

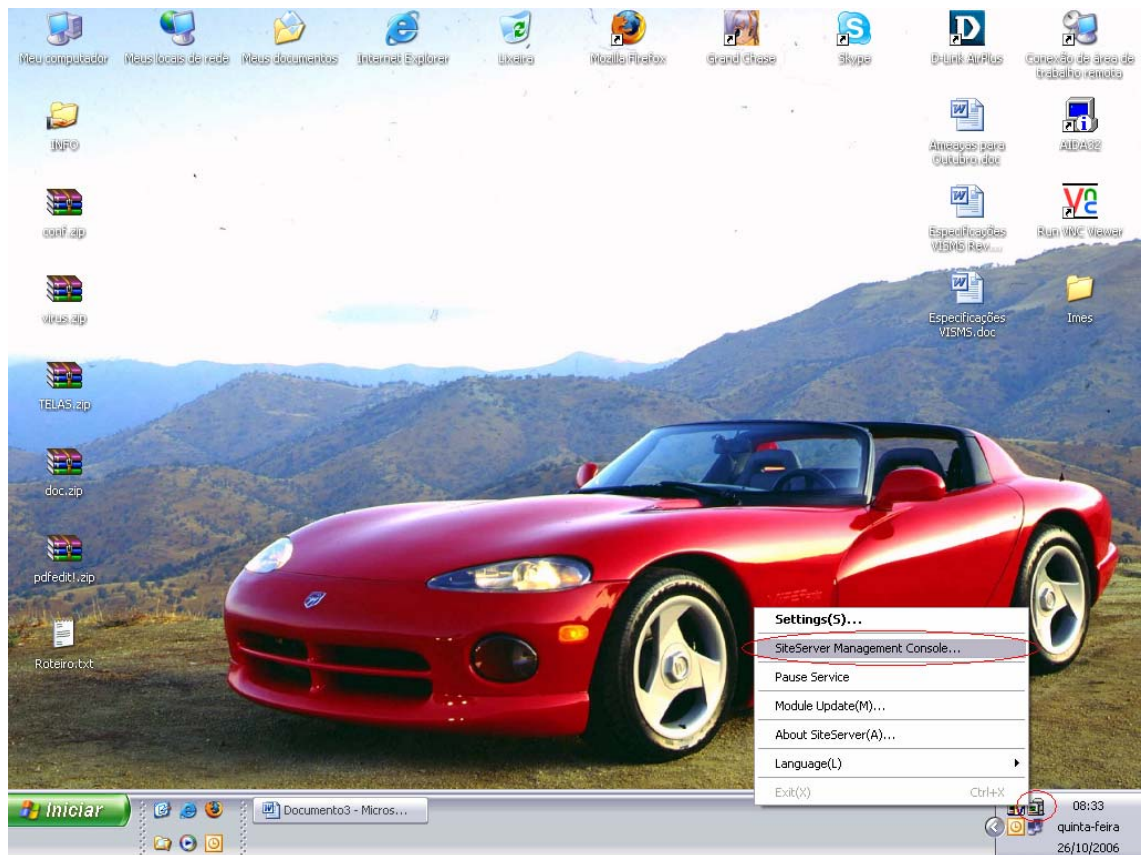
Manual de Configuração de Policy VISMS 3.0

Este manual tem como objetivo ajudar o usuário nas configurações das Policy do VISMS 3.0

Caso tenha alguma dúvida não esclarecida neste manual, favor entrar em contato com sua revenda ou enviar e-mail para suporte@hauri.com.br.

