

Etapas da configuração inicial de sistemas de FireSIGHT

Índice

[Introdução](#)

[Pré-requisito](#)

[Configuração](#)

[Passo 1: Instalação inicial](#)

[Passo 2: Instale licenças](#)

[Passo 3: Aplique a política do sistema](#)

[Passo 4: Aplique a política sanitária](#)

[Passo 5: Dispositivos gerenciado do registro](#)

[Passo 6: Permita licenças instaladas](#)

[Etapa 7: Configurar a detecção de relações](#)

[Passo 8: Configurar a política da intrusão](#)

[Etapa 9: Configurar e aplique uma política do controle de acesso](#)

[Etapa 10: Verifique se o centro de gerenciamento de FireSIGHT recebe eventos](#)

[Recomendação adicional](#)

Introdução

Depois que você nova imagem um centro de gerenciamento de FireSIGHT ou um dispositivo de FirePOWER, você precisa de terminar diversas etapas para fazer inteiramente o sistema - funcional e para gerar alertas para eventos da intrusão; como, instalando a licença, registrando os dispositivos, aplicando a política sanitária, a política do sistema, a política do controle de acesso, a política etc. da intrusão. Este original é um suplemento ao guia de instalação de sistema de FireSIGHT.

Pré-requisito

Este guia supõe que você leu com cuidado o guia de instalação de sistema de FireSIGHT.

Configuração

Passo 1: Instalação inicial

Em seu centro de gerenciamento de FireSIGHT, você deve terminar o processo de instalação registrando na interface da WEB e especificando opções de configuração inicial na página de instalação, descrita abaixo. Nesta página, você deve mudar a senha de admin, e pode igualmente especificar configurações de rede tais como o domínio e os servidores DNS, e a configuração do tempo.

Change Password

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password

Confirm

Network Settings

Use these fields to specify network-related information for the management interface on the appliance.

Protocol IPv4 IPv6 Both

IPv4 Management IP

Netmask

IPv4 Default Network Gateway

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

Time Settings

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock Via NTP from

Manually 2013 ▾ / July ▾ / 19 ▾ , 9 ▾ : 25 ▾

Current Time 2013-07-19 09:25

Set Time Zone [America/New York](#)

Você pode opcionalmente configurar atualizações de retorno da regra e do geolocation assim como backup automáticos. Todas as licenças de recurso podem igualmente ser instaladas neste momento.

Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

Install Now

Enable Recurring Rule Update Imports

Recurring Geolocation Updates

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

Install Now

Enable Recurring Weekly Updates

Automatic Backups

Use this field to schedule automatic configuration backups.

Enable Automatic Backups

License Settings

To obtain your license, navigate to _____ where you will be prompted for the license key _____ and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can.

License Key _____

Add/Verify

Type	Description	Expires
------	-------------	---------

Nesta página, você pode igualmente registrar um dispositivo ao centro de gerenciamento de FireSIGHT e especificar um modo de detecção. O modo de detecção e as outras opções que você escolhe durante o registro determinam as interfaces padrão, os grupos inline, e as zonas que o sistema cria, assim como as políticas que aplicam inicialmente aos dispositivos gerenciado.

Device Registration

Use this section to add, license, and apply initial access control policies to pre-registered devices. Note that you do not need to add devices to the secondary Defense Center in a high availability pair. If you enable the Apply Default Access Control Policies option, the applied policy for each device depends on the detection mode (Inline, Passive, Access Control, or Network Discovery) you configured for the device.

Click Add to add each device.

Apply Default Access Control Policies

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Add"/>

End User License Agreement

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT, THEN SOURCEFIRE IS UNWILLING TO LICENSE THE LICENSED MATERIALS TO YOU, IN WHICH CASE YOU MAY NOT DOWNLOAD, INSTALL OR USE ANY OF THE LICENSED MATERIALS.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT INITIATE USE OF THE PRODUCT. BY SELECTING "I ACCEPT," "OK," "CONTINUE," "YES," "NEXT" OR BY INSTALLING OR USING THE LICENSED MATERIALS IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE PRODUCT.

