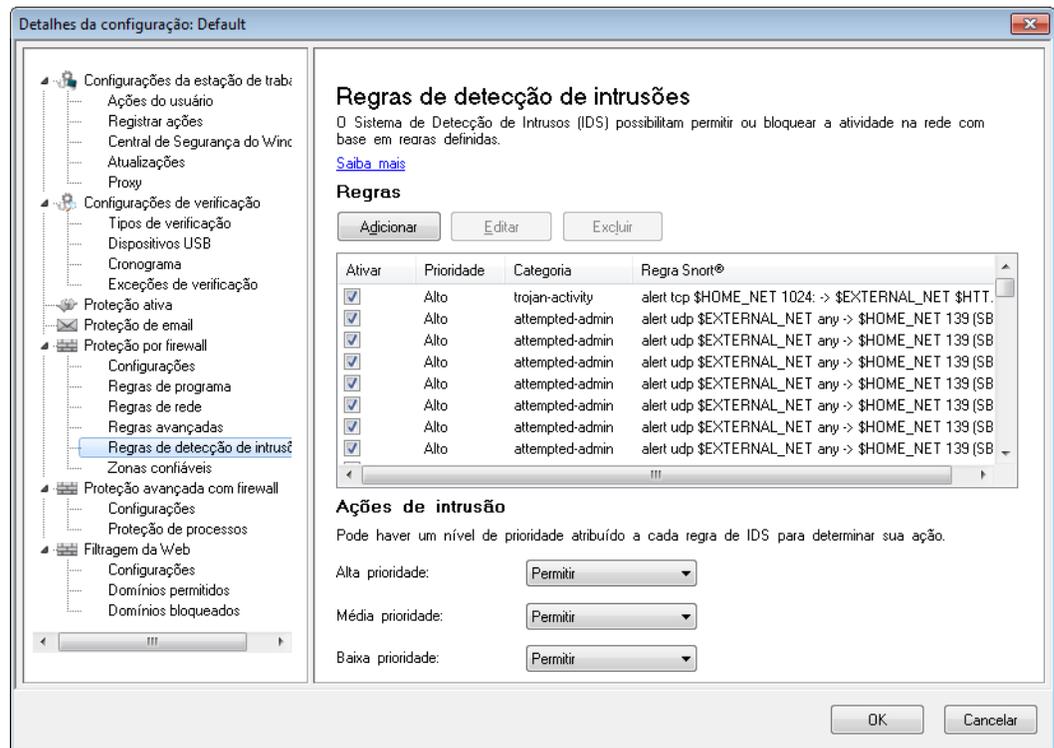
Clique em *Adicionar* para acrescentar uma regra avançada. Defina ou selecione as opções e clique em *OK*. Estes parâmetros aparecerão no painel *Regras avançadas*:

- *Nome*: o nome da regra.
- *Programa*: nome e caminho do programa.
- *Ação*: a ação executada pelo firewall para a comunicação do aplicativo, porta ou protocolo especificado (*Permitir*, *Bloquear* ou *Solicitar*).
- *Direção*: o sentido da comunicação (*Ambos*, *Entrada e saída*).
- *Protocolo*: o nome do protocolo.
- *Porta local*: detalhes da porta local.
- *Porta remota*: detalhes da porta remota.

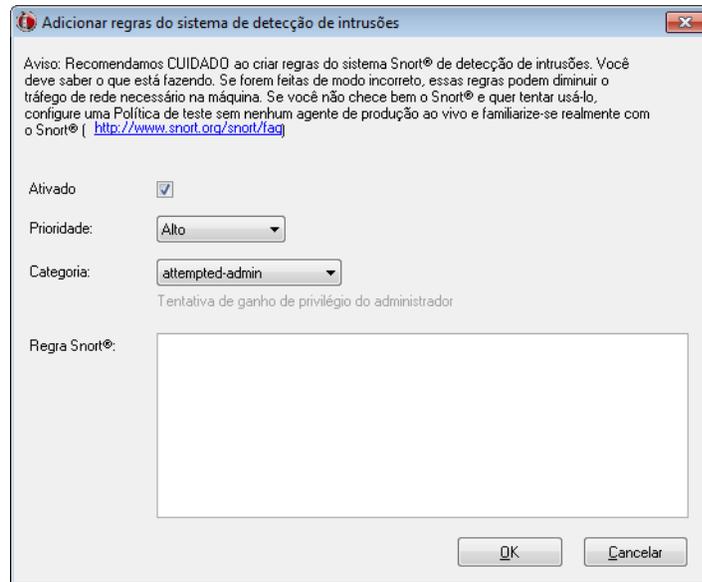


- Nó *Firewall Protection* > painel *Regras de detecção de intrusões*

O Sistema de detecção de intrusões (IDS) é usado para permitir ou bloquear a atividade na rede com base em uma regra de detecção definida. No painel *Regras de detecção*, especifique a ação (*Permitir* ou *Bloquear*) para cada regra com prioridade categorizada como *Alta*, *Média* e *Baixa* na tela. Clique em *Editar* para editar ou em *Excluir* para excluir uma regra.



Clique em *Adicionar* para acrescentar uma regra de detecção de intrusões. Defina ou selecione as opções e clique em *OK*. Os parâmetros a seguir são exibidos quando se clica em *Adicionar*.

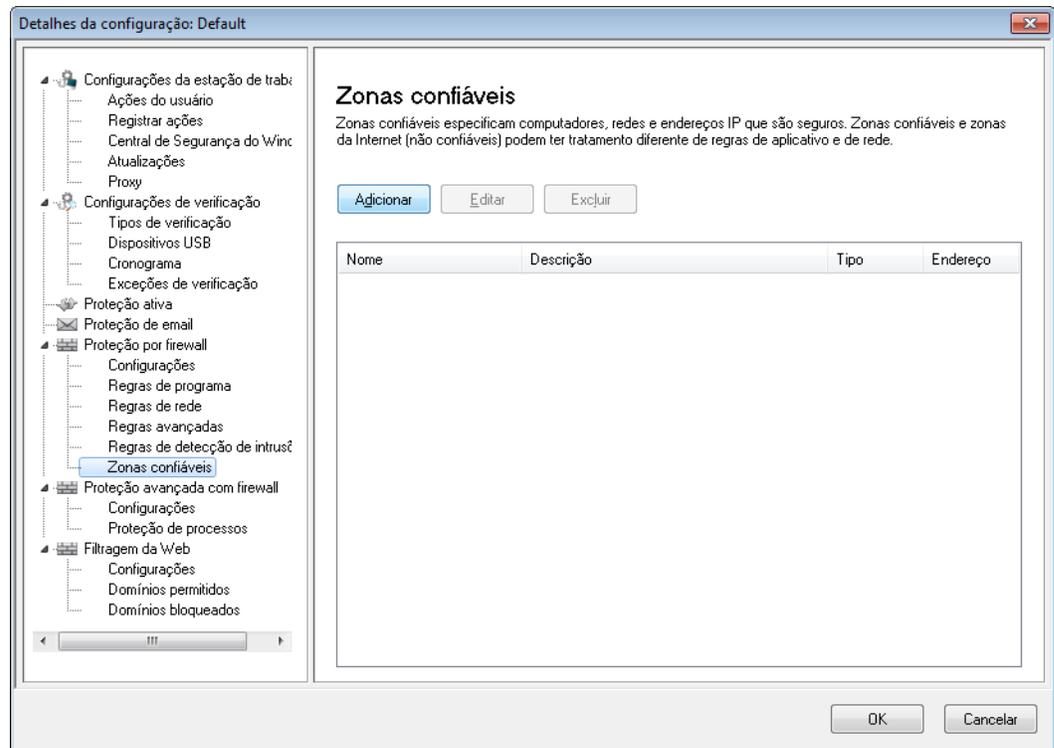


o - selecione se esta regra deve ser ativada.

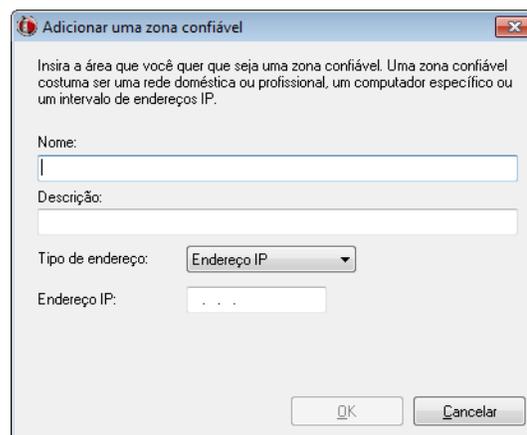
- *Prioridade*: selecione a prioridade *Alta*, *Média* ou *Baixa*.
- *Categoria*: defina a categoria (por exemplo, *nocivo/desconhecido*, *tentativa/admin*, *tentativa/dos* ou *tentativa/recon*).
- *Regra Snort*: especifique uma regra Snort. Para saber mais sobre regras Snort, visite www.snort.org/snort/faq.

- *Nó Firewall Protection* > painel *Zonas confiáveis*

Zonas confiáveis especificam computadores, redes e endereços IP seguros. Zonas confiáveis e zonas da Internet (não confiáveis) podem ter tratamento diferente das regras de programa e de rede.



Clique em *Adicionar* para acrescentar uma zona confiável. Defina ou selecione as opções e clique em *OK*. Os parâmetros a seguir serão exibidos.



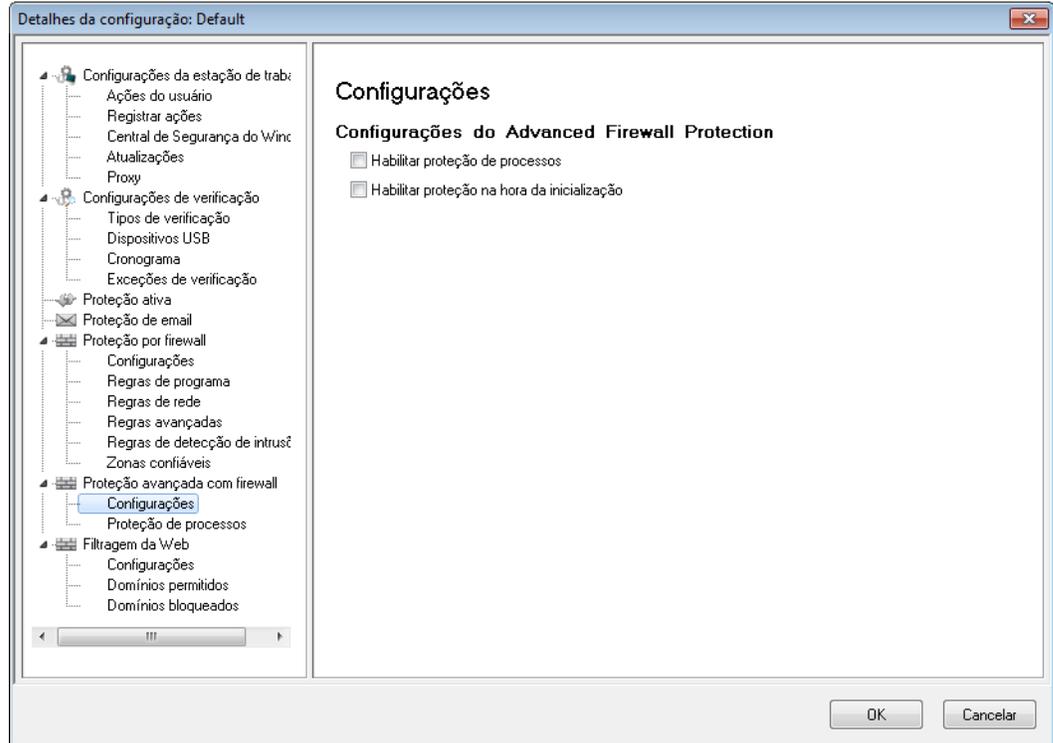
- *Nome*: nome da zona confiável.
- *Descrição*: descrição da zona confiável.
- *Tipo*: tipo da zona confiável (*Endereço IP*, *Intervalo de endereços* ou *Rede*).

10. Especifique as configurações no nó Advanced Firewall Protection.

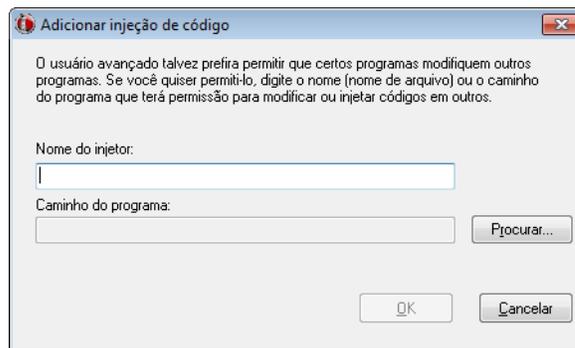
- Nó *Proteção avançada do firewall* > painel *Configurações*



O painel Configurações permite ativar e desativar a proteção de processos e de hora da inicialização.



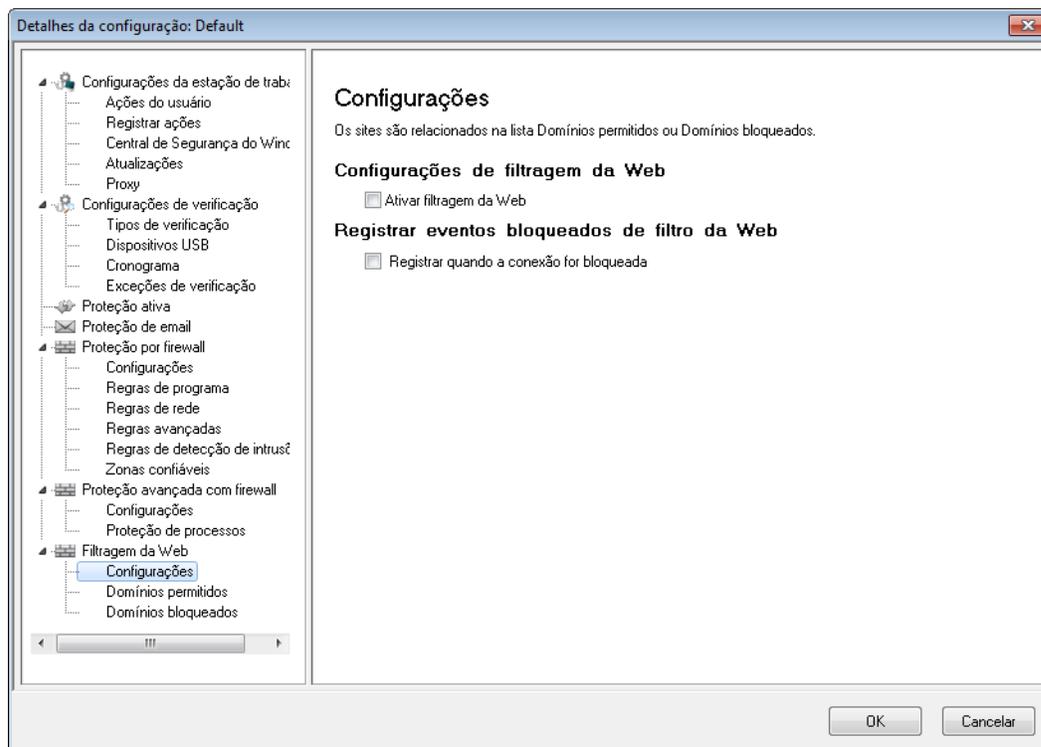
Escolha as opções e clique em *Aplicar*. Os parâmetros a seguir serão exibidos.