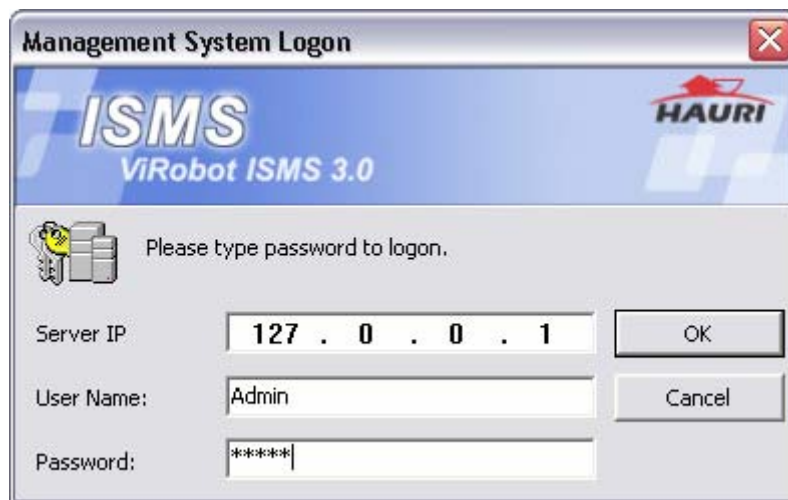
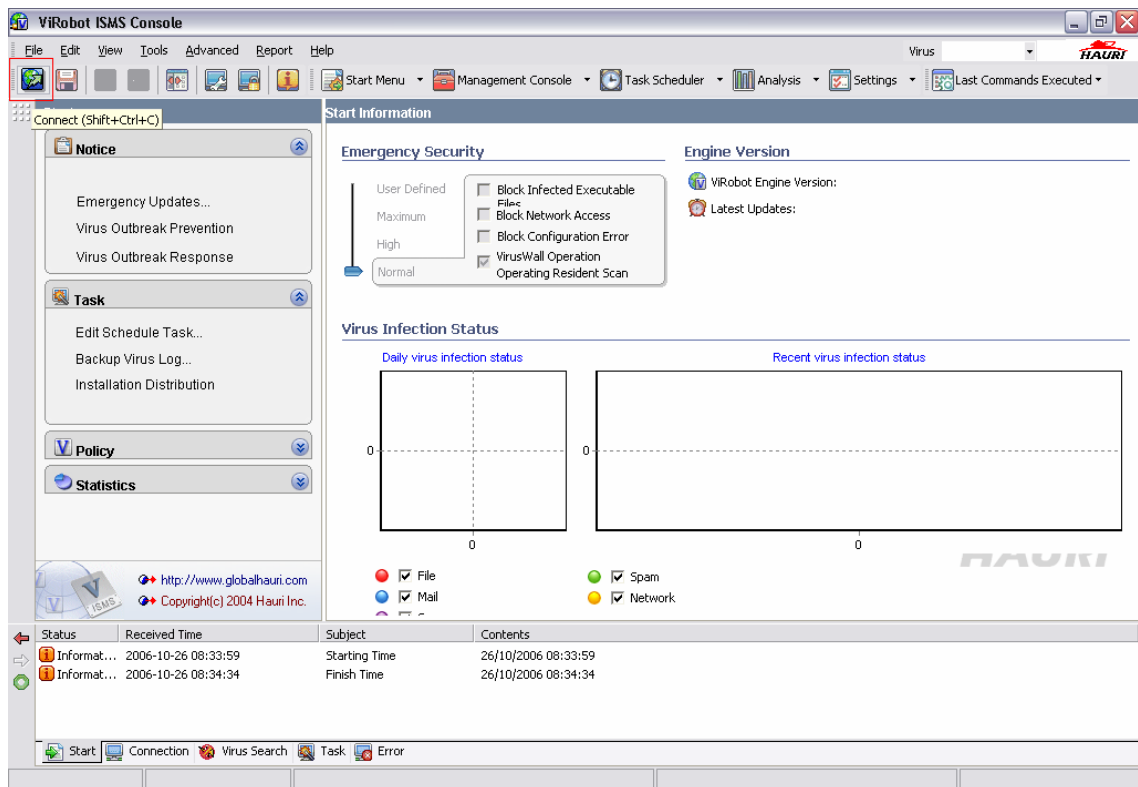
1. – Entrando no console de gerenciamento:

Clique com o botão direito do mouse no ícone Site Server 3.0, localizado ao lado do relógio do Windows, e selecione a opção Site Server Management Console.



