

Manual Técnico da Distribuição de Video-Vigilância

Manual técnico da Distribuição de Video-Vigilância WinREST



Versão: 1.0.1 Nº de actualizações: 1 2

Pre-

Índice

Requisitos para a instalação do WinREST [®] Videovigilância webserver	
Configuração do WinREST [®] FrontOffice	5
Actualização da licença FO	5
Criação do ficheiro video.ini	5
Configuração do winrest.ini para ativar servido vnc	5
Configuração das câmaras de vídeo vigilância	7
Alteração do IP da câmara	7
Configuração dos parâmetros da câmara	8
Posicionamento da câmara	9
Configuração do servidor de vídeo vigilância	10
Alteração do IP do servidor	11
Alteração da palavra chave	17
Configuração das câmaras	
Configuração dos postos FO	21
Configuração de acesso via internet	24
Alteração das configurações de rede	24
Registo de conta no NO-IP	24
Registo de endereço WDNS	26
Configuração do cliente NO-IP	28
Configuração do cliente WDNS	29
Atualização de versão	29
Ligação à internet via placa USB	29
Configuração de ligação com UPS	
Trobleshooting - resolução de problemas da vídeo-vigilância	

Requisitos para a instalação do WinREST® Videovigilância Webserver

- Computador a correr o sistema operativo Windows, com um browser de internet (Internet Explorer ou Firefox) ligado em rede ao servidor de vídeo vigilância;
- Plug-in para executar no browser aplicações Flash;
- Cliente de VNC instalado no computador acima.
- O utilitário PUTTY para acesso por consola de texto instalado no computador.
- Por motivos de segurança foi criada uma chave de acesso aos servidores de VV, por defeito cada servidor segue com uma chave do Grupo PIE, mas deverão acrescentar uma chave ou até substituir a chave de acesso do Grupo PIE por uma sua, ver abaixo como criar e associar uma chave ao servidor de VV.
- Licença para o WinREST FrontOffice (PRO ou Light) actualizada para a versão 5.8 ou superior e com o módulo de videovigilância activo, (na licença poderá verificar o modulo CONTROL);
- A distribuição WinREST Linux tem que estar na versão 406 ou superior;
- Se utilizar acesso remoto (Internet) ao WinREST® videovigilância webserver precisa ainda de:
 - Ligação à internet de banda larga com pelo menos 256 Kbps de UPLOAD;
 - Registo de conta para DNS dinâmico no www.no-ip.com (ver instruções na secção Configuração para acesso via internet) ou WDNS do GrupoPIE;
 - Conta de e-mail válida ainda não utilizada em nenhum registo no No-IP; (Atenção: esta conta é utilizada para o envio da password de acesso à conta No-IP, pelo que não pode ser uma conta de e-mail ficticia);
 - Se o WinREST[®] FrontOffice estiver instal do em Linux é obrigatória a utilização de um router (ADLS/Cabo) para acesso à Internet;
 - Se utilizar o Windows como sistema operativo do WinREST[®] FrontOffice poderá utilizar modems ADSL/Cabo. Neste caso, poderá ter de:
 - Instalar uma segunda placa de rede no servidor do FrontOffice;
 - Instalar um software de partilha de ligação à Internet;
 - Instalar um software de firewall;

Sugestão: mesmo em Windows, sempre que possível a ligação à internet deve ser feita com um router ADSL/Cabo. Além de maior facilidade na sua instalação, a fiabilidade e segurança são superiores.

Configuração do WinREST® FrontOffice

Actualização da licença de FO

Em Windows:

Na pasta config da sua instalação do WinREST[®] FrontOffice, deve:

- apagar o ficheiro wrstsc00.lic
- copiar o novo ficheiro de licença para esta pasta
- renomear o ficheiro de licença para wrstsc00.lic
- reiniciar o WinREST FrontOffice

Em Linux:

- Copiar o ficheiro da nova licença para a pasta modata/license da pen usb
- Arrancar com a pen usb no servidor e escolher o módulo "Licenciar programas"
- Escolher a licença correcta e pressionar OK.

Criação do ficheiro video.ini

Em Windows:

- Na máquina servidor do FO, navegar até à pasta onde se encontra o executável WinREST (por defeito é C:\Programas\GrupoPIE\WinREST)
- Criar nesta pasta uma nova pasta chamada log
- Na pasta log criar um ficheiro de texto chamado video.ini ou edita-lo se já existir
- Inserir as seguintes linhas neste ficheiro:
- Socket=IP do servidor de vídeo vigilância:2828 (porta a usar obrigatório usar esta porta)
- ClassControl=3

Em Linux:

- Num computador com Windows, aceder ao servidor do FO e navegar até à pasta /home/WinREST
- Criar nesta pasta uma nova pasta chamada log
- Na pasta log criar um ficheiro de texto chamado video.ini ou edita-lo se já existir
- Inserir as seguintes linhas neste ficheiro:
 - Socket=IP do servidor de vídeo vigilância: 2828 (porta a usar obrigatório usar esta porta)
 - ClassControl=3

Configuração do winrest.ini para activar servidor vnc

Em Windows:

- Na máquina servidor do FO, navegar até à pasta onde se encontra o executável WinREST[®] (por defeito é C:\Programas\GrupoPIE\WinREST)
- Criar nesta pasta um ficheiro de texto chamado winrest.ini ou edita-lo se já existir
- Inserir as seguintes linhas neste ficheiro (no fim do ficheiro):
 - VNCServer=Yes
 - VNCExclusive=No

Em Linux:

- Num computador com Windows, aceder ao servidor do FO e navegar até à pasta /home/WinREST
- Criar nesta pasta um ficheiro de texto chamado winrest.ini ou editá-lo se já existir
- Inserir as seguintes linhas neste ficheiro (no fim do ficheiro):
 - VNCServer=Yes
 - VNCExclusive=No

Nota: para gravar a imagem de múltiplos postos de WinREST[®] é necessário que seja configurado o ficheiro vídeoconfig. O WinREST[®] vai reger-se por este ficheiro para criar ou não imagens VNC para o servidor de vídeo vigilância, este ficheiro deverá estar localizado na pasta config do FO com o seguinte conteúdo:

#!/bin/bash # Socket="192.168.0.150" VideoServers="1 2"

Neste caso vai a imagem do WinREST[®] vai estar disponível para o servidor do IP 192.168.0.150 para os postos 1 e 2;

Configuração das câmaras de vídeo vigilância

Alteração do IP da câmara

Alterar o IP das câmaras pode ser feito de varias formas sendo que as mais simples são as seguintes:

Utilizando o utilitário da AXIS podemos pesquisar todos os dispositivos da AXIS na rede, mesmo que estejam em gamas de ip's diferentes, isto permite rapidamente alterar IP's e/ou configurações.