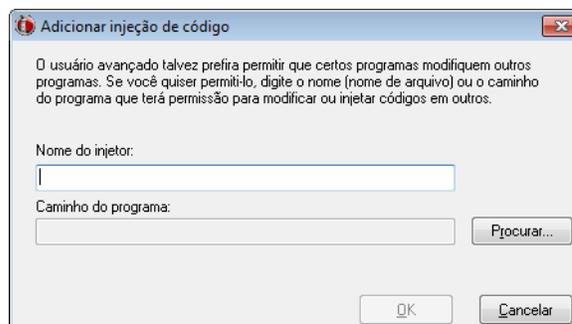
- *Ativar proteção de processos*: marque para ativar a proteção. Esse recurso é usado para definir a ação para injetores de código desconhecidos e adicionar injetores permitidos com base nas configurações do painel *Proteção de processos*.
- *Ativar proteção de hora da inicialização*: marque para ativar a proteção. O computador fica protegido na hora da inicialização pois o tráfego é bloqueado até que o Windows seja aberto.
- Nó *Firewall Protection* > painel *Proteção de processos*



A página de propriedades da proteção de processos é usada para definir a ação para injetores de código desconhecidos e adicionar injetores permitidos. Os processos são protegidos evitando que um programa injete códigos em outro programa. Em alguns casos, você pode especificar que programa poderá injetar códigos em outro.



Clique em *Adicionar* para acrescentar um Injetor de código. Defina ou selecione as opções e clique em *OK*. Os parâmetros a seguir serão exibidos.

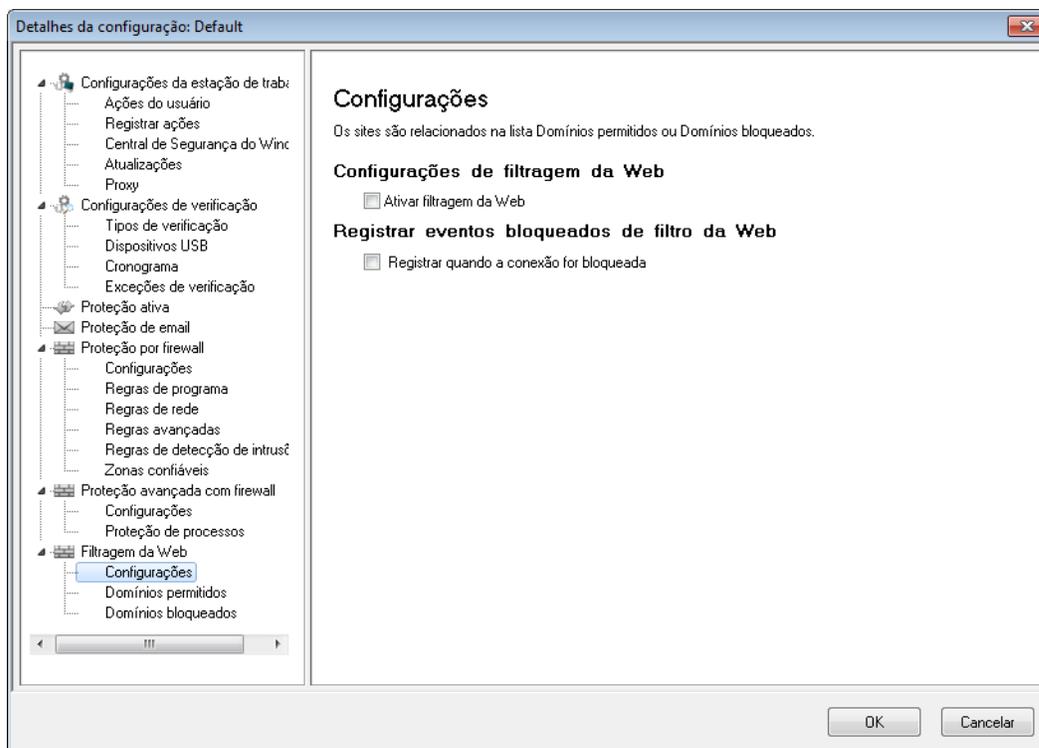


- *Nome do injetor*: defina o nome do injetor.
- *Caminho do programa*: procure e selecione o caminho.

11. Especifique as configurações no nó Filtragem da Web.

- Nó *Filtragem da Web* > painel *Configurações*

A Filtragem da Web bloqueia a exibição de certos tipos de informação no navegador. Nesse painel você pode definir a configuração padrão de Filtragem da Web.

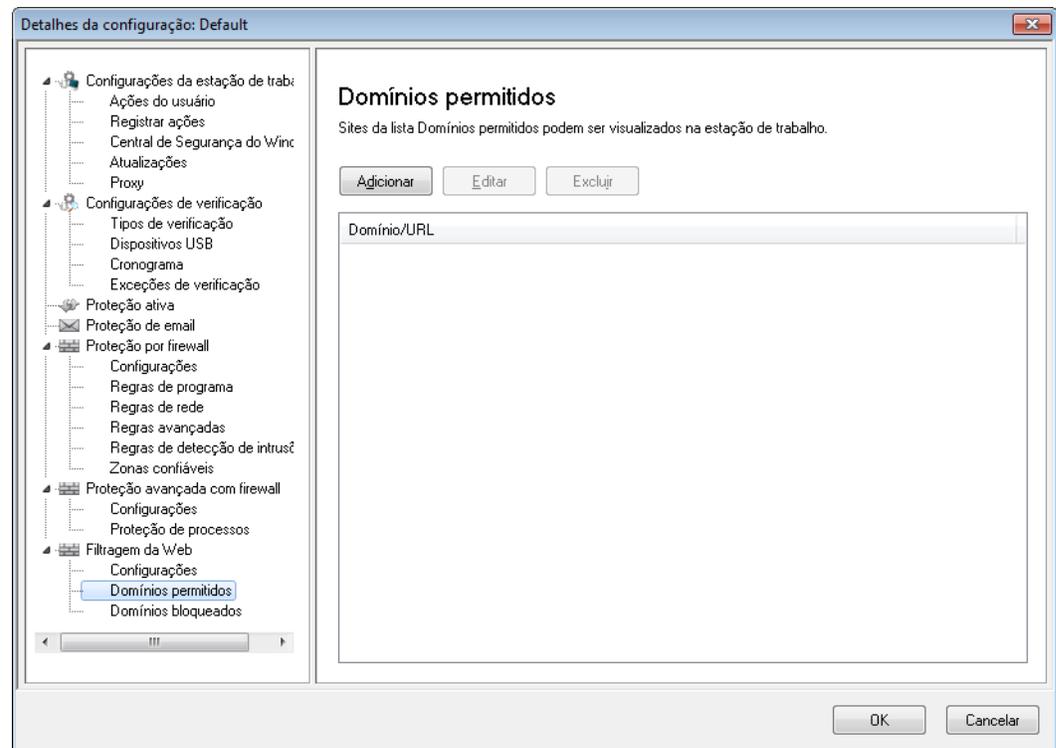


- Selecione *Ativar filtragem da Web* para ativar o recurso.
- Marque *Registrar quando a conexão for bloqueada* para que a ação executada pelo Faronics Anti-Virus seja registrada no arquivo de log.

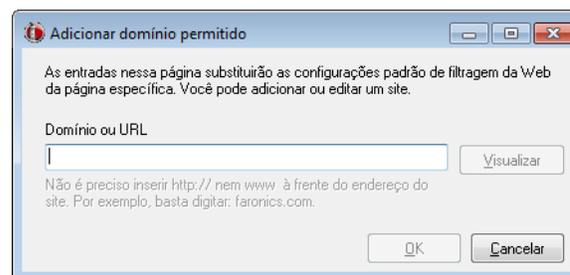


- Nó *Filtragem da Web* > painel *Domínios permitidos*

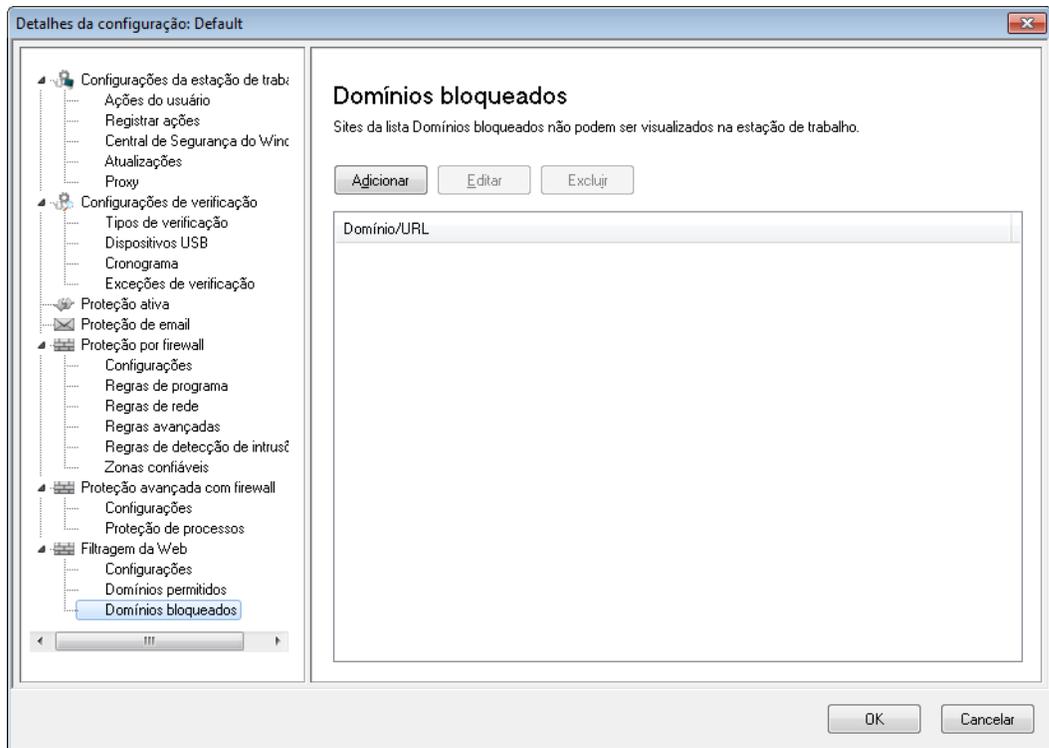
Os domínios permitidos prevalecem sobre as configurações de filtragem da Web e sites adicionados à lista Anúncios bloqueados.



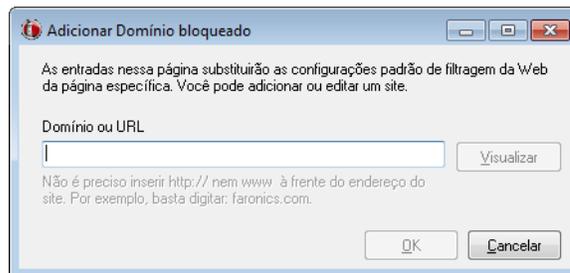
Clique em *Adicionar* para acrescentar um domínio permitido. Defina ou selecione as opções e clique em *OK*. Os parâmetros a seguir serão exibidos.



- **Domínio ou URL:** especifique o domínio ou URL a ser permitida. Clique em *Visualizar* para ver o domínio ou URL.
 - Nó *Filtragem da Web* > painel *Domínios bloqueados*
- Defina os domínios que devem ser bloqueados na rede.



Clique em *Adicionar* para acrescentar um domínio bloqueado. Defina ou selecione as opções e clique em *OK*. Os parâmetros a seguir serão exibidos.



- Domínio ou URL: especifique o domínio ou URL a ser permitida. Clique em Visualizar para ver o domínio ou URL.
12. Clique em *Ok*.
 13. Especifique o nome da configuração e clique em *OK*.

Aplicando a configuração do Anti-Virus

Execute estas etapas para aplicar a configuração do Anti-Virus:

1. Vá para o painel *Estações de trabalho*.
2. Selecione uma ou mais estações de trabalho.



3. Clique com o botão direito em uma ou mais estações de trabalho e selecione *Atualizar configuração* > *Anti-Virus* > [nome da configuração].

A configuração será aplicada às estações de trabalho selecionadas.



As alterações de configuração serão aplicadas automaticamente às estações de trabalho online. Se as estações de trabalho estiverem offline, as alterações de configuração serão aplicadas quando as estações de trabalho voltarem a estar online.

Editando as configurações Anti-Virus

Execute estas etapas para editar a configuração do Anti-Virus:

1. Vá para o painel Redes e grupos no Console corporativo.
2. Selecione *Configurações disponíveis* > *Anti-Virus* > [Nome da configuração].
3. Clique com o botão direito na configuração selecionada e selecione *Editar configuração selecionada*.
4. Edite as configurações conforme necessário.
5. Clique em *Ok*.

Excluindo a configuração do Anti-Virus

Execute estas etapas para excluir a configuração do Anti-Virus:

1. Vá para o painel Redes e grupos no Console corporativo.
2. Selecione *Configurações disponíveis* > *Anti-Virus* > [Nome da configuração].
3. Clique com o botão direito na configuração selecionada e selecione *Excluir configuração selecionada*.
4. Clique em *Ok*.



Usando o Faronics Anti-Virus no Console corporativo

Quando o cliente do Faronics Anti-Virus estiver instalado na estação de trabalho, diversas ações podem ser realizadas na estação de trabalho através do Console do Deep Freeze.