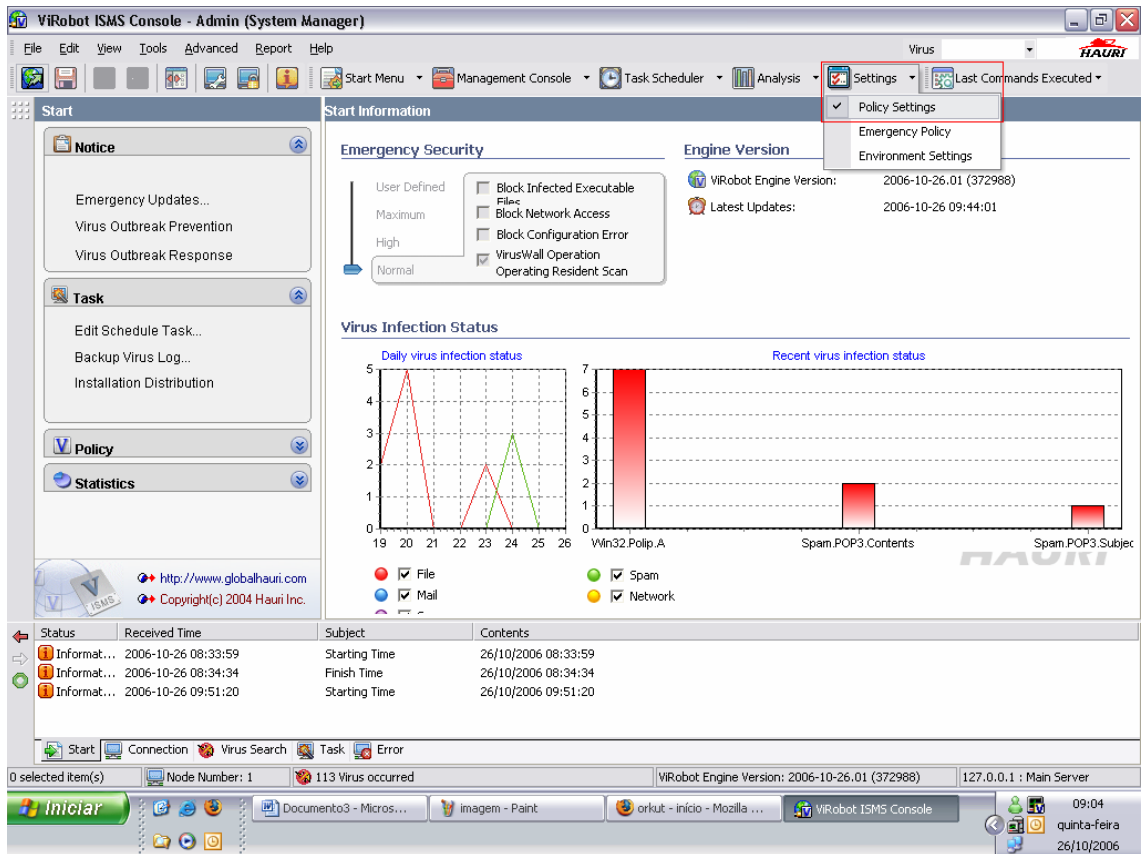
1.1. – Agora é preciso logar-se no console de gerenciamento para que possamos fazer e aplicar as alterações.

Para isso, clique no botão Conect no canto superior direito da tela principal do Management Console, e preencha a tela com seu usuário e senha.



2. – Chegando até as Configurações de Policy.

Após estar logado no Console, siga para o botão Settings>Policy Settings.