Para proceder à alteração do ip, basta clicar com o botão direito do rato na câmara em questão e escolher a opção ASSIGN IP, como mostra a imagem abaixo:



Caso não disponha deste software, pode no entanto configurar da seguinte forma:

- Ligar a câmara ao hub de rede e à corrente eléctrica
- Numa máquina em windows, com endereço IP na mesma gama do da câmara (192.168.0.xxx)
- ligada em rede, abrir uma janela de DOS. Para abrir uma janela de DOS faça:
 - Iniciar->executar
 - Escreva cmd e pressione enter
- Na janela de DOS escreva o seguinte comando
 - arp –s "IP escolhido" "mac address da câmara"
- e em seguida este comando
 - ping -l 408 -t "IP escolhido"
 - sem parar o comando anterior, desligue e volte a ligar a câmara
 - quando obtiver resposta ao comando ping, pressione ctrl-c para o parar e feche a janela de DOS

Nota: Se o IP a configurar for o 192.168.0.151 e se o MAC Address da câmara (que se encontra no autocolante no corpo da mesma) for 00:01:02:03:04:05, as instruções acima devem ser escritas da seguinte forma: arp -s 192.168.0.151 00-01-02-03-04-05 ping -l 408 -t 192.168.0.151 Nota 2: O IP por defeito destas câmaras é o 192.168.0.90

Configuração dos parâmetros da câmara

- Após ter efectuado o passo anterior, vamos testar e configurar a câmara. Na mesma máquina Windows utilizada no ponto anterior abra um browser de Internet (Internet Explorer ou Firefox)
- Digite na barra de endereços http://"IP da câmara"
- Neste momento deve estar a ver no seu browser a seguinte imagem

AXIS	🕮 📧 💽 💷 📟 📟
Configure Root Passw	vord
User name: root	
Password:	
Confirm password:	
	ОК
The password for the pre-configured ac before the product can be used.	ministrator root must be changed
If the password for root is lost, the pro settings, by pressing the button locate user documentation for more informati	duct must be reset to the factory default d in the product's casing. Please see the on.

- Escreva a password de root que escolheu e clique em OK
- Agora deverá estar a ver uma imagem semelhante a esta



- Clique em "Setup" e no menu do lado esquerdo escolha a opção 1 Users
- Marque a opção "Enable anonymous viewer login (no user name or password required)"
- Clique no botão de save
- Escolha agora a opção 3 Date & Time
- Marque a opção "Automatically adjust for daylight saving time changes"
- Na opção Time mode marque a última opção "Set manually"
- Na opção Date & Time format used in Images escolha o formato YYYY-MM-DD para a data e o formato 24h para as horas
- Por último carregue no botão de save
- Escolha agora no menu do lado esquerdo a opção Video & Image
- No entrada Image appearance no campo Compression escolha a opção "Very low"
- Na entrada Overlay settings marque as opções "Include date", "Include time" e "Include text". Nesta última escreva na caixa de texto qual o nome que quer dar á câmara. (Convém não usar espaços. Utilize antes o "_").
- Na entrada Video stream assegure-se que as duas opções "Unlimited" estão marcadas
- Carregue novamente no botão de Save
- Escolha agora a opção Advanced dentro do menu Video & Image e no campo Exposure priority escolha a opção Image quality
- Clique mais uma vez no botão de Save
- Clique na opção System options seguida da opção Network e depois na opção UpnP
- Certifique-se que, do lado direito, a opção "Enable UpnP" está desmarcada
- Carregue mais uma vez no botão Save.

Nota: a alteração de qualquer outro parâmetro da câmara, poderá fazer com que o sistema não funcione normalmente. Por favor não altere nenhum parâmetro além dos acima referidos.

Posicionamento da câmara

• Utilizando o link Live view, aponte e foque a câmara.

Configuração do servidor de vídeo vigilância

Equipamentos Suportados:

- ASROCK ION 330
- Micromáquinas c/Foxconn 945G7MD-8KS2H
- IFTEL c/Intel DG35 EC

Instalação:

- Ajustar as configurações da BIOS de acordo com o equipamento;
- Colocar o DVD de instalação no DVD-ROM da máquina;
- Aguardar até finalizar a instalação;
- Ajustar novamente as configurações da BIOS;

Configurações por defeito:

O servidor de video-vigilância vai configurado, por defeito, com os seguintes dados:

- IP = 192.168.0.150
- Gateway = 192.168.0.254
- DNS = 192.168.0.254
- Utilizador = pie
- Password = vídeo

No entanto antes de conseguir aceder ao servidor (remotamente) deverá criar a sua própria chave, para criar uma chave deverá executar o programa puttyGEN.exe, mudar o numero de bits para 4098 (em baixo) e clicar em GENERATE, depois inserir a chave completa dentro do ficheiro localizado em / root/.ssh/authorized_keys