Comandos Anti-Virus

Existem duas maneiras para os mesmos comandos via Console do Deep Freeze:

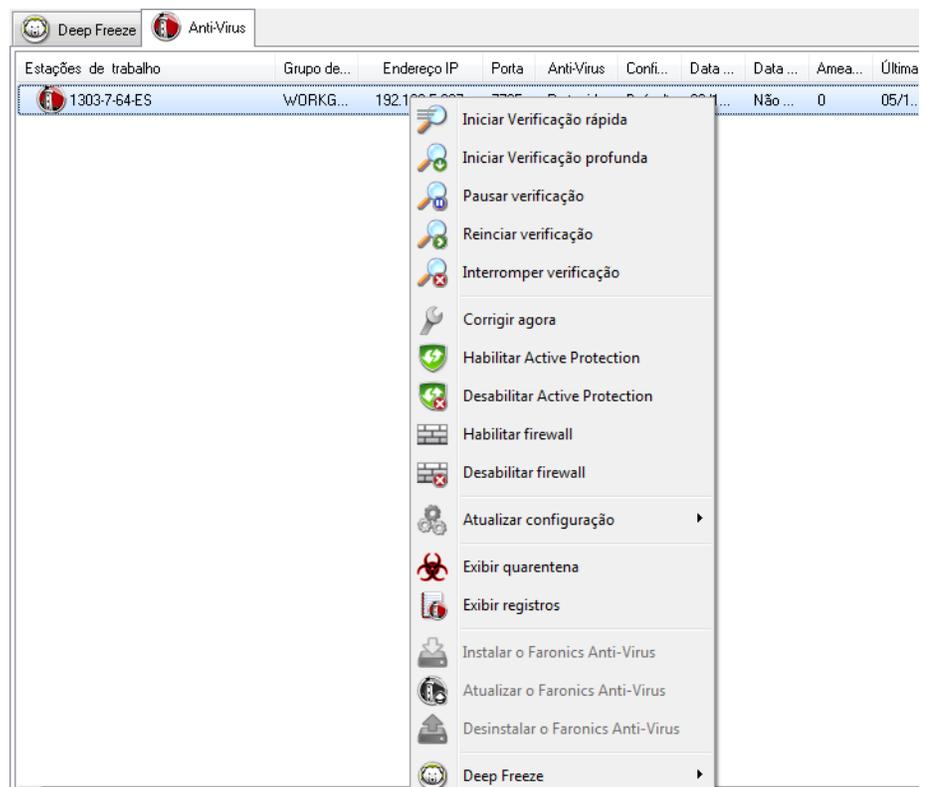
- Menu Anti-Virus (na barra de menus)
- Menu de conteúdo do Anti-Virus (clique com o botão direito no menu de contexto)

Os comandos do menu são explicados mais adiante nesta seção.

Estes comandos estão disponíveis no menu Anti-Virus:



Os mesmos comandos estão disponíveis a partir do painel *Estações de trabalho* na guia > *Anti-Virus* > Clique com o botão direito no menu de contexto:





Verificação rápida

A Verificação rápida verifica as áreas mais comumente afetadas do computador. Tem duração mais curta do que a Verificação profunda do sistema. A Verificação rápida também usa menos memória do que a Verificação profunda do sistema.

- Para iniciar uma Verificação rápida
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Iniciar Verificação rápida*.
- Para interromper uma Verificação rápida
Selecione uma ou mais estações de trabalho. Clique com o botão direito e selecione *Interromper verificação*.
- Para pausar uma Verificação rápida
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Pausar verificação*.
- Para reiniciar uma Verificação rápida
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Reiniciar verificação*.

Verificação profunda

A Verificação profunda realiza a verificação através de todas as áreas do computador. O tempo gasto na verificação depende o tamanho do disco rígido.

- Para iniciar a Verificação profunda
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Iniciar Verificação profunda*.
- Para interromper uma Verificação profunda
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Interromper Verificação profunda*.
- Para pausar uma Verificação profunda
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Pausar verificação*.
- Para reiniciar uma Verificação profunda
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Reiniciar verificação*.

Corrigir agora

A opção Fix Now baixa as definições de vírus mais recentes e realiza uma verificação rápida na estação de trabalho.

- Para Fix Now
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Fix Now*.



Proteção ativa

O AP (Proteção ativa) é um método em tempo real para detecção de malware. O AP fica imperceptível em segundo plano enquanto você trabalha ou navega na Internet, monitorando constantemente arquivos executados sem impacto notável sobre o sistema.

- Para habilitar Proteção ativa
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Ativar Proteção ativa*.
- Para desativar a Proteção ativa
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Desativar Proteção ativa*.

Firewall

O firewall oferece segurança bidirecional, protegendo o tráfego de entrada e de saída. Ele protege a rede contra intrusões não autorizadas.

- Para ativar o firewall
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Ativar firewall*.
- Para desativar o firewall
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Desativar firewall*.

Enviar mensagem

A opção *Enviar mensagem* é usada para enviar mensagem para as estações de trabalho online.

- Para enviar uma mensagem
Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Enviar mensagem*.

Visualizar informações de quarentena

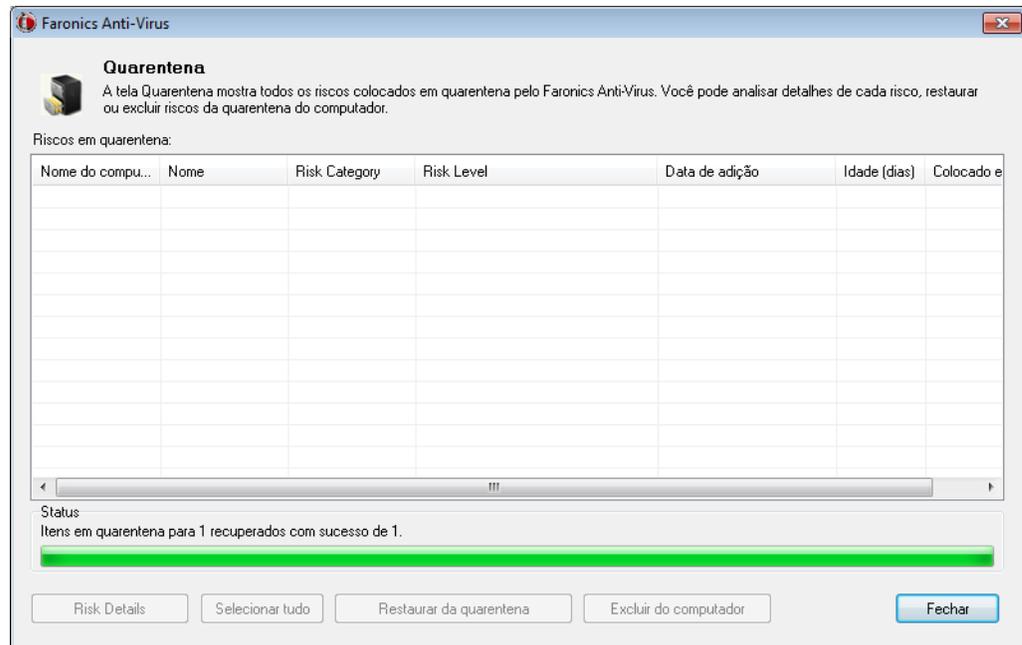
A quarentena é um local seguro no computador usado pelo Faronics Anti-Virus para armazenar malware e arquivos infectados que não podem ser desinfetados. Se o computador ou arquivos no computador não se comportarem normalmente quando um item for colocado em quarentena, você pode rever os detalhes do risco, analisar mais a fundo e removê-lo da



quarentena, restaurando-o ao local de origem no computador. Você também pode remover os riscos da quarentena permanentemente.

- Para visualizar a quarentena

Selecione uma ou mais estações de trabalho. Clique com o botão direito do mouse e selecione *Faronics Anti-Virus > Obter informações de quarentena*.



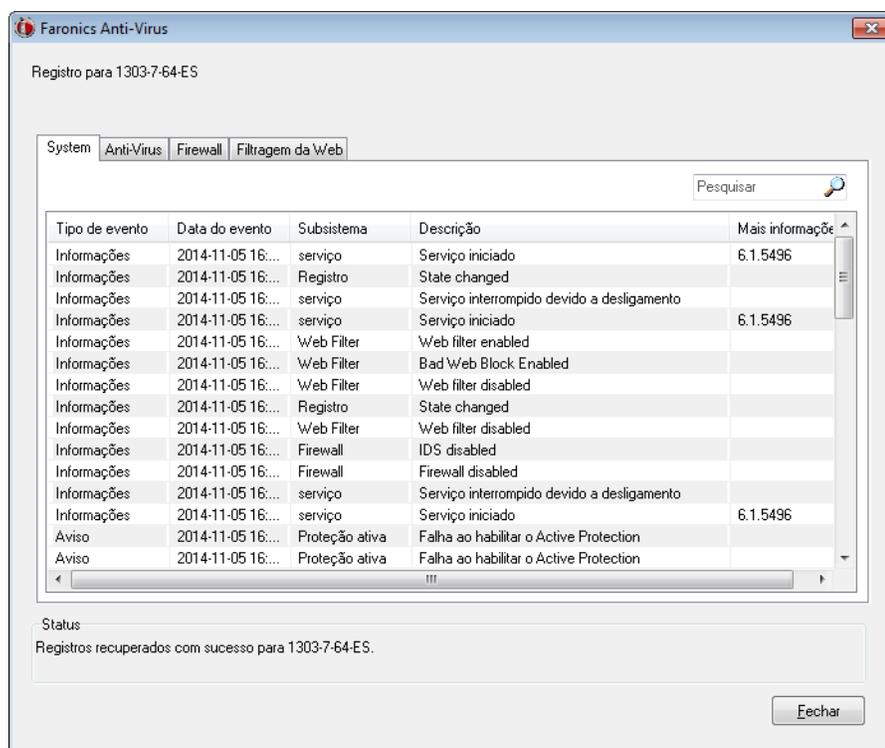
Visualizar informações do registro

O registro do Faronics Anti-Virus exibe todas as tarefas realizadas pelo Faronics Anti-Virus na estação de trabalho.

- Para visualizar as informações do registro:

Selecione uma única estação de trabalho. Clique com o botão direito do mouse e selecione *Faronics Anti-Virus > Visualizar informações de quarentena*. As guias a seguir serão exibidas:

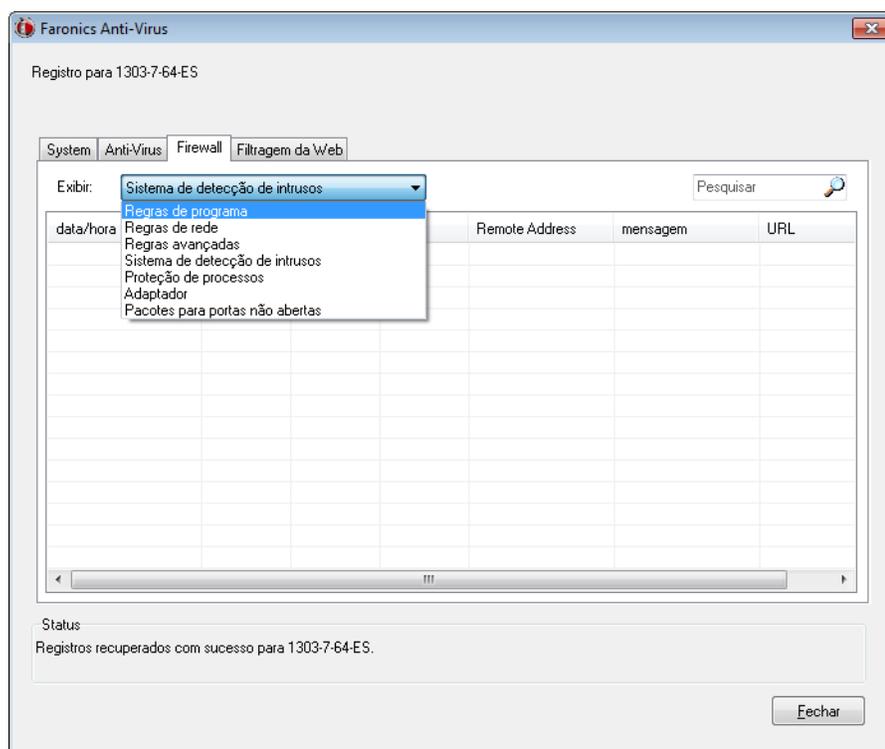
- Guia Sistema: mostra os eventos do sistema.



- Guia Anti-Virus: mostra os eventos do Anti-Virus. Selecione as opções a seguir no menu suspenso para visualizar os resultados selecionados para:
 - Verificar
 - Proteção ativa
 - Proteção de e-mail

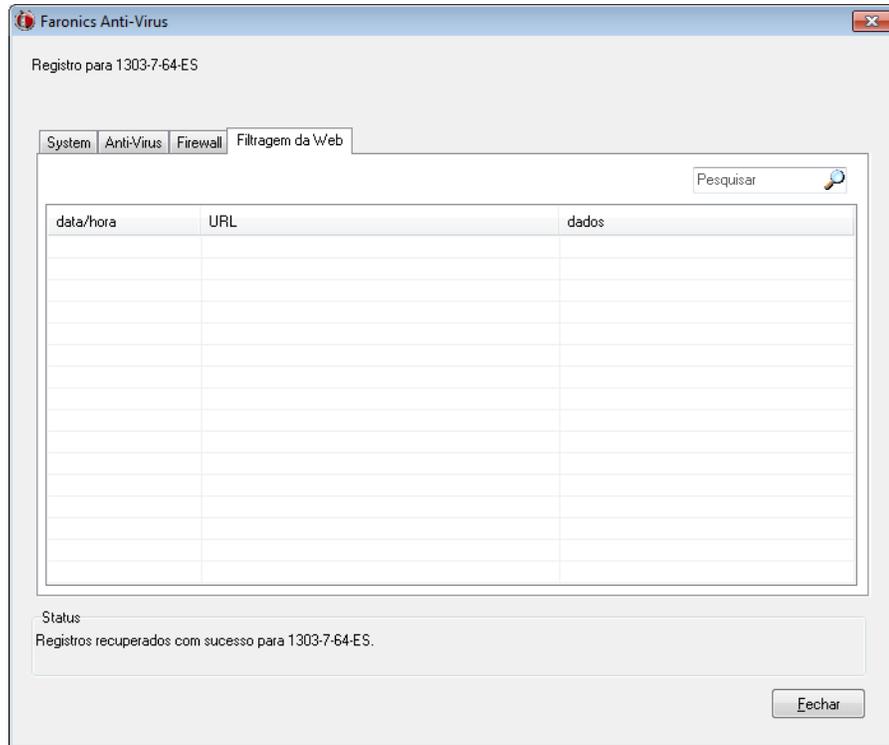


- Guia firewall: mostra os eventos do sistema. Procure eventos específicos no campo Pesquisar. Selecione as opções a seguir no menu suspenso para visualizar os resultados selecionados para:
 - Regras de programa
 - Regras de rede
 - Regras avançadas
 - Sistema de detecção de intrusões
 - Proteção de processos
 - Adaptador
 - Pacotes para portas não abertas





- Guia Filtragem da Web: mostra os eventos de filtragem da Web.