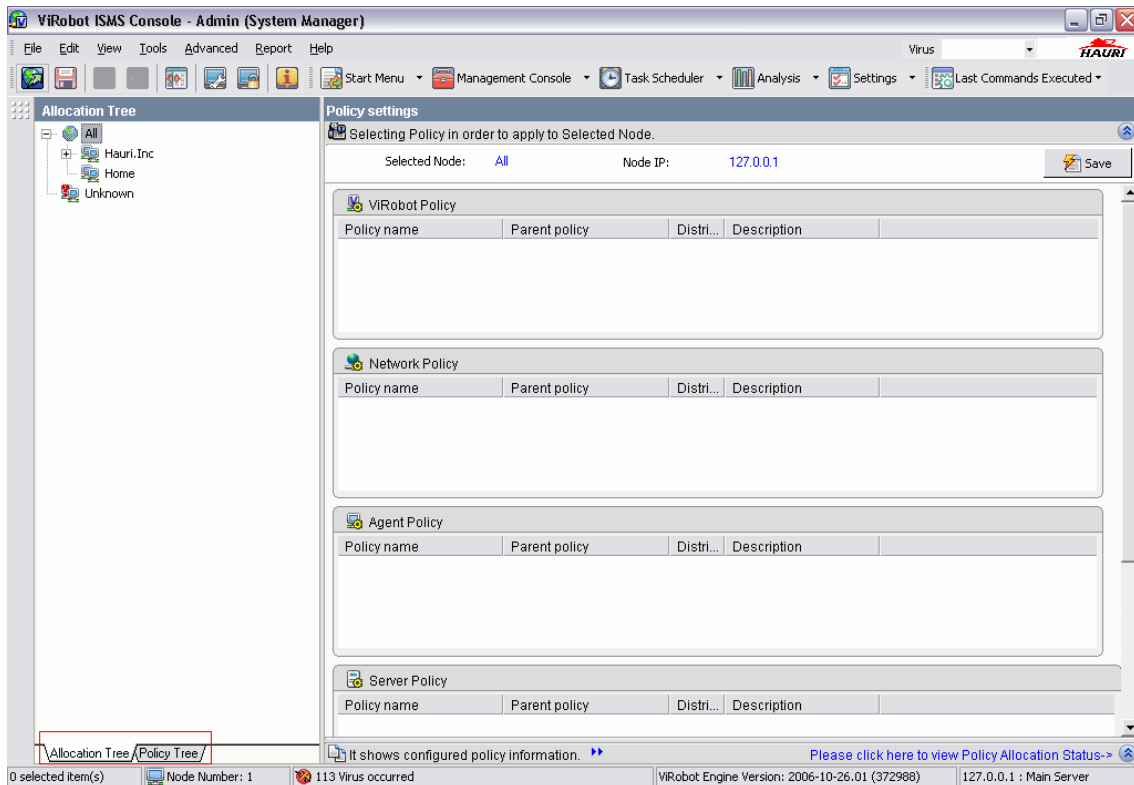


2.1. – Estamos agora na tela de aplicação de Policy, mas não temos nenhuma Policy configurada, antes de aplicarmos precisamos criá-las.

Na parte inferior esquerda temos 2 abas,

- Allocation Tree: Alocação de Policy, é o local onde aplicaremos a Policy após ela ter sido criada.

- Policy Tree: É o local onde criamos a Policy.



3. – Criando uma Policy

Temos 5 tipos de Policy:

- Protection Strategy: Configurações preventivas em caso de ataque virótico.
- ViRobot – Configurações do ViRobot Desktop 5.0.
- Network – Configurações do ViRobot VirusWall.
- Agent – Configurações do SiteClient.
- Server – Configurações para o Servidor e seus Sub-Servers.

Começaremos agora a criar Policy por Policy, lembrando que sempre que formos criar uma nova Policy devemos seguir os seguintes passos:

- Clique no tipo de Policy a ser criada:



- Clique em New Policy:



Agora você já tem sua Policy criada, mas ainda está sem configuração nenhuma, vamos configura-las uma a uma seguindo os tópicos abaixo.

Obs: Sempre desmarque a opção Inheriting from Parent, para que o painel de modificação

3.1. – Protection Strategy Policy:

Na aba Outbreak Prevention:

- Tire a Seleção de Inheriting from Parent.
- Coloque o Level 3 para manual.

The screenshot shows the configuration interface for a Protection Strategy Policy. It is divided into two main sections: 'Policy settings' and 'Protection strategy policy settings'.

Policy settings

- Policy Name: Protection strategy_Template1
- Description: (empty field)
- Parental Policy: (dropdown menu with a grey background and a three-dot icon)
- Saving Date: 26/10/2006 12:25:54

Protection strategy policy settings

Outbreak Prevention | Outbreak Response

Setting Outbreak Prevention Service Level.

- Inheriting from Parent (highlighted with a red box)
- Enable Outbreak Prevention Service

Level 1: Automatic Manual

Level 2: Automatic Manual

Level 3: Automatic Manual

Outbreak Prevention Feature prevents Outbreaks of New Viruses by Pattern Analysis.