If You are located outside of the United States, then Sourcefire International GmbH, a subsidiary located in Switzerland, shall be a party to this Agreement with You and the party licensing the Licensed Materials to You hereunder. This Agreement governs Your access and use of the Sourcefire Products, except to the extent there is a separate written agreement signed by both You and Sourcefire that expressly states that it governs Your use of the Sourcefire Products. In the event of a conflict between the provisions of such a written agreement and this Agreement, the order of precedence shall be (1) the separate signed agreement, and (2) this Agreement.

1. DEFINITIONS

The following capitalized terms shall have the following meanings in this EULA:

1.1. "Appliance" means any Sourcefire-branded network security appliance made available to You, consisting of Hardware and pre-installed Sourcefire Software and/or

I have read and agree to the END USER LICENSE AGREEMENT

Passo 2: Instale licenças

Se você não instalou licenças durante a página de instalação inicial, você pode terminar a tarefa seguindo estas etapas:

- Navegue à seguinte página: **Sistema > licenças**.
- Clique **adicionam** sobre a **licença nova**.

Add Feature License

License Key

License

Get License

Verify License

Submit License

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to

Using the license key, follow the on-screen instructions to generate a license.

Return to License Page

Se você não recebeu uma licença, contacte o representante de vendas de sua conta.

Passo 3: Aplique a política do sistema

A política do sistema especifica a configuração para perfis da autenticação e a sincronização de tempo entre o centro de gerenciamento de FireSIGHT e os dispositivos gerenciado. Para configurar ou aplicar a política do sistema navegue ao **sistema > à política do Local > do sistema**. Uma política do sistema padrão é fornecida mas precisa de ser aplicada a todos os dispositivos gerenciado.

Passo 4: Aplique a política sanitária

A política sanitária é usada para configurar como os dispositivos gerenciado relatam seu estado de saúde ao centro de gerenciamento de FireSIGHT. Para configurar ou aplicar a política sanitária navegue à **saúde > à política sanitária**. Uma política sanitária do padrão é fornecida mas precisa de ser aplicada a todos os dispositivos gerenciado.

Passo 5: Dispositivos gerenciado do registro

Se você não registrou dispositivos durante a página de instalação inicial, leia [este original](#) para instruções em como registrar um dispositivo a um centro de gerenciamento de FireSIGHT.

Passo 6: Permita licenças instaladas

Antes que você possa usar toda a licença de recurso em seu dispositivo, você precisa de permiti-lo para cada dispositivo gerenciado.

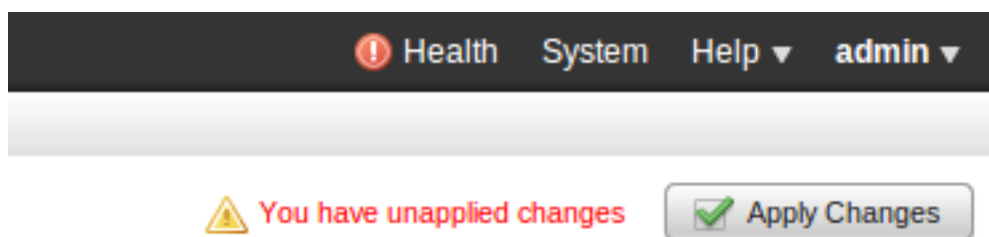
1. Navegue à seguinte página: **Dispositivos > Gerenciamento de dispositivos**.
2. Clique sobre o dispositivo para que você quer permitir as licenças e incorpora a aba do dispositivo.
3. Clique a **edição** (ícone do *lápiz*) ao lado da licença.

License

Protection:	Yes
Control:	Yes
Malware:	Yes
URL Filtering:	Yes
VPN	Yes

Permita as licenças exigidas para este dispositivo e clique a **salv guarda**.