PuTTY Key Ger	ierator	?
e Key Conversio	ns Help	
Key		
Public key for pastir	ng into OpenSSH authorized_key:	s file:
oBn+Gv2VGJ9Bxp gCiwMZ008Rojsq HH4wJImB2PtDtW MsYtTH1FQ9NMT	aDPKiqGnkcFNd4il1hGUVMqKh pTNWz9MISbnrHdilpo6ccW2nPI QXfymzQlxAt1u/xIEokZIVPTAbp 7Fln <mark>HVhVh15dC9GktWCj1aT9dl</mark>	eh6p/MvfQ47EGRdrSfk0juxoM2U hHALHNNa6WQ4yNW9RP7Q+cE KLSAh/1N7EVmcUjYH0htMeVohf wP1yALurg/r4m2xGWeuiQU=
NUME_DA_EMPR	ESA	
Key fingerprint:	ssh-rsa 4097 9c:28:e1:fb:97:	0c:25:4a:7e:15:d6:b2:10:ee:e4:cf
Key comment:	NOME_DA_EMPRESA	
Key passphrase:		
Confirm passphrase		
Actions		
Generate a public/p	private key pair	Generate
Load an existing pri	vate key file	Load
Save the generated	lkey Sa	ve public key Save private key
Parameters		
Type of key to gene OSSH-1 (RSA)	erate:	◯ SSH-2 DSA
KEALE OF DEELES AND	anneated base	4000

Depois de gerar a chave, clique em SAVE PRIVATE KEY, e utilize esse ficheiro sempre que faça uma ligação ao sistema de vídeo vigilância, para isso basta que no TAB de Auth indique o seu ficheiro ppk.



Sem a indicação deste ficheiro não é possível aceder remotamente (via ssh ou vnc) ao servidor de VNC.

Alteração do IP do servidor

Para aceder por VNC ao servidor de vídeo vigilância necessita de ter configurado um tunnel de VNC no seu PUTTY, deve fazê-lo da seguinte forma:

Session		Basic options for your Pu	TTY session
 Jession Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex Auth 	C	Specify the destination you want to Host Name (or IP address) [root@192.168.0.133 Connection type: Raw Telnet Riogin (Load, save or delete a stored sessi Saved Sessions server_133 server_133 server_135 server_136 server_136 server_137 Close window on exit: Always Never ① On	iv on clean exit

Depois dentro de SSH na categoria Tunnels, deverá configurar da seguinte forma: Source port: 5900

Destination: 127.0.0.1:5900

Keyboard	Option	is controlling SSH p	ort forwarding
 Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Teinet Rlogin SSH Kex Auth TTY X11 Tunnels Bugs Serial 	Port forwarding Port forwarding Local ports Remote por Forwarded port Add new forwa Source port Destination Local Auto	accept connection ts do the same (SS s: 5900 127.0.0.1:5900 Remote 0 IPv4	s from other hosts H-2 only) Remove Add O Dynamic O IPv6

E clicar em ADD, a partir deste momento poderá entrar no servidor de VV usando o VNC, execute o cliente de VNC. Vai ver o seguinte ecrá:



- Na caixa de texto VNC server escreva 127.0.0.1:5900
- Vai-lhe aparecer uma caixa a solicitar a palavra-chave
- Digite a palavra-chave pievideo e carregue em enter

Neste momento está a trabalhar no ambiente gráfico do servidor de video-vigilância e estará a ver o ecrá de login do servidor.

• No campo senha, deverá escrever a password video e em seguida clicar na seta verde.



• Após um ecrá de arranque do ambiente de trabalho deverá ver o seguinte ecrá:



- Para aceder à configuração da placa de rede, carregue no primeiro ícone, do lado esquerdo, da barra de tarefas ""
- No menu que lhe vai aparecer, procure pela entrada "Centro de controlo (dast)" que deverá estar no topo do menu, conforme a imagem abaixo



• Em seguida, vai-lhe aparecer a seguinte janela a solicitar a password de root. Escreva a password PIE e clique em OK.

actuals.	
~	
iomando: /sbin/yast2	
jenha:	
Manber a senha	

• Na janela abaixo, carregue na opção "Network devices" no menu do lado esquerdo.





• Agora na janela seguinte, carregue na opção "Network card" que está no menu do lado direito.

• Na nova janela deve carregar na opção "Edit"

		2	
letwork Card	Wetwork 0	Card Configuration Overview	
verview	1.000		
btain an overview of			
dditionally, edit their	Name	IP Address	
onfiguration.	ASUSTEK RTL-8139/8	3139C/8139C+ 192.168.0.153	
dding a Network			
ard:			
ress Add to configure a			
ew network card			
anually.			
diting or Deleting:			
hoose a network card to			
nange or remove. Then			
ress Edit or Delete as			
estred.			
	ASUSTEK RTL-8139)/8139C/8139C+	
	Device Nam	ne: eth-id-00:15:f2:e0:3a:3b	
	IP address: Started auto	192.168.0.153, subnet mask 255.255.255.0 matically at boot	
	Contest add	inducting as asso	
		1-1-1	
	Add Edit	Delete	

• Na janela que aparece agora, pode no campo "IP Address" mudar o IP e a Subnet Mask do servidor

Software Individual Software Hiddware Software Hiddware Software Software Configure your IP addres Software Network Device Network Devices Also select this if you do not head network. Network Services Also select this if you do not head adomatically by the system administrator or your calle or DSL provider. Novell AppArmor Of DSL provider. Mechanization or your calle or DSL provider. Network Devices Miscillaneous Chicking Met completes the figure do not head adomatically from the server. Security and Users Network completes the entority mathin. Miscillaneous Chicking Met completes the entority mathin. Otherwse, network address stup globaratic Address stup (via DHCP) P Address globaratic Address stup (via DHCP) P Address globaratic Address stup P Address globaratic Address stup (via DHCP) P Address globaratic Address stup P Address globaratic Address stup P Address globaratic Address stup P Address globaratic Address stup (via DHCP) Chicking Met corp (or your configliglobaratinglight address stup) globarat	Edit Help		
Hardware Configure your IP address. System Not use select synamic type how a DROP synamic network. Network Devices Not select this if you do not network. Network Devices Also select this if you do not network. Network Devices Network services Network Devices Network addresses are then obtained automatically from the server. Network Devices Network addresses are then obtained automatically from the server. Network Devices Network addresses are then obtained automatically from the server. Network Devices Network addresses are then obtained automatically from the server. Clicking Next completes the configuration. Automatical durines (e.g., optice), and optice), the network agteway IP addres. Defailed Settings agteway IP addres. Seture Network address (e.g., optice), and reserver. Defailed Settings agteway IP addres. Defailed Settings (gateway IP addres). Continitier tor for more information about the network configuration. Metwork Address Setup (locally agteway IP addres).	Software	9	
	Hardware Hardware System System Network Devices Network Devices Novell Apparmor Security and Users Miscellaneous Clicking Next configuration Computer, the next of the same and the server. Miscellaneous Clicking Next configuration Computer, the next of the configuration contact your next contact your next	Irres. ic you I do not ss m m cable ethen tity ethen	
	ad ministrator fo information about network configura	ore 8 n.	