3.1.1. – Outbreak Response

- Somente retire a opção Inheriting from Parent.

Policy settings

Policy Name: Protection strategy_Template1


Description:

Parental Policy: ...

Saving Date: 26/10/2006 12:25:54

Protection strategy policy settings

Outbreak Prevention **Outbreak Response**

 Recovery and patch of infected file and registry is performed automatically according to infection status.

Inheriting from Parent

Enable Outbreak Response Feature

Level 1

Automatic Manual

Level 2

Automatic Manual

Level 3

Automatic Manual

3.2. – ViRobot Policy

- Selecione a opção Advanced;

3.2.1 – Vírus Scan:

Agora na aba Vírus Scan, no sub-menu General Scan faça as seguintes alterações:

- Marque as check box:

- Exclusion Settings for Threat Scan.
- Auto Termination of there`s no Threats Detected

Em Failed to repair/Unrepairable coloque:

- Auto Delete.

Policy settings

Policy Name:

Description:

Parental Policy:

Saving Date:

ViRobot policy settings ● General ● **Advanced**

Virus Scan Spy/Adware Scan Mail Protection Access Control Restriction Policy Other Configurations

General Scan
 Real-Time Monitoring
 Protect Messenger
 Scheduled Scan

Inheriting from Parent

Scan Target Settings

All Files Advanced

MS Office Files

Executable Files

User Defined Extension

Include Compressed File

Exclusion Settings for Threat Scan

Auto Termination if there's no Threats Detected

Making Signal when a Virus Found

Create Log

Scan Operation Settings

When Threats Detected

Failed to repair/Unrepairable

Option Settings for Program Start-up

Progress Memory Scan

Progress Process Scan

Progress Boot Sector Scan

Scan ViRobot Self Infection

No sub-menu Real-Time Monitoring:

- Marque as check box:
 - Executable Files;
 - Registered as Hidden mode.

Em Failed to repair/Unrepairable coloque:

- Auto Delete.

Policy settings

Policy Name:

Description:

Parental Policy: ...

Saving Date:

ViRobot policy settings General **Advanced**

Virus Scan | Spy/Adware Scan | Mail Protection | Access Control | Restriction Policy | Other Configurations

General Scan
 Real-Time Monitoring
 Protect Messenger
 Scheduled Scan

Inheriting from Parent

Scan

All Files(A)

Executable Files(E)

MS Office Files(O)

User Defined Extension(U)

Auto-Run Resident Scan upon Windows Start-up

Floppy Disk Boot Scan upon Windows Shutdown

Create Log

Set up Repair

Registered as Hidden mode

Repairable

Failed to repair/Unrepairable

No sub-menu Protect Messenger:
Em Failed to repair/Unrepairable coloque:
- Auto Delete.

Policy settings

Policy Name:

Description:

Parental Policy: ...

Saving Date: 4/11/2006 23:30:51

ViRobot policy settings General **Advanced**

Virus Scan | **Spy/Adware Scan** | Mail Protection | Access Control | Restriction Policy | Other Configurations

General Scan Real-Time Monitoring **Protect Messenger** Scheduled Scan

Inheriting from Parent

Internet Messenger Protection

Protecting Internet Messenger from Viruses

Include Compressed File

Create Log

Set up Repair

Display the alert message to the user

Repairable

Failed to repair/Unrepairable

3.2.2 – Spy/Adware Scan:

Marque as check box:

- Scan Adware;
- Spyware;
- Key Logger;
- Remote Control Program;
- Adware;
- Joke;
- Etc.

Em When Detecting Spy/Adware coloque a opção:

- Delete without confirmation during repair(delete).

Policy settings

Policy Name:


Description:

Parental Policy: ...

Saving Date: 4/11/2006 23:30:51

ViRobot policy settings General Advanced

Virus Scan **Spy/Adware Scan** Mail Protection Access Control Restriction Policy Other Configurations

 Delete spyware, adware, key logger, joke, remote control program. Set up the scan configure against Potentially Unwanted Program.

Inheriting from Parent

set up Scan

Scan Adware Advanced

Spyware Adware

Key logger Joke

Remote Control Program Etc.(Potentially Unwanted)

Create Log

Set up Repair

When detecting Spy/Adware ▾

If need to change the Internet Home page when repairing the infected file.