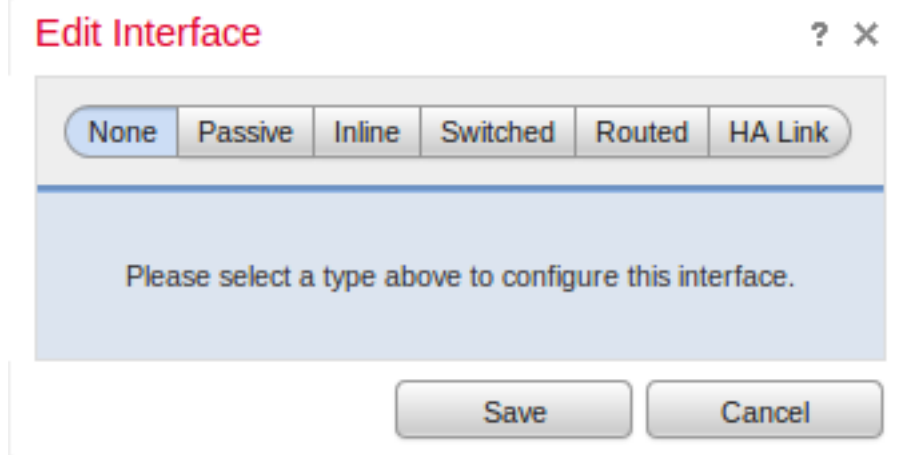
Observe a mensagem “*você para ter mudanças unapplied*” no canto superior direito. Este aviso permanece ativo mesmo se você navega longe da página do Gerenciamento de dispositivos até que você clique o botão das **mudanças da aplicação**.



Etapa 7: Configurar a detecção de relações

1. Navegue aos seguintes **dispositivos > Gerenciamento de dispositivos** da página.
2. Clique o ícone da **edição** (lápiz) para o sensor de sua escolha.

3. Sob as **relações** catalogue, clique o ícone da **edição** para a relação de sua escolha.



Edit Interface ? X

None Passive Inline Switched Routed HA Link

Please select a type above to configure this interface.

Save Cancel

Selecione uma configuração da interface passiva ou Inline. Comutado e as interfaces roteada são além do alcance deste artigo.

Passo 8: Configurar a política da intrusão

- Navegue à seguinte página: **Políticas > intrusão > política da intrusão**.
- Clique sobre a **política Create** e a seguinte caixa de diálogo é indicada:



Create Intrusion Policy ? X

Policy Information

Name *

Description

Drop when Inline

Base Policy

Variables

Use the system default value

Networks to protect

* Required

Create Policy Create and Edit Policy Cancel

Você deve atribuir um nome e definir a política baixa a ser usada. Segundo seu desenvolvimento que você pode escolheu ter a **gota da** opção **quando** permitido **Inline**. Defina as redes que você quer proteger para reduzir falsos positivos e melhorar o desempenho do sistema.

Clicar na **política Create** salvar seus ajustes e criará a política IPS. Se você quer fazer alguma alteração à política da intrusão, você pode escolher **cria e edita a política** pelo contrário.

Nota: As políticas da intrusão são aplicadas como parte da política do controle de acesso. Depois que uma política da intrusão é aplicada, todas as alterações podem ser aplicadas sem reaplicar a política inteira do controle de acesso clicando o botão **reaplicar**.

Etapa 9: Configurar e aplique uma política do controle de acesso

1. Navegue às **políticas** > ao **controle de acesso**.
2. Clique sobre a **política nova**.

New Access Control Policy ? X

Name:

Description:

