Norman Virus Control para Estações

Versão 5.81

Guia de Referência

Garantia Limitada

Norman guarantees that the enclosed diskette/CD-ROM and documentation do not have production flaws. If you report a flaw within 30 days of purchase, Norman will replace the defective diskette/CD-ROM and/or documentation at no charge. Proof of purchase must be enclosed with any claim.

This warranty is limited to replacement of the product. Norman is not liable for any other form of loss or damage arising from use of the software or documentation or from errors or deficiencies therein, including but not limited to loss of earnings.

With regard to defects or flaws in the diskette/CD-ROM or documentation, or this licensing agreement, this warranty supersedes any other warranties, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

In particular, and without the limitations imposed by the licensing agreement with regard to any special use or purpose, Norman will in no event be liable for loss of profits or other commercial damage including but not limited to incidental or consequential damages.

This warranty expires 30 days after purchase.

The information in this document as well as the functionality of the software is subject to change without notice. The software may be used in accordance with the terms of the license agreement. The purchaser may make one copy of the software for backup purposes. No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the explicit written permission of Norman.

The Norman logo is a registered trademark of Norman ASA.

Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

NVC documentation and software are

Last revised 9 June 2005.

Escritórios da Norman

Norman Data Defense Systems AS
Blangstedgårdsvej 1, DK-Odense SØ, **Denmark**
Tel. +45 6311 0508 Fax: +45 6590 5102
E-mail: normandk@normandk.com Web: http://www.norman.com/dk

Norman Ibas OY
Läkkisepäntie 11, 00620 Helsinki, **Finland**.
Tel: +358 9 2727 210 Fax: +358 92727 2121
E-mail: norman@norman-ibas.fi Web: http://www.norman.fi

Norman Data Defense Systems GmbH
Gladbecker Str. 3, D-40472 Düsseldorf, **Germany**.
Tel: +49 211 586 99-0 Fax: +49 211 586 99-150
E-mail: info@norman.de Web: http://www.norman.de

Norman/SHARK BV
Postbus 159, 2130 AD, Hoofddorp, **The Netherlands**.
Tel: +31 23 789 02 22 Fax: +31 23 561 3165
E-mail: support@norman.nl Web: http://www.norman.nl

Norman ASA
Mailing address: P.O. Box 43, N-1324, Lysaker, **Norway**.
Physical address: Strandveien 37, Lysaker, N-1324 Norway.
Tel: +47 67 10 97 00 Fax: +47 67 58 99 40
E-mail: norman@norman.no Web: http://www.norman.no

Norman Data Defense Systems AB
S.t Persgatan 19, SE-601 86 Norrköping, **Sweden**
Tel. +46 11 230 330 Fax: +4611 230 349
E-mail: support.se@norman.no Web: http://www.norman.com/se

Norman Data Defense Systems AG
Postfach CH-4015, Basel, **Switzerland**.
Tel: +41 61 487 2500 Fax: +41 61 487 2501
E-mail: norman@norman.ch Web: http://www.norman.ch

Norman Data Defense Systems (UK) Ltd
Unit 15, Linford Forum, Rockingham Drive, Linford Wood,
Milton Keynes, MK14 6LYPO, **United Kingdom**.
Tel: +44 08707 448044 Fax: +44 08717 176999
E-mail: norman@normanuk.com Web: http://www.normanuk.com

Norman Data Defense Systems Inc.
9302 Lee Highway, Suite 950A, Fairfax, VA 22031, **USA**
Tel: +1 703 267 6109, Fax: +1 703 934 6367
E-mail: norman@norman.com Web: http://www.norman.com/us

Treinamento e Suorte Técnico

Para treinamentos e suporte técnico, favor contactar o representante local da Norman ASA.

Convenções

Parágrafos claramente destinados para usuários em rede ou para administradores de sistema, e portanto com pouca utilidade para usuários finais, estão identificados com este ícone.

Este manual se destina ao Windows assim como aos usuários do OS/2. Sempre que diferenças afetem o NVC, o ícone estará sendo mostrado em especial para a plataforma OS/2.

Requisitos do Sistema

Esta versão suporta a instalação em máquinas com Windows 95/98/Me, Windows NT/2000/XP/2003, Linux, OS/2 Warp 4, OS/2 Warp Server, Workspace On-demand, e eComStation.

Para o Windows 95, o WinSock2 **tem** que estar instalado, e o Internet Explorer 5.5 é recomendado.

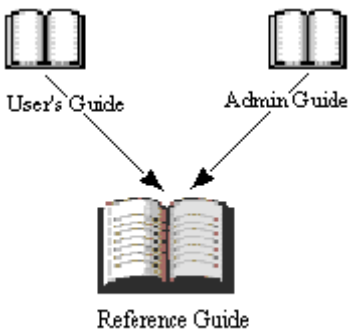
Para Windows NT, versão 4 com SP4 (ou maior) e Internet Explorer 4.0 (ou maior) são requeridos.

Para OS/2 recomendamos Warp 4 fp 15 (ou maior) e Java 1.1.8.

Para Linux, a glibc 2.2 é necessária.

De uma maneira geral, recomendamos que seja utilizada a mais recente versão de Services Packs / ou atualizações relacionadas com segurança de sua plataforma.

Quem deve ler este manual?



Este manual cobre todas as funções encontradas no NVC e por isso é destinado a todos os usuários do NVC — usuários finais assim como administradores — que necessitem de informações mais aprofundadas do produto.

Além deste manual, o *Guia do Administrador* cobre tópicos que são particularmente úteis em instalações em rede, e o *Guia do Usuário* que é uma introdução básica às funções do NVC.

A instalação *não* é discutida neste manual. Para instalações em rede ou em máquinas stand-alone (não conectadas à rede), veja o *Guia do Administrador* e o *Guia do Usuário* respectivamente.

Pré-requisitos

Para obter a melhor performance de todas as funções do NVC, você deve ter um bom entendimento dos diferentes módulos que compõem o NVC, e de como eles trabalham em conjunto, como descrito neste manual.

Se estiver rodando o NVC em um ambiente com rede, você deve ter conhecimentos detalhados sobre o seu sistema operacional de seu servidor e de suas estações.

Suporte Técnico

A Norman provê suporte técnico e serviços de consultoria para o NVC e itens relacionados à segurança em geral. O suporte também envolve a garantia de qualidade de sua instalação de antivírus, incluindo assistência para adequação do NVC ao seu ambiente.

Atente para o fato de que esses serviços variam tanto no seu escopo quanto em custo entre os diferentes distribuidores espalhados pelo mundo.

Conteúdo

Sobre o NVC

O que é o NVC?

O Norman Virus Control (NVC) é um programa antivírus que monitora o seu PC contra software nocivos, também conhecidos por *malware*. Malware são vírus, worms, e outras variedades de códigos nocivos destrutivos. O NVC pode detectar e remover vírus conhecidos e desconhecidos existentes nos discos rígidos, disquetes, anexados aos emails, etc.

O NVC checa os arquivos quando eles são acessados, e possíveis vírus são removidos automaticamente. No caso do NVC ser incapaz de limpar o arquivo infectado, você receberá um aviso e instruções de como deve proceder.

Você pode — e nós recomendamos que assim faça—realizar um rastreamento manual de áreas selecionadas em seu computador, e fazer uso do Editor de Tarefas e do Programador para definir o que se deve rastrear e quando

Note: O NVC se instala com configurações pré-selecionadas, as quais consideramos suficientes para protegê-lo contra ataques de vírus. Os módulos podem ser reconfigurados, para que o NVC se adapte melhor às suas necessidades.

Informações Gerais sobre o NVC 5

O NVC v5 emprega dois mecanismos de rede diferentes:

- Para instalação, distribuição e configuração, é empregado o compartilhamento normal de arquivos utilizando letras como drives, ou caminhos UNC.
- Para mensagens e relatórios (log), um protocolo de rede proprietário foi criado e é o utilizado.

O sistema de mensagens faz parte da instalação básica do NVC em um computador em rede, e ele é ativado tão logo o agente, que está residente, seja iniciado. Dentre um sem número de vocações, o agente gerencia o tráfego entre os diferentes

módulos de envio (output) e recebimento (input). O administrador simplesmente terá que configurar o sistema de forma que mensagens de importância variada sejam passadas para o módulo de envio correto.

O engine do rastreador agora detectará e removerá os vírus baseados em instruções de Floating Point Unit (FPU) e instruções Multi Media Extensions (MMX). Apesar de nos dias atuais existirem apenas poucos vírus baseados nas instruções FPU ou MMX, este número irá com certeza crescer.

O novo emulador 32-bit do scanner permitirá a detecção e ajuda na análise de vírus complexos, encriptados, polimorfos.

Resumindo algumas das mais proeminentes modificações no NVC v5 podemos listar:

- Instalação Simplificada
- Gerenciamento simplificado
- Facilidade de uso
- Invisibilidade

A interface do usuário do NVC v5 é formada por quatro grupos principais:

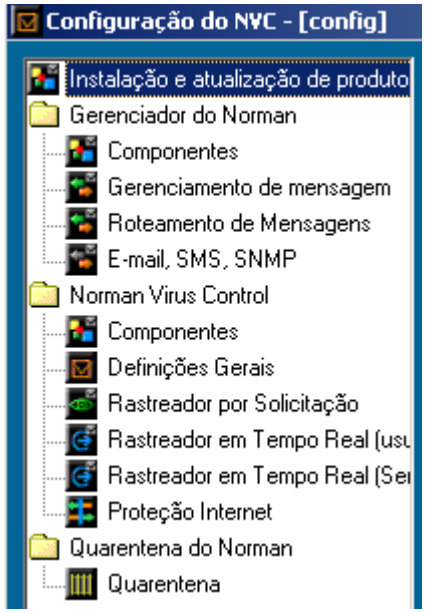
- Editor de Configuração
- Editor de Tarefas
- Utilitários
- Internet Update

Estes itens aparecem de forma separada nos grupos do programa do Norman.

Estes grupos estão localizados no diretório do Norman no OS/2 desktop.

⇨ Veja ‘Editor de Configuração’ on page 17, ‘Editor de Tarefas’ on page 89, ‘Utilitários’ on page 96, e ‘Internet Update do Norman’ on page 102.

Programas e módulos do NVC



Este capítulo mostra como o NVC — e outros possíveis produtos da Norman — são mostrados no editor de configuração. No lado esquerdo do editor aparece uma lista de produtos e seus módulos e componentes. Esta lista mostrará quais produtos Norman você possui instalados, assim como os correspondentes módulos e componentes, os quais estão organizados como *pastas* — com a mesma lógica e aparência de um ambiente Windows Explorer. Os módulos possuem um ou mais diálogos acessados através das "abas" onde as opções de configuração estão presentes para serem editadas.:

O primeiro item no exemplo acima, **Instalação e atualização de produtos**, afeta a instalação dos produtos Norman disponíveis para serem executados neste ambiente, e a manutenção deles — notadamente a funcionalidade do Internet Update. Quando você seleciona um dos itens do lado esquerdo, as possíveis opções de configuração do módulo selecionado surgem do lado direito do diálogo.

O **Gerenciador do Norman** incorpora módulos que podem ser compartilhados por diferentes programas do Norman ou por plug-ins prontos para serem incluídos nesta interface de usuário. Os módulos nesta pasta são controlados pelo ***Zanda*** (Zero Administration Network Distribution Agent).

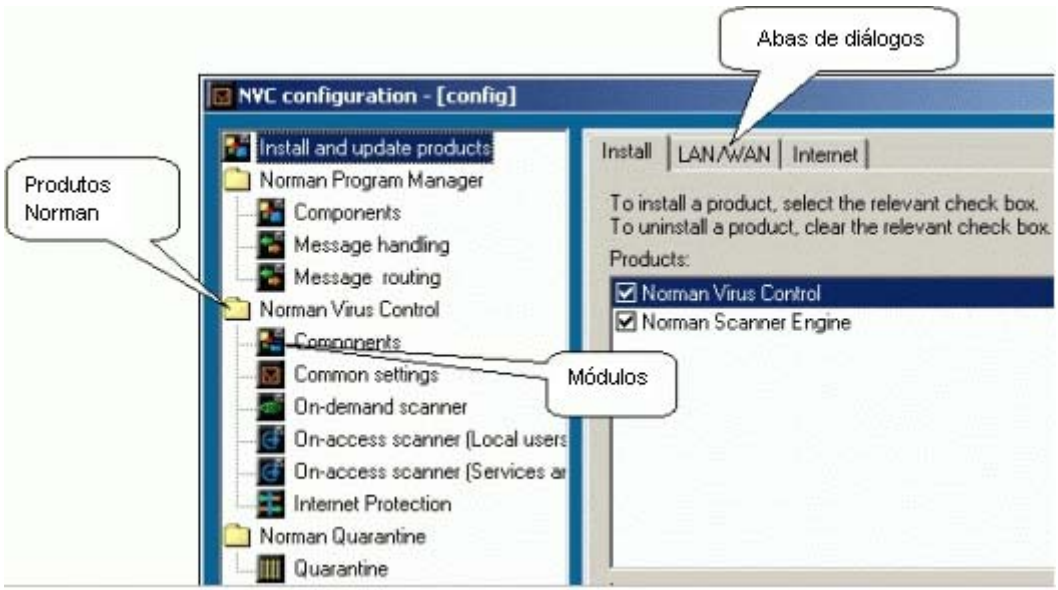
⇨ 'Gerenciador do Norman (NPM)' on page 106.

Os módulos específicos do produto estão listados sob o nome **Norman Virus Control**. Selecione **Componentes** para uma lista

de componentes que constituem o NVC. Você pode instalar e remover os componentes neste diálogo.

Visão geral do NVC

Como descrito na seção anterior, a interface para o usuário do NVC v5.8 se parece como abaixo mostrado:

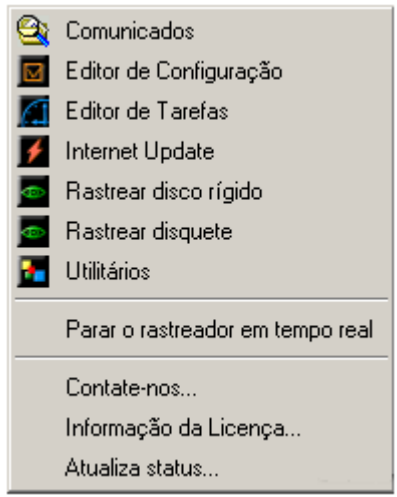


Atalho para os módulos e rastreamento do NVC

Durante o setup, um ícone do Norman é colocado na barra de tarefas no lado inferior direito da tela. Este ícone confirma que o NVC está instalado em seu micro. Veja também na page 14.

OS/2: O NVC aparece como uma entrada no desktop menu. Clique com o lado direito do mouse e selecione *Norman Virus Control*.

Os itens listados acima da linha de separação do menu que aparece quando clicamos no ícone da barra de tarefa, são cópias dos itens que surgem quando pressionamos *Iniciar* | *Programas* | *Norman Virus Control*.



Este é um atalho para os principais módulos do NVC, assim como para tarefas típicas no que se refere a rastreamentos. No Windows, você clica com o lado direito do mouse no ícone para mostrar este menu. Ele lhe dá um fácil acesso aos módulos do NVC e às tarefas de rastreamentos. Você pode **Iniciar / Parar o rastreamento em tempo real** com um simples clique do mouse. Selecione **Contate-nos** para mostrar informações sobre contatos dos escritórios da Norman. Finalmente, você poderá ver o status dos produtos, incluindo aqui as informações sobre o arquivo de definição de vírus.

Aqui, nesta função, temos a origem das mensagens relativas a possível desatualização do arquivo de vírus, período de expiração da licença e outras informações.

Avisos

O ícone do Norman também fornece informações a respeito da situação da instalação de seu NVC. Se o ícone aparecer assim:

significa que os componentes que estão sendo executados não correspondem àqueles que foram selecionados para serem carregados na aba **Iniciar** no editor de configuração **Norman Virus Control|Componentes|Iniciar**. Se o 'N' do ícone do Norman estiver piscando, posicione a ponta do mouse no símbolo, e o NVC lhe dirá qual componente precisa ser atualizado ou com possíveis erros.

Note: Durante o início, o símbolo vermelho fica visível até que todos os módulos tenham iniciado. Quanto mais antigo e lento for o PC, mais lento será para carregar todos os

módulos. Entretanto, não deverá demorar mais do que 1 ou 2 minutos.

Para usuários do Windows XP com o SP2 instalado:
Microsoft incluiu seu "Centro de Segurança" com características e opções para Firewall, atualizações automáticas e proteção contra vírus. O NVC é um dos vendedores de AntiVirus (AV) o qual o sistema detecta. Se a definição de vírus do NVC estiver desatualizada, ou o rastreador em tempo real não estiver sendo executado, você também receberá um aviso do Windows de que algo está errado. O símbolo do Centro de Segurança aparece.

Caso o ícone apareça desta forma na barra de tarefas,

significa que umas das seguintes situações está acontecendo:

1. O Rastreador em Tempo Real está instalado, mas foi de forma manual desabilitado. Para iniciar ele, selecione o item do menu da barra de tarefas, ou vá para a aba "Iniciar" no Editor de Configuração existente em **Norman Virus Control|Componentes|Iniciar**. Selecione *Rastreador em Tempo Real* e depois clique em **Salvar**.
2. Você provavelmente selecionou **Re-iniciar mais tarde** em uma solicitação anterior, e o NVC está aguardando.
3. Um erro de instalação que um re-início pode sanar.

Arquivos de definição de vírus obsoletos

Um triangulo amarelo *piscando* significa que os arquivos de definições de vírus estão desatualizados, i.e. eles pertencem há pelo menos 10 dias atrás. O mesmo acontece se o Rastreador em Tempo Real estiver desligado.

Ícones informativos

Quando o ícone do Norman aparece com uma engrenagem, significa que o Gerenciador do Norman está trabalhando, mais comumente com uma atualização. Não recomendamos que você

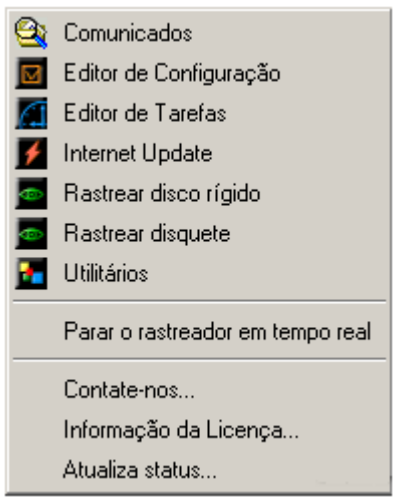
desligue a máquina quando o Gerenciador do Norman (NPM) estiver trabalhando, ou seja, com o símbolo descrito visível.

Editor de Configuração

O Norman Virus Control (NVC) vem com um conjunto de componentes que serão instalados durante a instalação. Quando ela estiver completa, você poderá remover os componentes que não deseje. O NVC é uma aplicação baseada em plug-in, e novos plug-ins, i.e. programas, podem possívelmente ser introduzidos de acordo com novas tecnologias ou ameaçaas a segurança surjam.

Comum para todas as abas:

Em um ambiente de rede, o **campo Acesso** na parte inferior de cada uma das abas aparecerá caso você possua direitos de administrador. O administrador do sistema decide o que deverá ser visível e/ou configurável pela estação. O usuário normal poderá, portanto, ver tudo ou apenas algumas abas, mas não necessáriamente poderá alterá-las.



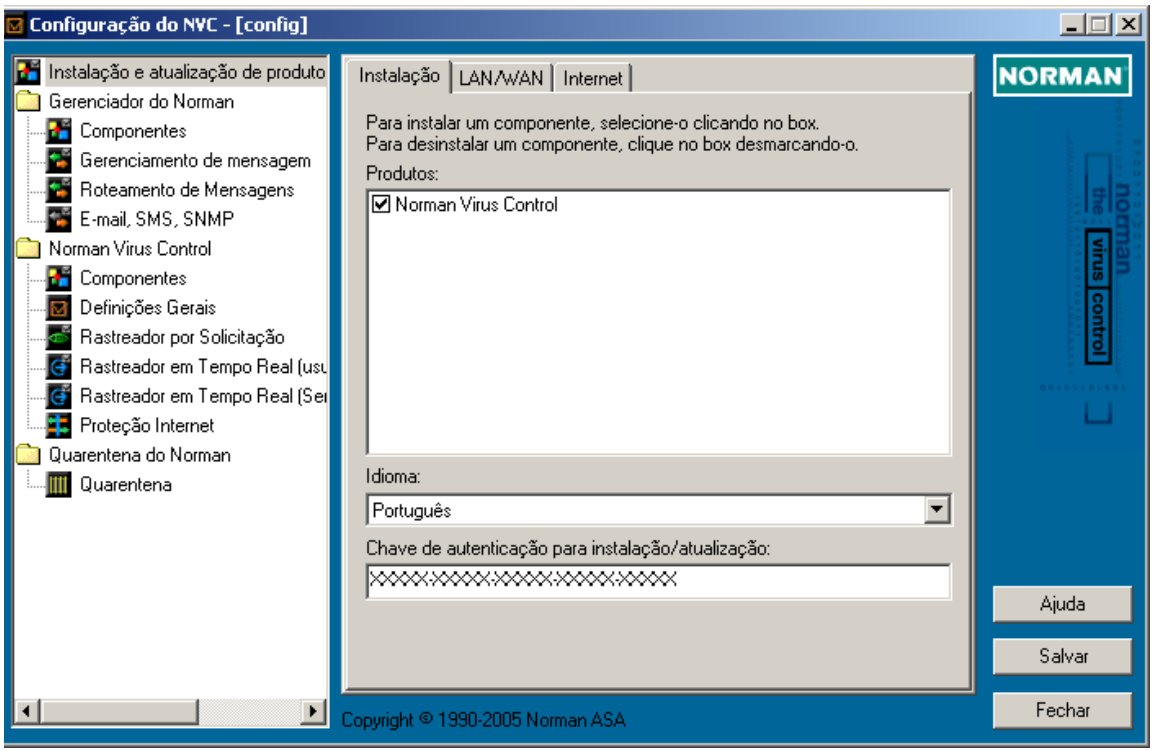
Você pode configurar as diferentes funções no NVC de apenas um ponto central — o Editor de Configuração. Selecione o item *Editor de Configuração* do grupo / pasta Norman que aparece quando você clica com o lado direito do mouse no símbolo verde 'N' na barra de tarefas:

A lista dentro da caixa de diálogo reflete quais são os componentes que decidiu que fossem instalados. Por exemplo, componentes do tipo *Roteamento de Mensagens* e *E-mail, SMS, SNMP*, não serão mostrados em uma instalação para single-user, ou uma estação stand-alone.

Cada componente tem a sua própria aba com sua caixa de diálogo com um conjunto de configurações possíveis para aquele item do componente. Clique no componente que deseja configurar e faça as suas escolhas nas janelas correspondentes a cada aba.

Instalação e atualização dos produtos

Instalação



☑ Norman Virus Control

Qualquer instalação do NVC necessita que este dois produtos estejam instalados; o produto *Norman Virus Control* e aquele que realmente realiza o trabalho duro, o *Engine rastreador*. Na medida em que mais produtos venham a ser disponibilizados nesta interface, por exemplo o Firewall da Norman ou o *NVC for Domino*, eles irão aparecer na lista.

☑ **Engine Rastreador do Norman**

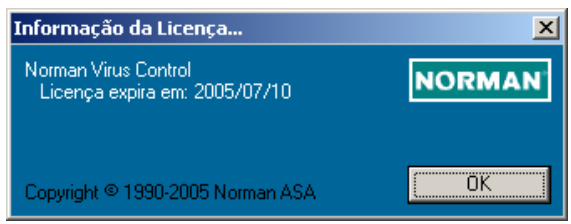
O Engine rastreador é o núcleo tecnológico de qualquer aplicação antivírus. Você pode considerar que a interface seja como uma embalagem, a qual é inútil sem o Engine rastreador e os componentes do NPM (veja page 31).

Idioma:

Selecione em qual idioma os componentes deverão estar através do menu pull-down. Clique na seta para mostrar os que estão disponíveis. A lista está sujeita a alterações na medida em que novos idiomas poderão ser incluídos.

Chave deAutenticação para instalação/atualização:

É o serial que você recebeu quando da aquisição do NVC, e que informou durante o processo de instalação. Ele aparece neste campo e contém as informações sobre sua licença que possibilita o uso do NVC de acordo com a aquisição. Note que você poderá ver estas informações clicando com o lado direito do mouse no ícone do Norman e selecionando *Informação da Licença*:



Atualizando o NVC

Novos vírus aparecem todos os dias, e a Norman fornece frequentes atualizações do arquivo de definição de vírus, assim como do programa em si.

Note: O arquivo de definição de vírus e os outros componentes são tão integrados que aconselhamos a atualizar **todos** os componentes. Não é suficiente instalar apenas a atualização das definições de vírus.

Você pode atualizar o NVC de disversas formas, via Internet, via rede, ou de um CD. O mecanismo de atualização fornece

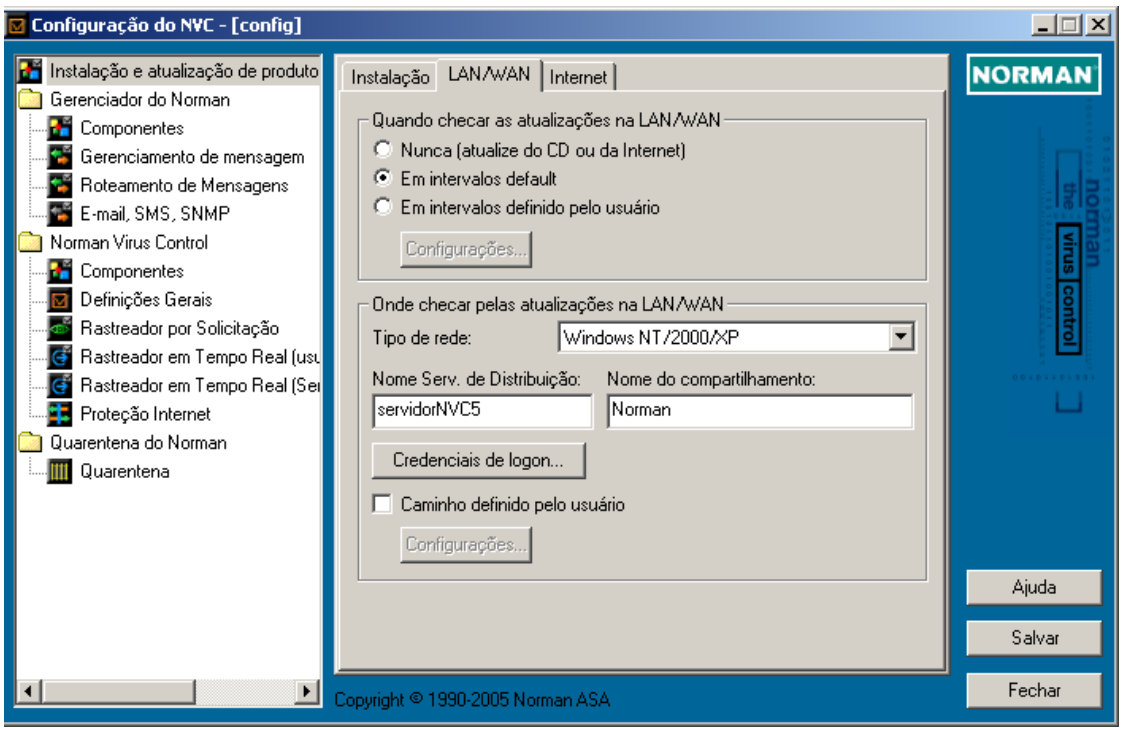
atualizações para servidores e estaçõesassim como para máquinas standalone (máquinas que não estão em redes), e existem várias possibilidades diferentes de opções de configuração com as quais você pode escolher.