Programação de tarefas Anti-Virus

As tarefas Anti-Virus a seguir podem ser processadas a partir do Console do Deep Freeze com base em uma programação predefinida.

- Desativar Proteção ativa
- Ativar Proteção ativa
- Iniciar Verificação rápida
- Iniciar Verificação profunda

O procedimento para agendar tarefas é explicado em detalhes na seção [Agendando tarefas do Deep Freeze](#).

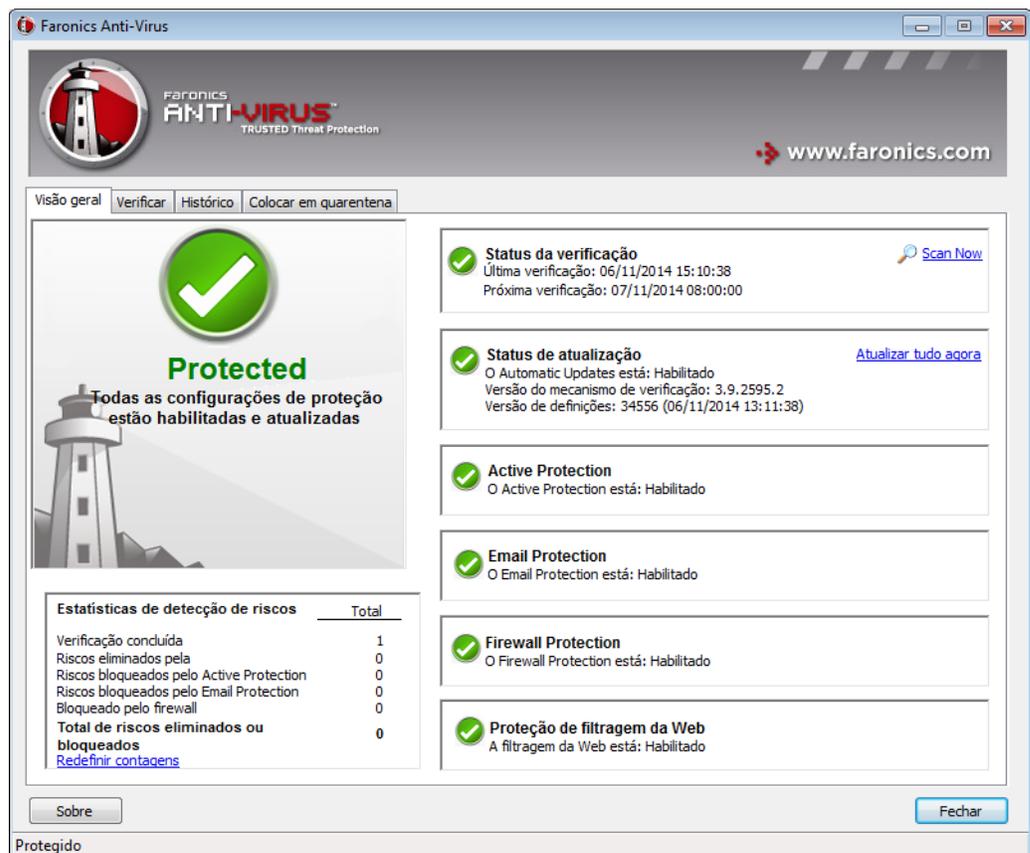


Usando o Anti-Virus na estação de trabalho

Os recursos disponíveis no Anti-Virus na estação de trabalho dependem totalmente das configurações selecionadas na Configuração do Anti-Virus. Para obter mais informações sobre a Configuração do Anti-Virus, consulte [Configuração do Anti-Virus](#).

Iniciando o Anti-Virus na estação de trabalho

Vá para *Iniciar > Programas > Faronics > Anti-Virus Enterprise > Faronics Anti-Virus Enterprise*. Ou clique duas vezes no ícone do Faronics Anti-Virus na bandeja do sistema.



Os painéis a seguir mostram informações importantes para o usuário.

- *Protegido* ou *Não protegido* aparece, informando se o computador está sob proteção. Se aparece *Não protegido*, clique no botão *Fix Now*, embaixo do sinal *Não protegido*.
- *Status da verificação* mostra quando a última verificação foi feita. Para realizar uma verificação, clique no link *Scan Now*.
- *Status da atualização* mostra quando foi feita a última atualização. Para atualizar as definições de vírus, clique no link *Atualizar tudo agora*.
- *Active Protection* informa se a proteção em tempo real está habilitada.
- *Email Protection* diz se o e-mail está protegido pelo Faronics Anti-Virus.

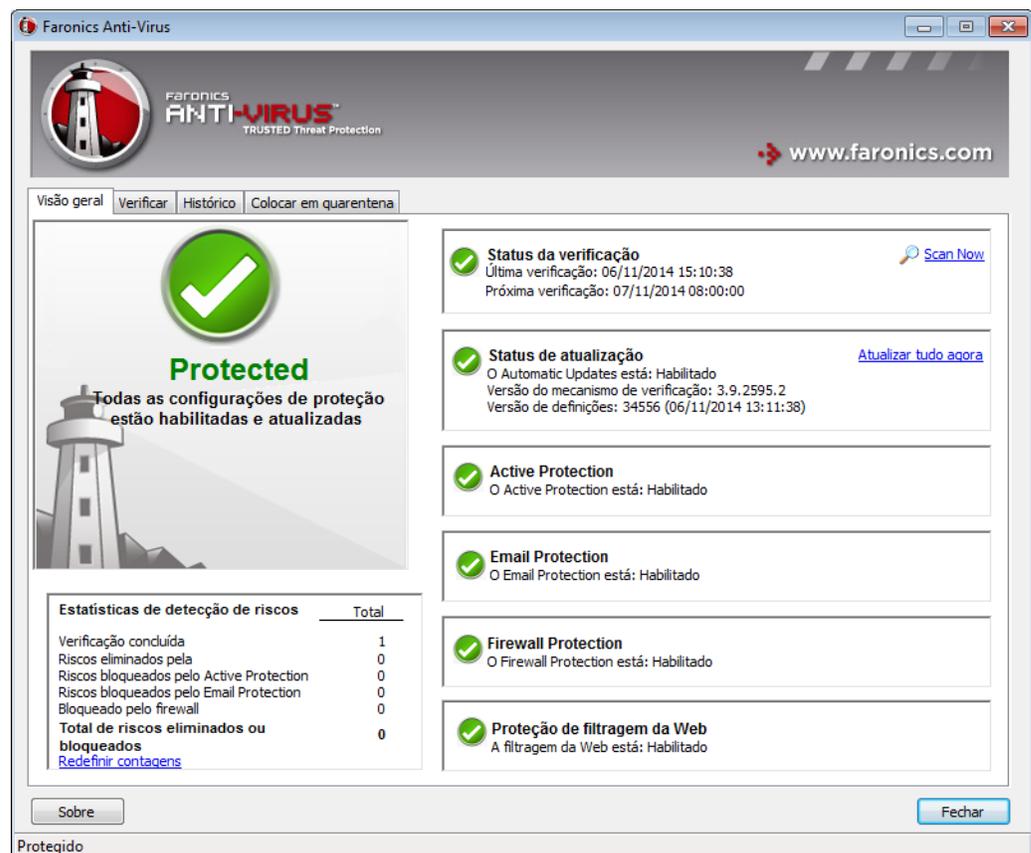


- *Firewall Protection* mostra se a estação de trabalho está protegida pelo firewall.
- *Proteção de filtragem da Web* diz se a estação está protegida pelo recurso de filtragem da Web do Faronics Anti-Virus.
- *Estatísticas de detecção de riscos* mostra estatísticas das ações realizadas pelo Faronics Anti-Virus. Clique em *Redefinir contagens* para zerar a contagem.

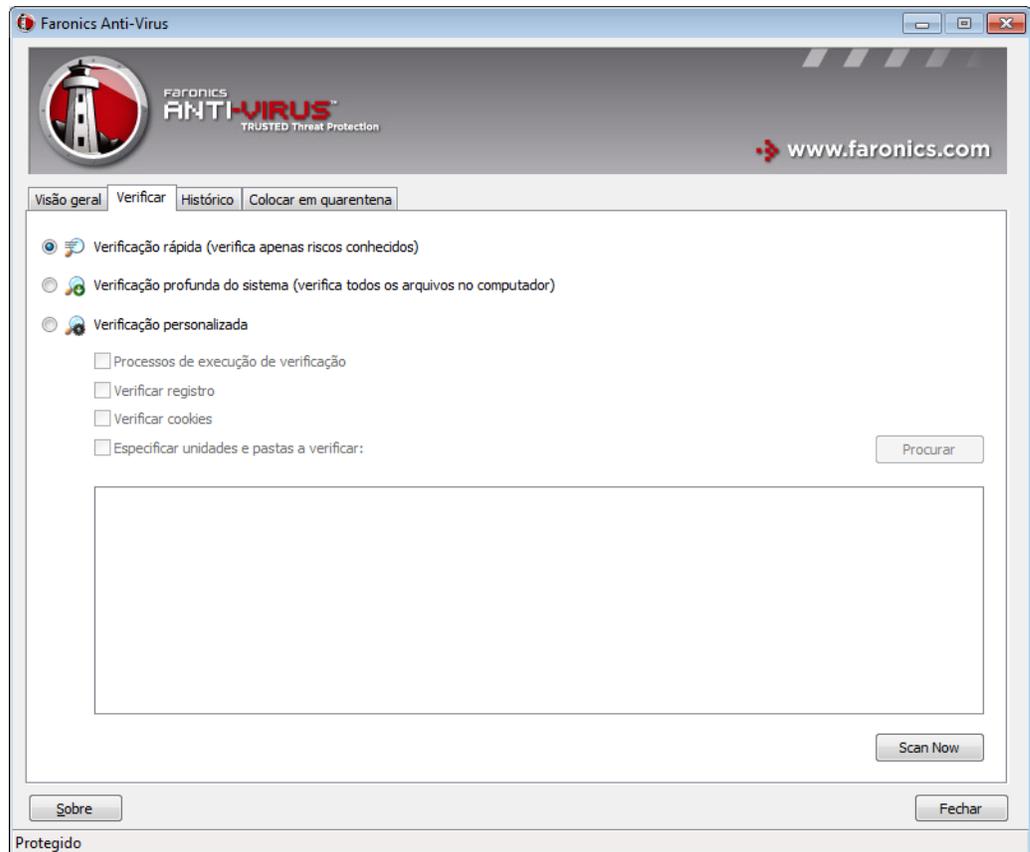
Verificando a estação de trabalho

Siga estas etapas para verificar uma estação de trabalho:

1. Vá para *Iniciar* > *Programas* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Ou clique duas vezes no ícone do Faronics Anti-Virus na bandeja do sistema.



2. No painel *Status da verificação*, clique em *Scan Now*. Aparecerá a guia *Verificar*. Você também pode clicar na guia *Verificação*.



3. Selecione uma das seguintes opções:
 - *Verificação rápida*: verifica apenas ameaças conhecidas.
 - *Verificação profunda do sistema*: verificação minuciosa de todos os arquivos na estação.
 - *Verificação personalizada* (selecione das opções a seguir).
 - *Verificar execução de processos*: verifica processos em execução na estação de trabalho.
 - *Verificar registro*: verifica o registro.
 - *Verificar cookies*: são verificados os cookies armazenados na estação.
 - *Especificar unidades e pastas a verificar*: Clique em *Procurar* para selecionar pastas.
4. Clique em *Scan Now*. O ícone giratório indica que há uma verificação em andamento. Os resultados são exibidos após a conclusão da verificação.
5. Selecione os arquivos e estas opções ficarão disponíveis:
 - Selecione *Alterar ação de limpeza*>*Ação recomendada* para realizar a ação sugerida pelo Faronics Anti-Virus.
 - Selecione *Alterar ação de limpeza*>*Colocar em quarentena/Desinfetar* para colocar o arquivo em quarentena ou desinfetá-lo.
 - Selecione *Alterar ação de limpeza*>*Excluir* para excluir o arquivo.
 - Selecione *Alterar ação de limpeza*>*Permitir* para permitir o arquivo.
 - Clique *Selecionar tudo* para selecionar todos os arquivos exibidos no *Resultado da verificação*.



- Clique em *Detalhes* para ver detalhes do risco.
- Clique em *Cancelar* para fechar a caixa de diálogo sem realizar nenhuma ação.
- Clique em *Limpar* para remover o arquivo e fechar a caixa de diálogo.

Verificando um arquivo ou pasta através do clique com o botão direito

É fácil verificar vírus em pastas e arquivos, um a um ou vários de cada vez. Quando o Faronics Anti-Virus é instalado na estação de trabalho, a opção Verificar vírus é adicionada ao menu contextual.