- Se necessitar de alterar o endereço de DNS, deve no ecrá acima clicar na opção
- Host name and name server"
 Na nova janela deverá alterar os DNSs primário e secundário para os do operador de Internet
 Se necessitar de mudar também o Gateway, carregue na opção "Routing" e na nova janela,
- no campo "Default gateway" escreva o IP do router que é o Gateway da rede.

routing can be set up in dialog. The Default eway matches every	Routing Configuration	
othe destination, but by <i>B</i> any other entry is that matchins the stad matchins is used and of the default notine add of the default notine add of the default notine may to exable you to "and everything else ind go here." ble IP Forwarding f pythem is a notifer.	Default Sphenory [192.148.0.254	
	Routing Table	
_	Add grave frequencies	

- Carregue em OK e retornará à janela de configuração do IP. Nesta janela deve agora clicar no botão "Next". Na janela que aparece em seguida carregue novamente no botão "Next". Devido à mudança do IP do servidor, neste momento a sua ligação VNC acabou de dar um erro de comunicação.
- Execute novamente o cliente de VNC e introduza na janela que lhe aparece o IP que acabou de configurar para o servidor. A palavra-chave mantém-se em pievideo. Deverá estar novamente a ver o ambiente de trabalho do servidor de videovigilância.

Alteração da palavra-chave

• Abra novamente um browser no seu computador e digite na barra de endereço http://<IP do servidor de vídeo>

🤨 VideoVigilänciaPIE - Mozilla Firefox	E 6 🔀
Elle Edit View Go Boolimanis Isolis Help	0
S S C C C C C C C C C C C C C C C C C C	
(Who: //1982.168.0.130/	*
Video Videa Andra Pie Windter Fo	
Bern vindo ao mais recente produto da WinREST FO!	
As duas grandes vertentes deste produto são: - Possibilidade de visualizar imagens ou filmes relaccionados com eventos que se passem r - Possibilidade de visualizar video enfine das diversas câmaras do sistema. P.f. introduza à sua passevord i	ho POS;
Password: Login	
Suporte: 252 290 610 <u>webmasteriðgrupople.com</u> @ 2006 Copyright GrupoPIE Portugal, S.A. <u>Ter</u>	mas e condicões
Done	🗠 0.8 🔗 🕲

- No ecrá de login do software de videovigilância digite a palavra-chave pievideo
- Após a verificação da velocidade de ligação, verá o ecrá principal deste software

Ano: Mês: Dia: Hora: 2006 • 05 • 06 • - • <	Gaveta: Operador: lodos> Vodos> V	Evento: <lodos></lodos>	Parâmetro: <todos> <</todos>	Valor: <todos> Per</todos>	advisar
2008/54 0.00 00 - Resultado Pesquisa Evento lazas		2006/05/06	00:00:00		
	No data File: 0000.ft	lv	N File	lo data : 0000.flv	
	ro_sar		Pre_camicow	io data	
	File: 0000.f	•	File PIE_Cam3	: 0000.flv	•

- Para alterar a palavra-chave de acesso ao software, carregue no link "Alterar palavra-chave" no fim da página.
- Na nova janela que abriu proceda á alteração da palavra-chave e carregue em OK.

🕹 http://192.168.0.130 - Altera 🔳 🗖 🔀
Password actual:
Confirme nova password:
Cancelar OK
Done 🖄 0:8 🛞 🧐

Configuração das câmaras

Agora vamos configurar quais as câmaras que vão estar ligadas ao software. Para isso clicamos no link "Gerir câmaras" que se encontra no fundo da página. Este é o aspecto da nova página.

10 HORA FIM PF	
O HORA FIM PR	
	REVIEW
O HORA FIM I IN	AAGEM
	O HORAFIM D

• Para adicionar uma câmara, clique no link "Adicionar nova câmara"

Neste momento tem uma nova janela visível com os seguintes campos:

Câmaras IP

Nota: as explicações e dados fornecidos respeitam apenas ao modelo AXIS 206 e AXIS 207. Esta câmara é o único modelo certificado para trabalhar com este software.

😻 http://19	2.168.0.130 - VideoV 🔳 🗖 🔀
Nome:	*
VDS URL:	
CLOCK URL:	
INIT URL:	
FPS:	1 💌
Hora Início:	hh mm
Hora Fim:	hh mm
Login:	
Password:	
Activo :	Não 💌
	Cancelar OK
	* - Campos de preenchimento obrigatório
Done	🖄 0:8 🔕 🧾

Nome – Este campo é o nome pelo qual a câmara vai ser reconhecida pelo software de videovigilância. Dê um nome à câmara, tendo o cuidado de não utilizar espaços entre as palavras. Pode utilizar o "_". Sugestão: escreva aqui o mesmo nome que atribui à câmara na secção Configuração dos parâmetros da câmara

VDS URL – Este campo é o endereço http da câmara. O endereço é:

http://IP_DA_CAMARA/axis-cgi/mjpg/video.cgi?resolution=640x480&fps=6

Nota : o parâmetro resolution pode ser alterado. Neste caso estamos a solicitar à câmara que nos forneça uma imagem de 640x480. Caso desejemos uma imagem menor, devemos alterar este valor para 320x240.