LAN/WAN

Note: Antes de qualquer alteração neste diálogo, você ***deve*** verificar as instruções constantes no *Guia do Administrador*.

Este diálogo é para atualização do NVC em redes e portanto é útil para os administradores de redes.

Nele você pode digitar as informações requeridas sobre a sua rede e q frequencia com que o NVC deve buscar pelas atualizações do programa, configurações e arquivos de tarefas, além de configurar diferentes opções.



Quando checar as atualizações na LAN/WAN

O Nunca (atualize do CD ou da Internet)

ISe não desejar atualizar o NVC através de sua rede, selecione esta opção e vá para o próximo diálogo para especificar como seria a atualização da Internet. Use esta opção, também, quando receber uma versão nova através de CD-ROM da Norman.

Note: Quando receber o CD-ROM, o arquivo de definição de vírus estará com certeza, desatualizado e já reposto por outros mais novos no servidor da Norman. Isso se deve por causa do tempo gasto na produção e envio do mesmo. Apesar de que novos arquivos podem estar disponíveis na web minutos após estarem prontos, podem demorar uma ou duas semanas para serem preparados e distribuídos através do CD-ROM. ***Sempre*** verifique o servidor da Norman a procura de novos arquivos de definição de vírus e novos componentes do programa depois de ter instalado as novas versões de seu CD-ROM. A Norman fornece uma ferramenta apropriada para esta tarefa—Internet Update. Veja page 102.

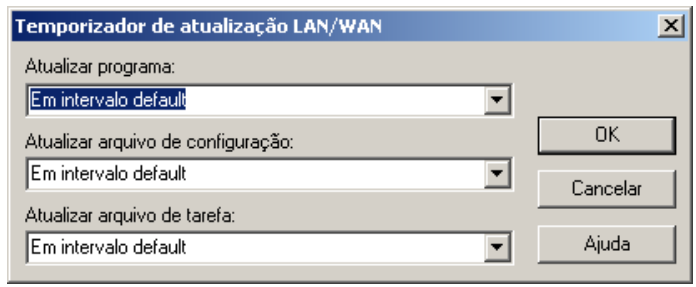
⊙ Em intervalos default

As atualizações são checadas em intervalos estabelecidos pelo Gerenciador do Norman (NPM). O NPM faz distinção entre servidores de distribuição do NVC e clientes.

⇨ Por favor veja a seção sobre o NPM no *Guia do Administrador* (especialmente a passagem “Intervalos de atualização e tráfego na rede” para uma compreensão maior desses mecanismos).

O Em intervalos definido pelo usuário

Esta oção permite que se especifique o intervalo de atualização do programa, dos arquivos de configuração e de tarefas. Clique em **Configurações** para mostrar o seguinte diálogo:



A opção default para todas as atualizações é “Em intervalos default”, e repõe a opção “Automaticamente do servidor” das versões anteriores do NVC5. Se selecionar o intervalo default, as atualizações serão replicadas do servidor de distribuição 3 minutos depois do logon, e depois a cada hora nas estações e a cada 5 minutos nos servidores de distribuição. Essas são as opções default, mas poderá configurar outros esquemas. Selecione-os no menu drop-down-menus no diálogo.

Note: Se não tiver uma conexão permanente à Internet, não recomendamos a opção default, o qual gerará conexões dial-up caras. A melhor solução seria configurar para a cada hora, por exemplo. Moreover, com uma conexão dial-up para a Internet, o servidor de distribuição deve estar localizado localmente.

Onde checar pelas atualizações na LAN/WAN

Depois de determinar o intervalo de atualizações, deve então determinar onde as atualizações estão localizadas.

Primeiro, especifique que tipo de rede você possui selecionando da lista **Tipo de Rede**. Você pode escolher dentre os seguintes:

- Windows NT/2000/XP/2003
- Workgroup ou rede ponto-a-ponto, e
- Novell NetWare.

Para Windows NT/2000/XP/2003 e Workgroup ou rede ponto-a-ponto, digite:

- Nome do servidor de distribuição
- Nome do compartilhamento

Para Novell NetWare, digite:

- Nome do servidor de distribuição
- Nome do Volume e do diretório raiz

Note: Simplesmente digite o nome do servidor de distribuição sem backslashes ou qualquer outro caracter especial.

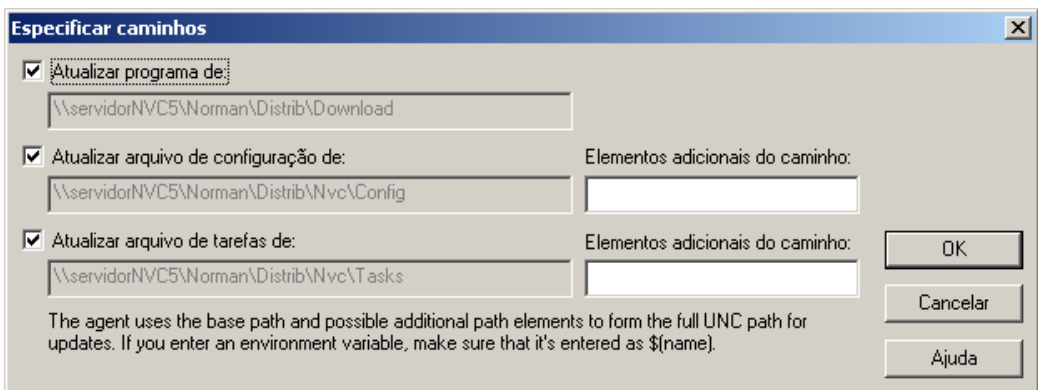
Quando os 3 campos no *Onde checar pelas atualizações na LAN/WAN* estiverem completados, o NVC interpretará as informações para estabelecer o caminho completo dos arquivos.

Credenciais de logon

Se estiver rodando uma rede Windows, digite o Nome do usuário, Senha, e Nome do domínio pressionando o botão **Credenciais de logon**.

Caminho definido pelo usuário

Se deseja ter diferentes arquivos de configuração e de tarefas entre diferentes departamentos na sua organização, por exemplo, você deve selecionar **Caminho definido pelo usuário** e pressionar em **Configurações**. O seguinte diálogo aparecerá:



Neste diálogo, os campos já estarão completados baseados nas informações fornecidas para *Nome do Serv. de distribuição* e *Nome do compartilhamento* (*Nome do Volume e do diretório raiz* em Novell).

☑ **Atualizar programas de:**

Identifica o caminho do servidor onde as atualizações do programa podem ser obtidos depois de baixados da Internet, por exemplo. Esta caixa mostra o servidor e o compartilhamento/ volume informados no diálogo anterior, adicionados do caminho default da localização dos pacotes do programa.

☑ **Atualizar arquivo de configuração de:**

Esta caixa mostra o servidor e o compartilhamento/volume informados no diálogo anterior, adicionados do caminho default da localização dos arquivos de configuração.

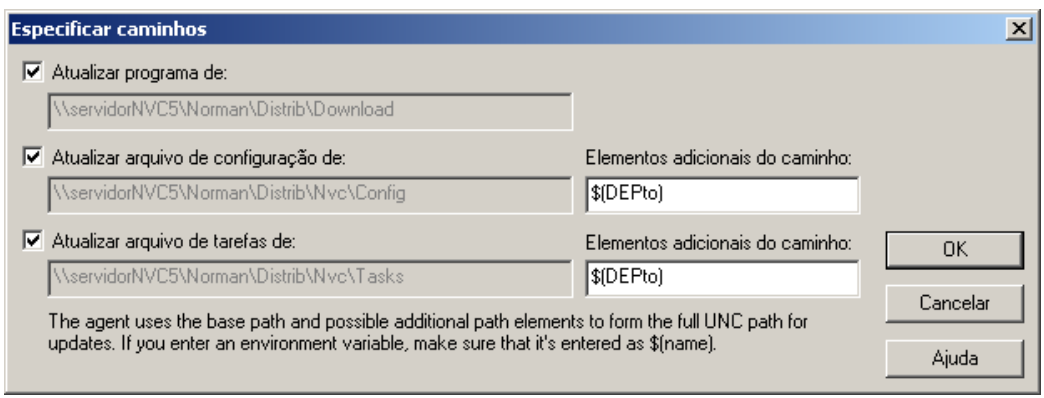
☑ **Atualizar arquivos de tarefas de:**

Esta caixa mostra o servidor e o compartilhamento/volume informados no diálogo anterior, adicionados do caminho default da localização dos arquivos de tarefas.

Elementos adicionais do caminho:

Este campo adicional dos *Arquivos de configuração* e *Arquivos de Tarefas* lhe fornece a oportunidade de distribuição de arquivos de configuração e tarefas especialmente feitos para realidades específicas dentro de sua organização.

Quando fornecer um elemento de caminho adicional, tenha a certeza de que forneceu a variável de ambiente no formato $(nome), o qual habilita o NPM e estabelecer um caminho UNC completo. Exemplo:



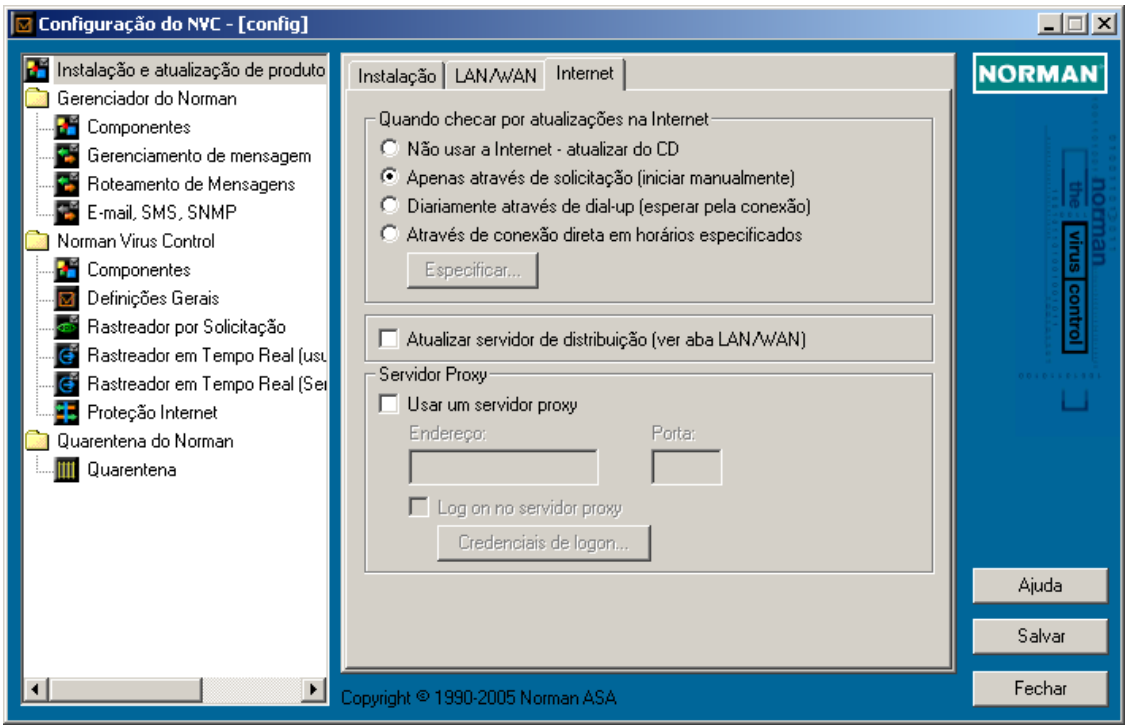
Internet

Sua escolha nesta seção afeta o modo em que o Internet Update (IU) gerencia as atualizações da Internet.

A Internet é o método mais rápido e eficiente de distribuição das atualizações de arquivos de definições de vírus e de outros componentes do NVC. Você precisa baixar todas essas atualizações o mais rápido possível para que possa manter uma proteção otimizada. Deve então, tomar muito cuidado nas escolhas desta opção, para que ela lhe proporcione a melhor de suas necessidades.

O programa Internet Update (IU) gerencia as atualizações do NVC. Elas estão disponíveis como pacotes, e o IU decide quais aqueles que são relevantes para você, baseado em seu sistema operacional e idioma. Entretanto, uma rede semre possui diversos sistemas operacionais e diferentes versões de idiomas do NVC. Em ambientes heterogêneos você deve portanto executar uma ferramenta separada de configuração para o IU (NIUcf), afim de assegurar-se de que as atualizações cobrirão todos os sistemas existentes em sua rede, assim como todos os idiomas. O NIUcf está descrito na seção “Instalando e

distribuindo" para Windows NT e Novell NetWare no *Guia do Administrador*.



Quando checar por atualizações na Internet

Note: Se sua máquina é protegida por um firewall ou servidor proxy, você deverá fornecer as informações requeridas na seção **Servidor Proxy** deste diálogo (page 29).

O Não usar a Internet - atualizar do CD

Se escolher esta opção, nunca será questionado ou lembrado sobre downloads disponíveis na Internet. Na medida em que novos CDs normalmente são distribuídos apenas quando novas versões são lançadas, você receberá CDs aenas de 3 em 3 meses, ou mais. Nós **não** recomendamos esta opção.

⊙ Apenas através de solicitação (iniciar manualmente)

Selecione esta oção se desejar rodar o IU manualmente através do menu do NVC para checagem de atualizações, ou através do

programa do Windows **Agendador de Tarefas** (localizado no **Painel de Controle**).

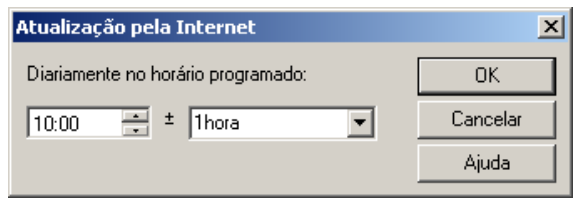
O Diariamente através de dial-up (esperar pela conexão)

Se faz uso de um modem para conexão à Internet, selecione esta opção para checagem diária nos servidores da Norman. Basta acessar a Internet normalmente, e o programa irá checar se as atualizações estão disponíveis.

Se a conexão acontece várias vezes por dia, o IU irá checar apenas da primeira vez naquele dia. Por isso recomendamos, se esse for o seu caso, que sempre realize a verificação manual, pois dependendo da hora em que você se conectar pela primeira vez, talvez ainda não exista uma atualização disponível.

O Através de conexão direta em horários especificados

Caso tenha uma conexão permanente à Internet, esta é a opção recomendada. Pressione em **Especificar** para programar um horário:



Primeiro especifique quando o NVC deve checar or atualizações. Digite a hora, e depois use o pull-down menu no '+-' para permitir ao sistema que gerencie a melhor hora para evitar possíveis cargas no mesmo.

Note: Se o Internet Update não estiver sendo executado por 24 horas, o programa checará automaticalmente no próximo início.

☐ Atualizar servidor de distribuição (ver aba LAN/WAN)

Se escolher esta opção, habilitará ao cliente a baixar as atualizações para o servidor de distribioção do NVC. Além disso, irá ser preciso que o usuário logado nesta máquina possua

direitos de escrita no diretório de distribuição (…`\Norman\Distrib\Download`).

O **Atualizar servidor de distribuição** não é uma opção default. Portanto, qualquer cliente tentando rodar o Internet Update (NIU.EXE) irá atualizar o seu próprio caminho (sua própria instalação) (`...\Norman\Download`), e não o diretório de distribuição (`...\Norman\Distrib\Download`). Isso pode ser muito útil para notebooks, por exemplo, os quais são atualizados pelo seu servidor de distribuição enquanto estão conectados em seu escritório, e executando o Internet Update individualmente quando fora dele.

Se o *cliente* que roda o IU tem habilitado o **Atualizar servidor de distribuição**, e não estiver conectado a rede onde existe este servidor de distribuição, nenhum dos dois serão atualizados.

Se o IU roda no *servidor de distribuição*, a ação **Atualizar servidor de distribuição** não deve estar selecionada.

A ação **Atualizar servidor de distribuição** é tipicamente selecionada apenas em algumas máquinas, as quais estão sempre conectadas a rede. (Veja a seção de distribuição com diversas configurações no *Guia do Administrador* para maiores informações).

Em instalações onde Novell Netware é o servidor de distribuição, esta opção tem que estar selecionada em pelo menos uma máquina.

Servidor Proxy

Servidores Proxy odem exigir autenticação dos usuários. Se faz uso dessas opções, neste diálogo, você deve digitar as mesmas informações para logar-se no servidor proxy e autenticar-se no mesmo.

Os dois esquemas de autenticação são:

1. Basico, e
2. Windows NT desafio/resposta *aka* NTLM.

Servidor Proxy

☐ **Usar um servidor proxy**

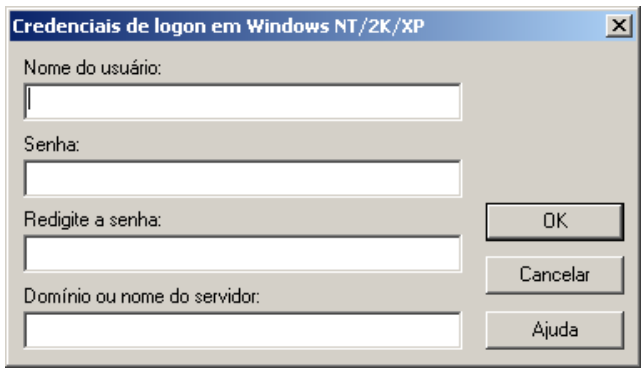
Entre com o **Endereço** e **Porta** do firewall do proxy HTTP.

Se tiver informações especificadas para o proxy HTTP em seu browser, deverá digitar exatamente as mesmas aqui.

☐ **Log on no servidor proxy**

Note: Esta opção é relevante apenas se seu servidor proxy requerer autenticação.

Pressione em **Credenciais de Logon** para mostrar:



As informações aqui digitadas devem ser as mesmas as quais você normalmente entra quando se loga em seu servidor proxy.

Nome do usuário:

Digite um nome válido.

Senha:

Informe a senha.

Domínio (para Windows NT desafio/resposta)

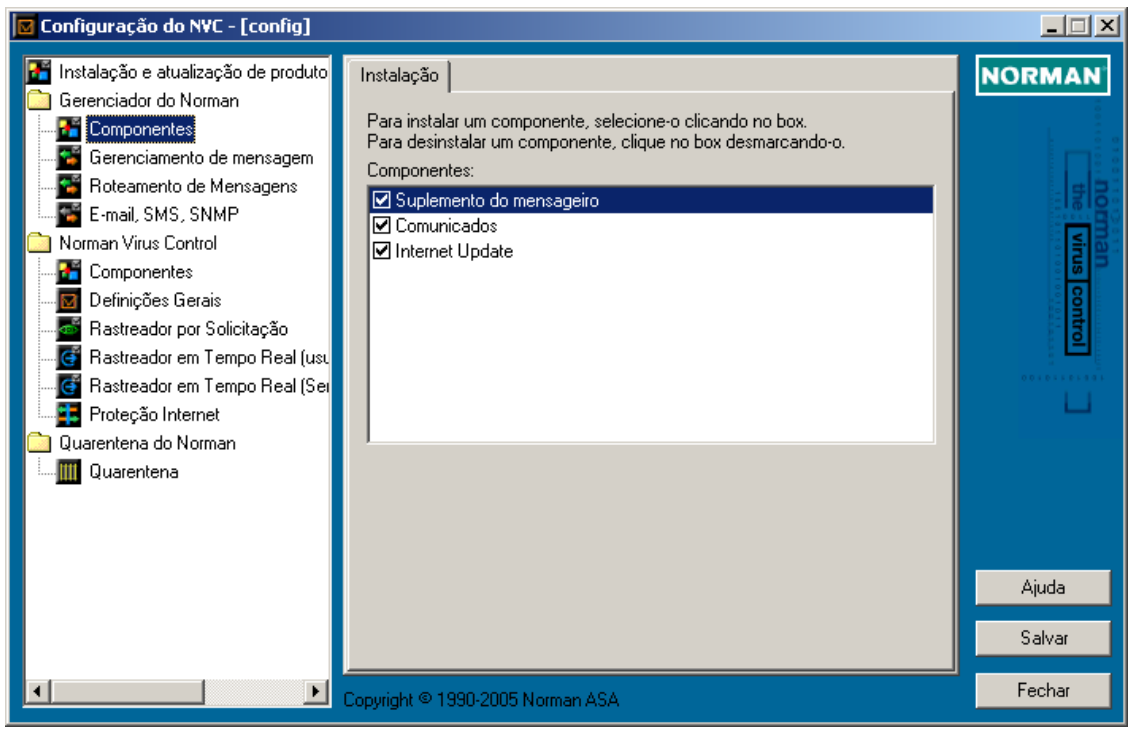
Este campo não é relevante para servidores proxy que usem autenticação básica.

Digite o nome do domínio. Se este campo for deixado em branco, o *nome da máquina* será utilizado.

Gerenciador do Norman

Esta pasta contém 3 módulos proprietários do Norman os quais gerenciam a comunicação interna entre as diferentes partes do produto.

Roteamento de mensagens permite ao administrador selecionar que tipos de mensagens serão roteadas para outros PCs rodando NVC na rede. Por favor, veja no capítulo “Mensagens” no *Guia do Administrador* uma detalhada descrição sobre o sistema de mensagens.



Componentes

Instalação

☑ **Suplemento do Mensageiro**

Dependendo de sua licença, o Suplemento do Mensageiro provê módulos de mensagens adicionais, mais precisamente a funcionalidade de SMS, SNMP e E-mail, este último muito útil em ambientes de rede. Este módulo está descrito em detalhes na page 40.

☑ **Comunicados**

Mostra informações úteis no formato web browser, assim como novos releases, incluindo links para áreas de download, etc.

☑ **Internet Update**

Use esta ferramenta para baixar a última versão do NVC de forma automática, assim como as últimas definições de vírus. Pode ser configurado para rodar em intervalos pré-agendados.

⇨ 'Internet Update do Norman' on page 102.

Sobre relatórios e mensagens

Você deve usar a ferramenta de mensagens para determinar quais incidentes gostaria de estar sendo avisado sobre.

O mod tradicional de relatórios é escrevendo mensagens para um arquivo de log. No NVC v5, essa funcionalidade fica or conta de um de seus módulos de saída que é carregado pelo NPM. Consequentemente, as mensagens recebidas pelo NPM são passadas para um arquivo de saída, **Mensagens** no grupo **Utilitários** (page 96).

Gerenciamento de mensagem

O gerenciador de mensagens trata das mensagens selecionadas para um arquivo de log, mostra mensagens em uma console, e decide o que deverá ser enviado para o Event Log do Windows NT/2000/XP/2003. Por último, existe uma opção para que seja definida mensagens a serem informadas a todos (broadcast). Isso

nos leva a 4 abas de diálogo nesta janela, onde as opções são idênticas mas 3 primeiras janelas. As escolhas aqui tomadas, decidem quais serão as informações que aparecerão no arquivo de log, na console de mensagens, e no Event Log do Windows NT/2000/XP/2003.

No OS/2, o NVC salva as mensagens no *system error log*.

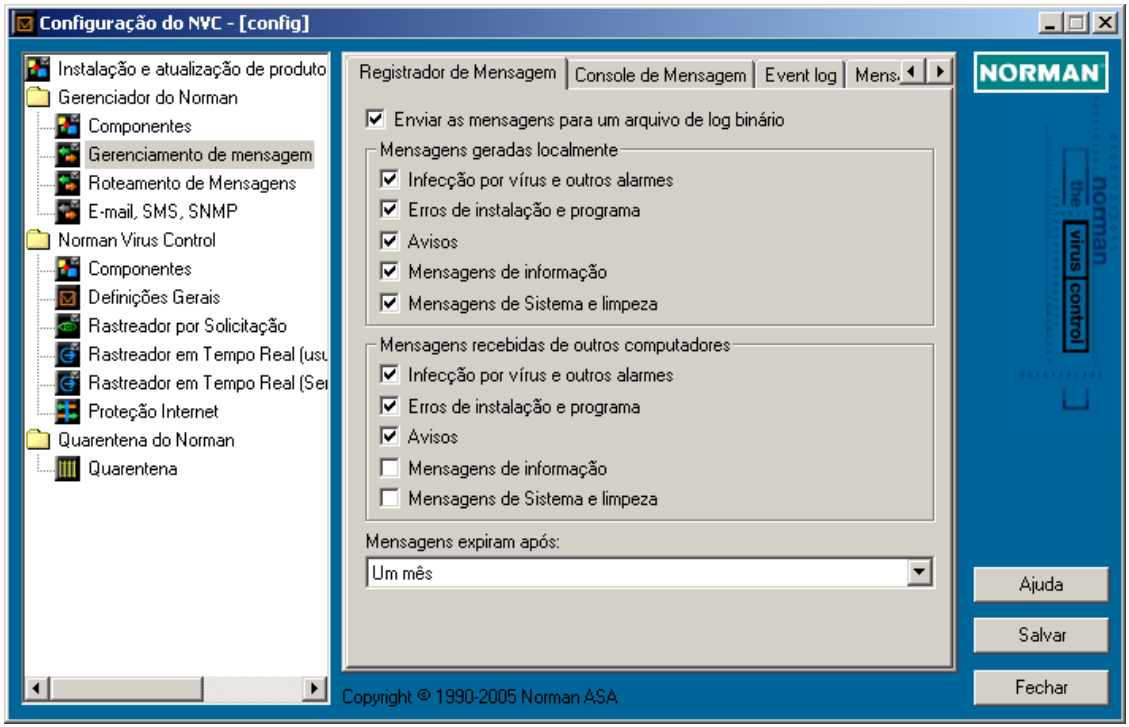
O gerenciador de mensagens permite aos usuários assim como aos administradores selecionar que tipo de mensagens são mostradas ou mantidas *localmente*. A funcionalidade de mensagens é um modo efetivo de se ter em mãos todas as atividades relacionadas aos componentes do NVC tanto locais quanto aqueles em rede.

Quando o **Registrador de Mensagem** está ativado, mensagens geradas localmente e/ou mensagens recebidas de outras máquinas são *enviadas para* um arquivo binário de log.

Quando o **Console de Mensagem** está ativado, mensagens geradas localmente e/ou mensagens recebidas de outras máquinas são *enviadas para* um console de mensagem.

Quando o **Event log** está ativado, mensagens geradas localmente e/ou mensagens recebidas de outras máquinas são *enviadas para* o Event log do Windows NT/2000/XP/2003.

Registrador de Mensagem



☑ Enviar as mensagens para um arquivo de log binário

Você deve selecionar esta opção para ter acesso à outras opções aqui existentes. Se a desmarcar, fará com que o registrador de mensagem seja desligado.

Note: O arquivo de log binário está encriptado e pode apenas ser visto através do módulo **Utilitários** (no componente **Mensagens**). Veja page 99. Arquivos de log textuais são também criados, com o mesmo critério de um arquivo binário. Todos os arquivos de log (textuais assim como binários) estão salvos no diretório MSG, normalmente `c:\norman\msg`.