Execute as etapas a seguir para verificar um arquivo ou pasta no computador:

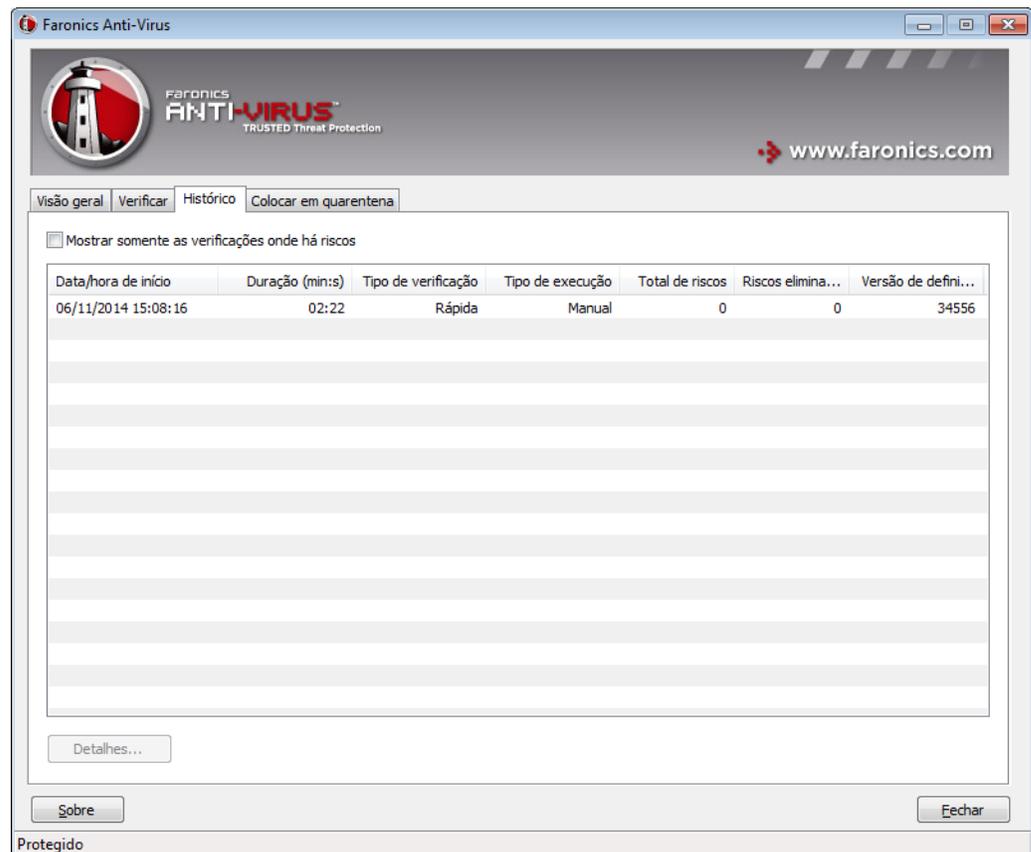
1. Clique com o botão direito no arquivo ou pasta.
2. Selecione *Verificar vírus*.

A verificação será feita e os resultados, exibidos.

Visualizar histórico de verificação

Execute estas etapas para visualizar o histórico de verificação:

1. Vá para *Iniciar > Programas > Faronics > Anti-Virus Enterprise > Faronics Anti-Virus Enterprise*. Ou clique duas vezes no ícone do Faronics Anti-Virus na bandeja do sistema.
2. Clique na guia *Histórico*.



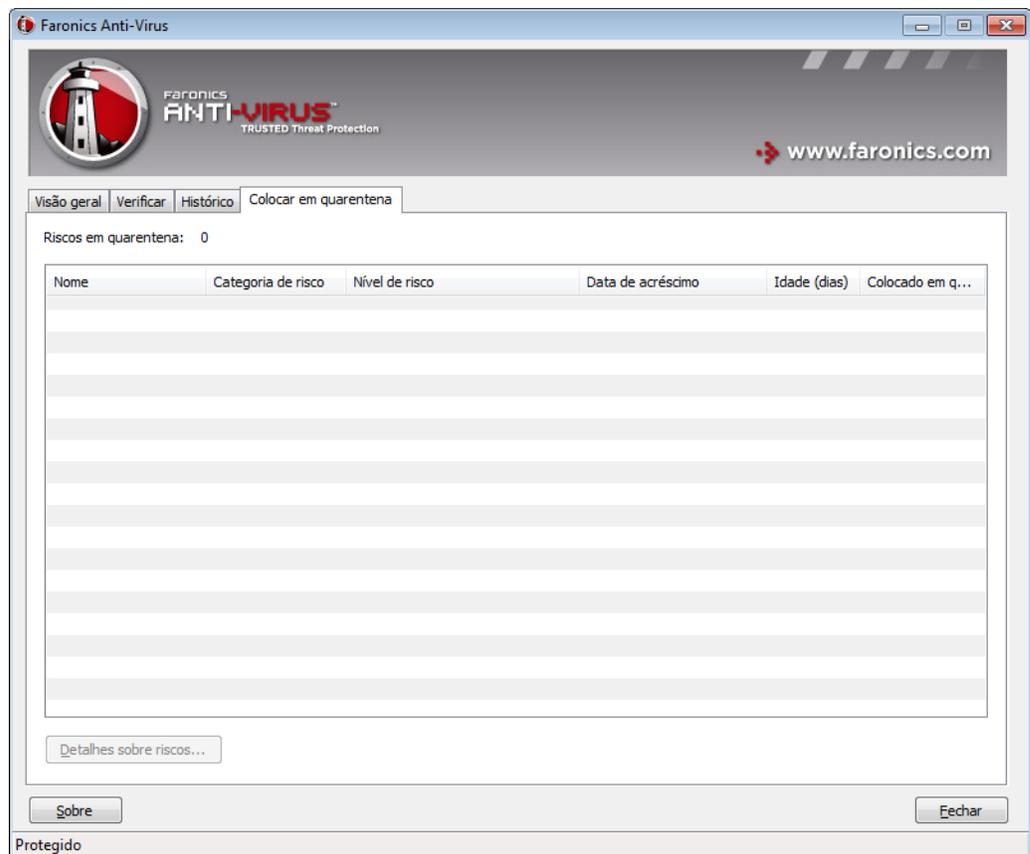


3. Marque as ações a seguir.
 - *Mostrar somente as verificações onde há riscos* - selecione esta opção para visualizar apenas as verificações onde foram encontrados riscos.
 - *Detalhes* - selecione uma entrada e clique em detalhes para visualizar os detalhes da verificação.

Visualizar e executar ação em arquivos em quarentena

Execute estas etapas para visualizar a quarentena:

1. Vá para *Iniciar > Programas > Faronics > Anti-Virus Enterprise > Faronics Anti-Virus Enterprise*. Ou clique duas vezes no ícone do Faronics Anti-Virus na bandeja do sistema.
2. Clique na guia *Quarentena*.



3. Clique em *Detalhes sobre riscos*. Serão exibidas estas informações sobre cada arquivo infectado:
 - Nome
 - Categoria de risco
 - Nível de risco
 - Data de adição
 - Idade (dias)

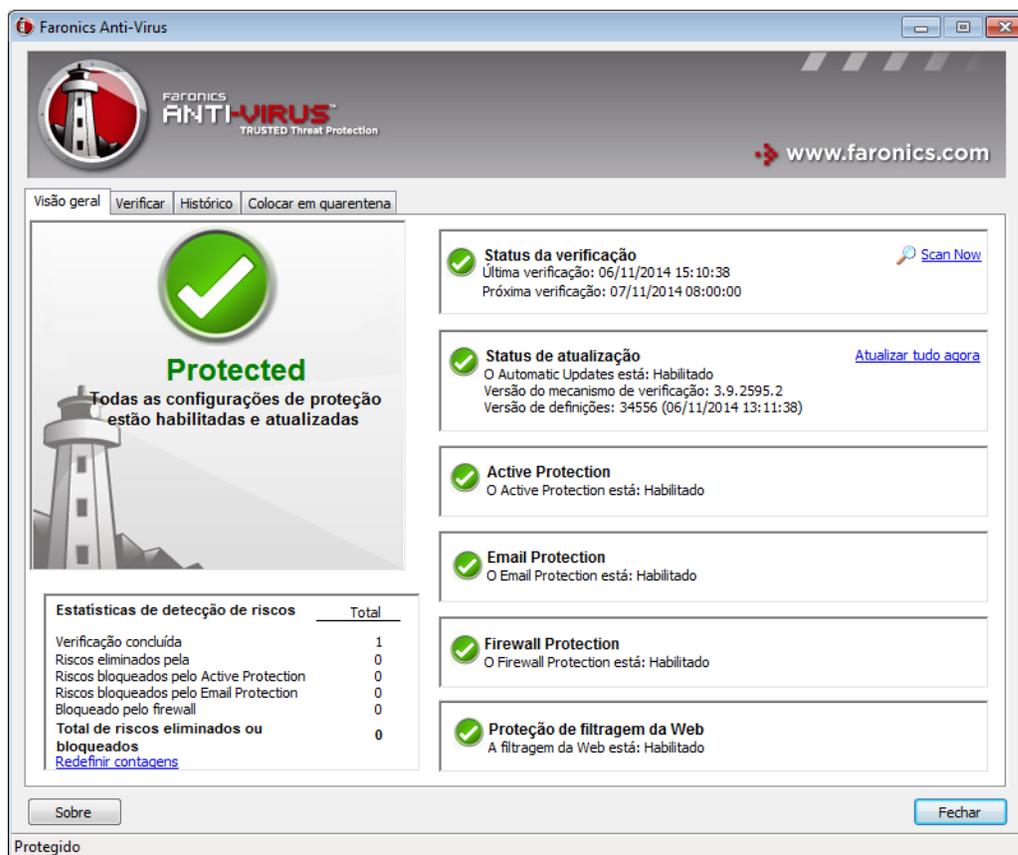


- Colocado em quarentena por
- 4. Marque as ações a seguir.
- *Detalhes*: selecione um arquivo infectado e clique em *Detalhes* para ver seus detalhes. A ação recomendada também é exibida.

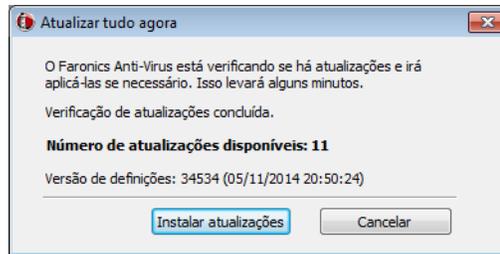
Atualizando definições do Anti-Virus na estação de trabalho

Siga as etapas abaixo para atualizar definições do Anti-Virus em uma estação.

1. Vá para *Iniciar* > *Programas* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Ou clique duas vezes no ícone do Faronics Anti-Virus na bandeja do sistema.



2. No painel *Status da atualização*, clique em *Atualizar tudo agora*. Aparecerá a caixa de diálogo *Atualizar tudo agora*.



3. Clique em *Instalar atualizações*. As definições de vírus serão atualizadas na estação.

Gerenciando o Anti-Virus na estação de trabalho através da bandeja do sistema

O Faronics Anti-Virus na estação pode ser gerenciado pelo menu disponível na bandeja do sistema.

Clique com o botão direito no ícone do Faronics Anti-Virus na bandeja do sistema. Estas opções estão disponíveis:

- Abrir Faronics Anti-Virus: inicia o programa na estação de trabalho.
- *Proteção ativa*
 - *Active Protection>Habilitar Active Protection*: ativa o Active Protection.
 - *Active Protection>Desabilitar Active Protection> [selecionar opção]*: define o período pelo qual o Active Protection ficará desativado. Selecione 5, 15 ou 30 minutos, 1 hora, Até reinicialização do computador ou Permanentemente. Essa opção só aparecerá se tiver sido marcada na política do Anti-Virus.
- *Scan Now>[selecionar opção]*: escolha Cancelar verificação, Pausar verificação, Retomar verificação, Verificação rápida ou Verificação profunda. Essa opção só aparecerá se tiver sido marcada na política do Anti-Virus.
- *Firewall Protection>Ativar* ou *Desativar*



Verificar atualizações do Anti-Virus

O Console do Deep Freeze permite verificar se existem novas versões disponíveis do Faronics Anti-Virus.

Vá para *Ajuda > Verificar atualizações*. Isso verifica se existe uma nova versão do Faronics Anti-Virus disponível.



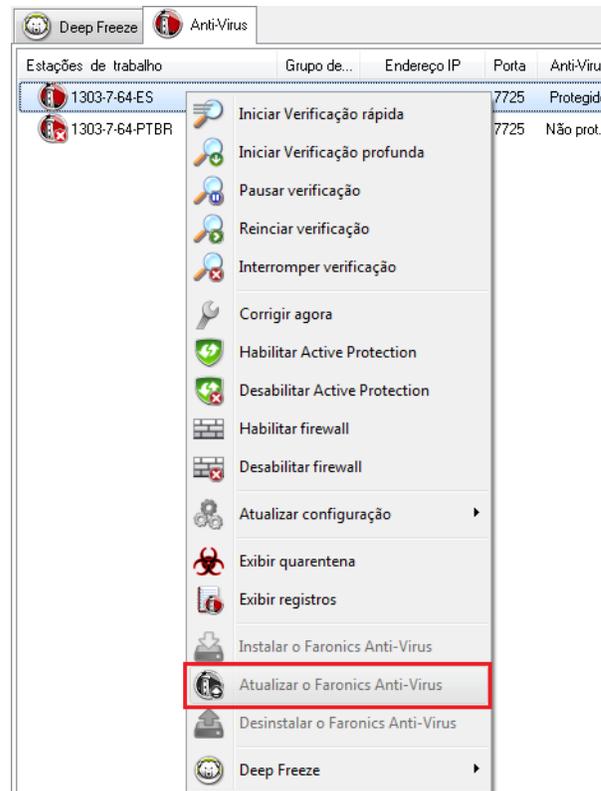
Se uma nova versão estiver disponível, clique em *Baixar a versão mais recente* para atualizar o Faronics Anti-Virus.



Atualizar o Faronics Anti-Virus

Se você tem verificado as atualizações e houver uma nova versão disponível, execute estas etapas para atualizar para uma nova versão na estação de trabalho:

1. Vá para a guia *Anti-Virus* no painel *Estações de trabalho*.
2. Selecione uma estação de trabalho (ou várias estações de trabalho) de
3. Clique com o botão direito do mouse e selecione *Atualizar o Faronics Anti-Virus*.



4. Clique em *OK* para confirmar a ação.

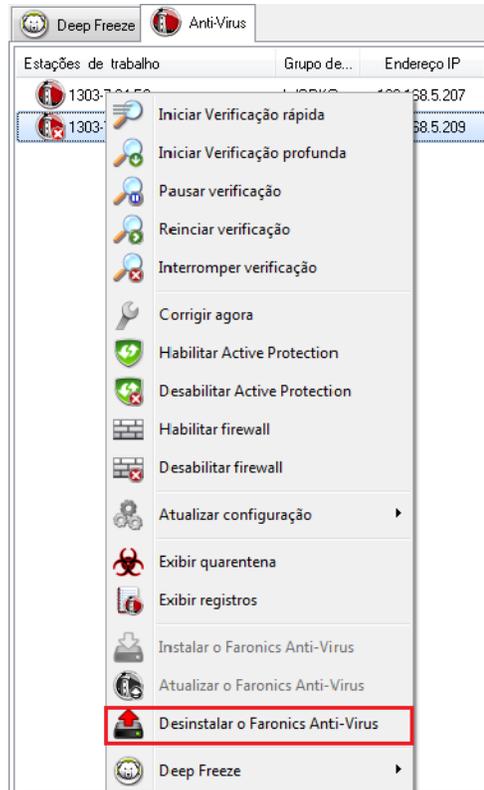
A estação de trabalho é reinicializada e o cliente Faronics Anti-Virus é atualizado nas estações de trabalho.