CLOCK URL – Este campo é usado para garantir que o relógio da câmara está sempre sincronizado com o relógio do servidor de videovigilância. É muito importante que este campo seja sempre utilizado para garantirmos que não há discrepância de tempo entre as câmaras. A instrução a colocar aqui é:

http://IP_DA_CAMARA/axis-cgi/admin/date.cgi?action=set&year=%Y&month=%m&day=%d&ho ur=%H&minute=%M&second=%S

INIT URL – Este campo serve para se passar outros parâmetros para a câmara quando a mesma é iniciada. Para o modelo de câmara usado não é necessário preencher este campo.

FPS – este campo numérico é usado para configurar o número de frames, por segundo, para esta câmara. Deverá sempre escolher 2 frames por segundo.

Hora Início e Hora Fim – nestes 2 campos poderão definir qual o intervalo de tempo em que as câmaras estarão a recolher imagens. Se pretender que seja 24 horas por dia deve colocar 00h00 na Hora Início e 23h59 na Hora Fim.

Login – campo onde pode indicar qual o utilizador da câmara (neste caso é root)

Palavra-chave – campo onde pode indicar qual a palavra-chave da câmara para o utilizador indicado em Login

Activo – este campo é utilizado para activar a recolha de imagens da câmara.

Após preencher os campos acima, carregue em OK para adicionar a câmara.

Neste momento retornou ao ecrá de gestáo de câmaras, sendo agora visível a entrada referente à câmara que acabou de adicionar. No entanto, para a câmara ficar efectivamente activa (luz verde e a palavra "on" no lado direito) deve clicar no botáo "REINICIAR SISTEMA (activar alterações)". Só após clicar neste botáo é que a câmara fica activa, podendo utilizar o respectivo botáo de "Preview" para ver o "live feed" da câmara.

Deverá repetir este processo para todas as câmaras que deseja adicionar ao sistema de videovigilância.

Nota: Se estiver a utilizar as câmaras na sua resolução máxima (640x480) e estiver também com o acesso via Internet activo, é aconselhável criar para cada câmara 2 feeds (o de alta resolução e um de baixa resolução - 320x240). Este 2º feed será o utilizado na visualização dos vídeos (quando com 4 imagens em simultâneo) de forma a garantir uma velocidade de consulta, via Internet, aceitável. Se num determinado momento desejar ver em pormenor um determinado período, pode sempre escolher a visualização de apenas uma câmara (em alta resolução).

Câmaras Analógicas

Nome – Este campo é o nome pelo qual a câmara vai ser reconhecida pelo software de video-vigilância. Dê um nome à câmara, tendo o cuidado de não utilizar espaços entre as palavras. Pode utilizar o "_". Sugestão: escreva aqui o mesmo nome que atribui à câmara na secção Configuração dos parâmetros da câmara

VDS URL – Este campo é o endereço http da câmara. O endereço é:

http://localhost:8100 para a VGA1 http://localhost:8101 para a VGA2

Os outros campos são deixados em branco.

Configuração dos postos de FO

Vamos agora adicionar os postos do FO que vão ficar ligados ao sistema de videovigilância. Para criarmos um posto de FO, temos de, na janela "Gerir câmaras" carregar no botão "adicionar novo VNC" que abrirá uma nova janela com os seguintes campos:

🐸 http://19	2.168.0.130 - VideoV 🔳 🗖 🔀
Nome:	*
URL:	
PORTA:	
FPS:	1 🕶
Hora Início:	hhmm
Hora Fim:	hh mm
Login:	
Password:	
Activo :	Não 💌
	Cancelar OK
	* - Campos de preenchimento obrigatório
Done	2:8 😣 😼 🔡

Nome – Este campo é o nome pelo qual o terminal de FO vai ser reconhecido pelo software de videovigilância. Dê um nome ao terminal, tendo o cuidado de não utilizar espaços entre as palavras. Pode utilizar o "_".

URL – Este campo é o endereço IP do terminal do FO. Deverá digitar apenas o endereço IP, sem http e sem barras. (Exemplo: 192.168.0.1)

PORTA – Este campo é usado para informar o sistema de videovigilância qual a porta de comunicação com o terminal de FO. Esta porta é sempre a soma de 5900 com o número do posto que queremos. Por exemplo, para o servidor a porta será 5900+1=5901.

FPS – este campo numérico é usado para configurar o número de frames, por segundo, para o posto VNC. Deverá sempre escolher 2 frames por segundo.

Hora Início e Hora Fim – nestes 2 campos poderão definir qual o intervalo de tempo em que os postos VNC estarão a enviar imagens. Se pretender que seja 24 horas por dia deve colocar 00h00 na Hora Início e 23h59 na Hora Fim.

Login – não utilizado nos postos VNC

Palavra-chave – não utilizado nos postos VNC

Activo – este campo é utilizado para activar a recolha de imagens do posto VNC.

Após preencher os campos acima, carregue em OK para adicionar o posto do FO.

INIT URL – Este campo serve para se passar outros parâmetros para a câmara quando a mesma é iniciada. Para o modelo de câmara usado não é necessário preencher este campo.

FPS – este campo numérico é usado para configurar o número de frames, por segundo, para esta câmara. Deverá sempre escolher 2 frames por segundo.

Hora Início e Hora Fim – nestes 2 campos poderão definir qual o intervalo de tempo em que as câmaras estarão a recolher imagens. Se pretender que seja 24 horas por dia deve colocar 00h00 na Hora Início e 23h59 na Hora Fim.

Login – campo onde pode indicar qual o utilizador da câmara (neste caso é root)

Palavra-chave – campo onde pode indicar qual a palavra-chave da câmara para o utilizador indicado em Login

Activo – este campo é utilizado para activar a recolha de imagens da câmara.