Mensagens geradas localmente

As escolhas aqui feitas determinarão que tio de incidentes que ocorrem **localmente** aparecerão no arquivo de log.

☑ **Infecção por vírus e outros alarmes**

Cria entradas no arquivo de log de detecção de vírus ou outro código nocivo.

☑ **Erros de instalação e programa**

Cria entradas no arquivo de log de erros de instalação de programas do NVC ou deles durante seu funcionamento.

☑ **Avisos**

Cria entradas no arquivo de log de avisos que apareçam.

☐ **Mensagens de informação**

Cria mensagens de natureza informativa. Você deve considerar cuidadosamente esta opção em função de que lea gera uma grande quantidade de mensagens.

☑ **Mensagens de sistema e limpeza**

Cria entradas no arquivo de log relacionadas a atividades de rede no sistema. Está sempre ativada.

Mensagens recebidas de outros computadores

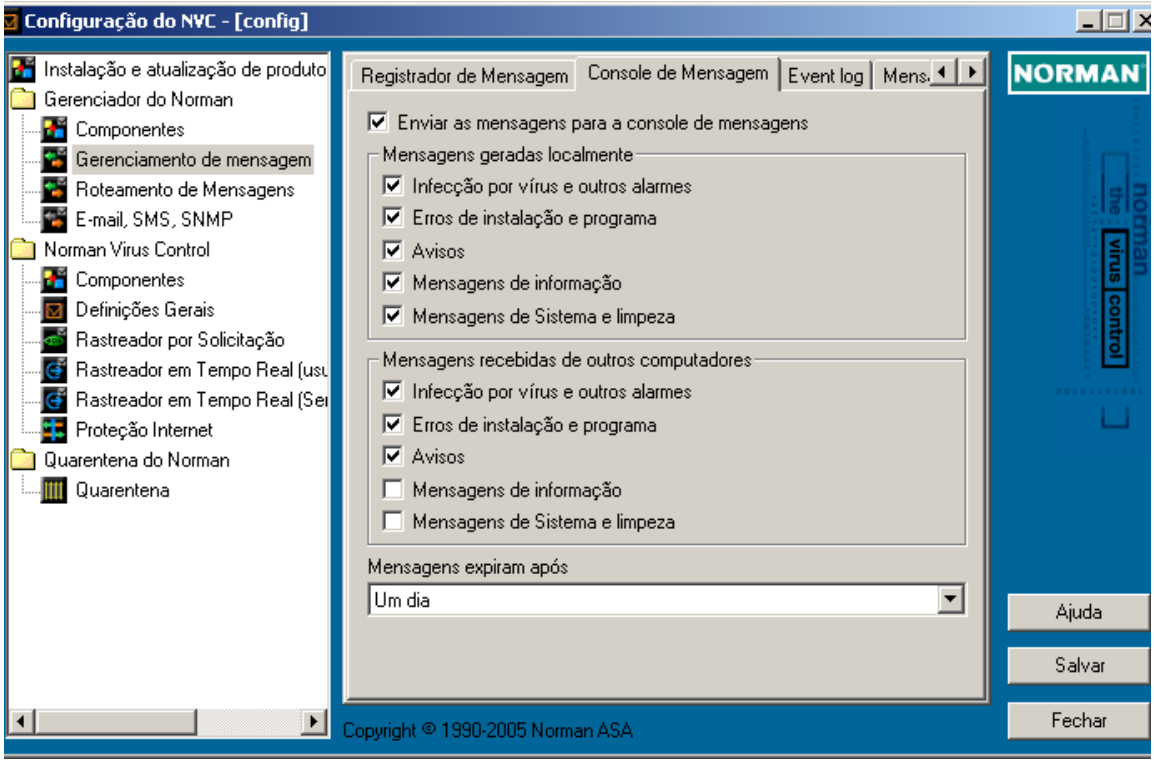
Na seção anterior, você selecionou quais seriam os incidentes que estariam acontecendo na máquina **local** que deveriam ser registrados. Nesta seção você decidirá que tipos de mensagens dos incidentes em **outros** computadores deverão ser guardados no arquivo de log.

Você poderá selecionar exatamente da mesma maneira em que o fez na seção anterior.

Mensagens expiram após:

Selecione por quanto tempo deseja que as mensagens no arquivo de log sejam mantidas. As suas opções são expiram depois de um dia, dois dias, uma semana, um mês, ou nunca.

Console de mensagem



Você deve selecionar

☑ **Enviar as mensagens para a console de mensagens**

para poder ter acesso às opções de configuração, as quais são idênticas as discutidas na seção “Registrador de Mensagem”, com início na page 34.

Mensagens expiram após:

Especifique por quanto tempo deseja que as mensagens sejam mantidas na console. Escolha por expirá-las aós uma hora, oito horas, um dia, dois dias, uma semana, um mês , ou nunca.

As oções remanescentes de configuração são idênticas àquelas da seção anterior.

Event log

Você tem que selecionar

☑ **Enviar as mensagens para o Event Log do Windows NT/ 2000**

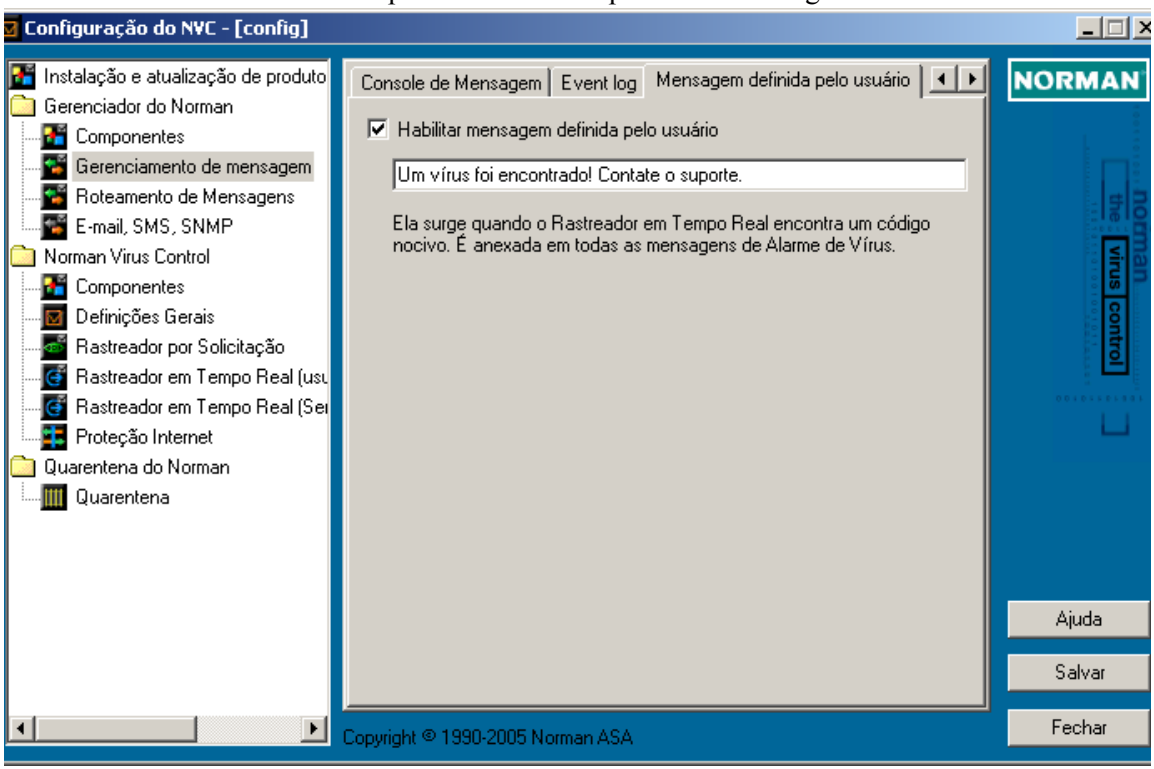
para poder ter acesso às opções de configuração, as quais são idênticas as discutidas na seção “Registrador de Mensagem”, com início na page 34.

Mensagem definida pelo usuário

Você deve selecionar

☑ **Habilitar mensagem definida pelo usuário**

para acessar o campo onde a mensagem deverá ser escrita.



Quando o Rastreador em Tempo Real detecta uma infecção, o texto que digitou neste campo irá aparecer nas estações. Essa mensagem poderá conter instruções exatas ou referencias da

estratégia da empresa para um correto comportamento quando um malware for encontrado em uma rede.

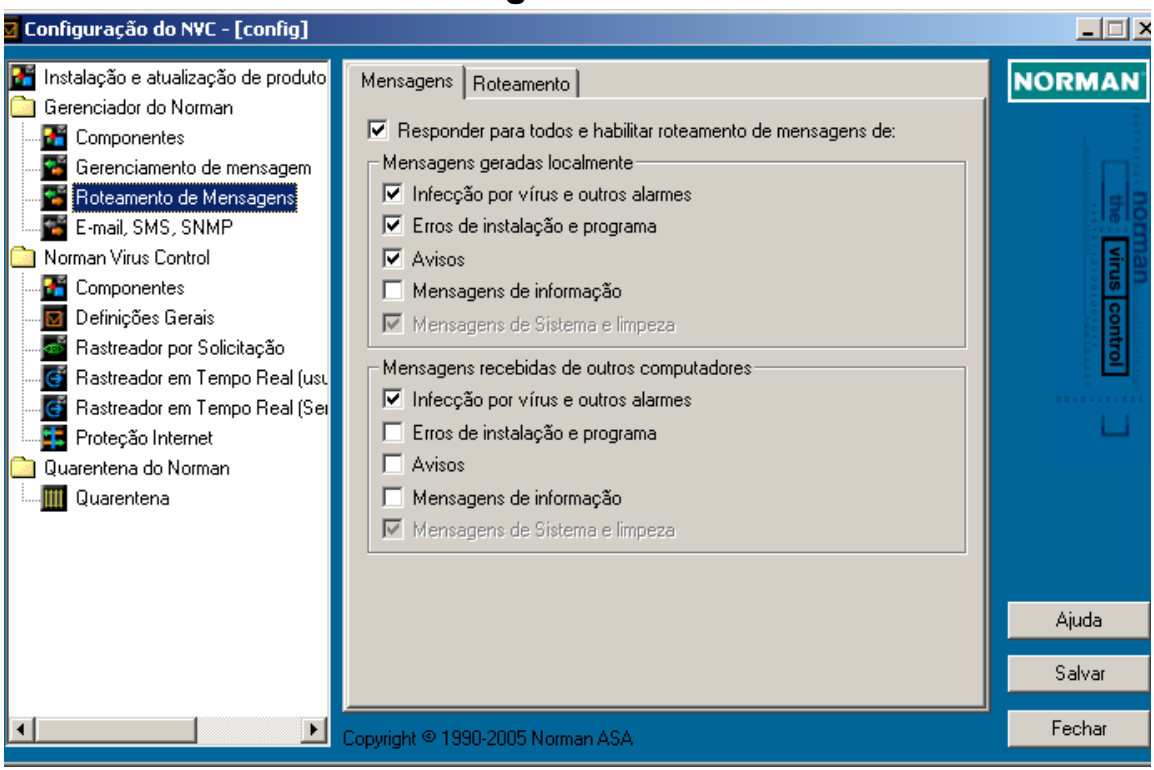
Essa mensagem á também anexada às mensagens enviadas em broadcast através do sistema interno de broadcasting do NVC.

Assegure-se de que as opções de broadcast e roteamento estão ativas no módulo **Roteamento de Mensagens** (page 38). Veja também no *Guia do Administrador* maiores detalhes de como o NVC gerencia mensagens e alarmes.

Roteamento de Mensagens

Note: Este módulo só existe em instalações em rede.

Mensagens



Este módulo de saída de mensagens suporta IP assim como IPX networks. É baseado em conexões, usando TCP/IP e/ou SPX.

Note: Veja o *Guia do Administrador* para informações detalhadas de como o NVC trata mensagens e alarmes.

☑ **Responder para todos e habilitar roteamento de mensagens de**:

Você deve selecionar esta opção para ter acesso à outras opções aqui existentes. Se a desmarcar, fará com que o roteamento de mensagens seja desligado.

Broadcasting é o envio simultâneo da mesma mensagem para inúmeros destinatários.

Mensagens geradas localmente

Selecione quais incidentes que acontencem na máquina ***local*** que o roteamento de mensagens deverá passar adiante.

☑ **Infecção por vírus e outros alarmes**

Encaminha mensagem se um vírus ou outro código nocivo for encontrado.

☑ **Erros de instalação e programa**

Encaminha mensagem se um programa do NVC reporta um erro, ou se durante a instalação do NVC um erro ocorre.

☑ **Avisos**

Encaminha mensagem que aparecer.

☐ **Mensagens de Informação**

Encaminha mensagem de natureza informativa. Deve-se, tendo em vista o alto índice de quantidade de mensagens geradas, tomar cuidado com esta opção.

☑ **Mensagens de sistema e limpeza**

Encaminha mensagem relacionadas à atividades de rede no sistema. Esta oção está sempre ativada.

Mensagens recebidas de outros computadores

Na seção anterior você selecionou quais os incidentes que ocorreram na máquina ***local*** deveriam ser enviados. Nesta seção você decidirá quais mensagens dos incidentes ocorridos nas ***outras*** máquinas deseja que sejam passadas.

As opções de seleção são exatamente iguais àquelas existentes na seçãoanterior.

Roteamento

Se habilitou o roteamento de mensagens, especifique o(s) destinatário(s) delas aqui.

Enviar mensagens para:

Clique em **Adicionar** e digite o endereço IP ou o nome da máquina do destinatário. Você tem que repetir a operação para cada um dos destinatários que deseja adicionar a lista. Nomes e endereços podem ser editados ou removidos da lista, bastando selecioná-los e pressionando o botão da operação desejada.

Normalmente apenas um destinatário deve ser especificado para que se evite duplicação de mensagens. Veja o *Guia do Administrador* para maiores detalhes.

☑ **Mensagens enviadas**

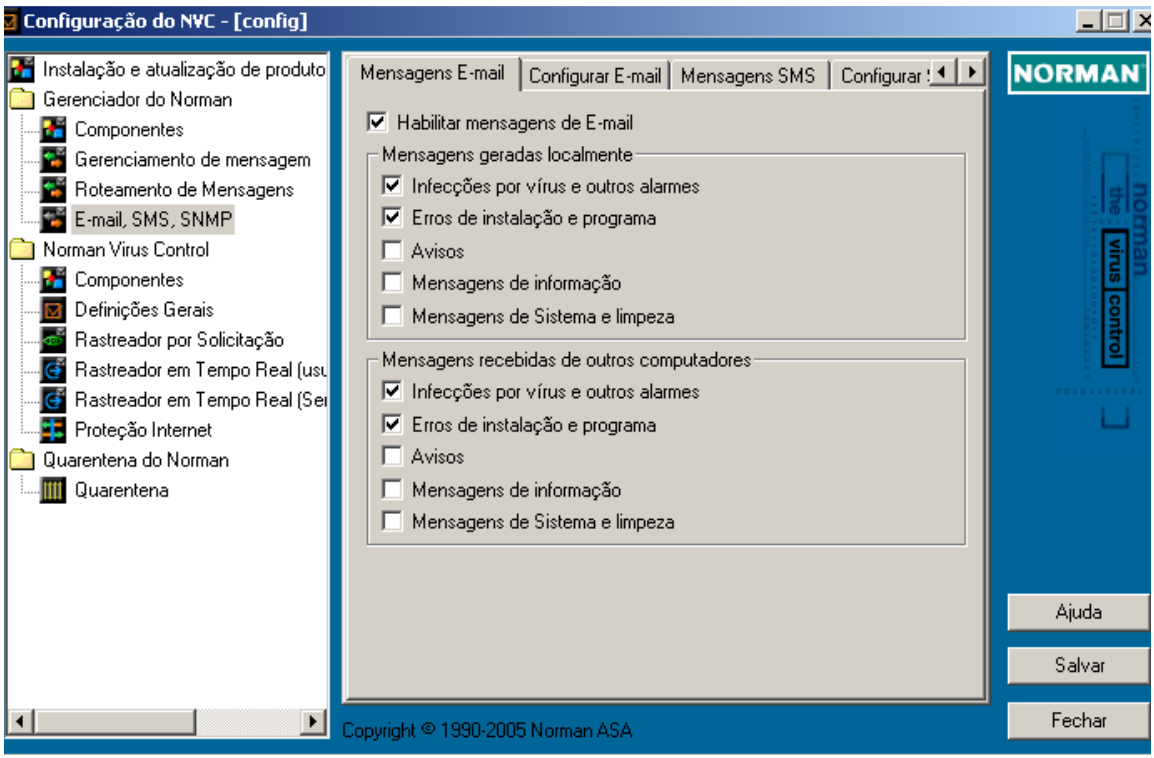
Selecione esta opção para enviar as mensagens que chegam aos membros da lista. Você poderá também selecionar quando elas expiram, onde as opções são 1, 8, ou 24 horas, 1 ou 4 semanas, ou nunca. O valor default é 1 semana.

E-mail, SMS, SNMP

Este módulo fornece as oções para envio de e-mails ou mensagens SMS sobre os eventos selecionados em PCs standalone (fora de rede) assim como de máquinas em rede. Para redes com SNMP, o NVC pode ser configurado para enviar traps SNMP.

Mensagens de E-mail, SMS, e SNMP

Você pode filtrar os eventos que dispararão um e-mail, uma mensagem, ou um trap SNMP exatamente da mesma maneira em que foram selecionados os eventos relevantes para **Roteamento de mensagens** e **Gerenciamento de mensagem**, com a mesma gama de opções:



Da mesma forma dos outros módulos de mensagem, você deve distinguir entre as mensagens geradas **localmente** das mensagens **recebidas** de outras máquinas.

Valores Default

Os valores default para mensagens locais e recebidas de outros computadores são:

☑ **Infecções por vírus e outros alarmes**

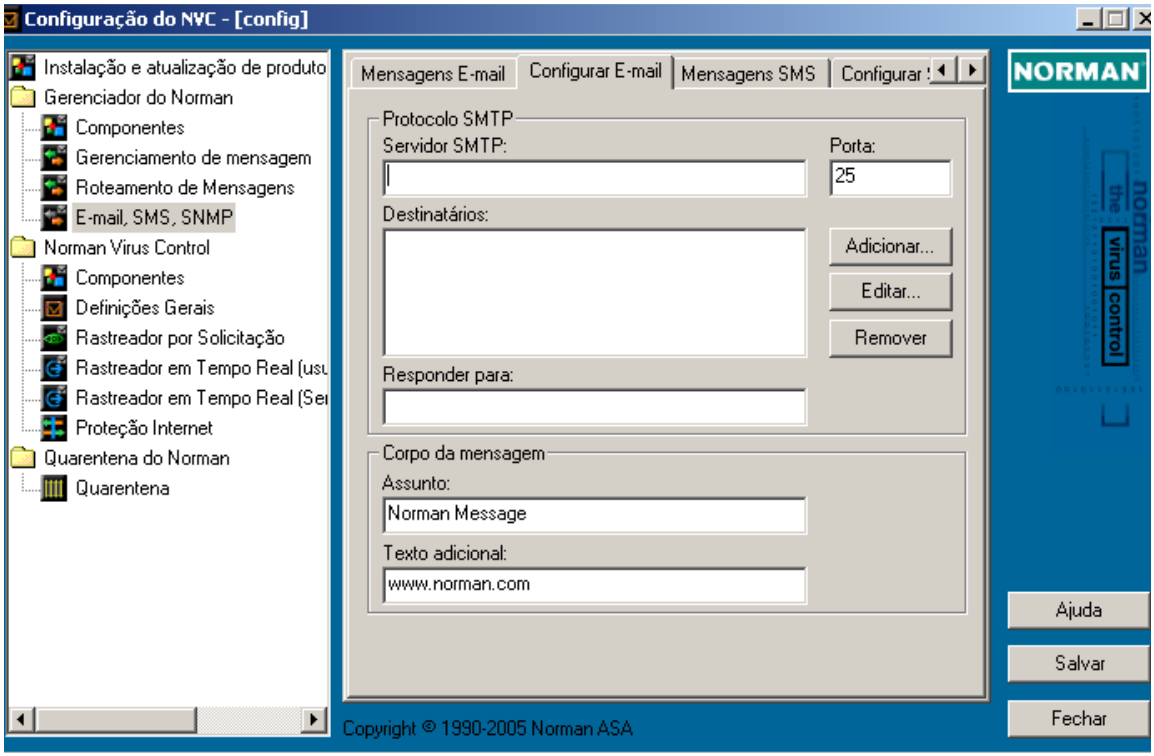
Encaminha mensagem na detecção de um vírus ou se outro código nocivo for encontrado.

☑ **Erros de instalação e programa**

Encaminha mensagem se programas instalados do NVC reportarem algum erro, e se ocorrer, durante a instalação, algum tipo de erro.

Para mensagens SMS, apenas a primeira opção é a default.

Configurar E-mail



Esses campos devem ser completados na seção *Protocolo SMTP* deste diálogo:

Servidor SMTP

The server name or the IP address for the e-mail server which can receive the SMTP message.

Porta

A porta default SMTP é a ‘25’, a qual é o valor correto a menos que você tenha especificado uma outra porta.

Destinatários

Informe o(s) endereço(s) de e-mail daquele(s) que deve(m) receber a mensagem.

- Clique em **Adicionar** e digite o endereço de email do destinatário.

- Selecione um endereço da lista e pressione **Editar** para alterá-lo.
- Selecione um endereço da lista e pressione **Remover** para excluí-lo.

Responder para

Forneça o endereço de email do recipiente ao qual pode-se responder às mensagens recebidas, por exemplo, o administrador da rede.

Na seção *Corpo da mensagem*, você pode especificar:

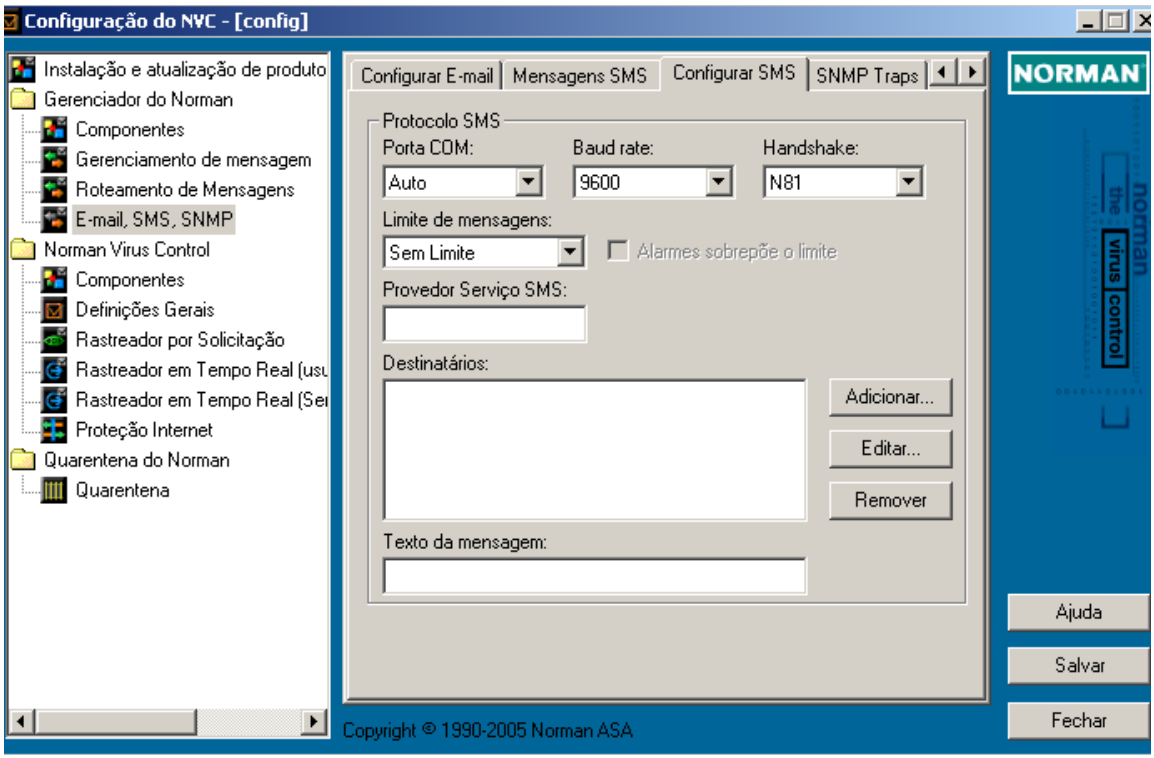
Assunto

É o título da mensagem, por exemplo, “Mensagem do NVC”. Seria bem interessante que o assunto refletisse o que disparou o respectivo alarme.

Texto adicional

Digite um texto que virá no rodapé da mensagem enviada.

Configurar SMS



Complete os seguintes campos:

Porta COM

Especifique a porta SMS com através da lista existente no menu pull-down. Esta é a porta que você especifica quando configura seu telefone celular como um modem com o driver fornecido pelo fabricante. Caso não saiba, selecione ‘Auto’ e deixe que o programa identifique a porta correta.

Baud rate

O baud rate especifica os parâmetros seriais de comunicação a serem aplicados ao modem GSM. Caso não saiba o baud rate, veja na documentação técnica de seu modem. O NVC suporta o comando Extended Hayes para SMS - “ETSI GSM 07.07”, e durante os testes encontramos que o modem recomendado é o Falcom GSM Modem (veja em: ***www.falcom.de***.)

Handshake

O formato mais comum para comunicações seriais é o **N81**. Clique no menu pull-down para mais opções.

Limite de mensagens

Você pode limitar o número de mensagens que envia durante um certo período de tempo. Se não deseja a opção default 'Sem limite', escolha alguma outra do menu pull-down:

1/15 significa uma mensagem a cada 15 minutos

1/hora significa uma mensagem a cada hora, etc.

Note que se tiver selecionado 1/15, por exemplo, *todas* as mensagens depois da primeira dentro do limite de 15 minutos serão descartadas.

☑ **Alarmes sobrepõe o limite**

Se selecionou um limite, i.e. qualquer opção exceto 'Sem limite', esta opção estará ***marcada*** por default. Isso é para ter-se certeza de que mensagens importantes (alarmes) não serão perdidas por causa de que mensagens teriam usado a cota estabelecida. Se especificou apenas '**Infecções por vírus e outros alarmes**' e esta opção estiver ativa, não haverá limite para os alarmes.

Provedor Serviço SMS

Digite o telefone de seu provedor de serviço SMS.

Destinatários

Digite o número de telefone de todos os destinatários das mensagens SMS.