Desinstalar o Anti-Virus do Console corporativo

Execute estas etapas para desinstalar o Faronics Anti-Virus da estação de trabalho do Console corporativo:

1. Vá para a guia *Anti-Virus* no painel *Estações de trabalho*.
2. Selecione uma estação de trabalho (ou várias estações de trabalho) de
3. Clique com o botão direito do mouse e selecione *Desinstalar o Faronics Anti-Virus*.



4. Clique em *OK* para confirmar a ação.

A estação de trabalho é reinicializada e o cliente Faronics Anti-Virus é desinstalado das estações de trabalho.



Se o Cliente Anti-Virus for desinstalado da estação de trabalho, a Seed do Deep Freeze será deixada para trás.

A Seed do Deep Freeze não pode ser desinstalada quando o Cliente Anti-Virus está instalado na estação de trabalho.



Desativar o Faronics Anti-Virus no Console corporativo

O Anti-Virus pode ser desativado no Console do Deep Freeze caso não seja necessário ser usado.

Execute estas etapas para desativar o Faronics Anti-Virus do Console do Deep Freeze:

1. Vá para *Ferramentas > Licenciamento > Licença do Faronics Anti-Virus*.
2. Limpe a caixa de seleção *Gostaria de usar o Console do Deep Freeze para gerenciar o Faronics Anti-Virus*.



3. Clique em *Fechar*.
4. Reinicie o Console corporativo para que as configurações entrem em vigor.





Controle de linha de comando do Deep Freeze

Este capítulo descreve o uso dos comandos do Deep Freeze.

Tópicos

Controle de linha de comando do Deep Freeze (DFC.EXE)

Sintaxe da linha de comando do Deep Freeze

Sintaxe da linha de comando do Faronics Anti-Virus



Controle de linha de comando do Deep Freeze (DFC.EXE)

O controle da linha de comando do Deep Freeze (DFC) oferece aos administradores de rede maior flexibilidade no gerenciamento de computadores Deep Freeze. O DFC trabalha em combinação com ferramentas de gerenciamento corporativo de terceiros e/ou soluções de gerenciamento central. Essa combinação permite aos administradores atualizar computadores rapidamente e sob demanda.

É importante observar que o DFC não é um aplicativo autônomo. O DFC se integra perfeitamente com qualquer solução que possa executar arquivos de script, incluindo scripts de logon padrão executados apenas uma vez.

Os comandos DFC exigem uma senha com direitos da linha de comando. As OTPs não podem ser usadas.

Liste todos os comandos chamando o DFC sem parâmetros.

Os arquivos são copiados para (32 bits)

```
<WINDOWS>\system32\DFC.exe
```

Os arquivos são copiados para (64 bits)

```
<WINDOWS>\syswow64\DFC.exe
```

Valores de retorno do DFC

Na conclusão de qualquer comando DFC, o DFC retorna os seguintes valores:

Sintaxe	Descrição
0	SUCCESS ou booleano FALSE, para comandos que retornam um resultado booleano
1	Booleano TRUE
2 ERROR	O usuário não tem direitos de administrador
3 ERROR	Comando DFC não válido nesta instalação
4 ERROR	Comando inválido
5 - * ERROR	Erro interno ao executar comando



Sintaxe da linha de comando do Deep Freeze



O Deep Freeze tem um limite máximo de 63 caracteres para senha. Se uma senha maior for inserida, o comando não será executado com êxito.

Sintaxe	Descrição
<code>DFC password /BOOTTHAWED</code>	Reinicia o computador no estado Descongelado; só funciona em computadores Congelados.
<code>DFC password /THAWNEXTBOOT</code>	Define o computador para ser reiniciado Descongelado na próxima vez em que for reiniciado; só funciona em computadores Congelados e não força computadores a reiniciar.
<code>DFC password /BOOTFROZEN</code>	Reinicia o computador no estado Congelado; só funciona em computadores Descongelados.
<code>DFC password /FREEZENEXTBOOT</code>	Define o computador para ser reiniciado Congelado na próxima vez em que for reiniciado; só funciona em computadores Descongelados e não força computadores a reiniciar.
<code>DFC get /ISFROZEN</code>	Consulta o computador para saber se está Congelado. Retorna nível de erro 0 se Descongelado. Retorna 1 se Congelado.
<code>DFC password /CFG=[caminho] depfrz.rdx</code>	Substitui as informações de configuração do Deep Freeze. Funciona em computadores Descongelados ou Congelados. As alterações de senhas entram em vigor imediatamente. Outras alterações exigem reinicialização.
<code>DFC get /version</code>	Exibe o número da versão do Deep Freeze.
<code>DFC get /CLONE</code>	Define o sinalizador clone para fins de processamento de imagem.
<code>DFC password /UPDATE=[caminho para o arquivo instalador]</code>	Configura o computador para reiniciar no estado Descongelado e instala uma atualização do Deep Freeze
<code>DFC password /LOCK</code>	Desativa o teclado e o mouse no computador. Funciona em computador Congelado ou Descongelado e não exige uma reinicialização.
<code>DFC password /UNLOCK</code>	Ativa o teclado e o mouse no computador. Funciona em computador Congelado ou Descongelado e não exige uma reinicialização.



Sintaxe	Descrição
DFC password /THAWLOCKNEXTBOOT	Configura o computador para reiniciar em um estado Descongelado com o teclado e o mouse desativados; somente funciona em computadores Congelados
DFC password /BOOTTHAWEDNOINPUT	Reinicia o computador em um estado Descongelado com o teclado e o mouse desativados; somente funciona em computadores Congelados
DFC get /LICENSESTATUS	Exibe o status da licença e a data de expiração da licença (se houver). Os diferentes tipos de licença possíveis e os códigos de retorno associados são: 111: Não licenciado — o Deep Freeze não está licenciado e irá operar no modo <i>Avaliação</i> por 30 dias a contar da instalação. 112: Avaliação — licenciado para avaliação com uma data de expiração fixa. 113: Licenciado — licenciado sem data de expiração. 114: Expirado — o período de avaliação já expirou.
DFC get /LICENSETYPE	Exibe o status da licença e a data de expiração da licença (se houver). Os diferentes tipos de licença possíveis e os códigos de retorno associados são: 111: Nenhuma (não licenciado) — o Deep Freeze não está licenciado e irá operar no modo <i>Avaliação</i> por 30 dias a contar da instalação. 112: Avaliação — licenciado para avaliação com uma data de expiração fixa. 113: Padrão (Licenciado) — licenciado sem data de expiração. 114: Não destinado à revenda — Licenciado sem data de expiração.
DFC password /LICENSE=licensekey	Altera a chave de licença. <i>senha</i> é a senha do administrador do Deep Freeze. <i>licensekey</i> é a chave da licença do Deep Freeze. Se existir um erro, os códigos de erro a seguir serão exibidos: 101: A chave de licença não é válida 102: A chave da licença fornecida já expirou.



Sintaxe	Descrição
<code>DFC password /WU [/UNLOCK] [/NOMSG /NOMESSAGE] [/THAW]</code>	<p>As atualizações do Windows serão baixadas e instaladas na estação de trabalho.</p> <p><code>[/UNLOCK]</code> parâmetro opcional para ativar o teclado e ou mouse durante a atualização do Windows.</p> <p><code>[/NOMSG /NOMESSAGE]</code> parâmetro opcional para suprimir todas as mensagens informativas/avisos do Deep Freeze durante a atualização do Windows.</p> <p><code>[/THAW]</code> parâmetro opcional para retornar a máquina ao estado Descongelada após conclusão da atualização do Windows.</p>
<code>DFC password /ENDTASK</code>	<p>Encerra a Tarefa de estação de trabalho em andamento e reinicia no estado Congelado. Tarefa de arquivo de lote e Tarefa de período Descongelado são encerrados imediatamente. A tarefa Windows Update é concluída</p>



Sintaxe da linha de comando do Faronics Anti-Virus

Conclua estas etapas para executar os comandos do Faronics Anti-Virus:

1. Na estação de trabalho, vá para <Diretório do Sistema>:\Arquivos de Programas\Faronics\Faronics Anti-Virus Enterprise via prompt de comando.
2. Digite AVECLI/[comando]

Estes comandos estão disponíveis:

Sintaxe	Descrição
definitionversion	Mostra a versão da definição de vírus.
scanengineversion	Mostra a versão do mecanismo de verificação.
updatedefs	Atualiza e aplica definições de vírus.
fixnow	Baixa as definições de vírus mais recentes. Habilita o Active Protection e o Email Protection. Realiza uma verificação profunda padrão.
scanquick	Inicia uma verificação rápida.
scandeeep	Inicia uma verificação profunda.
enableap	Ativa o Active Protection.
applydefs [caminho para definições]	Aplica o arquivo de definições salvo em um local.
fixnow /quick	Executa uma <i>verificação rápida</i> , se aplicável.
resetpolicy	Redefine a política do Anti-Virus para a política padrão.
setlicense [chave]	Aplica uma chave de licença.

Sintaxe:

AVECLI/definitionversion



Apêndice A Portas e protocolos

A chave para configurar a arquitetura do Deep Freeze é saber quais portas usar. O fator importante é saber quais portas estão em uso na rede e usar portas que não estarão em conflito com aquelas. A porta padrão, 7725 foi registrada oficialmente para o Deep Freeze.

O três componentes a seguir fazem parte da arquitetura do Deep Freeze:

- Cliente (com a seed instalada)
- Console remoto (serviço local ativado)
- Console (conectado ao Console remoto)

Enquanto os clientes e a conexão Console remoto usarem a mesma porta não deve haver quaisquer conflitos de porta entre os diferentes componentes:



As portas também podem ser usadas para dividir clientes. Se o serviço local estiver configurado para ser executado por três portas (7725, 7724 e 7723), os Consoles corporativos podem se conectar a três portas diferentes para ver um conjunto diferente de clientes em cada porta.

No diagrama a seguir, o(s) cliente(s) usam os protocolos TCP e UDP para se comunicar com o Console remoto. Os Consoles que se conectam ao Console remoto usam somente o protocolo TCP para se comunicar com o Console remoto. É importante lembrar as portas e protocolos que estão sendo usados para evitar que firewalls, comutadores ou roteadores os bloqueiem.





Apêndice B Exemplos de rede

Os exemplos a seguir mostram diferentes cenários envolvendo o serviço local ou o Console remoto.

- Exemplo 1 - Sub-rede única
- Exemplo 2 - Várias sub-redes, um serviço local
- Exemplo 3 - Várias portas, Console acessado remotamente
- Exemplo 4 - Múltiplas sub-redes, múltiplos serviços locais

Cada exemplo explica como diferentes componentes do Deep Freeze interagem em ambientes de rede diferentes.



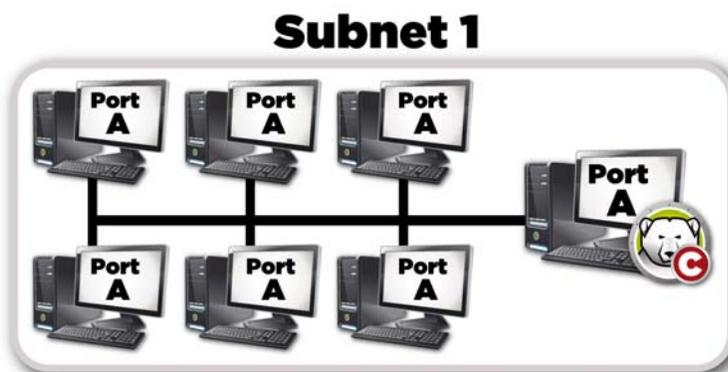
Nos exemplos a seguir, as máquinas cliente têm a instalação da estação de trabalho ou a Seed da estação de trabalho do Deep Freeze instalada. Ambas as instalações contêm os componentes de comunicação que se comunicam com o Console/Console remoto. A diferença entre a instalação da estação de trabalho e a Seed da estação de trabalho é que a instalação da estação de trabalho realmente instala o Deep Freeze enquanto a Seed só tem os componentes de comunicação.



Exemplo1 - Sub-rede única

Neste ambiente, todas as máquinas cliente estão contidas na mesma sub-rede assim como a máquina Console. Este ambiente não exige um Console remoto controlado, embora um possa ser usado. Neste exemplo, o Console remoto não é usado. Esse é o ambiente de rede mais simples. Também é o mais fácil de configurar.

Os diagramas a seguir mostram a topologia de rede:



As máquinas clientes, representadas pelos ícones de computador, estão localizadas na mesma sub-rede da máquina do Console corporativo do Deep Freeze representado pelo ícone do Console do Deep Freeze.

Neste cenário, os clientes estão usando a porta A enquanto o Console foi configurado como uma conexão de serviço local para a mesma porta. Essa porta é configurada na guia *Opções avançadas*, antes de criar o arquivo de Instalação da estação de trabalho ou a Seed da estação de trabalho.