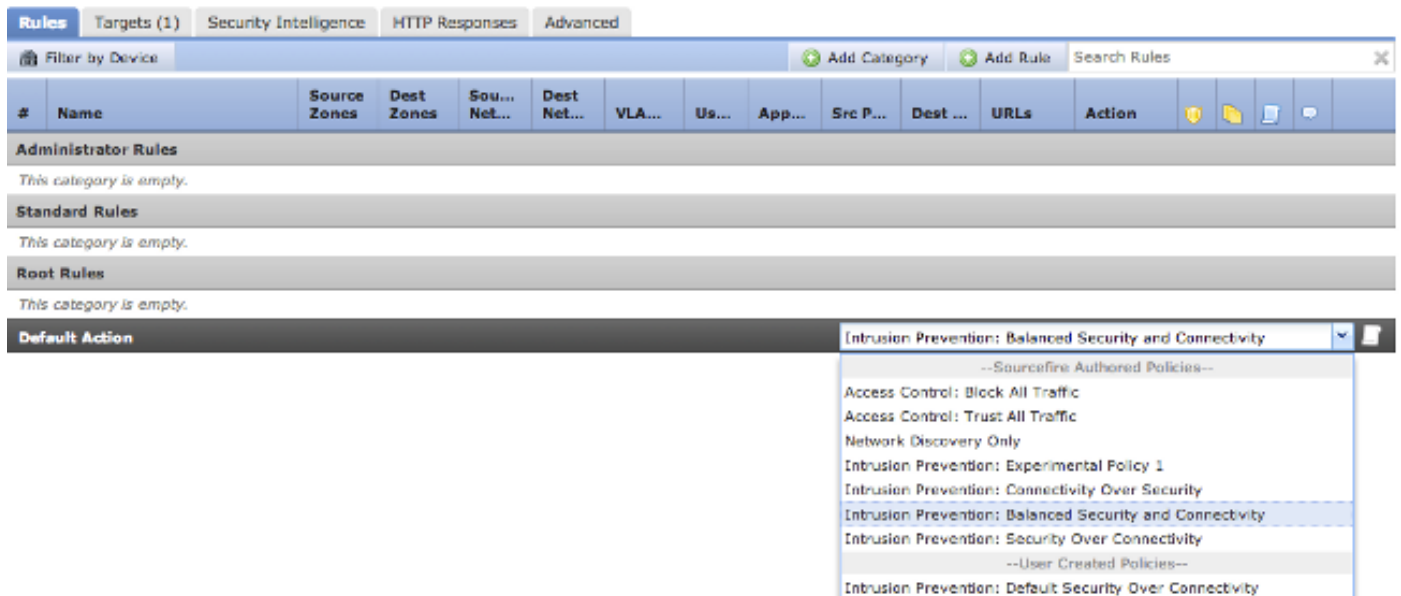
Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