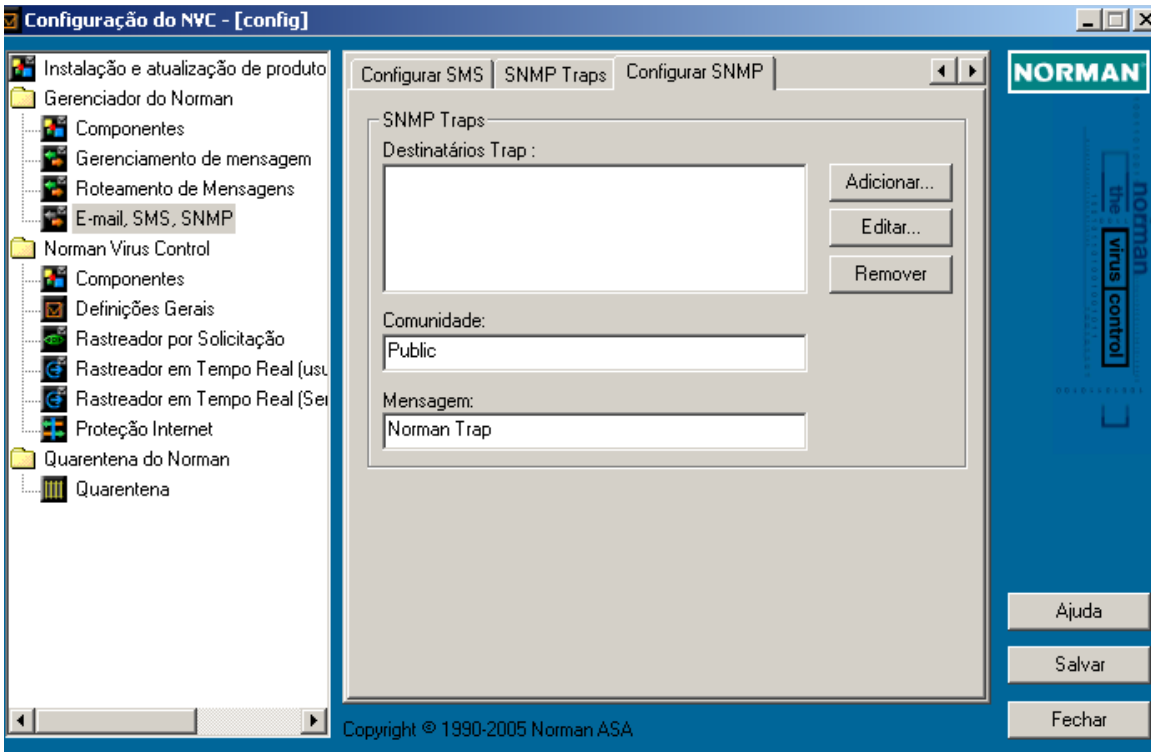
- Clique em **Adicionar** para entrar com o número de telefone do destinatário.
- Selecione um telefone da lista e clique em **Editar** para alterá-lo.
- Selecione um telefone da lista e clique em **Remover** para deletá-lo.

Texto da mensagem

Texto significando a razão da mensagem, que irá aparecer sempre que uma mensagem é enviada. Esta mensagem poderá,

por exemplo ser, “Chamar Adm”. Note que o tamanho máxima da mensagem é de 12 caracteres.

Configurar SNMP



Complete esses campos para ativar o traps SNMP:

Destinatários Trap

Informe o(s) nome(s) da(s) máquina(s) destinatária(s) ou seu(s) IP(s).

- Clique em **Adicionar** para informar o nome ou endereço do destinatário SNMP.
- Selecione um destinatário da lista e pressione em **Editar** para alterá-lo.
- Selecione um destinatário da lista e pressione em **Remover** para excluí-lo.

Note: Destinatários deverão ter o MIB do Norman instalado para assegurar-se de que o trap será decodificado corretamente.

Comunidade

Cada objeto SNMP gerenciado, como um trap, pertence a uma comunidade. A autenticação é baseada em um texto (claro, plano) do nome da comunidade, o qual você deve informar aqui. “Public” é frequentemente usado como um nome de comunidade.

Mensagem

Este campo é para informar o que vai ser enviado, por exemplo, “Algo de errado aconteceu...”.

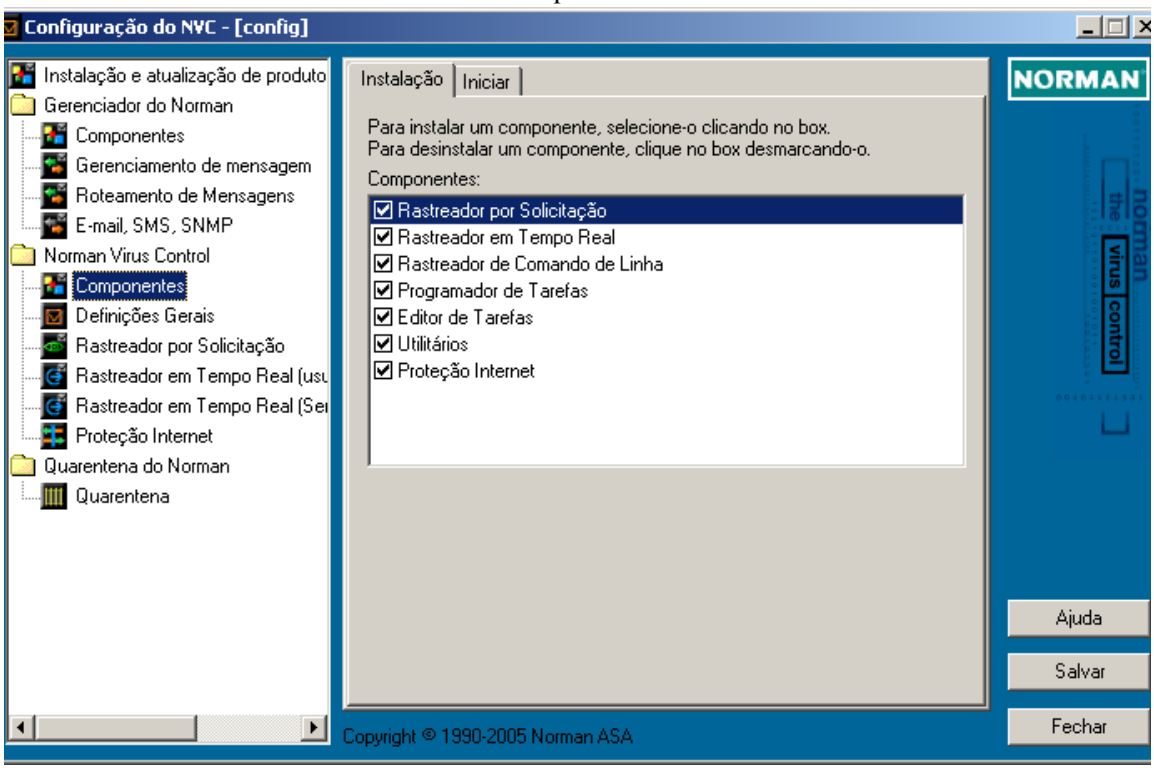
Norman Virus Control

Componentes

Um produto como o Norman Virus Control (NVC) possui muitos componentes, e a maioria dos usuários obterão benefícios de instalá-los *todos* eles.

Instalação

Perceba que a qualquer momento você poderá voltar a esta janela e adicionar/remover componentes. Por default, todos eles são selecionados quando o NVC é instalado.



☑ **Rastreador por Solicitação**

O Rastreador por Solicitação permite a você realizar periodicamente a verificação em áreas selecionadas de seu

computador. Se estiver usando o Programador de Tarefas (veja abaixo), irá necessitar da instalação do Rastreador por Solicitação.

⇨ ‘Rastreador por Solicitação’ on page 53.

☑ Rastreador em Tempo Real

O Rastreador em Tempo Real é um processo avançado que monitora atividades críticas em seu sistema. Dependendo de sua configuração, isso pode envolver acesso a arquivos e cópia/movimentação para outros drives ou diretórios.

⇨ ‘NVC em Windows Terminal Server’ on page 87.

☑ Rastreador de Comando de Linha

O Rastreador de comando de linha é uma alternativa ao rastreador baseado em GUI e oferece a possibilidade de através de arquivos “bat” executar tarefas de rastreamento. Ele é uma ótima alternativa para aqueles que são familiares neste ambiente.

⇨ ‘Iniciando o Rastreador por comando de linha’ on page 107.

☑ Programador de Tarefas

O Programador de Tarefas é uma ferramenta que é usada para executar arquivos de tarefas em horários determinados.

⇨ ‘Sobre o programador’ on page 95.

☑ Editor de Tarefas

Use esta ferramenta para criar arquivos de tarefas e para ver/alterar eventos no programador de tarefas. Um atalho de um arquivo de tarefa pode ser colocado em sua área de trabalho como um ícone, ou adicionado ao menu Iniciar como um item. Os arquivos de tarefas devem estar localizados em `...\nvc\tasks`.

Você pode colocar o OS/2 shadow para um arquivo de tarefa sempre onde quer que deseje. O arquivo real, entretanto, deve estar em `...\nvc\tasks`.

⇨ ‘Editor de Tarefas’ on page 89.

☑ Utilitários

Esta ferramenta ermite a você visualizar e editar arquivos de tarefas, arquivos em quarentena, e mostra mensagens que o sistema proprietário de mensagens gerou.

⇨ ‘Utilitários’ on page 96.

☑ Proteção Internet

O Norman Internet Protection (NIP) é um módulo desenhado para interceptar mensagens que chegam e que saem, retirando ou bloqueando todos os anexos infectados com conteúdo indesejado.

Note: O NIP é um módulo de *estação*. ***Não*** use o NIP em servidores que rodem o serviço de SMTP separado, ou em terminal servers. Em terminal servers o NIP poderá proteger ***apenas*** o primeiro usuário a logar-se, e portanto é sem utilidade neste tipo de ambiente.
O NIP é instalado como módulo default na primeira vez que fizer a instalação do NVC—tanto em servidores como em terminal servers. Nós, portanto, recomendamos que o desinstale ou pare de rodar o NIP nessas plataformas.

⇨ ‘NVC em Windows Terminal Server’ on page 87.

Iniciar

Você pode escolher quais componentes poderão ser iniciados automaticamente, i.e. serão carregados quando inciar seu computador. Alguns não são, por definição, determinados a iniciarem de forma automatica, como o Rastreador por Solicitação.

Por outro lado, o Rastreador em Tempo Real é projetado para monitorar o seu sistema em tempo real, e por isso é por default selecionado a ser carregado.

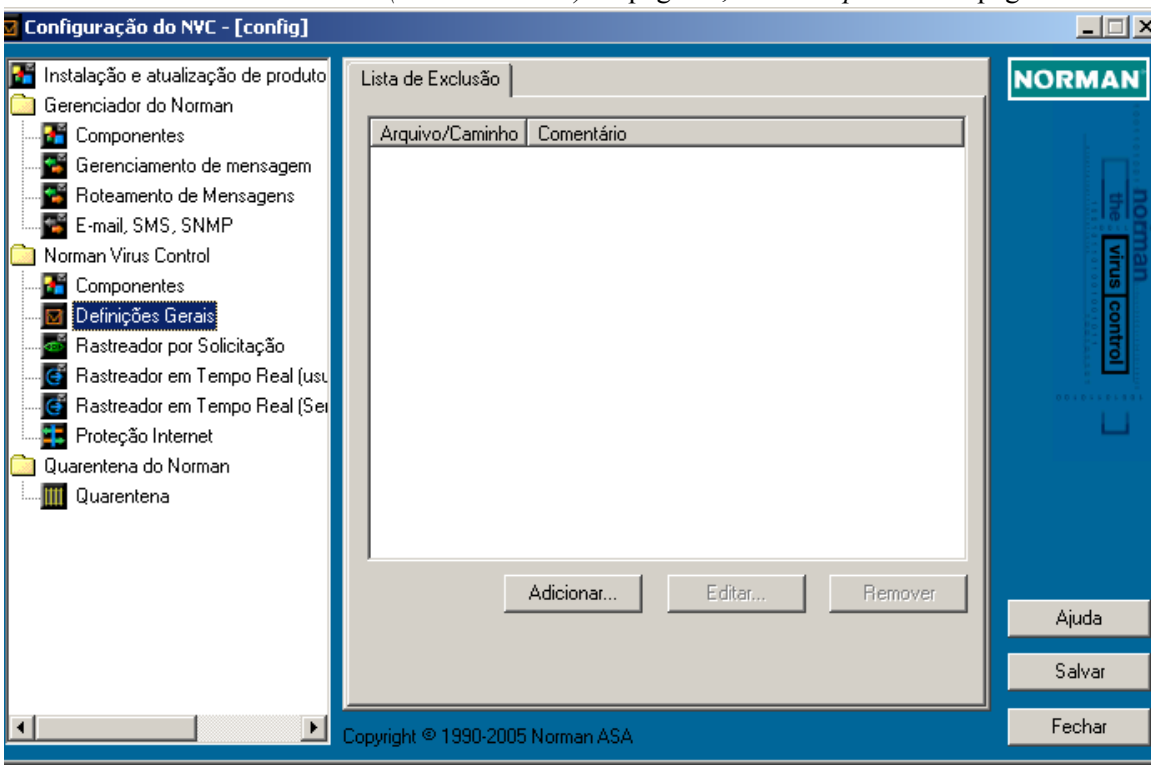
Você pode também escolher o Programador de Tarefas para ser automaticamente carregado, assim como o NIP - Proteção Internet.

Sempre que fizer uma alteração em um componente, deverá pressionar **Salvar** para ativar a mudança. O componente

permanecerá selecionado/deselecionado até que de forma manual você altere e clique em **Salvar** novamente.

Definições Gerais

Definições gerais afetam antes de tudo o tratamento de malware, e esse módulo é consequentemente um suplemento dos módulos de rastreamento *por Solicitação* na page 53, *em Tempo Real (usuários locais)* na page 61, e *em Tempo Real* na page 61.



Lista de Exclusão

Note well: Listas de exclusão devem ser manuseadas com extremo cuidado, na medida em que representam um risco potencial de segurança. Nós recomendamos que rastreie manualmente a lista de exclusão (usando o rastreador por solicitação) regularmente, e também

inclua esses arquivos ou áreas em rastreamentos programados.

Especifique arquivos, diretórios, ou drives inteiros os quais não deseja que o NVC verifique. Siga os passos abaixo para excluir itens de serem rastreados:

1. Clique em **Adicionar** informe o arquivo, diretório, ou letra do drive. Você também pode usar o botão " browse " na janela para selecionar o objeto desejado. Wildcards ('*' e '?') são aceitos.

   Exemplos:

   `c:\dir`

   Exclui todos os arquivos no diretório, incluindo subdiretórios

   `*.xyz`

   Exclui todos os arquivos com extensão .xyz

   `c:\dir\*.xyz`

   Exclui todos os arquivos com a extensão dentro do diretório.

   `example.exe`

   Exclui o arquivo especificado independente de onde ele se encontre.

   `c:\winnt\system32\xyz.sys`

   Exclui este arquivo em particular.

Note: ***NÃO*** use apostrofes (" or ') quando especificar os itens para exclusão.

2. Use o campo **Comentários** para uma explanação opcional das razões pelas quais o(s) objeto(s) foram excluídos. Com isso fica bem mais fácil determinar, quando de uma revisão periódica nos itens, se ainda existe ou não razão para que aquele item lá esteja.
3. Para alterar um item existente, selecione-o e pressione o botão **Editar** ou **Remover**.
4. Clique em **Salvar** quando terminar.

Rastreador por Solicitação

O propósito do Rastreador por Solicitação é a de fazer verificações periódicas em áreas selecionadas de seu sistema. Você pode iniciar i Rastreador por Solicitação de diferentes formas:

1. Coloque o cursor em qualquer objeto do sistema, por exemplo no Windows Explorer, clique com o lado direito do mouse e seleciono o NVC do menu.

⇨ ‘Rastreamento com o lado direito do mouse’ on page 60.

2. Selecione o Editor de Tarefas do menu do Norman em sua barra de tarefas e programe o rastreador por solicitação para ser executado em um horário específico.

⇨ ‘Editor de Tarefas’ on page 89.

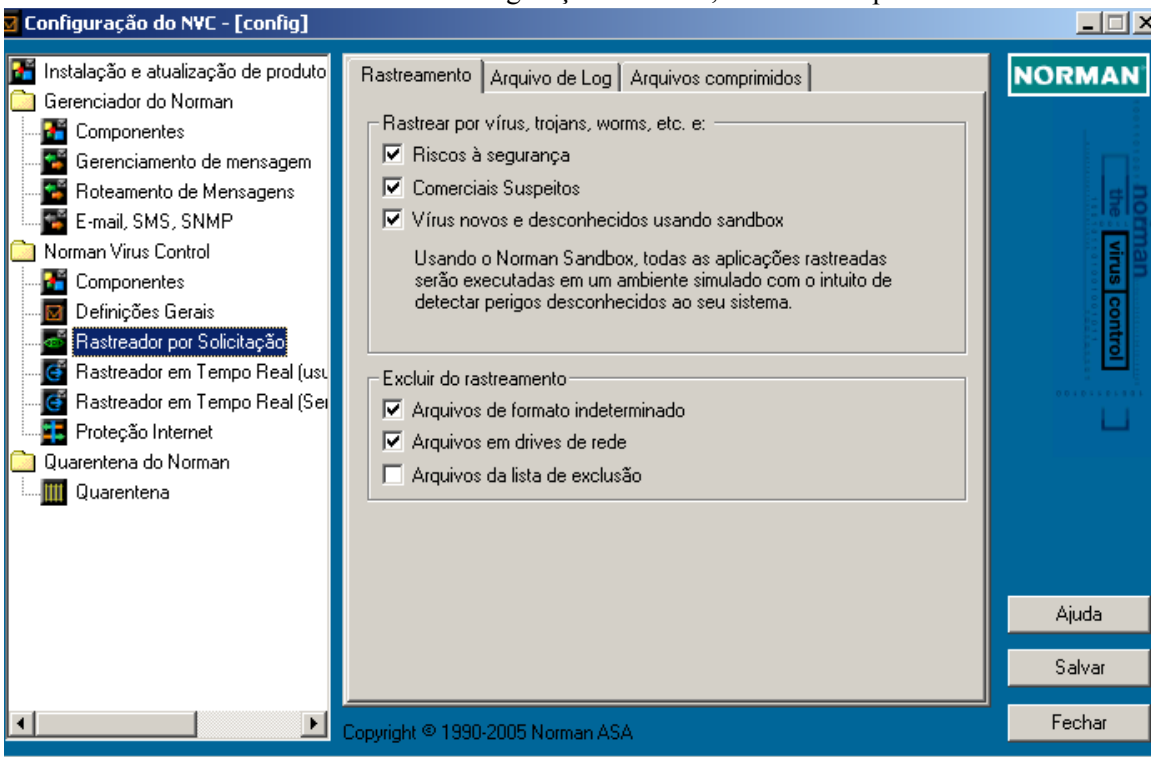
3. Use os atalhos do menu do Norman; **Rastrear disquete** ou **Rastrear disco rígido**.

⇨ ‘Atalho para os módulos e rastreamento do NVC’ on page 14.

Rastreamento

Veja também o diálogo ‘Definições Gerais’ on page 51 para configuração básica do Rastreador por Solicitação. Essas configurações são as suas primeiras opções de rastreamento, e aquelas que serão usadas se você escolher o valor default nesta janela.

Se você tiver uma necessidade temporária de rastreamento com uma configuração diferente, essa aba lhe permitirá fazê-lo.



Rastrear por víirus, trojans, worms, etc., e:

☑ Riscos à segurança

Esta opção instrui ao NVC para rastrear objetos que representam um possível risco a segurança. Alguns administradores instalam programas tais como quebradores de senha e ferramentas de administração remota que são perfeitamente legais e úteis também. Entretanto, a falta de atributos de segurança em algumas dessas ferramentas podem expor as máquinas a usuários e crackers não autorizados. O NVC detecta a atividade deste tipo de ferramenta e o avisará de potenciais riscos à segurança. Esses avisos reportarão o nome do programa, e então você poderá decidir se ele é ou não legítimo, ou se é realmente um programa não autorizado que disparou o alarme.

☑ **Comerciais suspeitos**

Às vezes, programas indesejados estão anexados a outros programas os quais baixamos da Internet para, por exemplo, testes de avaliação. Eles não lhe informam sobre a presença deles (é claro), e quando você desinstala o programa original, o rograma oculto ainda assim se mantém instalado em seu computador. Ele é dificil de se encontrar e não possui nenhum tipo de procedimento desinstalador. Em intervalos randômicos, esses programas se logon na Internet e baixam por eles mesmos comerciais. Eles não são nocivos como os tradicionais vírus, mas são incômodos e geram tráfego desnecessário na rede.O NVC ode detectar e remover esse tipo de programa. Perceba que, talvez, um programa gratuito que tenha baixado acabe por não funcionar tendo em vista a atitude do NVC, quando essa opção estiver habilitada.

☑ **Vírus novos e desconhecidos usando Sandbox,**

O NVC emprega sua funcionalidade chamada de Sandbox para detectar vírus novos e desconhecidos. Selecione esta oção se deseja que o NVC procure pelas variantes de novos vírus. O sandbox estpa particularmente preparado para encontrar novos worms e vírus do tipo email-, network- e ponto-a-ponto, e também reagirá a ameaças de segurança desconhecidas. quando um novo pedaço de código nocivo é encontrado, o administrador do sistema é avisado, recebendo uma mensagem através do sistema de mensagens do NVC, o qual estará listando fatos vitais. (Veja page 116 para um exemplo.)

Quando esta oção está selecionada, o tempo de rastreamento irá crescer, porém a performance do sistema não será afetada de forma considerável. Para maiores informações sobre o sandbox, veja o ‘Apêndice A - Sandbox’ on page 114.

Excluir do rastreamento

Você pode querer aumentar a velocidade de rastreamento excluindo alguns arquivos do processo. Atenção para o fato de que a exclusão de alguns arquivos ou áreas de serem verificados é uma decisão que afeta a sua segurança.

☑ **Arquivos de formato indeterminado**

Selecione esta oção para instruir ao NVC para ignorar arquivos de formato indeterminado. Tais arquivos podem ser arquivos danificados, ou arquivos com um formato desconhecido.

☐ **Arquivos em drives de rede**

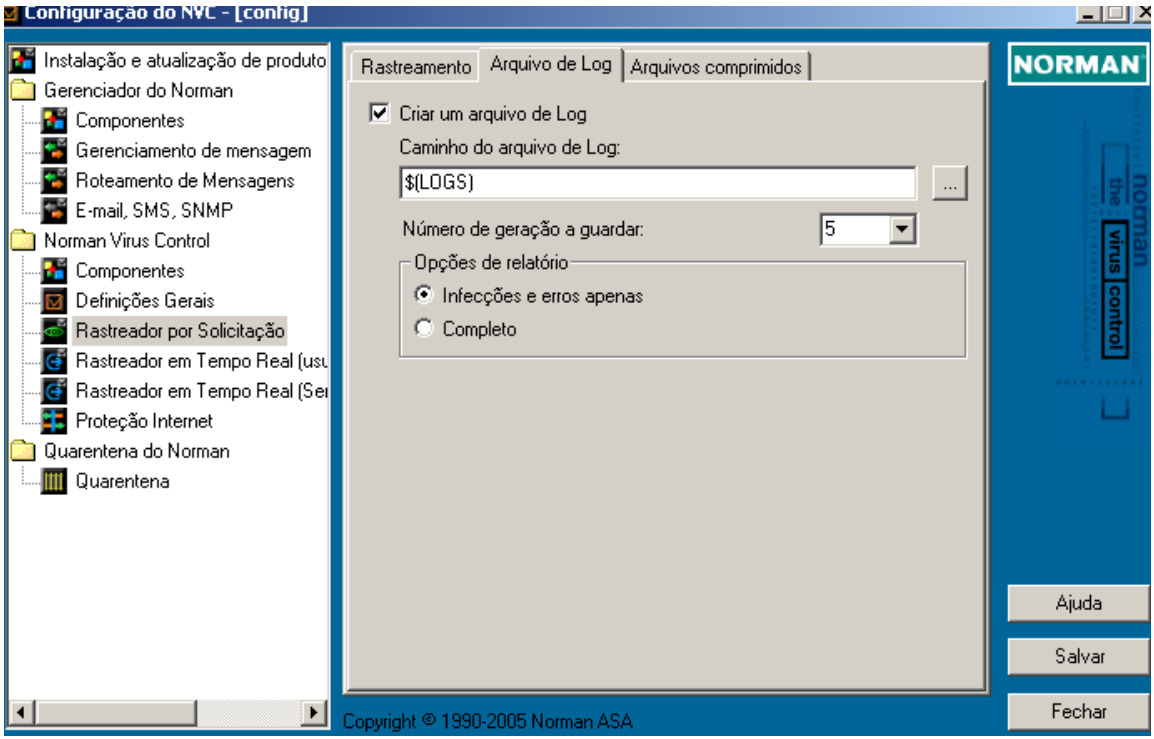
Em redes, você pode não permitir a todos os usuários a rastrear arquivos no servidor. Selecione esta oção se você apenas permitir o rastreamento de arquivos localizados localmentena estação.

☐ **Arquivos da lista de exclusão**

Selecione esta oção se deseja ativar a lista de exclusão. Não recomendamos que esta opção seja selecionada em função de que arquivos constantes na lista devem ser rastreados regularmente.

Arquivo de Log

Por default, o NVC gera um arquivo de log quando você realiza um rastreamento manual. O arquivo de log possui uma localização e nome default, e você pode escolher entre um relatório detalhado ou um que contenha apenas os erros e as infecções encontradas.



☑ Criar um arquivo de log

Cria um arquivo de log sempre que você executar o rastreamento por solicitação. Se estiver desmarcado, nenhum arquivo de log será criado na execução do rastreamento por solicitação.

Caminho do arquivo de Log:

O caminho default para o arquivo de log é `c:\norman\logs`. Clique no botão de browse para especificar um novo caminho.

Número de geração a guardar :

Se você deixar a opção default no valor de 5, o NVC irá sobrepor o arquivo mais velho quando o de número 6 for gerado. O primeiro arquivo tem o nome de `nvc00000.log`, o segundo de `nvc00001.log` etc. Similarmente, se você "guardar" 10 gerações, o primeiro arquivo será sobregarvado depois que o `nvc00010.log` for gerado.

Opções de relatório

⊙ **Infecções e erros apenas**

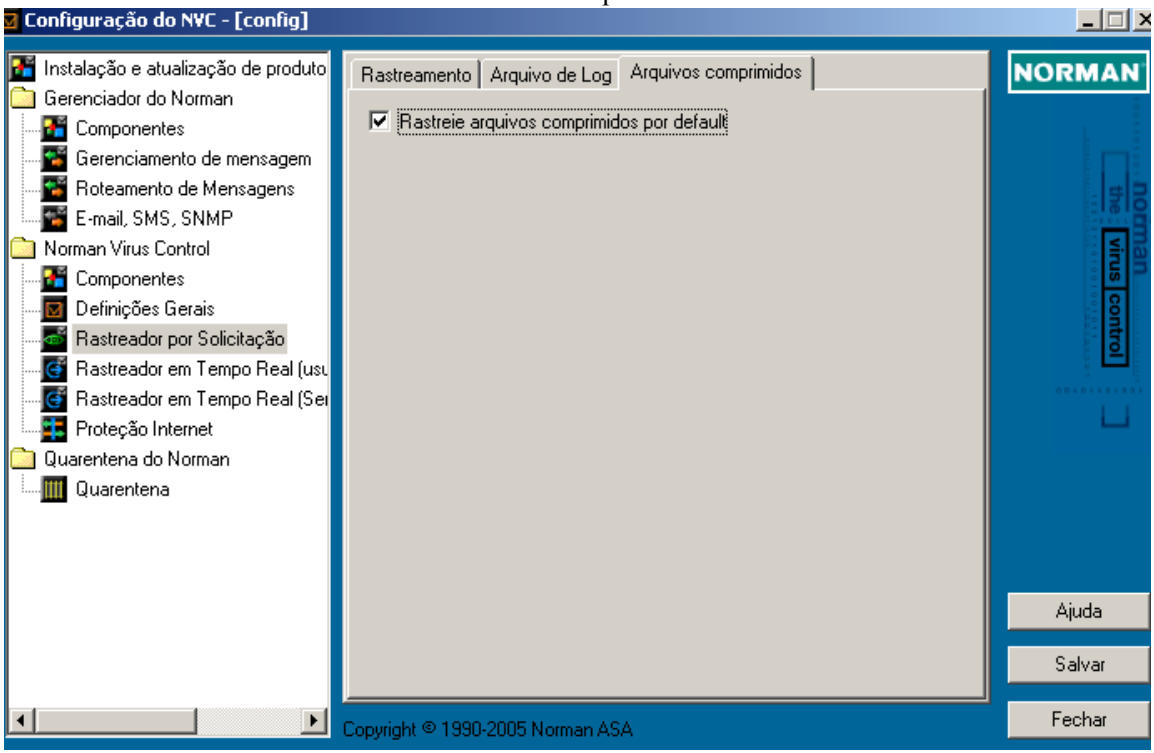
Esta é a opção defautl a qual apresenta um sumário da área que foi rastreada incluindo o tempo de rastreamento e o número de arquivos verificados, detalhes de possíveis infecções e erros de programa, versão do rastreador, e as datas dos arquivos de definição dos vírus.