Address:

Set up Monitoring

Set Monitoring

The detected Spy/Adware will be repaired automatically if set up Monitoring.

Scan Interval ▾ Every Hour

Display Alert message when Spy/Adware Diagnosis

3.2.3 – Mail Protection:

Marque as check box:

- Enable Spam Filtering;
- Enable Malicious Script Scan;
- Support Mail Attached File Scan.

Em Failed to Repair/Unrepairable coloque a opção:

- Auto Delete.

Em Limit of Mail Size coloque o tamanho MÁXIMO de e-mail que deseja receber, qualquer e-mail acima do valor estipulado, serão ignorados e excluídos.

Policy settings

Policy Name:


Description:

Parental Policy: ...

Saving Date:

ViRobot policy settings General Advanced

Virus Scan Spy/Adware Scan **Mail Protection** Access Control Restriction Policy Other Configurations

 E-mail Protector is monitoring E-mail packets on real-time and blocking all Virus, Worm, Spam. Set up the Configuration for E-mail protection.

Inheriting from Parent

Set up Scan

Auto-Run E-mail Protector upon System Boot-up

Include Compressed File

Create Log

Set up Repair

Display the alert message to the users

Repairable

Failed to repair/Unrepairable

Applicable Range

Limit of Mail size Kbyte(s)

Script-Gater

Enable Spam Filtering

Enable Malicious Script Scan

Support Mail Attached File Scan

3.2.4 – Access Control:

Marque as check box:

- Inheriting from Parent.

Policy settings

Policy Name:


Description:

Parental Policy: ...

Saving Date: 4/11/2006 23:30:51

ViRobot policy settings General Advanced

Virus Scan Spy/Adware Scan Mail Protection **Access Control** Restriction Policy Other Configurations

 Access Control is that it protects the important files by allowing the only authorized users have an access to the selected files. Set up the configuration for Access Control.

Inheriting from Parent

General Environment Settings

- Auto-Run File System Access Control upon Bootup
- Set Hauri Product Protection (Recommended)
- Create Log

3.2.5 – Restriction Policy:

Marque as check box:

- Use Full UI;
- Password Settings for Real-time Monitor;
- Client LockDown Configuration Options.

No campo de texto digite a senha desejada para destravar as configurações do antivírus nas estações.

- Allow Vírus Scan Configuration.

Desmarque todas as outras check box.

Policy settings

Policy Name:


Description:

Parental Policy: ...

Saving Date: 4/11/2006 23:30:51

ViRobot policy settings General Advanced

Virus Scan Spy/Adware Scan Mail Protection Access Control **Restriction Policy** Other Configurations

 Password can be set to lockdown Environment Settings and Real-time Monitor.

Inheriting from Parent

ViRobot UI Settings

No Change Use Full UI Use Easy UI

Password Settings

Password Settings for Real-time Monitor

Client Lockdown Configuration Options

Password:

Lockdown ViRobot Configuration

Allow ViRobot Advanced Settings Configuration

Allow Virus Scan Configuration

Allow Firewall Configuration

Allow Mail Scan Configuration

Allow Access Control Configuration

Allow Quarantine Configuration

Allow Log Manager Configuration

Allow Resident Scan Configuration

Allow Malicious Program Configuration

Allow Messenger Protection Configuration

Allow Other Environment Settings Configuration

3.3. – Network policy:

Em Basic Information marque as check box:

- Enable Pc Firewall;
- Enable network Access Control Policy.

Policy settings

Policy Name:


Description:

Parental Policy: ...

Saving Date: 5/11/2006 00:08:53

Network policy settings

Basic Information | Network Rule | Process Rule | Settings | Restriction Policy | Share Folder

 Setting Security Items of PC Firewall.

Inheriting from Parent

Enable PC Firewall

Component

Use Network Block Feature

Enable Network Access Control Policy

Enable Process Access Control Policy

Enable Emergency Lock

3.4. – Client policy:

Em Connection Time Interval coloque o tempo em segundos para que os clientes se conectem com o servidor em busca de atualizações.