Deep Freeze Administrador de configuração

Arquivo Ajuda

Novo Abrir Salvar Salvar como Ajuda Criar

Senhas Unidades Tarefas da estação de trabalho Windows Update Arquivo de lote Opções avançadas

Opções de rede

LAN LAN/WAN

Usar porta padrão

IP do console

Nome do console

Opções avançadas

Desativar opções de linha de comando

Ativar políticas locais do Deep Freeze

Permitir que usuário altere o relógio

Gerenciar senha do canal seguro

Reiniciar no logoff

Proteger Registro mestre de inicialização (MBR)

Atrase o Congelamento e reinicie para concluir as atualizações do Windows

Modo Furtivo

Mostrar ícone Congelado na bandeja do sistema

Mostrar ícone Congelado na bandeja do sistema

Licença

Chave de licença:

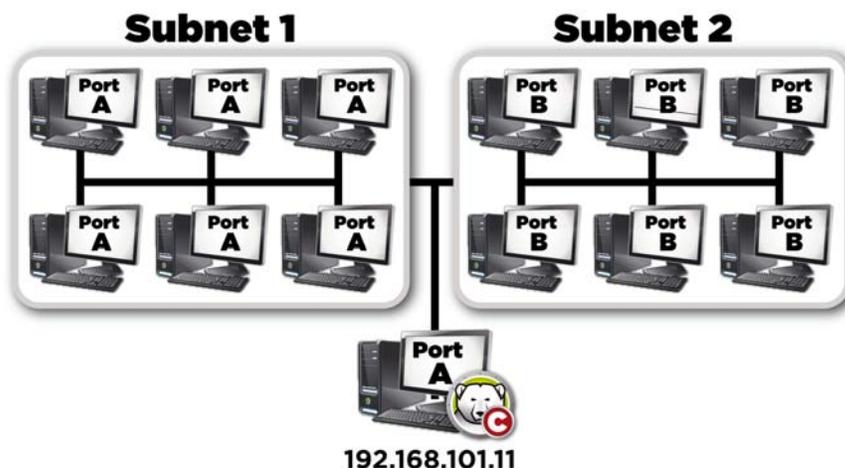
Tipo de chave de licença:

Data de expiração:



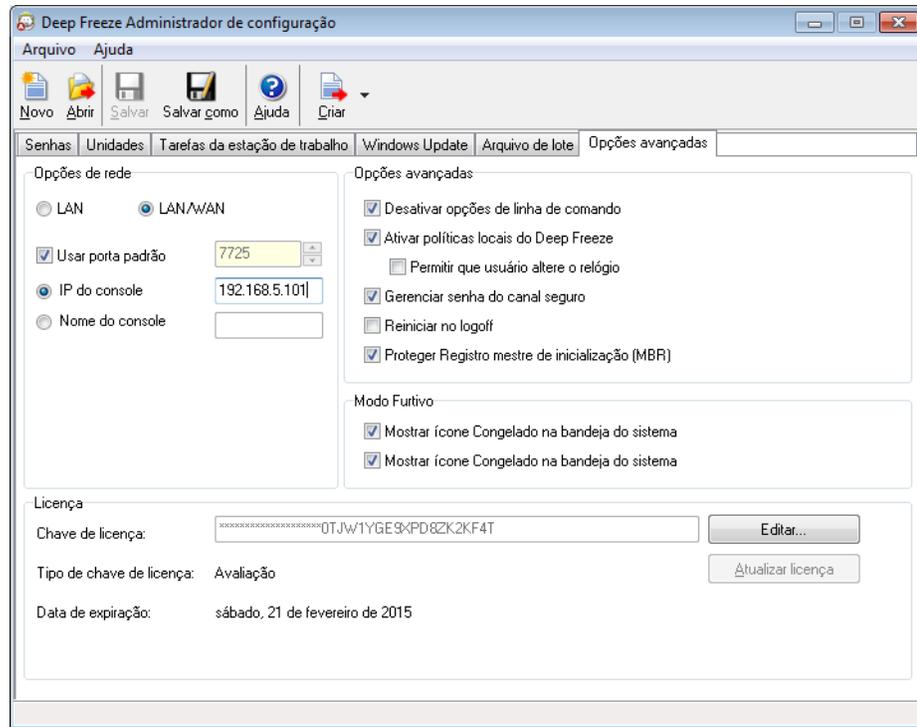
Exemplo 2 - Várias sub-redes, um serviço local

Neste ambiente, os clientes estão localizados em mais de uma sub-rede. Existe apenas um Console sendo usado. Este ambiente não exige um Console remoto, embora um possa ser usado. Os diagramas a seguir mostram a topologia de rede:



Neste cenário (similar ao [Exemplo 1 - Sub-rede única](#)) ambos os clientes e a conexão hospedada pelo Console estão usando a mesma porta. Essa porta é configurada no Administrador de configuração do Deep Freeze na guia *Opções avançadas*, antes de criar o arquivo de Instalação da estação de trabalho ou a Seed da estação de trabalho.

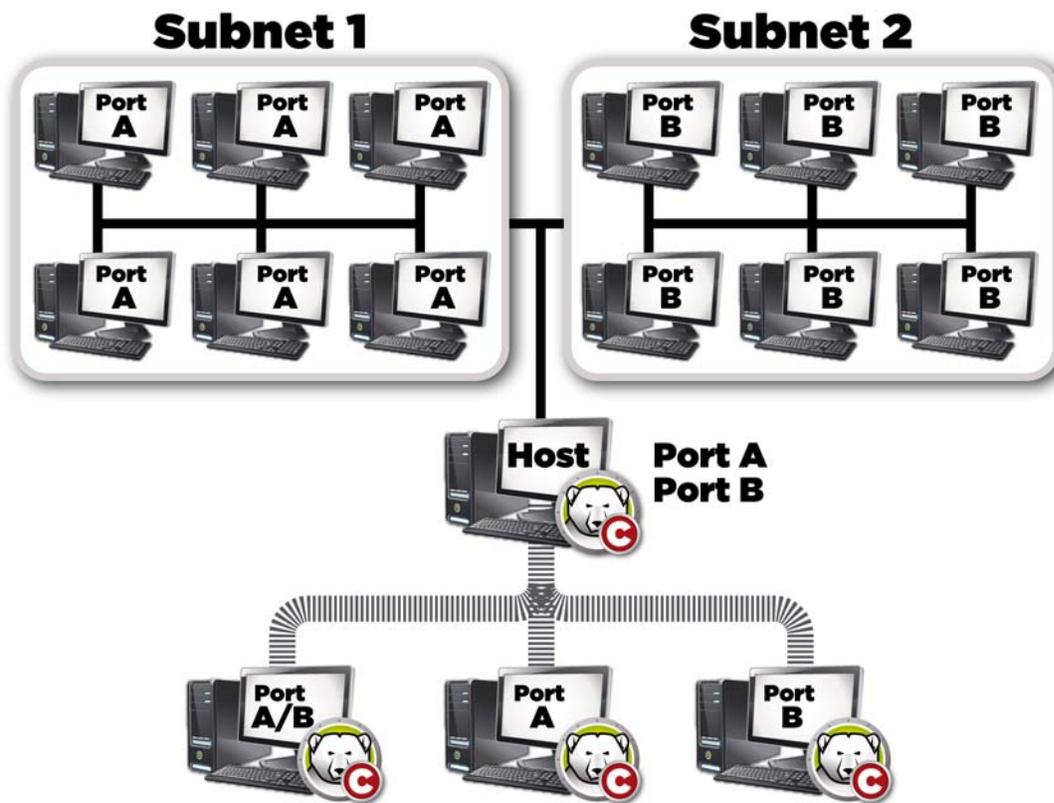
Para que os clientes sejam vistos, eles precisam estar configurados para usar uma conexão LAN/WAN. Quando a opção LAN/WAN é selecionada, um campo *IP do console* é exibido. Especifique o IP da máquina que executará o Console corporativo. Um exemplo destas configurações é mostrado na guia *Opções avançadas* a seguir:





Exemplo 3 - Várias portas, Console acessado remotamente

Neste ambiente os clientes estão novamente localizados em várias portas. Neste caso, mais de um Console está sendo usado. Vários consoles são acessados usando-se um serviço local cujo administrador (host) liberou as informações de conexão. Os diagramas a seguir mostram a topologia de rede:



Neste cenário, o host configurou uma conexão usando o serviço local. Observando no diagrama acima, três outros Consoles conectam-se ao host de maneira a ver os clientes de acordo com suas portas. Os consoles não têm que fazer parte de sub-redes individuais, contanto que eles possam ver o host.

Mais especificamente, o Console conectado através da porta A/B pode ver o Console host, assim como cada computador atribuído às portas A e B. Os outros Consoles conectados através da porta B podem ver o host e somente os computadores atribuídos à porta B.



Exemplo 4 - Múltiplas sub-redes, múltiplos serviços locais

Neste exemplo, existem dois locais separados.

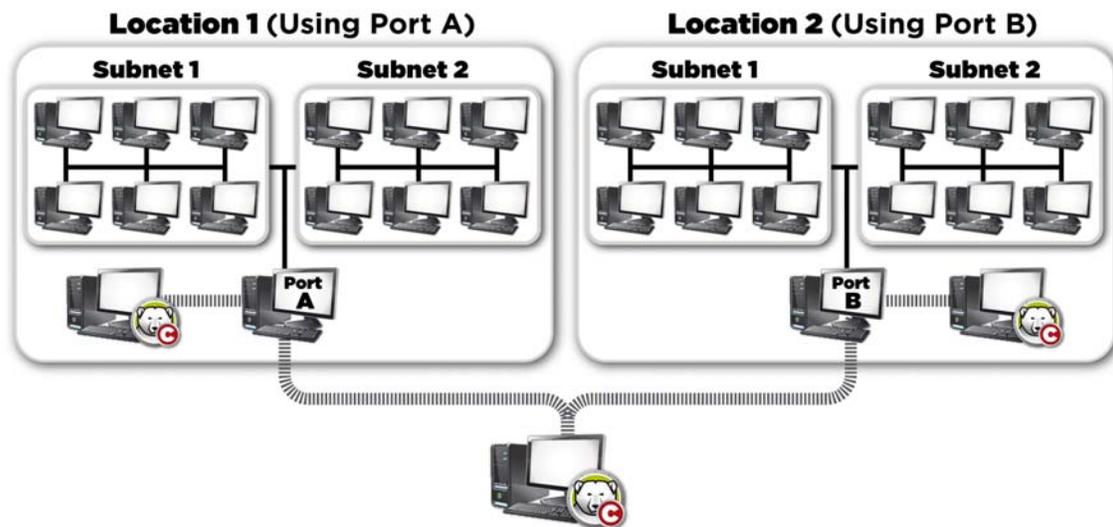
A seguir encontra-se uma lista de suposições que são feitas em relação a esse exemplo em particular:

- os locais estão afastados e têm apenas uma ligação mínima entre cada um deles
- existe um administrador de rede para cada local, que é responsável por cuidar do Deep Freeze naquele local
- ambos os locais necessitam ser administrados de um terceiro local

Neste exemplo, o Console remoto está configurado em cada local e o serviço local é usado:

- Local 1 (um laboratório de computadores no campus) usa a porta A para se comunicar com os clientes e as conexões hospedadas pelo Console. Os computadores da biblioteca escolar usam a porta B. O Console no departamento de suporte técnico usa as conexões hospedadas por ambos os consoles do laboratório e da biblioteca.
- Qualquer console que não esteja em comunicação direta com um computador deve ter o serviço local desligado.

Os diagramas a seguir mostram a topologia de rede:



O benefício desta configuração é que ela permite que todos os pacotes enviados dos clientes no Local 1 estejam contidos em aquele local. Quanto menor a distância que um pacote tem de viajar, menor a chance de falha do pacote.

O administrador no laboratório pode se conectar ao serviço local no mesmo local 1, mas não pode se conectar ao serviço local na biblioteca. O motivo disso é que o administrador do laboratório não conhece a senha para acessar o serviço local da biblioteca. O mesmo acontece com o administrador na biblioteca. Se o suporte técnico conhece a senha para ambos os locais de serviço (laboratório e biblioteca), o serviço local em ambos os locais pode ser conectado, de maneira a administrar todos os clientes.





Solução de problemas para uma conexão de console remoto

Sem clientes no console

A seguir, alguns motivos comuns porque clientes falham ao aparecer no console.

1. O console e os clientes não contêm as configurações de rede corretas.

Se o Console está definido para ser executado em uma porta e os clientes estão usando outra, eles não serão capazes de ver um ao outro. Além disso, se os computadores estiverem configurados para LAN/WAN, o IP deve ser igual ao IP da máquina onde o Console está sendo executado.

A configuração padrão de LAN funciona, contanto que todas as máquinas que executam o computador e o Console existam na mesma sub-rede. Caso contrário, se uma VLAN estiver sendo executada ou se existirem várias sub-redes onde os clientes existem, a instalação do computador deverá ser configurada para ser executada nas configurações da LAN/WAN.

2. Alguma coisa na rede está bloqueando a porta usada entre o Console e os clientes.

Verifique a existência de uma conexão usando um ping. Os clientes não estão conseguindo enviar pacotes para o Console/Console remoto porque não parece existir uma rota para o host. A tentativa de fazer ping no IP do Console/Console remoto não parece funcionar. Para resolver este problema, certifique-se que as duas máquinas podem se conectar uma à outra.

Se um servidor, roteador ou comutador da rede não estiver permitindo a transmissão pela porta, os clientes não serão vistos. Por padrão, 7725 é a porta que sendo usada.

3. As estações de trabalho foram criadas em um Customization Code diferente do Console.

Quando o Administrador de configuração do Deep Freeze é executado pela primeira vez, uma solicitação para um Customization Code é exibida. Esse código é muito importante porque ele criptografa o software. Isso significa que qualquer estação de trabalho criada é criptografada com este Customization Code. Se o Console tiver sido criado usando outro administrador que foi instalado com um Customization Code diferente, ele não poderá ver as estações de trabalho criadas sob o código original. As estações de trabalho devem ser criadas sob um Administrador de configuração instalado usando exatamente o mesmo Customization Code.



A porta está em Erro de uso ao iniciar o Console

Ao tentar iniciar o Console, a mensagem de erro *Não foi possível iniciar o Console: Porta em uso* é exibida. Existem vários motivos pelos quais essa mensagem de erro pode ser exibida:

1. Existe uma Instalação de estação de trabalho do Deep Freeze/Seed de estação de trabalho instalada na mesma porta que o Console ou no mesmo computador.

É possível que o Deep Freeze tenha sido instalado no modo furtivo (o ícone não aparece na bandeja do sistema). A seed não mostra um ícone. O melhor teste é executar um arquivo de instalação da estação de trabalho no computador. Se a opção de desinstalação for exibida, o arquivo de instalação da estação de trabalho ou a Seed da estação de trabalho está instalado e pode ser desinstalado. Se a opção desinstalar não aparecer, o arquivo de instalação da estação de trabalho ou a Seed da estação de trabalho não está instalado.

A solução mais simples seria primeiro, desligar o serviço local e, depois, conectá-lo a um Console que pode ser acessado remotamente.

2. Outro programa ou serviço está usando a porta nesta máquina.

Isso pode envolver a execução de um farejador de porta na máquina em questão para ver quais portas estão abertas. Existem várias ferramentas disponíveis na Web para realizar essa ação. O aplicativo *netstat.exe* encontrado no Windows também deve mostrar se a porta que o Deep Freeze está usando já está em uso.

3. O cabo de rede está desconectado.

Essa mensagem pode ocorrer se não houver uma conexão de rede na máquina.