Após preencher os campos acima, carregue em OK para adicionar a câmara.

Neste momento retornou ao ecrá de gestáo de câmaras, sendo agora visível a entrada referente à câmara que acabou de adicionar. No entanto, para a câmara ficar efectivamente activa (luz verde e a palavra "on" no lado direito) deve clicar no botáo "REINICIAR SISTEMA (activar alterações)". Só após clicar neste botáo é que a câmara fica activa, podendo utilizar o respectivo botáo de "Preview" para ver o "live feed" da câmara.

Deverá repetir este processo para todas as câmaras que deseja adicionar ao sistema de videovigilância.

Nota: Se estiver a utilizar as câmaras na sua resolução máxima (640x480) e estiver também com o acesso via Internet activo, é aconselhável criar para cada câmara 2 feeds (o de alta resolução e um de baixa resolução - 320x240). Este 2º feed será o utilizado na visualização dos vídeos (quando com 4 imagens em simultâneo) de forma a garantir uma velocidade de consulta, via Internet, aceitável. Se num determinado momento desejar ver em pormenor um determinado período, pode sempre escolher a visualização de apenas uma câmara (em alta resolução).

Câmaras Analógicas

Nome – Este campo é o nome pelo qual a câmara vai ser reconhecida pelo software de video-vigilância. Dê um nome à câmara, tendo o cuidado de não utilizar espaços entre as palavras. Pode utilizar o "_". Sugestão: escreva aqui o mesmo nome que atribui à câmara na secção Configuração dos parâmetros da câmara

VDS URL – Este campo é o endereço http da câmara. O endereço é:

http://localhost:8100 para a VGA1 http://localhost:8101 para a VGA2

Os outros campos são deixados em branco.

Configuração dos postos de FO

Vamos agora adicionar os postos do FO que vão ficar ligados ao sistema de videovigilância. Para criarmos um posto de FO, temos de, na janela "Gerir câmaras" carregar no botão "adicionar novo VNC" que abrirá uma nova janela com os seguintes campos:

🙂 http://193	2.168.0.130 - VideoV 🔳 🗖 🔀
Nome:	*
URL:	
PORTA:	
FPS:	1 💌
Hora Início:	hh mm
Hora Fim:	hh mm
Login:	
Password:	
Activo :	Não 🔽
	Cancelar OK
	* - Campos de preenchimento obrigatório
Done	🖹 0:8 😡 🥹 🤢

Nome – nome pelo qual o terminal de FO será reconhecido pelo software de videovigilância. Dê um nome ao terminal, tendo o cuidado de não utilizar espaços entre as palavras. Pode utilizar o "_".

URL – Este campo é o endereço IP do terminal do FO. Deverá digitar apenas o endereço IP, sem http e sem barras. (Exemplo: 192.168.0.1)

PORTA – Este campo é usado para informar o sistema de videovigilância qual a porta de comunicação com o terminal de FO. Esta porta é sempre a soma de 5900 com o número do posto que queremos. Por exemplo, para o servidor a porta será 5900+1=5901.

FPS – este campo numérico é usado para configurar o número de frames, por segundo, para o posto VNC. Deverá sempre escolher 2 frames por segundo.

Hora Início e Hora Fim – nestes 2 campos poderá definir o intervalo de tempo em que os postos VNC estarão a enviar imagens. Caso pretenda 24 horas por dia, deve colocar 00h00 na Hora Início e 23h59 na Hora Fim.

Login – não utilizado nos postos VNC

Palavra-chave - não utilizado nos postos VNC

Activo – este campo é utilizado para activar a recolha de imagens do posto VNC.

Após preencher os campos acima, carregue em OK para adicionar o posto do FO.

Neste momento retornou ao ecrá de gestão de câmaras, sendo agora visível a entrada referente ao posto de FO que acabou de adicionar. No entanto, para o posto ficar efectivamente activo (luz verde e a palavra "on" no lado direito) deve clicar no botão "REINICIAR SISTEMA (activar alterações)". Só após clicar neste botão é que o posto fica activo, podendo utilizar o respectivo botão de "Preview" para ver o "live feed" do posto.

Configuração para acesso via Internet

Para se aceder ao servidor de video-vigilância pela Internet é necessário que o cliente possua uma ligação de banda larga, com uma velocidade de UPLOAD mínima de 256 K. Se a instalação do WinREST FrontOffice estiver em Linux, o cliente terá obrigatoriamente de possuir um router (ADSL/Cabo) compatível com o seu ISP.

Se for em Windows, o cliente poderá utilizar um modem, desde que o mesmo esteja ligado numa máquina Windows, que será responsável pela partilha da ligação à Internet. Contudo, mesmo nesta situação aconselhamos que a ligação à Internet seja efectuada através de um router (ADSL/Cabo) compatível com o ISP.

Nota: consoante a versão do Windows utilizada, poderá ser necessário a instalação de um software de partilha de ligação à Internet, bem como de um software de firewall.

Em todos os casos acima descritos, deverá ser configurado no respectivo router e/ou software de partilha de ligação à Internet e na Firewall a abertura e re-direcionamento das portas da tabela para o servidor de video-vigilância.

Serviço	Porta	Protocolo	Redireccionamento IP
www	80	TCP	IP local do servidor Video Vigilância
SSH	22	TCP	IP local do servidor Video Vigilância
VNC	5900	TCP	IP local do servidor Video Vigilância
Câmera 1	8081	TCP	IP local do servidor Video Vigilância
Câmera n	808n	TCP	IP local do servidor Video Vigilância

Alteração das configurações de rede

Seguindo as instruções descritas no tópico "Alteração do IP do servidor" deverá alterar o Gateway para o IP interno do router que está a utilizar e os DNSs primário e secundário para os do operador de Internet.