O Completo

Um relatório completo fornece um descrição detalhada, especificando cada arquivo que foi rastreador, o tempo de rastreamento por arquivo, status, etc.

Arquivos comprimidos

Arquivos comprimidos são às vezes grandes e podem conter um alto número de arquivos.



☑ **Rastreie arquivos comprimidos por default**

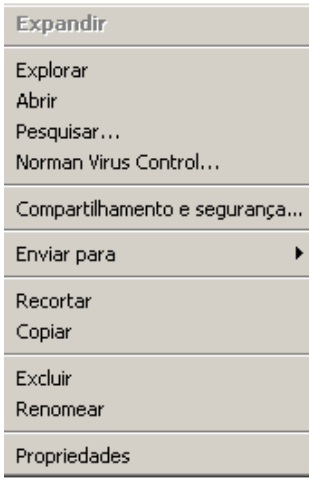
O NVC está configurado para sempre rastrear arquivos comprimidos.

Arquivos infectados em arquivos comprimidos

Se um arquivo infectado for encontrado dentro de um arquivo comprimido, o NVC tentará repará-lo primeiro. Caso não seje possível, o arquivo infectado é deletado do arquivo comprimido, e o original é colocado em quarentena.

O Rastreador por solicitação agirá de acordo com as opções de quarentena especificados no módulo **Quarentena**.

Rastreamento com o lado direito do mouse



Uma maneira fácil de se chamar o Rastreador por Solicitação é o uso da funcionalidade do clique com o lado direito do mouse. Selecione uma ou mais áreas de seu sistema e clique com o lado direito do mouse para inciar o rastreador: Ele tem o seu prório nome no menu que se abre quando coloca o cursor em algum objeto tais como discos, diretórios, arquivos etc e se clica com o lado direito do mouse.
Muitos usuários consideram um rastreamento contra vírus um mal necessário. Acreditamos que quanto mais fácil é o rastreamento, mais vezes ele é realizado. O Rastreador por solicitação não requer duplo-clique em um ícone ou a execução de um arquivo executável. Você simplesmente seleciona a área (ou objeto) que deseja rastrear de seu Windows Explorer ou desktop do OS/2, por exemplo, e depois *Norman Virus Control* do menu.

O rastreador do lado direito usará as configurações que você especificou em ‘Rastreador por Solicitação’ on page 53.

O rastreador pode detectar e remover todos os tipos de vírus de forma automatica, com exceção para os vírus do setor de boot nos discos rígidos.

⇨ ‘Limpando Arquivos infectados’ on page 107.

Diagnóstico

Quando o Rastreador por Solicitação tiver completado a sua tarefa, todas as informações relevantes irão aparecer na janela do diálogo. Existem entradas separadas para arquivos infectados e para arquivos que não puderam ser rastreados. O campo de nome ***Diagnóstico*** o avisa do porque o NVC não pode rastrear um arquivo em particular. A razão mais comum é que o mesmo esteja danificado. Um arquivo “danificado” não é

necessariamente inútil para o usuário, mas o NVC não consegue reconhecê-lo como um formato conhecido e consequentemente não o rastreia. Se alguma outra, menos prováveis situações ocorrerem, você será informado sobre a razão pela qual o arquivo não pode ser rastreado. O arquivo de log forncerá maiores informações.

Rastreador em Tempo Real

Rastreamento em Temo Real envolve um constante monitoramento dos arquivos de sistema. Para uma aplicação de antivírus, é imperativo a detecção e bloqueio de um vírus antes dele ser ativado. No processo de rastreamento em tempo real, o NVC está se comunicando com o sistema operacional em baixo nível que propicia ao rastreador "ver" todas as atividades no sistema. Este processo dá ao NVC uma vantagem contra os vírus e permite então uma imediata ação.

Sempre que um arquivo for acessado em uma operação de leitura/escrita ou um programa for executado, o rastreador em tempo real é notificado e verifica o arquivo "on-the-fly" (sem interrupção), se assim estiver configurado.

Da mesma forma que o Rastreador por Solicitaçao, o Rastreador em Temo Real do NVC detecta e repara todos os tipos de vírus. Sempre que possível, um arquivo infectado é reparado antes de ser utilizado por uma aplicação. Caso o reparo falhe, o acesso é negado ao mesmo.

⇨ 'Limpando Arquivos infectados' on page 107.

Rastreador em Tempo Real em Windows NT/2000/XP/2003

Para essas plataformas, o rastreador em tempo real está dividido em dois diferentes módulos; ***Usuários locais*** e ***Serviços e usuários remotos***. Sob circunstâncias normais, uma estação roda no modo 'Usuários locais', ao passo que um servidor roda no modo 'Serviços e usuários remotos'. Em qualquer caso, você deve configurar ambos os módulos para cobrir as diferentes formas que o Windows NT/2000/XP/2003 pode atuar. Estas são

as formas com as quais as funções podem ser entendidas no que tange ao rastreamento no NVC:

Usuários locais:

Controle de vírus para um usuário logado, o qual inclui tudo que o usuário faz na máquina. Caso o susário se “desloge” (dê um log off) ou a máquina atue como um servidor, o modo ‘Serviços e usuários remotos’ entra em açao e se faz aplicar.

Serviços e usuários remotos:

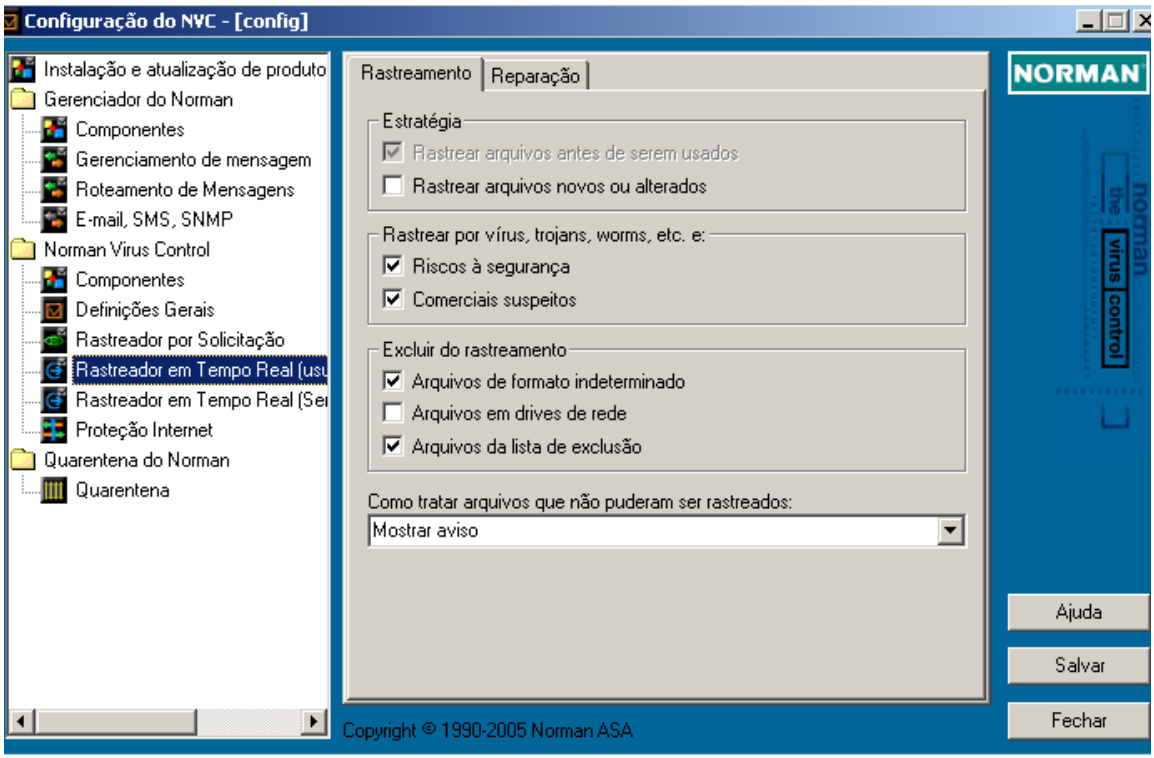
São todas as outras atividades que acontecem em uma máquina logada, tal como acesso de outras máquinas aos diretórios que estão compartilhados. O modo ‘Serviços e usuários remotos’ se aplica a qualquer máquina NT/2000/XP/2003 que não esteja com um usuário logado.

O cenário típico onde o modo ‘Serviços e usuários remotos’ tem lugar é um servidor. Entretanto, se alguém fisicamente se loga nele, o modo ‘Usuários locais’ se aplica.

Sobre Rastreador em Temo Real em Windows 95/98/Me

Diferente das instalações em Windows NT/2000/XP/2003, o rastreador em tempo real em Windows 95/98/Me consiste apenas de um módulo. Por default este módulo rastreará os arquivos no momento em que o usuário acessá-los. Na aba de configuração para este módulo, você poderá alterar o modo em que o rastreador se comporta— como por exemplo, quais operações monitorar, quais arquivos excluir do rastreamento, e como se comportar quando vírus ou outros malware forem emcontrados.

Rastreamento



Estratégia

(Aplica-se a Windows 95/98/Me e módulo 'Usuários locais' em Windows NT/2000/XP/2003 and OS/2)

Nesta seção você seleciona se quer rastrear os arquivos em ambas as situações, antes de serem usados e quando novos arquivos são criados ou quando arquivos existentes são modificados. Em outras palavras, você seleciona a estratégia para o rastreamento em tempo real ter lugar quando um usuário estiver fisicamente logado no computador.

Pense nas opções como em um ambiente de 'estação'.

☑ **Rastrear arquivos antes de serem usados**

Esta oção instrui ao Rastreador em Temo Real a verificar os arquivos que são abertos para leitura/execução e é mandatório por razões de segurança.

Exemplo: Quando você abre um arquivo de um disquete, um documento de seu disco rígido, ou um anexo de seu emails, o Rastreador em Tempo Real rastreará o arquivo de forma transparente (on-the-fly) e tomará as atitudes se um malware for encontrado. É claro que isso irá requerer que os arquivos de definição de vírus estejam atualizados.

☐ **Rastrear arquivos novos ou alterados**

Esta opção instrui ao Rastreador em Tempo Real que rastreie os arquivos que são abertos para escrita, tais como quando se faz alterações em um documento ou novos arquivos são criados em seu disco rígido.

Em Windows NT/2000/XP/2003 o módulo 'Serviços e usuários remotos' irá prevenir outros usuários (remotos) de salvar arquivos infectados em seu computador. Para usuários locais, não recomendamos a combinação desta opção com o **Rastrear arquivos antes de serem usados**, tendo em vista que assim sendo irá afetar seriamente a performance de leitura/escrita das aplicações.

Entretanto, nós recomendamos selecionar esta opção em clientes Windows 95/98/Me que possuam compartilhamento de arquivos e/ou impressoras habilitados.

Estratégia

(Se aplica apenas em máquinas com Windows NT/2000/XP/ 2003 e OS/2)

Neste módulo você seleciona se deseja que os arquivos sejam rastreados antes de serem usados e/ou quando novos arquivos são criados, ou quando arquivos existentes são alterados. Em outras palavras, seleciona a estratégia para o rastreamento em tempo real que irá se alicar quando outros computadores escrevem arquivos em seu micro/servidor.

Pense nas opções como em um ambiente de 'servidor'.

☐ **Rastrear arquivos antes de serem usados**

Esta ação instrui ao Rastreador em Temo Real a verificar os arquivos que são abertos para leitura/execução.

Exemplo: Se arquivos em servidor compartilhado (onde esta ação está marcada) são abertos de uma estação, os arquivos são rastreados antes dos usuários poderem acessá-los.

Entretanto, o tempo de rastreamento aumenta significativamente quando esta opção estiver selecionada. Você deve portanto não selecionar esta ação em servidores a menos que esteja vivendo uma forte infecção em sua rede.

☑ **Rastrear arquivos novos ou alterados**

Esta opção instrui ao Rastreador em Tempo Real para rastrear arquivos que são abertos para escrita, por exemplo quando usuários em uma rede salvam seus trabalhos ou arquivos criados no servidor.

A opção **Rastrear arquivos novos ou alterados** é selecionada por default. Não recomendamos que você combine esta opção com **Rastrear arquivos antes de serem usados** a menos que esteja experimentando uma séria infecção em sua rede, tendo em vista que isso afeta significativamente a sua performance.

Importante: Mais especificamente, rastreamento na escrita significa que arquivos novos ou alterados são verificados no fechamento. Suponha que vcoê tenha um computador cliente não protegido, que está infectado com um vírus que se espalha através de compartilhamento em redes. Sempre que esse vírus infectar um arquivo no servidor, onde o Rastreador em Tempo Real está configurado para rastrear arquivos novos ou alterados, o Rastreador em Temo Real detecta e remove o vírus. Infelizmente, a detecção e remoção com rastreadores tradicionais acontece *depois* da real infecção ocorrer. Para vírus como o VBS/Loveletter, isso significa que o vírus pode jogar fora muitos arquivos em seu caminho. De qualquer forma, arquivos infectados serão postos em quarentena e estarão portanto indisponíveis para usuários da rede re-ativarem a infecção nela.

Rastrear por vírus, trojans, worms, etc. e

(Aplicado em todas as plataformas suportadas)

O NVC procura por vírus, trojans, worms, e outros códigos nocivos ou programas indesejados que podem danificar o seu PC.

Além disso, você pode solicitar ao NVC que rastreie por:

☑ **Riscos à segurança**

Esta opção instrui ao NVC para rastrear objetos que representam um possível risco a segurança. Alguns administradores instalam programas tais como quebradores de senha e ferramentas de administração remota que são perfeitamente legais e úteis também. Entretanto, a falta de atributos de segurança em algumas dessas ferramentas podem expor as máquinas a usuários e crackers não autorizados. O NVC detecta a atividade deste tipo de ferramenta e o avisará de potenciais riscos à segurança. Esses avisos reportarão o nome do programa, e então você poderá decidir se ele é ou não legítimo, ou se é realmente um programa não autorizado que disparou o alarme.

☑ **Comerciais suspeitos**

Às vezes, programas indesejados estão anexados a outros programas os quais baixamos da Internet para, por exemplo, testes de avaliação. Eles não lhe informam sobre a presença deles (é claro), e quando você desinstala o programa original, o rograma oculto ainda assim se mantém instalado em seu computador. Ele é dificil de se encontrar e não possui nenhum tipo de procedimento desinstalador. Em intervalos randômicos, esses programas se logon na Internet e baixam por eles mesmos comerciais. Eles não são nocivos como os tradicionais vírus, mas são incômodos e geram tráfego desnecessário na rede.O NVC ode detectar e remover esse tipo de programa. Perceba que, talvez, um programa gratuito que tenha baixado acabe por não funcionar tendo em vista a atitude do NVC, quando essa opção estiver habilitada.

☑ **Vírus novos e desconhecidos usando Sandbox,**

O NVC emprega sua funcionalidade chamada de Sandbox para detectar vírus novos e desconhecidos. Selecione esta oção se deseja que o NVC procure pelas variantes de novos vírus. O sandbox estpa particularmente preparado para encontrar novos worms e vírus do tipo email-, network- e ponto-a-ponto, e também reagirá a ameaças de segurança desconhecidas. quando

um novo pedaço de código nocivo é encontrado, o administrador do sistema é avisado, recebendo uma mensagem através do sistema de mensagens do NVC, o qual estará listando fatos vitais. (Veja page 116 para um exemplo.)

Selecionando esta opção estamos primeiramente obtendo uma proteção adicional contra worms de rede, i.e. onde a máquina A está protegida e uma tentativa é feita para copiar um código viral em um recurso compartilhado na máquina A da máquina B.

Note: A opção Sandbox **não** fornece uma maior proteção para operações feitas por um usuário logado na máquina A. Tais operações são rastreadas usando-se o arquivo de assinaturas de virus e a tradicional procura heurística.

Quando esta oção está selecionada, o tempo de rastreamento irá crescer, porém a performance do sistema não será afetada de forma considerável. Para maiores informações sobre o sandbox, veja o ‘Apêndice A - Sandbox’ on page 114.

Excluir do rastreamento

Você pode querer aumentar a velocidade de rastreamento excluindo alguns arquivos do processo. Atenção para o fato de que a exclusão de alguns arquivos ou áreas de serem verificados é uma decisão que afeta a sua segurança.

☑ **Arquivos de formato indeterminado**

Selecione esta oção para instruir ao NVC para ignorar arquivos de formato indeterminado. Tais arquivos podem ser arquivos danificados, ou arquivos com um formato desconhecido.

☐ **Arquivos em drives de rede**

Em redes, você pode não permitir a todos os usuários a rastrear arquivos no servidor. Selecione esta oção se você apenas permitir o rastreamento de arquivos localizados localmentena estação.

☑ **Arquivos da lista de exclusão**

Selecione esta oção se deseja ativar a lista de exclusão. Não recomendamos que esta opção seja selecionada em função de que arquivos constantes na lista devem ser rastreados regularmente.

Como tratar arquivos que não puderam ser rastreados

(Aplicado em Windows 95/98/Me e no módulo 'Usuários locais' em Windows NT/2000/XP/2003 e OS/2)

Em algumas situações o NVC não consegue rastrear um arquivo. Exemplos são arquivos do Word protegidos por senhas, arquivos dannificados, ou quando erros internos de sistema ocorrem. Temos e opções disponíveis de tratamento para esses arquivos. Escolha do menu pull-down um deles:

Ignorar

O NVC ignorará os arquivos.

Mostrar aviso

O NVC avisa quando você acessa um arquivo de que ele não pôde ser rastreado. Você pode por sua conta e risco seguir adiante.

Avisar e não permitir acesso

O NVC avisa que o acesso foi bloqueado porque o arquivo não pode ser rastreado.

Modo Rastreador em Tempo Real (Não aplicável ao Windows)

☐ **Usar modo de rastreamento apenas para serviços e usuários remotos**

Quando o Rastreador em Tempo Real está no modo 'Usuários locais', diálogos que precisam ser respondidos aparecem com regularidade. Se esta oção estiver marcada, esses diálogos não aparecerão no servidor e as ações de configuração do modo de rastreamento 'Serviços e usuários remotos' serão aplicadas.

Esta opção é válida apenas para redes com servidores OS/2.

Para ambientes em rede:

O campo Acesso na parte inferior de cada uma das abas é invisível a menos que você tenha direitos de administrador . O administrador do sistema decide o que deverá ser visível e/ou configurável das estações. O usuário médio poderá portanto ver todas ou algumas das abas, mas não necessáriamente poderá alterá-las.

Reparação

Quando vírus, trojans, worms, ou outro malware são detectados, você pode selecionar como o NVC deverá tratá-los.

Não permitir acesso

Se tentar executar um programa infectado, o acesso é bloqueado e documentos infectados também o serão.

Note: Para Rastreador em Tempo Real (Serviços e usuários remotos), esta oção é apenas relevante se tiver selecionado **Rastrear arquivos antes de serem usados** como estratégia de rastreamento. Em outras palavras, se estiver usando as opções default, você **não** deve selecionar esta opção.

Remover

O NVC tentará remover o vírus do arquivo infectado. Selecione esta oção para instruir ao NVC para repará-lo automaticamente. O NVC pode remover a maioria dos vírus de forma transparente (on-the-fly), exceto o vírus de setor de boot. O NVC irá sempre avisar para o usuário tomar alguma atitude antes de remover qualquer vírus de setor de boot. Atente para o fato de que um arquivo pode ser deletado se contiver apenas o código nocivo, nada mais.

Perguntar o que fazer

Se você não deseja que a remoção seja feita automaticamente, tampouco que tenha o seu acesso bloqueado ao arquivo infectado, selecione esta opção. Quando você tenta abrir um arquivo infectado, receberá um aviso do incidente. No diálogo que se abrirá poderá escolher entre removê-lo ou sair.

Recomendações:

- Assegure-se de que sua instalação esteja atualizada. Essa é a melhor proteção contra ataques de vírus, e então estará habilitado a pará-los antes de que eles entrem em seu sistema.
- Instale programas antivírus em servidores de email e gateways.
- Restrinja os direitos de usuários nos compartilhamentos o máximo que puder, por exemplo configurando para

apenas leitura onde aplicável, em arquivos que não são constantemente alterados.

- Faça back up de seus arquivos regularmente.

Rastreamento em Tempo Real em redes

O NVC por default rastreará arquivos que são acessados em drives de rede. O comportamento do Rastreador em tempo Real dependerá dos direitos do usuário logado quando rastrear os arquivos localizados em drives de rede. Quando o Rastreador em Tempo Real vê um arquivo que é aberto de um drive de rede, ele o verificará na forma usual. Entretanto, não poderá repará-lo, removê-lo ou colocá-lo em quarentena no caso de estar infectado a menos que o usuário logado tenha direitos de escrita no diretório ou arquivo em questão. Mesmo assim, o acesso ao arquivo infectado será negado.

O parágrafo acima não é uma recomendação de ser menos restritivo com os privilégios dos usuários. Se um Rastreador em Tempo Real atualizado protege o seu servidor da mesma forma que as estações, não é provável que o Rastreador em Tempo Real nas estações encontrarão malware em drives de rede.

De qualquer maneira, caso ocorra, a proteção está lá.

Quando o Rastreador em Temo Real detecta vírus ou outros malware em drives de rede, ele mostrará a localização como um caminho UNC e não como drive mapeado. Muitos usuários conhecem drives de rede como X, Y, Z etc. Os popups de alertas do Rastreador em Tempo Real mostrarão por exemplo o seguinte `\\Servidor\Compartilhamento\arqinfectado` ao invés de `X:\arqinfectado`.

Rastreador em Tempo Real em rede pode ser entendido quando servidores não executem controle de vírus, simplesmente para se evitar que o mesmo arquivo seja rastreado duas vezes—uma no servidor e depois novamente quando for aberto no cliente. Como consequência do duplo rastreamento pode-se ter que os log-ons e o backup fiquem mais vagarosos. Entretanto, o administrador de sistema deve ficar com a decisão final onde segurança por um lado, e operações de rede por outro são os dois maiores fatores a serem considerados.

Você pode desativar o Rastreamento em Tempo Real de arquivos em rede marcando a opção **Arquivos em drives de rede** no item 'Excluir do rastreamento'.

Norman Internet Protection (NIP)

Note: A versão corrente do Norman Internet Protection é apenas para plataforma Windows, e *não* funcionará com OS/2.

O Norman Internet Protection (NIP) é um filtro que o protege contra vírus que se espalham através de

- Mensagens de Internet,
- news readers,

A maioria dos vírus conhecidos atualmente usa mecanismos que proporcionam a eles se espalharem através de e-mails. Estatisticamente, um entre 30 e-mails enviados durante grandes epidemias continham algum tipo de código nocivo. A necessidade de proteção contra esse tipo de situação é portanto, imperativa.

O NIP é um módulo do NVC 5 projetado para interceptar emails que chegam e que saem além de news—retirando ou bloqueando todos os anexos infectados por conteúdo indesejado.

O NIP é não só capaz de rastrear os anexos por vírus conhecidos mas também de bloquear anexos pela sua extensão, mesmo que não contenham vírus.

Como um componente integrado ao NVC 5 ele pode ser distribuído através da rede, estabelecendo assim uma outra barreira na crescente ameaça de vírus vindos do "lado de fora".

Importantes limitações:

A atual versão do NIP está melhor projetada para estações do que para servidores, principalmente porque ele não consegue rastrear servidores locais de rede. Portanto, não deverá estar habilitado em servidores.

Definições

News reader

Um **news reader** é uma aplicação que lhe permite ler mensagens postadas no Internet newsgroups assim como postar suas próprias mensagens. Navegadores populares, como o *Internet Explorer* e *Netscape* possuem seus próprios news readers, e diversos outros news readers estão disponíveis.

Winsock

Winsock—abreviatura de *Windows Socket*—é uma interface de programação e de suporte que trata de requisições de entrada e saída para aplicações de Internet no Windows. Cada versão do Windows está equipada com sua própria versão `winsock.dll`. Falando simplesmente, o Winsock é uma ponte entre programas Windows e conexões TCP/IP (Internet).

De nada vale se outros vendedores/fornecedores de versões freeware e shareware do `winsock.dll` que **não** seguem os padrões Microsoft. Cada uma dessas versões diferem entre si de forma mínima. Para o usuário ou terceiros programadores de aplicativos para Internet na plataforma Windows, dificilmente teriam benefícios.

Note: Todos os produtos Norman envolvendo `winsock.dll` estão de acordo com os padrões Microsoft.

Protocolo

Um **protocolo** é definido como um formato para transmissão de dados entre dois dispositivos. Imagine-o como uma linguagem. Preocupe-se aenas em ser usuário, por que sua máquina faz o resto suportando os protocolos relevantes quando comunicando-se com outros computadores.