- Recomendamos entre 3600 e 7200 segundos.

Policy settings

Policy Name:


Description:

Parental Policy:

Saving Date:

Client policy settings

General | Notify | Update | Virus Protection | Restriction Policy | Window

 Modifying server Connection Time Interval and server address in agent.

Inheriting from Parent

Connection Time Interval
In every: Second(s)

Server Settings

Remove Server Address in Agent

Main Server or Sub-server Address:

| Server Address | Description |
|----------------|-------------|
| | |

3.4.1. – Notify:

Em Basic Information marque as check box:

- Hide Virus Repair Confirmation Window;
- Auto Repair.

Desmarque a check box:

- Show Instant Message.

Policy settings

Policy Name:


Description:

Parental Policy: ..

Saving Date: 5/11/2006 00:13:58

Client policy settings

General **Notify** Update Virus Protection Restriction Policy Window

 Select Notification Options.

Inheriting from Parent

Management Server

Display Auto-Update Window on Client Computer.

Show ViRobot Auto-Update Window

Select ViRobot Resident Display Option

Display ViRobot Resident Icon in Windows System Tray
(This option is inapplicable to ViRobot Advanced Server.)

Show ViRobot Resident Icon in Windows System Tray.

Select Message Display Options

User Notification Display Options.

Show Instant Message

Show Windows NT Message

Display Settings for Repair Confirmation Window

Choose Confirmation Window to be displayed at Client Computer.

Hide Virus Repair Confirmation Window

Auto-Repair (Do not repair if it's not set)

3.4.2. – Update:

Marque as 2 check box:

- ViRobot Update>Update through VISMS Server;
- Upon Click Update Button in ViRobot Desktop> Update through VISMS Server.

Policy settings

Policy Name:

Description:

Parental Policy:

Saving Date: 5/11/2006 22:41:56

Client policy settings

General Notify **Update** Virus Protection Restriction Policy Window



Configure Update Options

Inheriting from Parent

Intelligent Client Robot

Update via nearby client enables rapid distribution without network load for slow network or separated location.

Enable Intelligent Client Robot.

Report Update Error

Report an update error when update has not been performed for a specific

Number of Days :

Days (Default :14 days)

Set Auto-Update Option

Trying Auto-Update upon Clients' Boot-up.

Auto Update upon Boot-up

ViRobot Update

ViRobot Update is available through either VISMS Server or Internet.

Update through VISMS Server

Update through Internet

Upon Click of Update Button in ViRobot Desktop

Update is performed via VISMS Server or Internet.

Update via VISMS Server

Update via Internet

3.4.3. – Restriction Policy:

Em Select Lockdown Option, coloque a opção Disallow All.

Marque a check box:

- Using password for service lock, e coloque a senha que desejar;

Policy settings

Policy Name:


Description:

Parental Policy:

Saving Date: 5/11/2006 22:41:56

Client policy settings

General Notify Update Virus Protection **Restriction Policy** Window

 Apply a restriction policy to selected VMS clients in order to prevent them from configuring certain ViRobot options.

Inheriting from Parent

Client Lockdown Configuration Options

Select Lockdown Option :

Set Client Un-installation Password

Enter a password to prevent clients from removing VMS Client (Default: agentdown)

Un-installation Password:

No Password


Set up the password for client's service discontinue

Set up the password to prevent the discontinue of agent service by the user (Windows XP,NT,2000,2003)

using password for service interruption

password for client interruption

Restrict Update Time Settings

 Set a restricted time during which update is not to be performed.

Apply Update Restriction Cancel Update Restriction

Time : -

client message transmitting

The user allows or restricts the message transmitting to others.

using the instance message

3.5. – Server:

3.5.1. – General:

No campo Connection Time Interval, coloque o tempo desejado para que o servidor saia em busca de atualizações nos servidores Hauri.(Recomendamos entre 3600 e 7200 segundos).

Policy settings

Policy Name:

Description:

Parental Policy: ...

Saving Date:

Server policy settings

General | Advanced | Administrator | Network | Log | Others



General Settings can be changed.

Inheriting from Parent

Location Settings

Anti-Virus Directory:

Download Directory: ...

Connection Time Interval

In every: Seconds