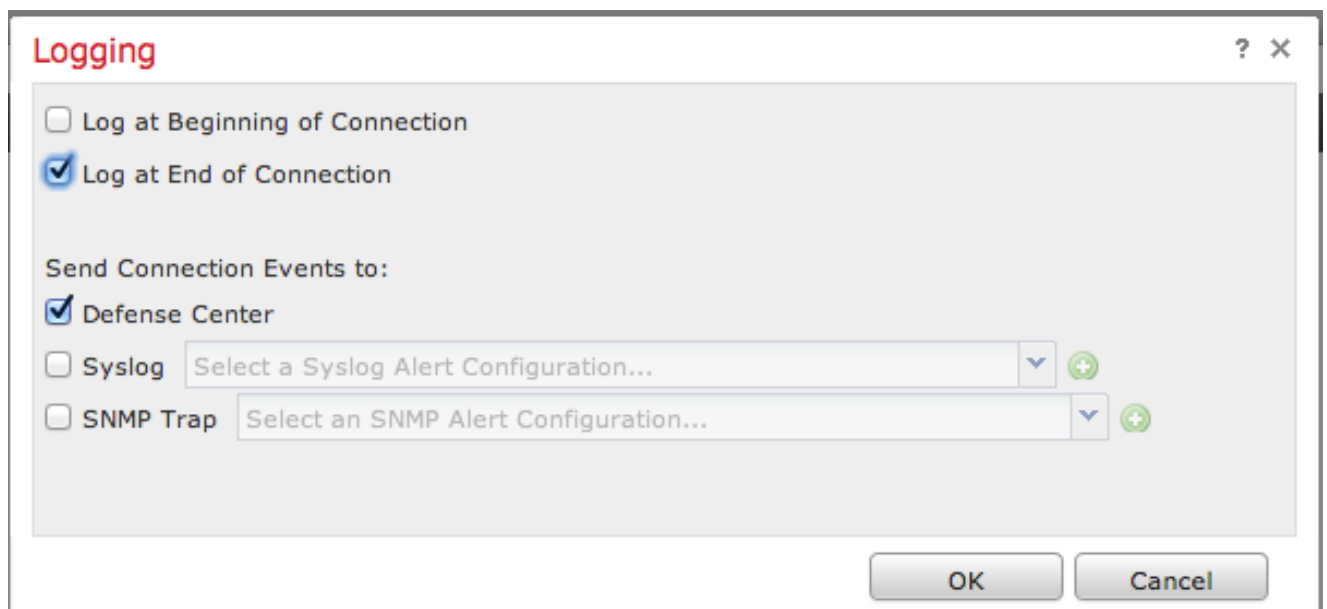
Available Devices

Selected Devices

3. Forneça um **nome** para a política e uma **descrição**.
4. Selecione a **prevenção de intrusão** como a **ação padrão** da política do controle de acesso.
5. Selecione finalmente os **dispositivos visados** a que você quer aplicar a política do controle de acesso, e clique a **salv guarda**.
6. Selecione sua política da intrusão para a ação padrão.



7. O registro da conexão deve ser permitido de gerar eventos de conexão. Clique o menu de gota para baixo que é direito da **ação padrão**.



8. Escolha registrar conexões no começo ou na extremidade da conexão. Os eventos podem ser entrados o centro de gerenciamento de FireSIGHT, um lugar do Syslog, ou com o SNMP.

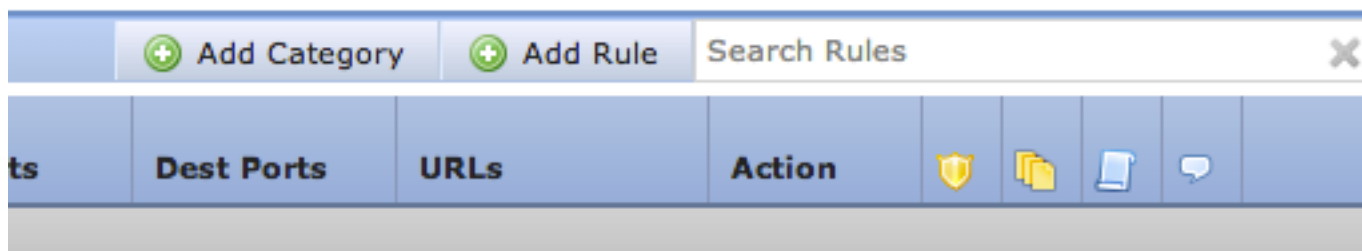
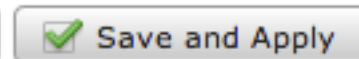
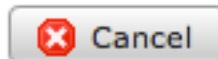
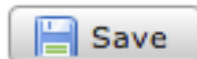
Nota: Não se recomenda registrar no ambas as extremidades da conexão porque cada conexão (exceto conexões obstruídas) será registrada duas vezes. Registrar no início é útil para as conexões que serão obstruídas, e registrar na extremidade é útil para todas conexões restantes.