A presente versão do NIP suporta os seguintes **protocolos**:

- POP3, para chegadas de e-mail
- SMTP, para saídas de e-mail
- NNTP, para newsgroups

Porta

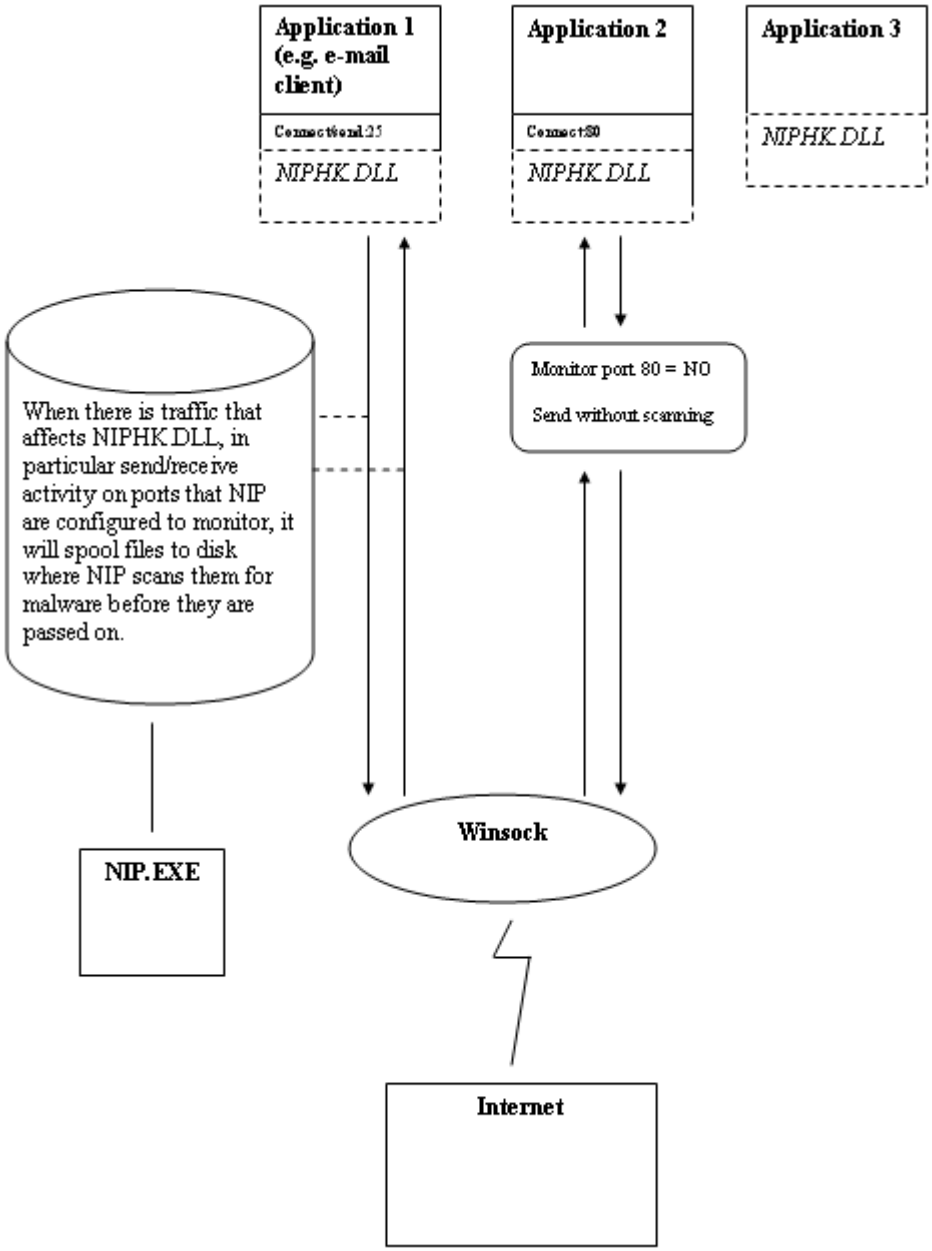
Uma porta é um “lugar de conexão lógico” na programação e especificamente — usando o protocolo TCP/IP da Internet— o modo que um programa especifica um programa servidor em particular em um computador de uma rede. Aplicações que usam o TCP/IP, como o protocolo web HTTP, tem portas com os números prédesignados. Essas portas são conhecidas como “well-known ports” (portas bem conhecidas) que foram homologadas por um comitê internacional oficial (IANA). Outro processo de aplicativos recebem números dinamicamente para cada conexão. Qundo um serviço (programa servidor) é iniciado dizemos que ele “amarra” um número de porta determinado. Se um programa cliente quer fazer uso daquele servidor, ele terá que usar aquele determinado número de porta.

Os números das portas variam de 0 até 65536. As portas de 0 até 1024 estão reservadas para uso previlegiado de certos serviços. Para o serviço HTTP, a porta 80 está definida como default e não precisa ser especificada na Uniform Resource Locator (URL).

Veja a seção ‘Avançado’ on page 82 e continuação dele para uma visão dos protocolos suportados pelo NIP e os seus correspondentes números de portas.

Como essas definições demonstram, a interconecção entre protocolos, portas e padrões representam um possível risco de “conflito de interesses”.

Como funciona



A DLL (*Dynamic Link Library*) `niphk.dll` está presente em todas as aplicações executadas e é capaz de monitorar/rastrear

todo o tráfego Winsock. O Winsock, o qual é discutido na page 72 trata das requisições de entrada/saída das aplicações Internet na plataforma Windows.

A atual versão do NIP suporta 3 protocolos: POP3 (chegada de e-mail), SMTP (saída de e-mail), e NNTP (newsgroups).

WSempre que o `niphk.dll` detecta uma operação que use qualquer desses protocolos, irá invocar o *`nip.exe`* para rastrear Digamos uma mensagem que chega com anexos na porta 110. O NIP *spools* (guarda de forma temporária) para o disco rígido onde o rastreamento terá lugar. Entretanto, caso o NIP não esteja configurado para monitorar as mensagens que chegam na porta 110, ele irá ignorar qualquer atividade naquela porta.

O NIP faz referência às portas padrões de tráfego para exercer o seu monitoramento. Se, por acaso, tiver alguma aplicação que faz uso de outras portas para o mesmo tipo de tráfego, deverá informar as mesmas na aba de configuração do NIP.

Ativar o NIP

Note: Os direitos definidos no `default.ndf` decidem quais alterações o usuário poderá fazer na instalação local.

Para instalar este módulo, vá para a aba **Instalação** na pasta do produto **Norman Virus Control|Componentes** no Editor de Configuração (ver page 32). Selecione ***Proteção Internet*** da lista e clique em **Salvar**.

Deois de alguns segundos, ***Proteção Internet*** aparece como uma entrada separada debaixo da aba **Iniciar**. Novamente, selecione-a e clique em **Salvar**.

Você precisará sair e re-iniciar o Editor de Configuração para ter acesso às opções de configuração do NIP.

Para parar o NIP, desmarque o box e clique em **Salvar**.

Rastreamento de vírus

Arquivos baixados são guardados temporariamente no disco rígido do cliente e rastreados contra vírus antes de serem disonibilizados para o usuário.

O NVC tentará limpar arquivos infectados antes de serem deletados ou postos em quarentena. Algumas vezes, limpeza

significa deleção, por exemplo, *trojans*, onde o arquivo por inteiro é o código nocivo.

Note: Uma cópia do arquivo deletado ou bloqueado é posto em quarentena por default.

Conteúdo reposto em mensagens

Quando o seu cliente de emails lhe informa de que existem novas mensagens e o NVC deleta uma delas porque está infectada, seu programa de email irá reagir como quando reporta que um email não chegou. Então o NVC irá passar sobre qualquer email que foi exposto ao processo de limpeza. Você ainda poderá ver quem originalmente enviou-lhe o email, com um texto explicativo.

Por exemplo, o NVC limpou um anexo do tipo Word antes da mensagem ser admitida pelo destinatário. No cabeçalho do corpo da mensagem poderá ler:

Norman Virus Control limpou o anexo Inventory.doc orque ele continha o virus W97M/Claud.A.

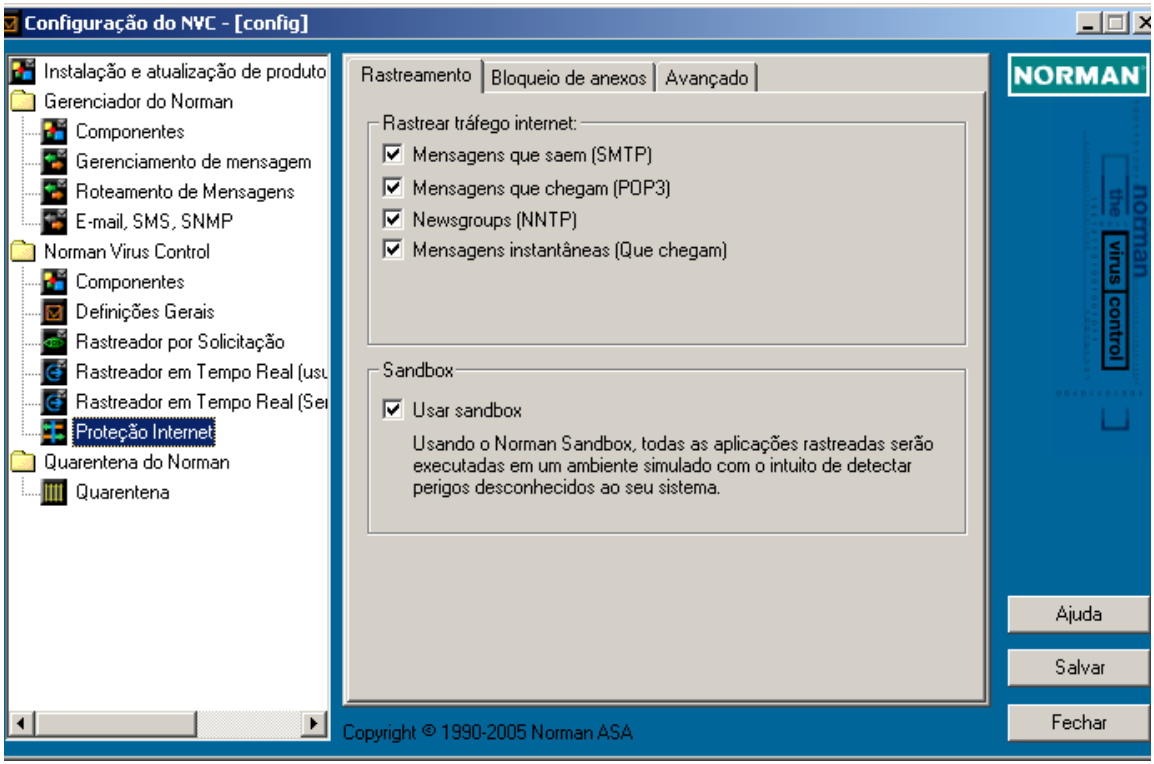
Caso outro malware for detectado, um texto similar irá aparecer.

Note: NÃO confunda essa mensagem com outros avisos de e-mails recebidos de outros produtos antivírus, dizendo que o seu computador está esalhando vírus. O texto reposto pelo NVC é simplesmente uma demosntração de que ele fez seu trabalho e que não tem nada a temer.

Configurando o NIP

O NIP é feito de de 3 abas de diálogo onde você decide quais elementos deverão ser rastreados, anexos bloqueados de forma geral ou específica, e mensagens de aviso enviadas quando vírus sejam detectados, além de definir o número das portas para os correspondentes protocolos.

Rastreamento



Selecione quais elementos deseja rastrear. Como opção default, todos estão marcados.

Rastrear tráfego Internet

☑ Mensagens que saem (SMTP)

Rastreia todas as mensagens que são enviadas de seu sistema. Se sua máquina está infectada por um malware que você não saiba, poderá sem querer enviar emails infectados para seus amigos e conhecidos profissionais, or exemplo.

☑ Mensagens que chegam (POP3)

Rastreia todas as mensagens que recebe dos outros. DE novo, mesmo o seu melhor amigo pode não saber que esteja infectado.

☑ Newsgroups (NNTP)

Rastreia o tráfego gerado entre o seu computador e os outros participantes do forum/grupo que esteja participando.

⇨ Veja ‘Definições’ on page 72 para mais detalhes sobre este assunto.

☑ Mensagens Instantâneas (Que chegam)

Rastreia os arquivos transferidos durante as sessões de mensagens instantâneas com o MSN Messenger e o Windows Messenger. Quando esta ação está selecionada, o NIP rastreará os arquivos que chegarem. Caso esteja infectado, uma mensagem pop-up irá aparecer.

Aenas a transferência de arquivos é verificada, portanto, links infectados continuam a ser uma ameaça.

Perceba que os arquivos transferidos são rastreador quando são escritos no diretório `...\Temporary Internet Files`. Se um malware for encontrado, será rovavelmente um arquivo do tipo `.tmp` posto em quarentena. Para restaurar um arquivo do tipo `.tmp` file em quarentena, selecione o arquivo desejado, escolha **Salvar como** do menu e salve-o com o nome que quiser, onde quiser.

⇨ Veja ‘Quarentena’ on page 85.

Sandbox

☑ Usar sandbox

O NVC faz uso de sua tecnologia de detecção de vírus novos e desconhecidos chamada de sandbox. Selecione esta ação se deseja que o NVC procure por novas variantes de vírus. O sandbox particularmente afinado para encontrar novos worms de email-, de rede- e ponto-a-ponto e vírus de arquivo, e também reagirá a ameaças desconhecidas de segurança. Quando um novo pedaço de código malicioso é encontrado, o administrador recebe uma mensagem através do sistema de mensagens do NVC listando fatos vitais. (veja page 116 para um exemplo.)

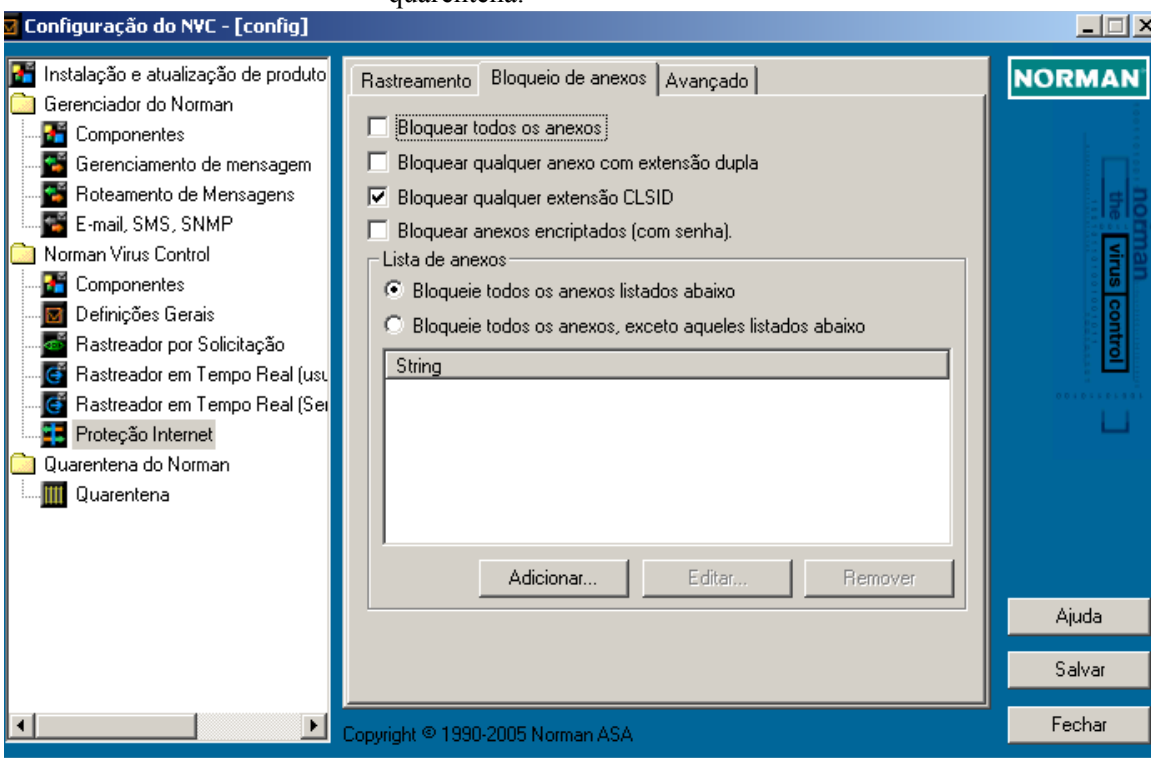
Quando essa opção é selecionada, o tempo de rastreamento aumenta, mas não a ponto de afetar de forma significativa a

performance. Para mais informações veja ‘Apêndice A - Sandbox’ on page 114.

Bloqueio de anexos

Você pode bloquear anexos fornecendo seu nome exato ou arquivos com certas extensões, por exemplo. Este atributo é particularmente útil quando worms de email estão perambulando e podem ser identificados pelo nome. Bloqueio de anexos é também muito útil para parar tipos de arquivo que não deseje receber em sua caixa postal.

Quando o NIP bloqueia um anexo, irá *movê-lo* para a área de quarentena ao invés de *deletá-lo*. Isso serve como um backup se o anexo for legítimo. Na área de quarentena ele não poderá de qualquer forma, causar nenhum mal. Por exemplo, se você tiver especificado que todos os executáveis (*.exe) deveriam ser bloqueados, saberá com segurança, que se precisar de algum deles poderá de qualquer forma restaurá-lo da área de quarentena.



☐ **Bloquear todos os anexos**

Todos os anexos são bloqueados.

☐ **Bloquear qualquer anexo com extensão dupla**

Muitos worms e vírus de e-mail usam a técnica onde uma extensão adicional é incluida, por exemplo, `<filename>.jpg.vbs`. A maioria dos clientes de email ocultarão a última extensão, e por isso o anexo parecerá ter apenas a extensão .jpg. Entretanto, esse atributo não é apenas usado pelos vírus — mas também por arquivos legítimos com nomes como `myfile.hlp.zip` e `todolist 20.dec.doc` ambos tratados como dupla extensão.

☑ **Bloquear qualquer extensão CLSID**

Alguns worms e vírus de e-mail usam a técnica de CLSID para enganar rastreadores de email e programas de bloqueio. Usam a vantagem de uma característica do Windows que faz possível que uma extensão .exe possa ser reposta por uma com {...} e então evadindo-se do bloqueio de arquivos .exe, por exemplo. Não existe razão para arquivos legítimos usarem este tipo de extensão, por isso são bloqueados por default.

☐ **Bloquear anexos encriptados (com senha)**

Dependendo das ferramentas usadas, arquivos comprimidos e encriptados são geralmente difíceis de serem rastreados, por isso, o NIP oferece a opção de estar bloqueando-os.

Lista de anexos

Use esta função para explicitar os anexos que deseja bloquear — ou permitir. Você pode informar o nome exato do arquivo, ou usar wildcard ('*') para bloquear certas extensões. Para bloquear todos os arquivos `.exe`, por exemplo, clique em **Adicionar** e digite `*.exe`. Clique em **OK**, e a entrada irá aparecer na janela que lista os objetos, onde poderá editar ou remover quando desejar.

⊙ **Bloquear todos os anexos listados abaixo**

Todos os nomes que **Adicionar** a lista são *bloqueados*. Entre com um nome específico ou use wildcard ('*') para identificar os anexos a serem bloqueados.

O **Bloquear todos os anexos, exceto aqueles listados abaixo**

Todos os nomes que **Adicionar** a lista são *aceitos*. Entre com um nome específico ou use wildcard (‘*’) para identificar os anexos a serem aceitos.

Note: É ***muito importante*** que você faça a distinção entre as duas opções com muito cuidado, pois representam dois extremos: *bloquear* todos da lista, ou *aceitar* todos da lista.

Recomendações

A lista de extensões abaixo não é definitiva, e será modificada sempre que necessário para refletir uma situação relacionada aos vírus e malware. Você pode utilizar essas recomendações se tiver selecionado ⊙ **Bloquear todos os anexos listados abaixo**.

Nível de segurança: Médio

Adicione as seguintes extensões à lista de arquivos que deseja bloquear:

*.BAT	*.CHM	*.CMD	*.COM	*.CPL
*.EXE	*.HLP	*.HTA	*.HTM	*.INF
*.JS	*.JSE	*.LNK	*.MSI	*.PIF
*.REG	*.SCR	*.SHS	*.SWF	*.VBE
*.VBS	*.WSC	*.WSH	*.URL	*.PL
*.SH	*.CLA	*.PI	*.DLL	

Nível de segurança: Alto

Selecione a opção ***Bloquear todos os anexos, exceto aqueles listados abaixo***. Se escolheu como nível de segurança o alto, você deve ter cuidado com o uso da função **Adicionar** à lista os tipos de arquivo permitidos. Dependendo do tipo que recebe de forma regular, você provavelmente tem uma boa idéia daqueles que deve colocar na lista.

Note: Lembre-se de que uma cópia do anexo bloqueado é posta em quarentena—*não* deletada—sendo portanto possível a restauração de algum que tenha sido bloqueado por engano.

Caso queira enviar um arquivo válido que consta na lista, por exemlo, digamos *.exe, com alguém conhecido, e não deseja que

o NIP o bloqueie, basta comprimi-lo no formato zip, por exemplo, e usar uma senha para tal.

String

É nesse campo que você especifica os nomes dos arquivos que devem ser bloqueados (ou permitidos). Wildcard (‘*’) pode ser usado para bloqueio de extensões. Por razões óbvias, o wildcard é apenas permitido para nomes de arquivos, i.e. `*.vbs`. Para o usuário comum, arquivos tipo `.vbs`, `.pif` ou `.lnk` não são críticos. Você deve considerar em estar bloqueando arquivos ou extensões do tipo `.exe`, `.com` e `.bat` na medida em que também representam um risco em potencial para infecções.

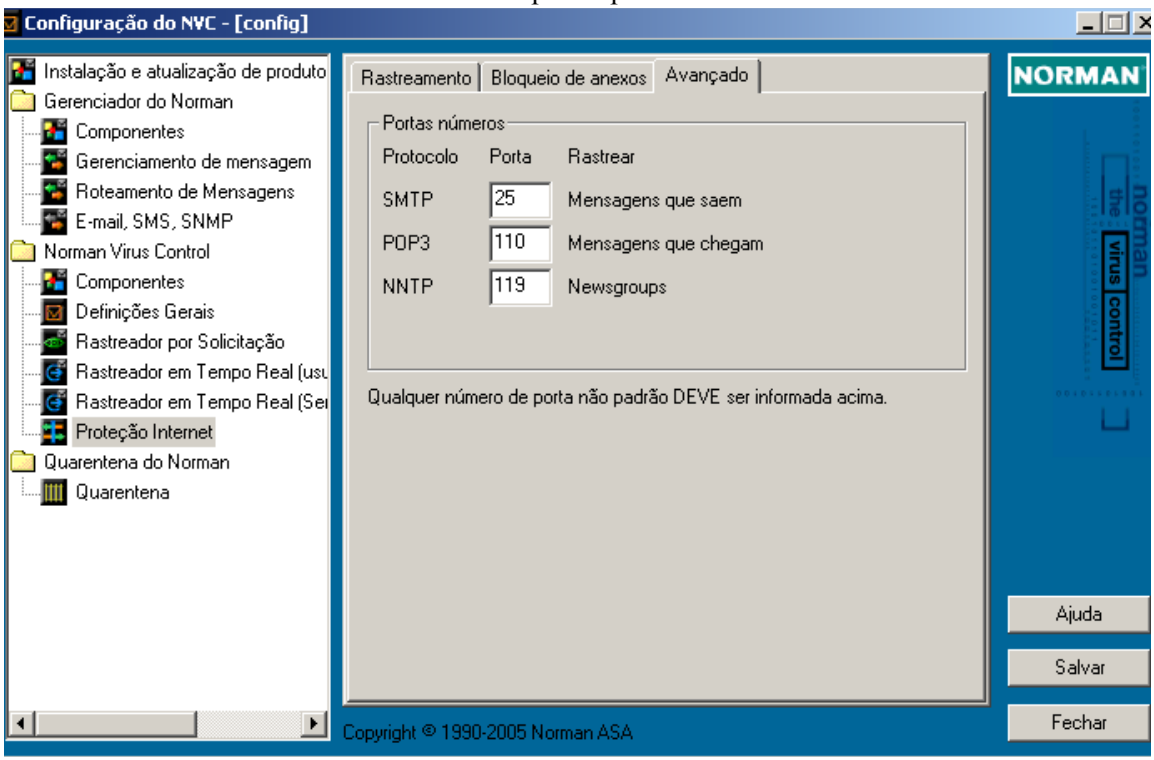
Aqui você também pode usar nomes para bloquear anexos específicos com nomes os quais você conhece que contenham vírus, como por exemplo, `AnnaKournikova.jpg.vbs`. Dessa forma, poderá bloqueá-los até que sejam incluídos nos arquivos de definição de vírus, por exemplo.

Note: O Outlook 2002 também possui um atributo de bloqueio de anexo, o qual será aplicado ***depois*** que tiver passado pelo NIP.

Avançado

Dentre os numerosos protocolos de comunicação entre computadores, existem alguns que são vitais para o uso da

Internet. Por razões de padronização, esses protocolos tem números de portas pré-determinado.



Portas números

No diálogo de **Rastreamento** na página 77, você selecionou qual tráfego Internet desejaria que fosse rastreado. Este diálogo identifica os protocolos necessários para o envio e recebimento de e-mails, por exemplo, e a correspondente porta no PC, de acordo com os padrões da indústria.

Você pode ter configurado números de porta diferentes para um ou mais protocolos listados aqui. Se este for o seu caso, deverá digitar no campo correspondente o número **real** da porta.

Os protocolos abaixo são aqueles suportados atualmente. Caso seja necessário, no futuro, a lista poderá ter modificações.

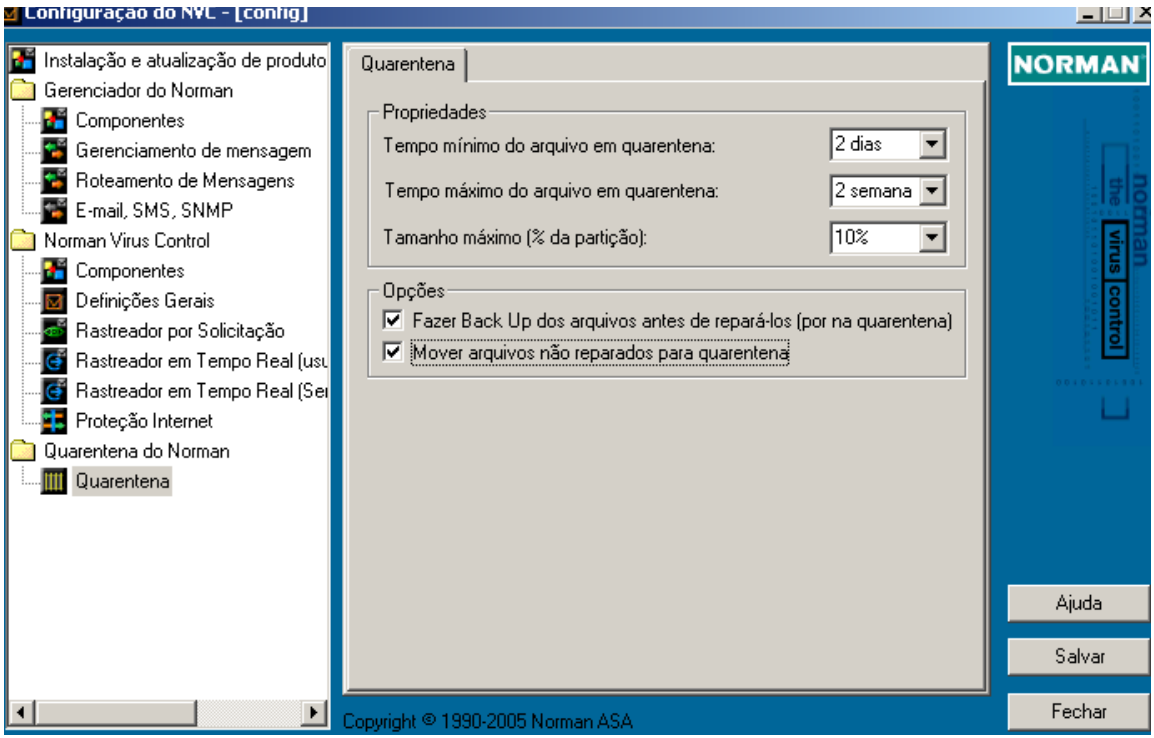
Aqui pode-se ver os nomes completos para as abreviaturas dos protocolos:

- **SMTP** (port 25) significa *Simple Mail Transport Protocol*

- **POP** (port 110) significa *Post Office Protocol*
- **NNTP** (port 119) significa *Network News Transfer Protocol*

Quarentena do Norman

Quarentena



Aqui você decide de que forma irá tratar os arquivos que o NVC identificou como infectados, bloqueados ou suspeitos. Caso você não delete ou lime esses arquivos, recomendamos que eles sejam colocados em uma área segura, a qual chamamos de quarentena.