Registo de conta no NO-IP

Para configurar a conta do cliente no serviço de DNS dinâmico No-IP, proceda da seguinte forma: • Num browser de internet digite o seguinte endereço **http://www.no-ip.com**



- Na página que aparece, semelhante à imagem acima, escolha a opção "No-IP Free"
- Na nova janela carregue no botão de "Sign Up Now"
- Preencha todos os campos do formulário que estão em Bold
- Marque a caixa "I have read and agree to the following terms of service:" e clique no botão "Sign Up Now"
- Irá receber na conta de e-mail indicada no formulário anterior uma mensagem com um link para activar a conta que acabou de criar.
- Após activar a conta volte ao website do No-IP e proceda ao login com os dados que escolheu.
- Agora deverá estar a ver uma página semelhante à seguinte imagem

e Edit Yew Go Bookmarks 🕻	Took Reb	•		
B http://www.no-ip.com/members	s/menu/index.php?sid=07666930	- 62e7854s3e33331230d55440		
Logged	h At: jandrade@grupople.co urret IP: 195 23 20.139 [2]	OUR NO-UP SERVICES SUPPORT DOWNLOADS C	COMPANY)	
Y 0 - - - - - - - - - - - - -	OUR NO-IP Houter / Redirects Amage Ugarde to Erhanced Plus Manage Oroups Ugarde to Erhanced Domain Registration SSL Certificates Mail Monitoring Squared Backup DIIS Squared Backup DIIS Your Account Remov / Activate	 Members Area Wetcome! You have successfully togged into NoP's member section. To start uning No-P's envices please select a meru tem on the left hand side. Your No-IP Notices Your No-IP Notices this time- Char state part into fact information regarding bothers. 	• News Lipdates Apr 17, 2005 Cons visit our new Regit The tupy will save as an instant of the same of the based of the same of the same of the same of the same of the same of the same of the same of the same of the same of the same of the sa	

- Carregue na opção "Add" no menu do lado esquerdo e adicione no campo "Hostname" o endereço de internet que quer usar para aceder à loja em questão.
- Em seguida escolha na lista qual a terminação que pretende para o endereço. Por defeito será ".no-ip.info"
- Finalmente, no fundo do ecrá carregue no botão "Create Host"

Exemplo: Se o restaurante se chamar "Farol" escreva no campo Hostname www.farol e se na lista escolheu .no-ip.info, o endereço para aceder ao servidor de videovigilância será *http://restaurante.no-ip.biz*

ATENÇÃO : todas as outras opções neste ecrá devem ficar exactamente como estáo.

Registo de endereço WDNS

Para configurar um endereço WDNS o utilizador deve proceder da seguinte forma:

- Num Browser de Internet aceder a http://www.winrest.pt;
- Entrar na área reservada com o utilizador e password do agente;

Gestão de Conta	Gestão de Utilizadores
² erfil ² edido de Alteração de Distribuidor	Gerir Sub-Utilizadores Gerir Clientes
Gestão de Encomendas	Gestão de Licenças
Encomendar Donsultar Encomendas	Consultar Hardlocks Alteração de Licenças Alteração de Licenças Antigas
Contratos de Actual	ização de Software PIE
consulta de Contratos de Actualização d Contratos a Expirar (0)	e Software PIE
Gestão d	e Parcerias
arceria BES	Parceria PT

• Aceder a "Consultar hardlocks" e através do filtro de pesquisa colocar o nº do hardlock de video-vigilância.

WinREST Vídeo Vigilância Webserver	(clique para atribuir).winrest.ws e gerar chave
---	---

• Escrever o sub-dominio na caixa sem a extensão winrest.ws:



• O website vai criar uma chave para o endereço introduzido.

Exemplo: Se o restaurante se chamar "farol" escreva no quadro anterior farol. O endereço para aceder ao servidor de videovigilância será *http://farol.winrest.ws*

Configuração do cliente NO-IP

Após ter criado a conta no serviço No-IP, tem de configurar o cliente responsável pela actualização do IP do servidor no serviço No-IP, que já se encontra instalado no servidor de videovigilância.

- Para configurar este serviço deve entrar no servidor de videovigilância por VNC, e abrir uma consola de texto.
- Para abrir uma consola de texto, carregue no ícone 📕 que se encontra na barra de tarefas
- Na nova janela, digite as seguintes instruções, tendo o cuidado de respeitar as maiúsculas e minúsculas
- /usr/local/bin/noip2 -u <endereço de e-mail> -p <password> -C e pressione <enter>
- <endereço de e-mail> substitua pelo endereço de e-mail da conta No-IP
- <password> substitua pela password da conta No-IP
- Neste momento deverá estar a ver as seguintes frases:
- Auto configuration for Linux client of no-ip.com.
- Please enter an update interval:[30]

• Escreva o intervalo de tempo para actualização. Escreva o número 5 e pressione <enter>(quer dizer que o IP dinâmico vai ser actualizado no serviço No-IP a cada 5 minutos)

- Na consola de texto apareceu agora a seguinte frase - New configuration file '/usr/local/etc/no-ip2.conf' created.
- Escreva agora rcnoip2 stop
- O servidor responde com Shutting down noip2.
- Escreva agora rcnoip2 start
- O servidor responde com Starting noip2.
- Feche a consola de texto

• Aguarde 5 minutos para a actualização do serviço No-IP ser efectuada e passará a ter o servidor de videovigilância disponível, via internet, no endereço que configurou no serviço No-IP.

Configuração do cliente WDNS

Após ter criado a conta no website do GrupoPIE, tem de configurar o cliente responsável pela actualização do IP do servidor no serviço WDNS, que já se encontra instalado no servidor de videovigilância:

• Aceder ao servidor de video-vigilância através do PUTTY como root, e executar o comando vi /etc/ ipsend.cfg e introduzir o endereço e a chave de acordo com as instruções do próprio ficheiro.

• Executar o comando /etc/init.d/wdns restart ;

• Aguardar 15 minutos para a actualização do serviço WDNS ser efectuada e passará a ter o servidor de videovigilância disponível, via internet, no endereço que configurou no serviço WDNS.