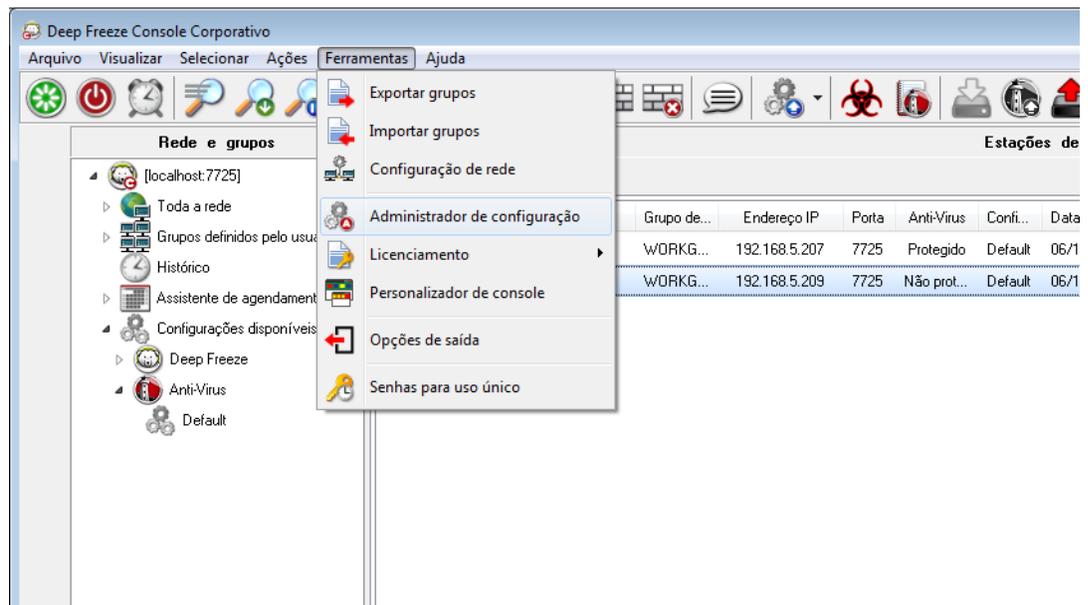


Criando um Console corporativo personalizado do Deep Freeze

O Console corporativo do Deep Freeze inclui a capacidade de criar um novo Console corporativo com habilidades limitadas. Um console personalizado e limitado pode ser distribuído na sua empresa para permitir a determinados usuários realizar tarefas desejadas, enquanto garante que eles não tenham acesso aos recursos completos do Console corporativo.

Neste exemplo, vamos criar um console limitado adequado para distribuição a um professor ou a um instrutor do laboratório de computação. Neste cenário, desejamos que o professor seja capaz de reiniciar máquinas, travar o teclado e o mouse sob demanda e enviar mensagens aos alunos. Porém, não desejamos que o professor seja capaz de reinicializar as máquinas no estado Descongelado, desinstalar o Deep Freeze ou realizar outras tarefas exclusivas de TI.

O Personalizador de console pode ser iniciado em *Ferramentas > Personalizador de console*.



Deixaremos as *Funções do console > Ativação* selecionadas. Isso assegura que se o novo Console for movido para um computador diferente, a Senha de uso único precisará ser inserida no computador para onde o novo Console foi movido. Se esta precaução de segurança não for uma preocupação no seu ambiente, não selecione esta opção.

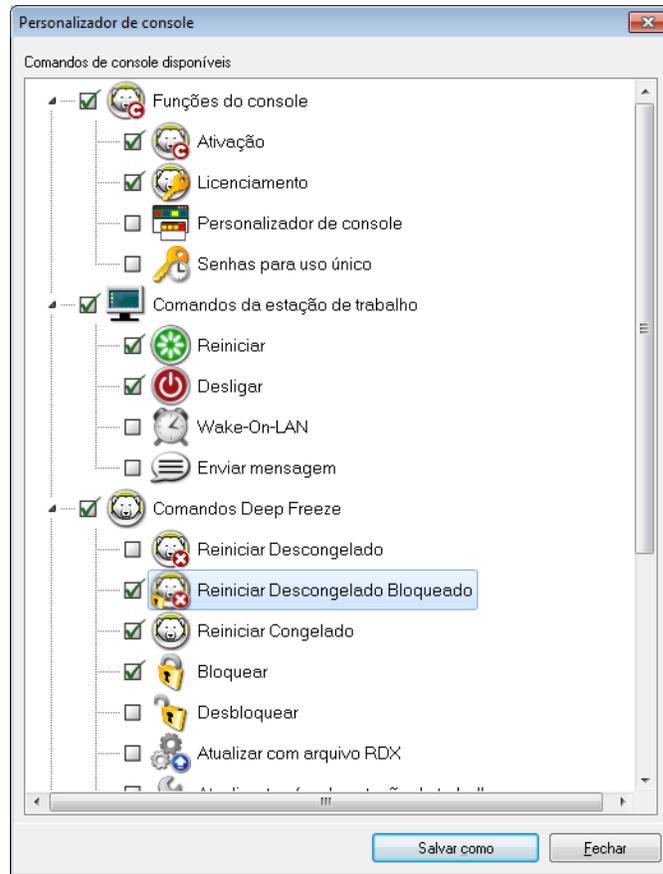
Funções do console > Senha de uso único não está selecionada porque não desejamos que o professor seja capaz de reinicializar o computador no modo Descongelado em nenhuma circunstância. Se o professor reinicializar o computador no modo Descongelado, os alunos podem instalar software desnecessário que será mantido mesmo após uma reinicialização.

Deixaremos todas as opções em *Comandos da estação de trabalho* selecionadas porque desejamos que o professor seja capaz de enviar mensagens aos alunos e de desligar, reiniciar e ativar computadores quando necessário.

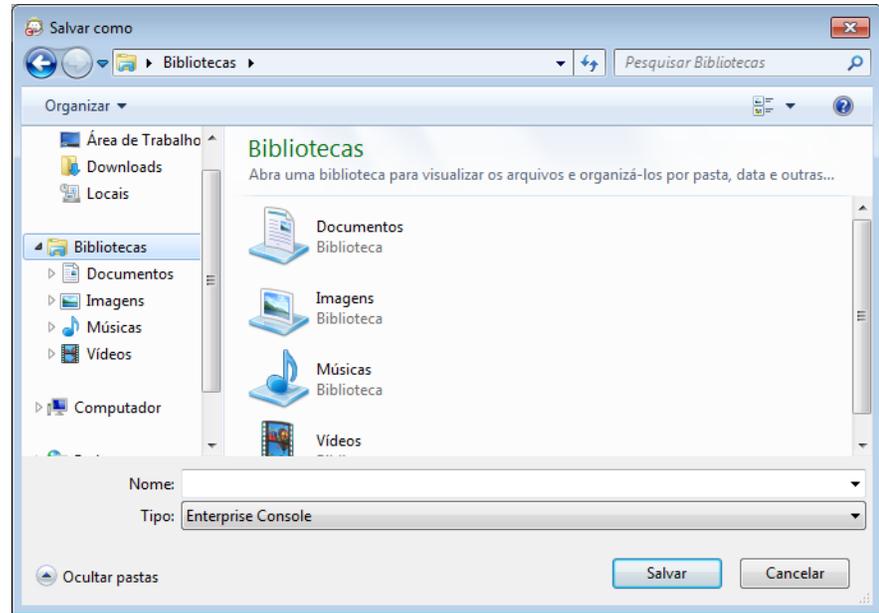


Deixaremos somente três opções nos comandos do Deep Freeze selecionados: *Desbloquear*, *Bloquear* e *Reinicializar no estado Congelado*. Isso irá permitir ao professor bloquear (e desbloquear) o teclado e o mouse nos computadores dos alunos quando necessário, assim como reinicializar computadores *Congelados* (apenas no caso de um computador alguma vez ser deixado *Descongelado* acidentalmente pela equipe de TI). Deixando todas as outras opções desmarcadas iremos garantir que um professor não é capaz de modificar um computador de forma permanente.

Finalmente, desmarcaremos todos os *Comandos de instalação/desinstalação na estação de trabalho* e todos os *comandos do Assistente de agendamento* porque não desejamos que nosso professor use quaisquer uma dessas opções.



Uma vez que todas as opções tenham sido selecionadas, clique em *Salvar como* para salvar um novo Console corporativo. Uma caixa de diálogo padrão *Salvar como* é exibida:



Salve o novo Console corporativo limitado e distribua-o para os usuários necessários.





Apêndice E Arquivos de ação do Deep Freeze - Exemplo RDC

Arquivos de ação do Deep Freeze

Um arquivo de ação do Deep Freeze é um arquivo XML que permite aos administradores definir funcionalidade adicional no Console corporativo do Deep Freeze. Um arquivo de ação define um método para chamar um arquivo em lotes externo e passar algumas informações (por exemplo, endereço IP da máquina, nome do computador) para o arquivo em lote ou script.

Arquivos de ação simplesmente chamam um programa externo ou script. Portanto, qualquer linguagem script que possa ser chamada a partir da linha de comando pode ser usada.

Exemplo de arquivo de ação

A estrutura do arquivo de ação do Deep Freeze que será usada é mostrada abaixo. O *DFEntConsoleCustomActions.xml* está disponível em *C:\Arquivos de programa\Faronics\Deep Freeze 7 Enterprise*. O arquivo pode ser editado para adicionar ações adicionais como a que é explicada a seguir:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Deep Freeze Default Custom Action file-->
<CUSTOMDEFINEDACTIONS>
  <ACTION1>
    <CAPTION>
      <ENGLISH>Control with RDC</ENGLISH>
      <GERMAN>Control with RDC German</GERMAN>
      <JAPANESE>Control with RDC Japanese</JAPANESE>
      <SPANISH>Control with RDC Spanish</SPANISH>
      <FRENCH>Control with RDC French</FRENCH>
      <CHINESE>Control with RDC Chinese</CHINESE>
    </CAPTION>
    <FILEMENU>Y</FILEMENU>
    <POPUPMENU>Y</POPUPMENU>
    <SILENT>Y</SILENT>
    <SUBITEMS/>
    <PARAMS/>
    <SYNC/>
    <LOG/>
    <EXECUTE>C:\Windows\system32\mstsc.exe /v:%%WKSNAME%% /f</EXECUTE>
    <WORKDIR>C:\Windows\system32\</WORKDIR>
```

No exemplo acima, o arquivo de ação personalizada contém o comando para executar a Área de Trabalho Remota no computador do Console e conectar o computador remoto especificado no parâmetro %%WKSNAME%%.

O arquivo *DFEntConsoleCustomActions.xml* contém 3 amostras:

- Controlar com RDC
- Execução remota
- Enviar por push e instalar arquivo MSI



Para obter mais informações sobre o uso dos exemplos acima, consulte a seção [Configurar ações personalizadas](#). Você pode editar o arquivo *DFEntConsoleCustomActions.xml* de acordo com as suas necessidades.



Estrutura do arquivo de ação do Deep Freeze

O seguinte esquema XML descreve as ações personalizadas definidas disponíveis para o usuário. Vários arquivos XML podem ser salvos com base no número de comandos necessários. Cada arquivo deve ser salvo para pasta Console e apenas o atributo somente leitura não deve ser selecionado.

Quaisquer alterações feitas devem ser acompanhadas de uma reinicialização do Console do Deep Freeze para entrar em vigor.

Parâmetro	Uso
<code><?xml version="1.0" encoding="UTF-8"?></code>	
<code><CUSTOMDEFINEDACTIONS></code>	
<code><CAPTION></code>	Texto que aparece no menu ou no submenu do arquivo
<code><ENGLISH>Caption</ENGLISH></code>	Texto em diversos idiomas
<code><GERMAN>Caption</GERMAN></code>	Texto em diversos idiomas
<code><JAPANESE>Caption</JAPANESE></code>	Texto em diversos idiomas
<code><SPANISH>Caption</SPANISH></code>	Texto em diversos idiomas
<code><FRENCH>Caption</FRENCH></code>	Texto em diversos idiomas
<code><CHINESE>Caption</CHINESE></code>	Texto em diversos idiomas
<code><FILEMENU>y</FILEMENU></code>	Define se esta ação estará no menu Arquivo
<code><POPUPMENU>y</POPUPMENU></code>	Define se esta ação estará no menu pop-up do botão direito do mouse
<code><SILENT>y</SILENT></code>	Define se o usuário será solicitado a confirmar a mensagem
<code><SUBITEMS></code>	Em subitens, o item que é um filho desse item pode ser definido
<code></SUBITEMS></code>	Se os subitens estiverem definidos então a ação para esses itens será ignorada
<code><SYNC>y</SYNC></code>	Especifica se o comando será executado de forma síncrona ou assíncrona
<code><PARAMS></code>	Escolher esta ação solicita aos usuários inserir parâmetros personalizados
<code><PASSWORD></code>	Nome no parâmetro
<code><VAR>%PARAM1%</VAR></code>	Nome da variável que será usada em EXECUTE
<code><ENGLISH>USERNAME Param (ENGLISH) </ENGLISH></code>	Texto em diversos idiomas



Parâmetro	Uso
<GERMAN>USERNAME Param (GERMAN) </GERMAN>	Texto em diversos idiomas
<JAPANESE>USERNAME Param (JAPANESE) </JAPANESE>	Texto em diversos idiomas
<SPANISH>USERNAME Param (SPANISH) </SPANISH>	Texto em diversos idiomas
<FRENCH>USERNAME Param (FRENCH) </FRENCH>	Texto em diversos idiomas
<CHINESE>USERNAME Param (CHINESE) </CHINESE>	Texto em diversos idiomas
</CAPTION>	
</USERNAME>	
</PARAMS>	
<LOG>	Define o comportamento do arquivo de log
<APPEND>y</APPEND>	Define se o arquivo de log será anexado ou se será criado um novo
<FILENAME>c:\alcom mand.log</FILENAME>	Define o nome do arquivo
<EXECUTE>c:\windows\vpn.exe %%IP%% %USERNAME% %PASSWORD% %%WKSNAME%%</EXECUTE>	Define o comando que será executado. Aqui, parâmetros e/ou itens do console podem ser usados
<WORKDIR>c:\windows</WORKDIR>	Define o diretório de trabalho



Parâmetros do console

Os parâmetros de console a seguir podem ser passados para o script ou aplicativo executado através do Console corporativo:

Parâmetro	Uso
%%WKSNAME%%	Nome da estação de trabalho
%%DOMAIN%%	Domínio da estação de trabalho
%%IP%%	IP da estação de trabalho
%%PORT%%	Porta da estação de trabalho
%%STATUS%%	Status da estação de trabalho
%%CFGDATETIME%%	Data/hora da configuração da estação de trabalho
%%MAC%%	Endereço MAC da estação de trabalho
%%DFVERSION%%	Versão do Deep Freeze da estação de trabalho.