Conforme mais produtos Norman sejam adicionados a sua instalação, eles compartilharão dessa função de quarentena e usarão as mesmas opções aqui especificadas. Assim, você poderá ter apenas uma consistente estratégia de quarentena.

Propriedades

Tempo mínimo do arquivo em quarentena:

Determina o período de um dia até uma semana. Arquivos mais recentes que o mínimo especificado nunca serão deletados.

Tempo máximo do arquivo em quarentena:

Especifica um período de uma a quatro semanas. Arquivos cuja "idade" seja maior do que o tempo máximo especificado serão deletados sem aviso.

Tamanho máximo (% da partição):

Especifica quanto de espaço em disco, em função da partição, os arquivos em quarentena poderão usar. O tamanho máximo poderá ser excedido no caso dos arquivos em quarentena não terem alcançado ainda o ***Tempo mínimo.***

Opções

☑ **Fazer Back up dos arquivos antes de repará-los (por na quarentena)**

Antes que o NVC repare um arquivo infectado, você poderá copiá-lo para a área de quarentena. De uma maneira geral, o risco representado pela operação de reparo é mínimo. Entretanto, recomendamos que mantenha essa opção selecionada.

☑ **Mover arquivos não reparados para quarentena**

Se o NVC não pode reparar um arquivo, aqui, você determina que ele seja movido para a área de quarentena.

Por razões de segurança, o NVC pode mover arquivos que não foram reparados para quarentena independentemente de suas seleções.

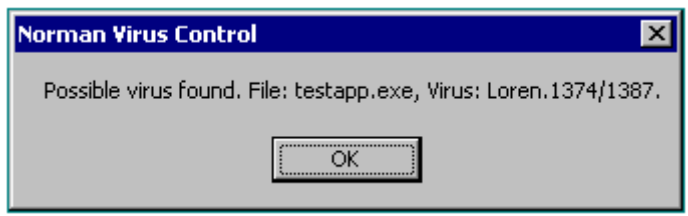
Note: Independente de sua escolha, o NVC moverá arquivos não reparados para quarentena se tiver selecionado no Rastreador em Tempo real (serviços e usuários remotos) a opção **Rastrear arquivos novos ou alterados** (page 61). A razão é porque essa opção representa uma estratégia que requer um ambiente livre de vírus. se o reparo falha, o arquivo infectado deve ser eliminado da máquina em questão, portanto.

NVC em Windows Terminal Server

Em ambientes de terminal servers em Windows NT ou Windows 2000, os usuários podem se conectar ao servidor através de clientes de terminal services. Usando esta configuração, um cliente terminal services não executa aplicações localmente , mas sim no servidor, dependendo dele, portanto, para executar as aplicações que estejam usando. O servidor distribui o layout das telas a cada usuário logado e executa as aplicações em nome do usuário.

Este desenho simplifica a manutenção do administrador de arquivos e aplicativos em um ambiente de multi usuários. O NVC com a mesma visão, valoriza esse ambiente e faz com que seja fácil ao administrador configurar o NVC de acordo.

Durante o rastreamento em tempo real nas sessões de clientes de Terminal server, o NVC sempre usará a configuração de ’Serviços e usuários remotos’ (ou servidor). Isso significa que não haverá diálogos de alertas de vírus no Terminal server caso um vírus seja encontrado. No cliente de Terminal server entretanto, uma janela como a abaixo será mostrada:

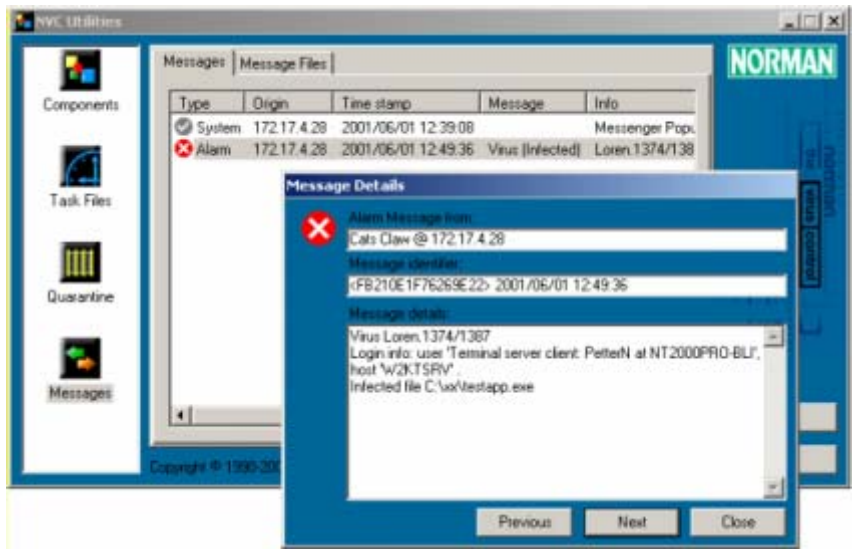


Essa mensagem tem carater ouramente informativa. O cliente terminal server não tem permissão de alterar o comportamento ou a configuração do rastreador.

Note que rastrear arquivos novos ou alterados é a configuração default para ’Serviços e usuários remotos’. Arquivos lidos ou

executados de um cliente terminal server client são ortanto não afetados pelo rastreamento em tempo real.

Na console de mensagens do Administrador, a seguinte mensagem irá ser mostrada:

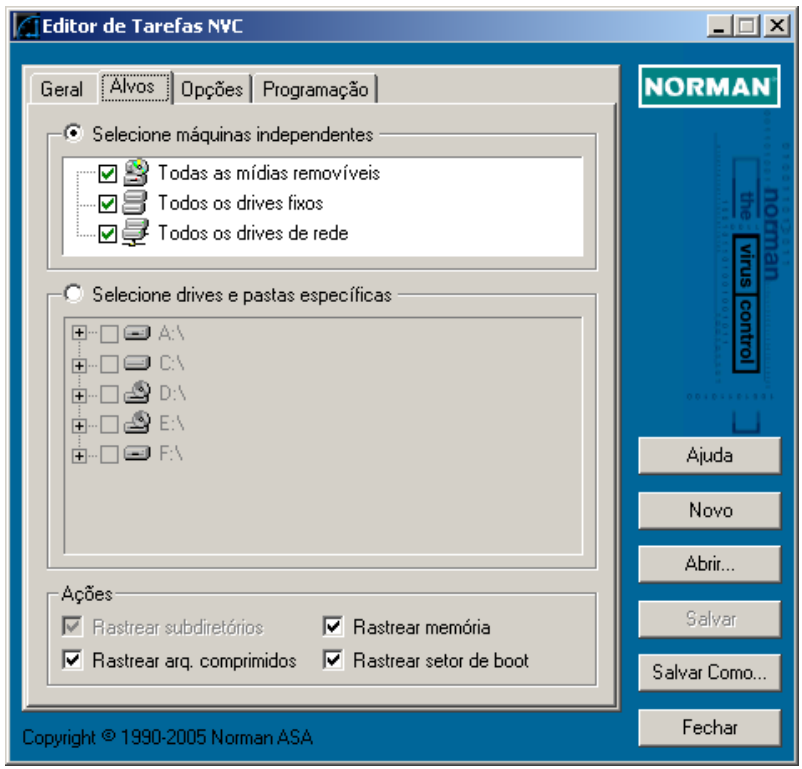


O nome do cliente terminal logado assim como a máquina é informado na mensagem de alerta de vírus. No exemplo acima, o usuário PetterN na máquina NT2000PRO-BLI causou uma mensagem de alerta de vírus no terminal server W2KTSRV.

O rastreamento por solicitação com o NVC é possível em cada sessão de terminal, sendo que a funcionalidade nesse caso não é diferente de qualquer outra configuração sobre o rastreador por solicitação já comentado.

Editor de Tarefas

Às vezes é conveniente que se defina tarefas que devam ser feitas por várias vezes e/ou em intervalos regulares. Rastreamento de vírus é um bom exemplo de tarefa que precisa ser realizada de forma regular, e o Editor de tarefas é a ferramenta que o NVC lhe fornece para tais propósitos.



Você pode criar um arquivo de tarefa para rastreamento de áreas que deseja de maneira regular, ou rastreamento especiais que deseja executar em ocasiões que requeiram esse tipo de ação. Por exemplo, se você baixa sempre arquivos da Internet em áreas prédeterminadas, poderá criar um arquivo de tarefa para verifcar essa área apenas, e executá-lo manualmente depois que tiver baixado os arquivos. Além disso, poderá programar para que

arquivos de tarefas sejam executados em horários pré-estabelecidos.

Os administradores podem criar arquivos de tarefas e espalhá-los para as estações na rede para assegurar-se de que determinadas áreas que poderiam estar requerendo atenção especial sejam constantemente rastreadas.

A localização default dos arquivos de tarefas é `...\nvc\tasks`. Você pode ver, editar, executar e deletar os arquivos de tarefas através do utilitário do NVC (veja page 96).

As seguintes seções, descrevem as abas do **Editor de Tarefas**.

Geral

Da aba **Geral**, use a caixa the **Descrição** para inserir uma descrição sobre a tarefa criada. Se você cria inúmeras tarefas, isso pode ser muito útil, pois lhe daria uma visão do porque aquela tarefa teria sido criada, e se já pode ser descartada, ou mesmo modificada.

Em **Utilitários|Arquivos de tarefas** você poderá ver uma lista completa de arquivos de tarefas existentes.

⇨ ‘Utilitários’ on page 96.

Alvos

Nesta aba você especifica as áreas que devem ser rastreadas, e de como esse rastreamento deverá acontecer, além de salvar as seleções em um arquivo de tarefas.

Existem duas seções nesta aba, a primeira para grandes entidades como discos rígidos, e a segunda para alvos mais específicos.

Dentro de um mesmo arquivo de tarefas, você não poderá combinar a seleção da primeira seção com a da segunda seção. Por exemplo, você não poderá selecionar todas as mídias removíveis e uma pasta especifica, em seu disco rígido, na segunda seção.

Selecionando alvos

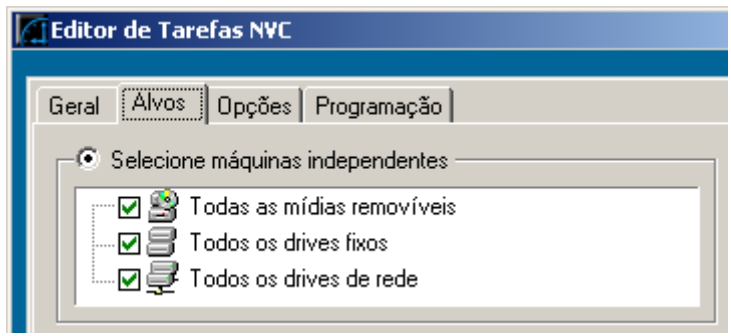
Para ambas as seções nesta aba, este é o procedimento que deve seguir para incluir áreas para rastreamento e salvar essas seleçoes em um arquivo de tarefas:

1. Clique em ⊙ para ativar a seção que deseja fazer a seleção.
2. Clique nas áreas que deseja incluir no rastreamento. Você pode adicionar diversas áreas em uma mesma seção.
3. Se selecionar drives e pastas específicas, todas as subpastas debaixo do drive ou asta selecionada, estarão marcadas automaticamente. Se quiser, desmarque aquelas pastas que não deseja verificar.
4. Quando tiver feito, clique em **Salvar** para guardar as suas seleções em um arquivo de tarefas. Por default ele será salvo em `...\nvc\tasks`.

Note: Se tiver programado um arquivo de tarefa, ele **tem** que estar localizado em `...\nvc\tasks`.

5. Para alteração de arquivos existentes, clique em **Abrir** e selecione o arquivo que deseja da janela que aparecer. Faça as alterações que deseja e clique em **Salvar**.

Selecione máquinas independentes



Pode escolher um, duas ou todas as opções em um único arquivo.

☑ **Todas as mídias removíveis**

Seleciona todos os disquetes, CD-ROM, e outras mídias removíveis disponíveis em seu sistema.

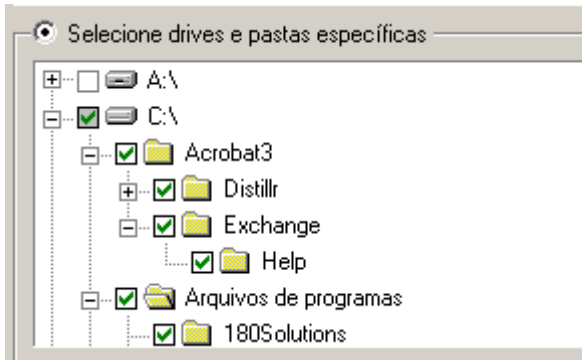
☑ **Todos os drives fixos**

Seleciona todos os drives locais não removíveis de seu sistema.

☑ **Todos os drives de rede**

Seleciona todos os drives de rede conhecidos em seu sistema.

Selecione drives e pastas especificas



Quando você seleciona um drive, por exemplo, toas as pastas e subpastas debaixo dele são automaticamente selecionados. Da mesma maneira, se selecionar uma pasta ou subpasta, todos os itens que existirem debaixo delas serão incluídos. Para excluí-los do rastreamento basta desmarcá-los.

Opções de rastreamento comuns

Na parte inferior da janela, existe um conjunto de opções de rastreamento comuns em *Ações*:

☑ **Rastrear subdiretórios**

Se tiver selecionado um ou mais drives ou diretórios, selecione esta opção para incluir os subdiretórios no rastreamento.

☑ **Rastrear arq. comprimidos**

Selecione esta opção para incluir arquivos comprimidos. Os seguintes formatos são suportados: ZIP, ARJ, RAR, ACE, ARC, GZIP, TAR and BZIP2.

☑ **Rastrear memória**

Quando você rastreia a área da memória, o NVC procura por vírus residentes. Sempre tenha a certeza de que não existem vírus na memória.

☑ **Rastrear setor de boot**

Nesta seleção, o NVC irá verificar o setor de boot das áreas que estarão sendo rastreadas.

Opções

Use esta aba ara decidir a forma como o NVC deverá aparecer durante o rastreamento, e quanto recurso do sistema deverá ser alocado para a tarefa.

Janela do rastreador:

O **Automática:Oculto até encontrar uma falha de reparo**

Instrui ao NVC para trabalhar de modo invisível. O NVC irá aparecer aenas se um vírus que NÃO pode ser limpo for encontrado. Perceba que é um pouco complicado cancelar uma tarefa que está sendo executada em modo oculto. This might serve as a useful hint for an administrator who wants scheduled tasks to run as planned, and as a warning to single-users who might find it hard to cancel an ongoing scan. A tarefa programada se inicia automaticamente se esta opção estiver selecionada.

O **Automática: Minimizado até encontrar uma falha de reparo**

Instrui ao NVC para trabalhar minimizado. O NVC aparecerá apenas se um vírus não puder ser limpo. A tarefa programada se inicia automaticamente se esta opção estiver selecionada.

⊙ **Automática: Minimizado até encontrar uma infecção**

Instrui ao NVC para trabalhar minimizado. O NVC aparecerá apenas se um vírus for encontrado.A tarefa programada se inicia automaticamente se esta opção estiver selecionada.

O **Manual: Janela normal**

Instrui ao NVC para trabalhar em uma janela aberta durante o rastreamento. Quando você programa uma verificação com esta opção, o diálogo de rastreamento aparece na hora determinadad e você tem que iniciá-lo ***manualmente*** clicando em **Rastrear.**

Recurso usado:

Sob condições normais de operação, um computador raramente funciona com tão baixos recursos que o sistema oeracional se vê forçado a determinar prioridade nas tarefas. Caso essa situação aconteça, uma tarefa do NVC terá que esperar até que o sistema obtenha recursos livres para executá-la caso tenha escolhido aqui a opção **Baixo**, ao passo que **Normal** colocará a tarefa do NVC dentre qualquer outra que esteja esperando para ser executada.

Note que os efeitos em estar selecionando **Baixo** ao invés de **Normal** irá variar dependendo do sistema operacional utilizado.

Programação

Quando você tiver configurado um arquivo de tarefas usando a aba aqui discutida, deverá ter em mente que essa tarefa será executada repetidamente em sua máquina.

☑ **Tarefa programada**

Assegure-se de ter selecionado esta opção se deseja usar o programador. Dois requisitos para que se execute uma tarefa programada são necessários: 1) A opção **Tarefa programada** tem que estar selecionada, e 2) O arquivo de tarefa deve estar localizado no diretório `...\nvc\tasks`.

Frequência

O próximo passo é a decisão de quando a tarefa deverá ser executada, onde você poderá escolher dentre diferentes intervalos desde **Uma vez** até **Mensalmente**.

Data de início/hora:

Especifique o dia/mês/ano que a tarefa programada deverá ser executada pela primeira vez. Use as seta de seu teclado (ou clique nas setas do box) para alterar a data. Você pode selecionar o ida, mês e ano e alterar os valores pressionando as chaves. O dia da semana irá se alterar automaticamente.

☐ **Universal Time Coordinates (UTC)**

Esta oção é para empresas que tem escritório espalhados pelo mundo e necessita realizar a tarefa de forma simultânea independente da hora local.

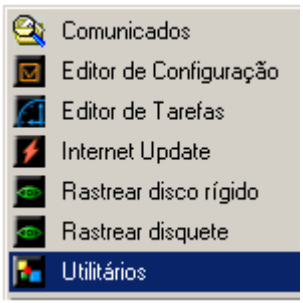
Sobre o programador

O obletivo principal do rogramador é executar uma tarefa em um determinado horário previamente estabelecido. Um arquivo de tarefa pode ser programado para ser executado diariamente, semanalmente, mensalmente ou apenas uma vez. Basta informar a hora de início e de quanto em quanto tempo deseja executá-lo. O dia e mês são os da data corrente.

Para companhias com escritórios em diversas partes do mundo com diferentes fusos horários, o Universal Time Coordinates (UTC) permite que uma tarefa seja executada ao mesmo tempo, não importando o fuso horário.

O programador sempre olhará no subdiretório “Tasks” para trabalhos programados, portanto é necessário que se mantenha na estrutura o diretório `...\nvc\tasks`.

Utilitários



O módulo Utilitários do NVC é uma ferramenta que apresenta uma visão geral do estado atual dos componentes do NVC em seu computador. Além de poder ver as informações chaves, você poderá alterar certos elementos selecionando algumas das entradas, por exemplo, arquivos de tarefas.

Você pode acessar o módulo Utilitários através do menu em sua barra de tarefas, ou através de Iniciar|Programas|Norman Virus Control.

Nesta versão, o módulo Utilitários é composto de 3 grandes categorias:

- Arquivos de Tarefas
- Quarentena
- Mensagens

Arquivos de Tarefa

Quando você cria um arquivo de tarefas usando o Editor de Tarefas do NVC, o arquivo é or default salvo no diretório `...\nvc\tasks`.

Note: Se quer programar uma tarefa, o arquivo de tarefa tem que residir neste diretório.

Você pode por exemplo usar o Windows Explorer ou o Editor de Tarefas para ver este diretório. Entretanto, a ferramenta mais flexível é o diálogo corrente, que permite a você ver, editar, criar, e abrir o arquivo de tarefas de diferentes formas. Além disso, poderá encontrar o status de todas as suas tarefas em apenas uma janela.

Você pode executar os arquivos de tarefas através de comando de linha. Este processo envolve estar iniciando o Rastreador por Solicitação e executar uma específica tarefa de comando através de linha oculto para o usuário.

⇨ See ‘Rodando arquivos de tarefas através de comando de

linha’ on page 108.

Campos na caixa de diálogo do arquivos de tarefas

Arquivos de tarefa

Mostra o nome do arquivo de tarefa.

Programação

Mostra se o arquivo de tarefa foi programado e em que intervalos.

Próxima execução

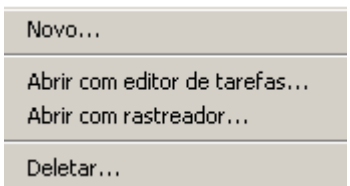
Mostra qual dia, mês, e hora essa tarefa terá lugar. Se este campo estiver limpo, significa que não há mais programação para ele.

Última execução

Mostra a última vez que a tarefa rodou com sucesso.

Opções do lado direito do mouse

Você pode selecionar uma entrada por vez, e clicar com o lado direito do mouse que o seguinte menu irá aparecer:



Novo

Abre o editor de tarefas onde poderá criar uma nova tarefa.

Abrir com o editor de tarefas

Abre a tarefa com o editor de tarefas, que dentre outras permite fazer alterações no arquivo de tarefa aberto.

Abrir com rastreador

Permite a execução da tarefa imediatamente com o rastreador.

Deletar

Deleta o arquivo selecionado.

Quarentena


Quarentena.

Se tiver habilitado as ações de quarentena na pasta **Quarentena do Norman** (‘Quarentena’ on page 85), arquivos classificados para ela aparecerão como uma lista nesta caixa de diálogo. Esses arquivos estão ou infectados, com um formato desconhecido, ou foram bloqueados pelo Proteção Internet (NIP). Veja maiores referências em ‘Bloqueio de anexos’ on page 79.

Campos na caixa de diálogo da Quarentena

Posto em quarentena

Mostra o caminho da localização do arquivo colocado em quarentena. Em algums situações um caminho não pode ser mostrado, por exemplo, para anexos a e-mails que são sempre verificados como arquivos temporários.

Arquivo

Mostra o nome do arquivo posto em quarentena

Data

Mostra a data em que o arquivo foi posto em quarentena.

Tamanho

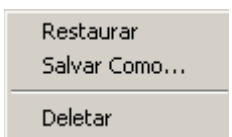
Mostra o tamanho do arquivo posto em quarentena.

Diagnóstico

Mostra o status do arquivo posto em quarentena. Podem ter como resultado: Infectado, Desconhecido.

Opções do lado direito do mouse

Você pode selecionar uma entrada por vez, e clicar com o lado direito do mouse que o seguinte menu irá aparecer:



Restaurar

Irá restaurar o arquivo para a sua forma original na localização original. Para anexos de e-mail, apenas o nome do arquivo aparece e você tem que usar a opção **Salvar como**.

Salvar como

Salva o arquivo com o nome e a localização que desejar.

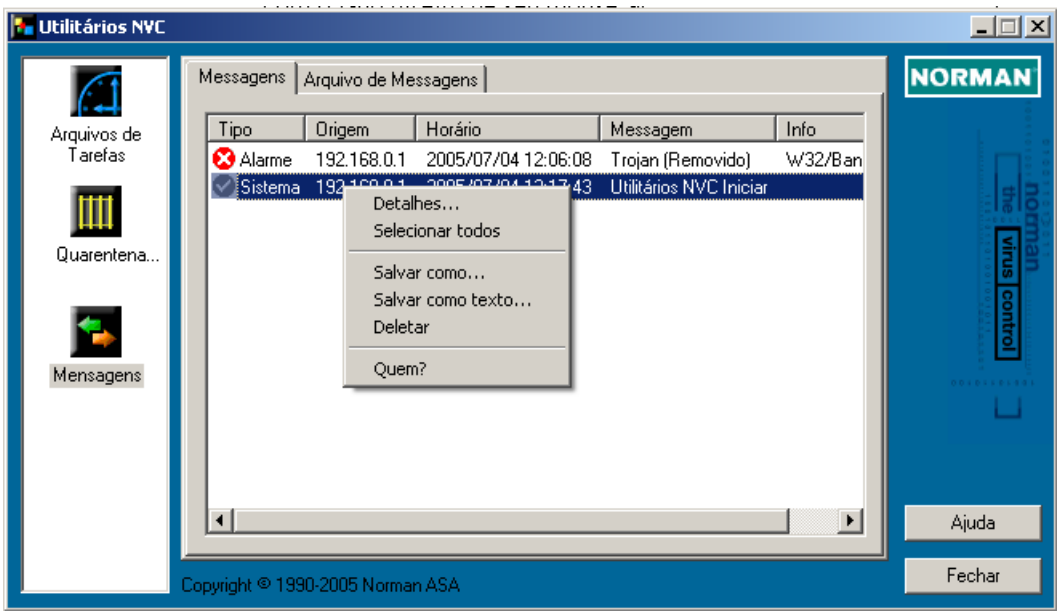
Deletar

Deleta o arquivo.

Mensagens

Aba Mensagens

Se tiver habilitado o serviço de mensagens (ver ‘Registrador de Mensagem’ on page 34), os tipos de mensagens que selecionou na ocasião estarão mostradas nesta aba. Você pode ver e editar essas mensagens aqui. Selecione uma entrada na lista e clique com o lado direito de seu mouse:



Campos na aba Mensagens

Tipo

Descrição do tipo/categoria da mensagem acompanhada de um ícone indicando tipo/severidade. As entradas que devem aparecer são do tipo especificadas no Registrador de Mensagens.

Origem

O endereço IP da máquina que originou a mensagem.

Horário

Ano/mês/dia e hora/minuto/segundo do incidente que originou a mensagem.

Mensagem

Palavra chave relacionada com o incidente, por exemplo “Virus”, “Conectado”, etc.

Info

Texto descritivo sobre a mensagem.

Opções do lado direito do mouse:

Detalhes

Mostra uma caixa de diálogo com informações sobre aonde a mensagem se originou, um identificador da mensagem, e um caixa de texto com maiores informações.

Selecionar todos

Seleciona todas as mensagens/entradas para salvamento, deleção, ou vistas dos detalhes, etc.

Salvar como

Salva uma ou mais entradas com o nome que você desejar. Você poderá acessá-los a qualquer momento na próxima aba, de nome **Arquivo de mensagens**. Mensagens salvas possuem como extensão `.nps`.

Salvar como texto

Salva a entrada selecionada como um arquivo de texto com o nome que desejar.

Deletar

Deleta a entrada selecionada.

Quem?

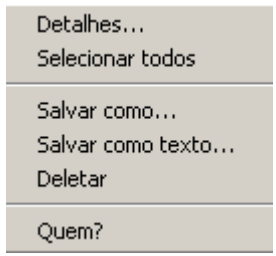
Envia um poll em Broadcasts.

Aba Arquivo de Mensagens

Se você salvou uma ou mais entradas de mensagens como arquivos com a função **Salvar como** na aba **Mensagens**, você pode abri-las na aba **Arquivo de Mensagens**.

Os campos nesta aba são idênticos aos da **aba Mensagens**.

Opções do lado direito do mouse



As opções de clique com o botão direito do mouse são idênticas às da aba **Mensagens**, exceto para:

Abrir

Coloque o cursor do mouse em um local vazio na caixa de texto, clique com o lado direito e selecione **Abrir** para mostrar o arquivo na caixa. Você verá todos os arquivos salvos (arquivos tipo `.nps`) no diretório default `...\norman\msg`.

Atualizando o NVC

Qualquer rastreador antivírus é apenas efetivo se estiver o mais atualizado possível, portanto, obter as frequentes atualizações é crítico para poder manter seguro o seu ambiente.