Actualização de versão

• Para actualizar a versão da distribuição o técnico deve entrar via PUTTY no sistema com o utilizador root e abrir a pasta /root/pie-scripts;

• Escrever o comando ./upgrade-distro;

O sistema inicia automaticamente a actualização e actualiza todos os pacotes Linux necessários. No final o servidor deverá ser reiniciado.

Ligação à Internet via Placa USB

O servidor de video-vigilancia suporta ligação à Internet via placas 3G Huawei e ZTE dos operadores Vodafone e TMN.

Para isso o utilizador deverá entrar com o utilizador root e abrir a pasta /root/pie-scripts:

- Ligar a placa numa porta USB livre com o PIN desactivado; Placas HUAWEI E200
- Digitar o comando ./switch2huawei vodafone (ex. para cartão vodafone) Placas ZTE MF 620
- Digitar o comando ./switch2zte TMN (ex. Para cartão TMN)
- Se o acesso pela placa for temporario no final digitar o comando ./switch2network

Configuração de ligação com UPS

UPSs Suportadas:

- APC BackUPS CS 350
- Mustek Powermust 600 USB (só por porta série)

Nota: UPS's que usem o mesmo protocolo de uma das indicadas em cima poderão também funcionar mas, não há qualquer tipo de garantias.

Como instalar:

APC BackUPS CS 350:

- Ligar a UPS entra a alimentação geral e a alimentação do PC.
- Ligar o Cabo USB da UPS a uma ranhura USB do PC.
- Abrir uma consola e digitar o seguinte comando: sudo /usr/sbin/switch2ups apc
- Digitar a password de root e premir 'Enter'.

Mustek Powermust 600 USB:

- Ligar a UPS entra a alimentação geral e a alimentação do PC.
- Ligar o Cabo Série da UPS à COM1 do PC.
- Abrir uma consola e digitar o comando: sudo /usr/sbin/switch2ups powermust
- Digitar a password de root e premir 'Enter'.

Como funciona:

Assim que haja uma quebra de energia, a UPS entra em modo de bateria. Logo que a bateria atinja um nível critico, a distribuição desliga-se automaticamente e, desliga também a UPS. Assim que a energia voltar a ser restabelecida, a UPS é ligada, ligando o PC automaticamente.

Notal: Se a energia voltar antes do modo critico ser alcançado, então o processo de desligar automático, nunca acontecerá.

Nota2: Para o PC ligar automaticamente assim que a energia for reposta, é necessário a BIOS do computador ser configurada para o efeito. Consulte a documentação para o efeito para ter esta funcionalidade activada.

Como remover:

- Abrir uma consola e digitar o seguinte comando: sudo /usr/sbin/switch2ups remove
- Digitar a password de root e premir 'Enter'.

Troubleshooting – Resolver problemas da vídeo vigilância

Após ter tudo configurado poderá ter algumas situações que não consegue resolver, aqui deixo umas dicas de problemas comuns e soluções simples, (todos os comandos indicados abaixo devem ser inseridos em letras minúsculas visto o linux ser case sensitive):

Erro: Hardlock not found;

Como diagnosticar: A página inicial da vídeo vigilância está em branco com o erro de HardLock not found.

Possível problema: Hardlock não ligado ao servidor de vídeo vigilância;

Solução: ligar o hardlock e re-iniciar;

Possível problema: Hardlock ligado mas a licença é incorrecta para esse hardlock

Solução: Aceder ao servidor de Vídeo vigilância por ssh ou por vnc e copiar a licença para /home/pie/ sys/bin com o nome de License.lic. Após copiar o ficheiro execute os seguintes comandos:

- chmod 777 License.lic

- chown pie:www License.lic

Possível problema: Licença errada para aquele HardLock

Solução: executar o seguinte:

- cd /home/pie/sys/bin
- ./hardsign License.lic

Depois deste comando se der erro de HardLock not found faça o seguinte:

- cat License.lic | grep SERIAL_NUMBER

E confirme se o número de licença coincide com o número do HardLock, caso não se confirme substitua a licença;

Erro: A pen não monta automaticamente para cópia da licença

Resolução: digita o seguinte comando:

- tail -f /var/log/messages

Neste ponto ligue a sua pen drive, ou desligue e ligue-a novamente, neste momento deverá aparecer algo deste género:

kernel: sdc: Write Protect is off kernel: sdc: Mode Sense: 00 00 00 00 kernel: sdc: assuming drive cache: write through kernel: sdc: sdc1 kernel: sd 3:0:0:0: Attached scsi removable disk sdc kernel: sd 3:0:0:0: Attached scsi generic sg2 type 0 kernel: usb-storage: device scan complete

Neste momento podemos verificar que é o dispositivo sdc1 agora para o utilizar usamos o commando:

- mount /dev/sdc1 /mnt

E a partir deste momento podemos aceder à pen da pasta mnt

Erro: Não aparece os eventos:

Possível problema: Falta o modulo CONTROL no WinREST FO;

Solução: Trocar a licença;

Possível problema: Falta o ficheiro vídeo.ini;

Solução: criar a pasta log dentro da raiz do winrest e criar o ficheiro vídeo.ini

Possível problema: o serviço winrest_events está parado:

Solução: executar o comando.

svc -d /service/winrest_eventssvc -u /service/winrest_events

Erro: O endereço WDNS não é actualizado:

Possivel problema: A hora do sistema está errada;

Solução: acertar a hora do sistema e executar o comando /etc/init.d/wdns restart;

Possivel problema: Não tem servidores de DNS configurados;

Solução: executar o comando nslookup dns.winrest.ws e verificar se aparece o nome e IP dos servidores.



Edifício GrupoPIE Rua Dr. Artur Aires, 100 4490-144 Póvoa de Varzim T. 252 290 600 F. 252 290 601

Filial: Av. Infante D. Henrique, 345, 2º Piso 1800-218 Lisboa T./F. 217 958 450

www.grupopie.com