9. Clique em **OK**. Note que a cor do ícone de registro mudou.

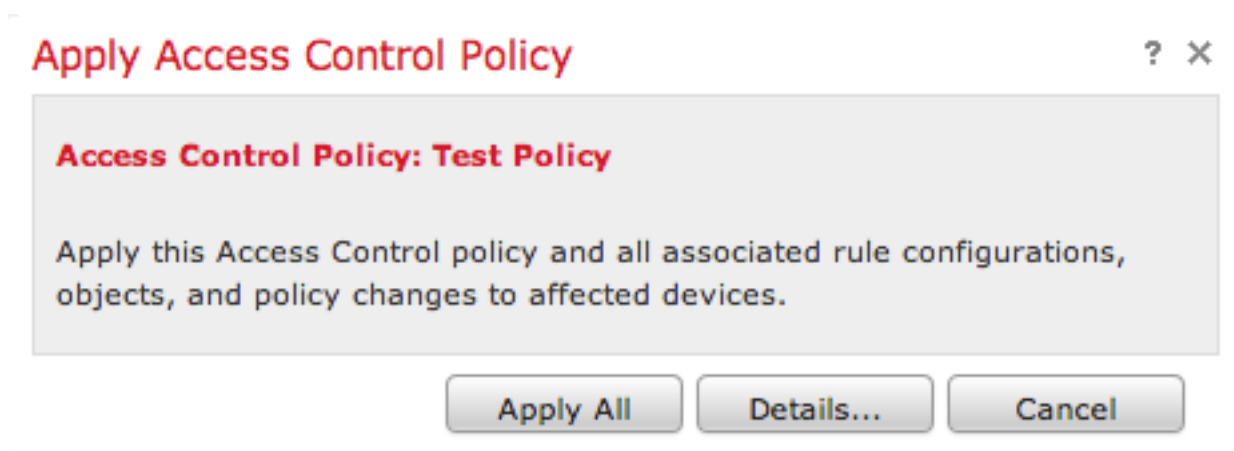
10. Você pode adicionar uma **regra do controle de acesso** neste tempo. As opções que você pode se usar dependem do tipo de licenças você instalou.

11. Quando você é fatura terminada muda. clique a **salvaguarda e o botão Apply Button**. Você observará uma mensagem indicá-lo para ter mudanças unsaved em sua política no canto superior direito até que o botão esteja clicado.

You have unsaved changes



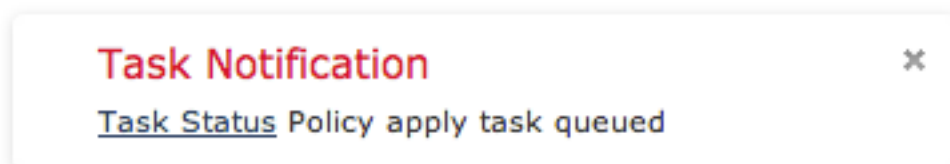
Você pode escolher **salvar** somente as mudanças ou clicar sobre a **salvaguarda e aplicar-se**. o seguinte indicador aparecerá se você escolhe os últimos.



12. **Aplique tudo** aplicará a política do controle de acesso e todas as políticas associadas da intrusão aos dispositivos visados.

Nota: Se uma política da intrusão será aplicada pela primeira vez, não pode ser unselected.

13. Você pode monitorar o estado da tarefa que clica na relação do **estado da tarefa** na notificação mostrada na parte superior da página, ou navegando a: **Estado do sistema > da monitoração > da tarefa**



14. Clique a relação do estado da tarefa para monitorar o progresso da política do controle de acesso aplicam-se.





Job Summary

Remove Completed Jobs

Remove Failed Jobs

Running	0
Waiting	0
Completed	7
Retrying	0
Failed	0

Jobs

Task Description	Message	Creation Time	Last Change	Status	
 Health Policy apply tasks 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
Health policy apply to appliance Health Policy Apply	Health Policy applied successfully	2013-07-19 18:25:39	2013-07-19 18:26:42	Completed	
 Policy apply tasks 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
Apply Default Access Control to Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

Etapa 10: Verifique se o centro de gerenciamento de FireSIGHT recebe eventos

Depois que a política do controle de acesso se aplica terminou, você deve começar ver eventos das conexões e segundo eventos da intrusão do tráfego.

Recomendação adicional

Você pode igualmente configurar os seguintes recursos adicionais em seu sistema. Refira por favor o Guia do Usuário para detalhes de implementação.

- Backup agendado
- Atualização de software automática, SRU, VDB, e transferências de GeoLocation/instalações.
- Autenticação externa através do LDAP ou do RAI0