Para aqueles que não atualização o NVC deixando que o Norman Program Manager (NPM) distribua elas em uma rede local, o Norman Internet Update—ou apenas Internet Update (IU)— é o método alternativo. O Internet Update é um programa que faz com que você esteja rodando sempre a última versão do NVC para sua plataforma, checando sempre os servidores da Norman por qualquer tipo de atualização, tais como alterações no programa, bug-fixes, novo engine rastreador, e atualizações dos arquivos de definição de vírus. Quando você roda o IU, o programa compara os componentes do NVC instalados em sua máquina com as correspondentes versões do Norman nos servidores da desenvolvedora. Se o time stamp for diferente, você é perguntado se deseja baixar as atualizações. Teoricamente, o programa inteiro pode ser alterado e então, estar sujeito de ser baixado integralmente.

Internet Update aparece como um item separado no grupo Norman.

Para executar o IU, precisa de uma conexão TCP/IP (Internet).

O IU pode ser usado por usuários simples para baixa de atualizações diretamente em sua máquina local, e or administradores que baixarão elas em um servidor de distribuição e deixarão que o NPM distribua os pacotes para as estações existentes na rede.

Internet Update do Norman

Iniciando o Internet Update

Para rodá-lo basta escolher Iniciar|Programas|Norman Virus ControlInternet Update, ou selecione ***Internet Update*** do menu

que aparece quando você clica com o lado direito do mouse no ícone do Norman existente em sua barra de tarefas.

Clique com o lado direito do mouse em seu desktop e selecione *Norman Virus Control*.

Internet Update e conexão à Internet

Para executar o Internet Update (IU), você precisa de uma conexão TCP/IP (Internet).

No editor de configuração, especifique como você deseja atualizar via Internet, como explicado na page 26. Se selecionar **Através de conexão direta em horários especificados** e deois clicar em **Especificar**, você pode entrar o intervalo de quando checar pels atualizações:

A opção **Apenas através de solicitação (iniciar manualmente)** está inteiramente baseada na ação manual do usuário. Você tem que lembrar de iniciar o Internet Update nos intervalos que deseja, e não será lembrado or isso pelo programa. A exceção disso é quando o programa tiver mais do que 7 dias de idade.

O **Diariamente através de dial-up (esperar pela conexão)** instrui o IU para checar por atualizações uma vez por dia. Esta verificação é feita quando você tiver uma conexão à Internet.

Se você tem uma conexão direta, poderá escolher a opção **Através de conexão direta em horários especificados**. Isso permite que você planeje quando o IU rodará e pode integrá-lo com outras tarefas planejadas. Veja no início desta página.

Em outras palavras, as duas últimas opções oferecem um processo automático de atualização via Norman's Internet Update.

Note: Se a máquina que realiza os downloads está protegido por um firewall, você deve digitar o endereço e porta para o firewall proxy HTTP. Veja servidor proxy na page 29.

Como o Internet Update funciona

Exceto para a opção **Sob solicitação** que é baseada em uma ação manual, o IU roda em "modo oculto", o que significa que não o verá atuando, até que o IU tenha estabelecido que atualizações estão disponíveis. Caso contrário, o IU termina o processo.

Nesta fase inicial, o IU manda a sua chave de validação para o servidor da Norman verificar sua licença, assim como uma "string de perfil" (profile string). Essa string contém informações sobre o sistema operacional e idioma de sua versão, elementos que determinam quais as atualizações que são elegíveis para a sua máquina.

Para administradores:

O IU também trata de redes com estações rodando diferentes sistemas operacionais. Quando o administrador roda o programa `niucf.exe` (localizado em `...\nvc\bin`), um arquivo chamado de `niucf.ndf` é criado em `...\nvc\config`. Este arquivo é uma esécie de formulário de pedido onde todas as informações necessárias sobre sua plataforma, idioma estão guardadas. O IU assegura-se de que tudo no arquivo apareça como elegível para atualizações, fornecidas pela sua licença. Você tem que executar o `NIUcf` antes de rodar o Internet Update pela primeira vez.

As atividades do IU podem ser melhor descritas em 3 fases:

Fase 1:

Envio da chave e string de perfil para o servidor de validação. O servidor retorna uma lista de pacotes. Os pacotes contém o código do programa NVC, arquivos de definição de vírus, ou outros componentes do NVC.

Fase 2:

O IU checa o time stamp dos pacotes existentes no servidor de produto contra o que está na máquina local no diretório de download. Caso o time stamp for diferente o pacote é considerado elegível para ser baixado .

Caso novos pacotes estejam disponíveis, um diálogo aparece especificando o total dele. O diálogo tem uma função de timer, e a menos que selecione **Sim/Não** dentro de 15 segundos, tem-se início o download.

Fase 3:

Os pacotes são baixados para o diretório de download.

Quando o download estiver terminado, o IU sai e o Norman Program Manager (NPM) toma conta de gerenciar a atualização do NVC em sua máquina.

LAN/WAN

Em um ambiente de rede, você pode atualizar as estações selecionando **Automaticamente do servidor**.

Note a opção de atualização de servidor usa as informações que você digita na caixa de diálogo da aba **LAN/WAN**.

Miscelânea no NVC

Gerenciador do Norman (NPM)

O NPM merece uma explanação mais detalhada do que os outros produtos—de uma certa forma porque ele é fundamental para o NVC e outros programas do Norman. Ele está envolvido com a instalação, atualização, e comunicação com outros programas e módulos. A sua presença é raramente visível apesar de estar sempre sendo executado.

O coração do NPM é o arquivo `Zanda.exe`—abreviatura de Zero Administration Network Distribution Agent. O NPM é o link entre auqeles componentes que precisam se comunicar entre si, e consequentemente essencial ao NVC como um programa. Como o nome sugere, está mais ativo em uma rede do que em um computador simples, e portanto será discutido mais exaustivamente no *Guia do Administrador*.

O gerenciador do Norman (NPM) fica residnte *localmente*, i.e. na estação ou no servidor. Quando intruído pela estação, o NPM irá obter os arquivos do servidor. Por exemplo, se o arquivo de configuração determina que a estação deve procurar por atualizações no servidor, todos os dias às 12:00 hrs, é o NPM que *busca* os arquivos. Além disso, o agente irá *enviar* mensagens da estação para o servidor. Note que a colaboração entre o NPM e o IU é particularmente importante durante as atualizações: um atualização *não* estará completada até que o NPM tenha descompactado e instalado os novos arquivos.

O Gerenciador do Norman está sempre rodando.

Estas são algumas das tarefas que ele toma conta:

- Gerencia as atualizações do NVC.
- Assegura que os módulos se iniciem como configurado.
- Assegura que a configuração está em concordância com que o administrador requereu para cada estação.

- Busca as atualizações, novos arquivos de configuração e de tarefas.

⇨ ‘LAN/WAN’ on page 21.

- Retrata seu próprio planejamento.

Para maiores detalhes sobre o agente, veja o *Guia do Administrador*.

Sobre o Rastreador por comando de linha

Além dos Rastreadores por Solicitação e em Tempo Real baseados em uma interface gráfica, o NVC oferece uma versão de rastreador por comando de linha.

O rastreador por comando de linha do NVC possui as mesmas funcionalidades das existentes no rastreador gráfico.

Ele não é dependente de qualquer outro módulo e pode ser executado através de arquivos “.bat”.

Iniciando o Rastreador por comando de linha

1. Do prompt do DOS ou OS/2, vá para o diretório onde o NVC reside.
2. A sintaxe é:

   ```
   nvcc [drive]:[path] [/parâmetro] [Enter]
   ```

   Um espaço deve preceder cada parãmetro que você usar.

   Simplesmente selecione a combinação de parâmetros que deseja usar e especifique-os no comando de linha.

⇨ Veja ‘Opções do rastreador de comando de linha’ on page 109 para uma completa listagem e explanação dos parãmetros disponíveis.

Limpando Arquivos infectados

Note: Na documentação e no programa NVC, “reparar”, “remover”, and “limpar” são considerados termos semelhantes. Todos eles se referem ao processo de

remoção de vírus de arquivos ou setor de boot, e restauração da área infectada à sua condição original.

O núcleo de tecnologia dos rastreadores do NVC (em tempo real, por solicitação, e por comando de linha) é o engine rastreador. As opções de rastreamento refletem a capacidade do engine. Além da detecção de vírus, o engine pode também removê-los (***reparar*** o arquivo ou setor de boot, e consequentemente ***limpar*** a máquina). Este processo é tecnicamente mais complicado do que a simples detecção.

Note que nos códigos nocivos como os **trojans**, onde o arquivo inteiro é o malfeitor, não existe o que limpar. Nestas situações a única cura é a *deleção de todo o arquivo*. Por isso usamos, em algumas situações, a expressão "Limpando pela deleção".

Os rastreadores podem remover todos os tipos de vírus automaticamente de discos rígidos e de disquetes, exceto os ***vírus do setor de boot***. Os vírus do setor de boot podem ser removidos automaticamente de disquetes, mas não de discos rígidos.

Se algo de errado aocntecer quando reparamos arquivos, isso é menos problemático do que quando reparamos um setor de boot. Um setor de boot corrompido pode fazer com que o sistema se torne inútil. Para asseguramos que um setor de boot mal reparado não colocará o sistema em uma situação ruim, não permitimos que o reparo desse tipo seja feito de forma automática

Se um vírus de setor de boot for detectado, você verá um diálogo recomendando-lhe que faça um back up dos dados importantes para uma mídia removível. No caso de falha da reparação, você poderá bootar a sua máquina através de um CD ou mesmo disquete e restaurar os arquivos importantes. Uma caixa de diálogo completa com ajuda online irá guiá-lo através do processo.

Rodando arquivos de tarefas através de comando de linha

Você pode executar o NVCOD de uma linha de comando afim de rodar um arquivo de tarefa.

Use o seguinte comando para iniciar a execução de um arquivo de tarefa:

```
NVCOD @<caminho do arquivo de tarefa>
```

A função é muito útil na medida em que a tarefa será executada oculta do usuário, podendo inclusive ser executada através de login script.

Exemplo:

Digamos que você criou um arquivo de tarefa chamado de `scan.sdf`. Ele está localizado no diretório default `c:\norman\nvc\tasks`. Você quer rodar o rastreamento na máquina com as configurações especificadas no arquivo de tarefa.

Do comando de linha você entra:

```
c:\norman\nvc\bin>nvcod.exe @c:\norman\nvc\tasks\myscan.sdf
```

Opções do rastreador de comando de linha

Do diretório onde o programa do Norman reside, execute o comando

```
nvcc /?
```

e uma lista de opções disponíveis irá ser listada. Abaixo seguem os parâmetros disponíveis com as respectivas explicações de sua função.

Parâm.:	Funções:
`/-help`	Mostra o help.
`/?`	Mostra o help.
`/ALD`	Rastreia todos os discos locais (exceto disquetes e CD-ROM).
`/AD`	Rastreia todos os discos (disquetes não). Possíveis drives de rede são rastreados além dos drives fixos locais.

Parâm.:	Funções:
/B	Sem alarmes de som se um vírus for encontrado (default OFF).
/BS-	Ignorar as áreas de sistema. As de um mesmo drive serão checadas apenas uma vez mesmo que várias especificações de arquivo para um mesmo drive lógico estejam especificadas (default OFF).
/BS+	Rastrear apenas área de sistema.
/C:	Rastrear arquivos comprimidos. /C:0 não, /C:1 sim (default no config).
/C	Rastrear arquivos comprimidos. Mesmo que /C:1 (default no config).
/CP	Rastrear programas comprimidos (default OFF).
/CL:	Reparar arquivos e setor de boot: /CL:0 não, /CL:1 sim, /CL:2 dentro de arquivo comprimido também (default no config).
/CL	Reparar arquivos e setor de boot. Mesmo que /CL:1 (default no config).
/CZ:	Tamanho máximo do arquivo comprimido em Kb. Implica /C (default no config).
/CR:	Tamanho máximo do arquivo comprimidos de forma recursiva. Implica /C (default no config).
/FLOPPY	Ler arquivos NSE em disquetes separados (apenas DOS).
/H	Mostra help.
/HUM	Trata macros não certificadas (precisa do NSE\NVCMACRO.CRT do CatsClaw).
/L:	Configura o nível de logging: /L:0=não, 1=sim, 2=verbose (default in config).
/LD:	Especifica diretório para arquivos de log (diretório default especificado no config).

Parâm.:	Funções:
/LF:	Especifica um nome de arquivo de log (sobrepõe LD: e /LG:). Digite o nome imediatamente após o parâmetro (sem espaços).
/LG:	Especifica o número de geração de arquivos log (default determinado no config).
/N	Não rastrear a memória.
/O	Ignorar arquivos que não podem ser abertos (default OFF).
/Q	Modo silencioso, sem nada na tela (default OFF).
/R	Repetir o rastreamento. Útil para vários disquetes (default OFF).
/S	Ver subdiretórios. Se tiver especificado um drive, os subdiretórios estarão inclusos automaticamente. Default quando checando drives.
/SB	Usar sandbox. 0=Não, 1=Sim
/SN	Impossibilidade de abortar tarefa (default OFF).
/TEMP:	Sobregrava ambientes TEMP/TMP. Se o ambiente não estiver definido, o programa o criará um nível acima da localização do diretório NSE.
/U	Não parar se encontrar vírus (default OFF).
/V	Modo Verbose (default OFF).
/W:	Esperar número especificado de millisegundos entre cada arquivo (default 0).
/YH	Abortar se vírus for encontrado (default OFF).

Combinando diferentes parâmetros

O rastreador por comando de linha é flexível ao ponto de poder combinar diversos parâmetros para realizar diversas tarefas em um comando.

Veja alguns exemplos de como pode combinar parãmetros. Do diretório onde o `nvcc.exe` se encontra, digite:

```
nvcc c:\*.exe /s /u /cl /lf:myscan.log
```

Esse comando rastreará todos os arquivos com a extensão `.exe` no drive local c: incluindo subdiretórios. O rastreador não irá interromper se encontrar arquivos infectados, os que puderem serão limpos, e o arquivo de log `myscan.log` será criado no diretório onde o `nvcc.exe` está instalado.

Depois digite:

```
nvcc *.txt a: c:
```

para rastrear arquivos `txt` no diretório corrente e depois nas áreas de boot e arquivos com extensões default rastreáveis em `a:` e `c:`.

Note: Especificando `c:\` (com a barra) rastreará arquivos apenas na raíz do drive, mas `c:` (sem a barra) fará ambos arquivos e áreas de sistema do disco.

Errorlevels do rastreador por comando de linha

Você pode automatizar os rastreamentos por comando de linha usando os error levels em arquivos bat. Os error levels para o rastreador or comando de linha são::

Errorlevel:	Significado:
13	Licença não permite que o programa inicie.
12	O arquivo `NVC32.CFG` não foi encontrado.
11	Alguns arquivos estão corrompidos.
10	Todos os arquivos não puderam ser abertos para rastreamento.
9	Rastreamento foi abortado pelo usuário.

Errorlevel:	Significado:
8	Erro interno: Rastreamento abortado.
7	Aviso. Alguns componentes como o `Nlog5.dll` não foram encontrados.
6	Erro de input/output no disco.
5	Erro de usuário: Critério de rastreamento ou parâmetro inválido.
4	A configuração de hardware mudou desde que o rastreador foi instalado.
3	Erro de usuário: O rastreamento iniciou sem que houvesse nenhum critério estabelecido.
2	Vírus encontrado na memória e removido.
1	Vírus encontrado e/ou reparado. Este código de erro sobregrava todos os outros exceto o 2.
0	Tudo OK. Nenhum vírus ou código nocivo encontrado.

Apêndice A - Sandbox

Visão geral

O desafio de inventar um método que detecte automaticamente vírus novos e desconhecidos é tão antigo quanto a indústria de antivírus. Através dos anos, os desenvolvedores de AV tem investido signaficativos recursos para encontrar uma solução que alcançe esse ambicioso objetivo..

Em 2001, na Virus Bulletin Conference, a Norman produziu um protótipo totalmente funcional de um engine rastreador com a funcionalidade chamada de sandbox.

O que é o sandbox?

Sandbox é o termo que melhor expressa a técnica que é usada para checar se um arquivo está infectado por um vírus desconhecido. O nome não foi obtido de forma randômica, porque o método permite a códigos virais desconhecidos e não confiáveis de ser acionado dentro do computador, – não no computador real, mas em uma área simulada e restrita dentro do computador. O sandbox está equipado com tudo que um vírus espera encontrar em um PC real. É um "pátio de recreio" onde é seguro deixa um vírus replicar-se, mas onde cada passo é cuidadosamente monitorado e relatado. O vírus se torna exposto no sandbox, e por causa que as suas atividades estão sendo gravadas, a cura para esse novo criminoso pode ser gerada de forma automática.

Atualmente, um novo worm de e-mail ode infectar milhares de comutadores em questão de segundos. Os desenvolvedores de AV devem encontrar a cura, atualizar os arquivos de definição de vírus, e distribuí-los para seus clientes imediatamente. A necessidade de velocidade é imperativa, porque a natureza dos atuais malware é como uma peça de código de "sucesso" que pode paralizar redes e causar sérios danos a um número ilimitado de computadores.

Técnicas de Sandbox

Sandbox usando emulação

Um vírus é um programa de computador, definido através de seu comportamento. Ele transferirá código/dados para um outro arquivo de computador. Quando esse outro arquivo por sua vez é executado, o código de vírus é de alguma forma ativado, tentando infectar outros arquivos. A esse processo chama-se de replicação. Para que um programa de computador possa ser chamado de "viral", ele tem que ser capaz de realizar essa tarefa de forma repetida.

O sandbox da Norman é um mundo virtual onde tudo é simulado. Ele é gerado por um emulador, permite que um possível vírus infecte executáveis binários da mesma forma que em um sistema real e verdadeiro. Quando a execução termina, o sandbox analisa as alterações ocorridas.

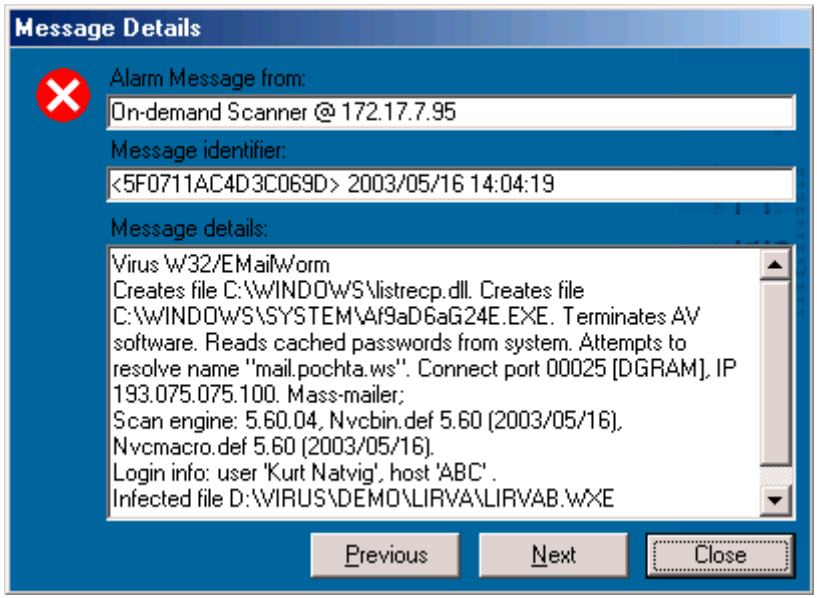
Sandbox usando uma máquina virtual

É também possível construir um sandbox criando-se uma VM (Virtual Machine ou máquina virtual). A idéia é bloquear todas as interrupções, então o executável que está examinando não pode "escapar". Entretanto, não consideramos esta solução como segura o bastante. Sempre haverá "um outro" exploit (programa que explora alguma falha) do processador do PC, tipo alguma interrupção/excessão/falha etc que permitirá ao código nocivo escapar da VM, e acabar por se espalhar em seu sistema real.

Como o sandbox afeta o usuário?

A idéia fundamental sobre o sandbox é oferecer a melhor proteção para o usuário. O maior desafio é integrar uma nova tecnologia no produto sem fazer com que fique vagaroso e pesado, diminuuindo a velocidade de rastreamento. Um outro problema capital —alarmes falsos—já foi resolvido. A tecnologia sandbox da Norman foioficialmente implementada com o NVC v5.60. O sandbox pode ser vísivel em algumas configurações de certos módulos.

Caso um código nocivo desconhecido for encontrado, o administrador será informado com algo parecido com o abaixo:



Considerando a avançada técnica envolvida nesse processo, o tempo de rastreamento tem um pequeno aumento quando a opção do sandbox estiver ativada. Entretanto, o preço é muito pequeno se comparado a possibilidade de estar detectando uma nova ameaça em sua rede.

O que fazer quando o sandbox detecta um novo vírus

Antes de tudo você deve verificar se a sua instalação está atualizada com a última definição de vírus. Caso o NVC esteja desatualizado, existe a possibilidade dos vírus encontrados pelo sandbox já estarem dentro da nova definição de vírus.

Caso tenha a certeza de que encontrou algo novo, apreciaríamos muito se comprimisse o arquivo (winzip, por exemplo), usasse uma senha para protegê-lo e enviasse para *analysis@norman.no*. Este procedimento está descrito no web site da Norman.

Para maiores detalhes sobre a tecnologia sandobx da Norman, por favor veja as publicações sobre o assunto disponíveis no web site da Norman:

http://www.norman.com/documents/nvc5_sandbox_technology.pdf

http://www.norman.com/documents/nvc5_sandbox_technology_2002.pdf

FAQ

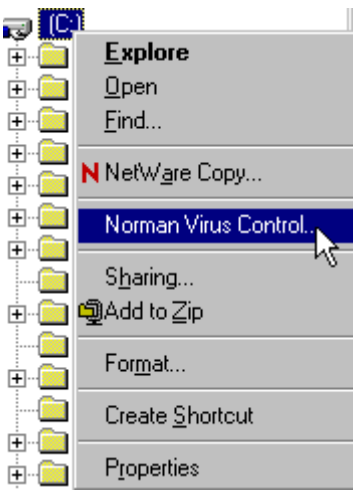
Se não encontrou o desejava nas páginas anteriores, veja na página na Internet se houve alguma atualização. O FAQ será sempre atualizado e poderá ser encontrado no endereço www.norman.com.

Seus comentários a respeito deste documento são bem-vindos. Envie-os para o endereço abaixo: documentation@norman.no.

Como inicio o NVC?

NVC's key components are started automatically when the operating system is loaded. Look for the little green Norman 'N' in the system tray.

Como rastreio minha máquina?



Rastreador em tempo real é a pedra fundamental de controle dos vírus no NVC v5. Quando acessa um arquivo, o NVC checa ele para ver se tem vírus. O "problema" é que ele é invisível, e você pode desejar realizar uma checagem mais tangível. Você pode:

1. Selecione qualquer objeto, por exemplo o drive (C:) dentro do Windows Explorer,
2. Pressione o lado direito do mouse,
3. Selecione "Norman Virus Control" dentro do menu,
4. Clique no botão **Rastrear** para realizar um rastreamento manual de todos os arquivos no drive(s), ou dos objetos selecionados para tal.

Iniciando e parando o rastreador em tempo real

Recomendamos que encerre o rastreador em tempo real quando fizer tarefas de manutenção de sistema. Se o encerrar, ele não irá ficar ativo novamente nesta seção, ou mesmo após o re-início, a menos que você o faça manualmente. Você pode parar e inciar o rastreador em tempo real de um item em separado no menu de sua barra de tarefas, ou ir até a aba **Iniciar** no módulo definições de instalação no editor de configuração.

Devo rastrear minha máquina diariamente?

Não necessariamente. Se combinar rastreamentos periódicos por solicitação e programados, o rastreador em tempo real poderá fazer todo o trabalho de monitoramento. Entretanto se usa muito baixar arquivos da Internet, recomendamos fazer a checagem mais regularmente.

Posso automatizar o rastreamento?

Sim. Selecione “Editor de Tarefas” onde poderá especificar as áreas que deseja que sejam rastreadas e quando.

Como atualizo o NVC?

Use o módulo “Norman Internet Update” (NIU) para atualizar o NVC. Para configurar o NIU, use o diálogo na aba **Internet** no editor de configuração (**Instalação e atualização de produtos**). Esta caixa de diálogo permite que você decida de que forma o NIU deverá realizar a atualização.

Como devo tratar os arquivos de atualização que baixei?

Deixe tudo por conta do NVC. Uma vez baixado o pacote, o agente do NVC irá executar a tarefa de atualização inteiramente sozinho, automaticamente. Em algumas poucas situações, o NVC poderá exigir que re-inicie seu computador.

De quanto em quanto tempo devo atualizar o NVC?

Recomendamos executar o NIU uma vez por dia. O site da Norman fornece informações sobre novos vírus, e em alguns países, se encontra disponível um serviço de aviso por email (consulte www.datasafe.srv.br).

Se achar um vírus, devo entrar em contato com a Norman?

De uma maneira geral, não. O NVC é capaz de remover a grande maioria dos vírus. Siga as instruções na tela para tal.

NVC em conjunto com outro programa antivírus

“Depois de instalar o NVC junto com uma outra solução de antivírus, o computador congelou e recebo diversas mensagens de erro.”

Diferentes produtos antivírus podem "brigar", na medida em que ambos querem rastrear o mesmo arquivo no mesmo momento.

Isso com certeza esta desestabilizando o seu micro e criando um comportamento estranho.

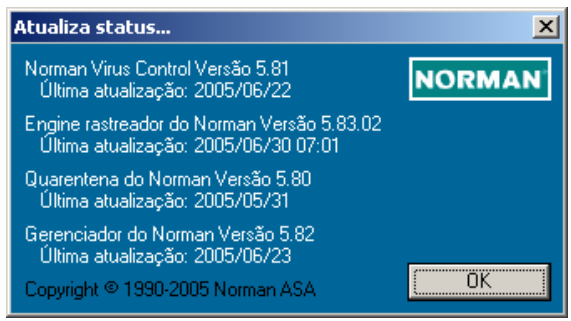
Recomendação: Você deve desinstalar o outro antivírus antes de instalar o NVC.

Se isso acontecer em máquinas Windows NT4, 2000, ou XP, você pode ter que iniciar o seu micro no modo de segurança antes que consiga desinstalar um dos antivírus. Para entrar em modo de segurança, pressione a tecla F8 durante o boot, antes que o Windows seja carregado.

Informações e versão do NVC5: Como checo que o meu NVC está atualizado?

Você pode encontrar a versão do NVC escolhendo em **Atualiza status** no menu do ícone do Norman em sua barra de tarefas (N).

Ali você encontrará os números para a versão do NVC, versão do engine rastreador, quarentena do Norman e do gerenciador do Norman. Os arquivos de definição de vírus - tanto binários como de macro - estão inseridos dentro do engine rastreador:



Para considerar o seu Norman Virus Control como atualizado, veja em nosso site (www.datasafe.srv.br) os números que aparecem em nossa página e compare-os com os que constam em sua instalação.

Não se preocupe com a diferença existente entre as versões do NVC e do Rastreador, pois este último tem seu número de versão em função de métodos internos no desenvolvedor.

Índice

—A—

—B—

—C—

—D—

—E—

—F—

—G—

—H—

—I—

—L—

—M—

—N—

—O—

—P—

—Q—

—R—

—S—

—T—

—U—

—V—

—W—

—Z—