Integration Plugin

XProtect[®] Milestone Clients SALTO Systems[®] Access Control

0

٥

S

by accessway

Manual de instalação e operação

Version: v1.2.007 Date: 2019/12/01



Índice

Acrónimos e abreviaturas3
Introdução3
Requisitos
Conteúdo do pacote de instalação7
Descrição dos ficheiros do plugin7
Descrição dos ficheiros do web service WCF8
Procedimento de instalação do plugin9
Instalação do Web service WCF9
Passo 1 Restore do ficheiro de base de dados9
Passo 2 Remoção do utilizador 'default'12
Passo 3 Criação de utilizador13
Passo 4 Instalação de ficheiros16
Passo 5 Configuração do web service20
Instalação do plugin22
Passo 1 Instalação dos ficheiros22
Passo 2 Configuração do plugin24
Licenciamento
Operação do plugin32
Gestão do plugin em backoffice34
1 General Settings
2 Associated Cameras
3 Access Control Events
4 Access Control Actions
5 Cardholders
5.1 Fotografias de cardholders40



Acrónimos e abreviaturas

MIP: Milestone Integration Platform (Plataforma de Integração Milestone)
AC: Access Control (Controlo de Acessos)
VMS: Video Management Software (Software de Gestão Video)
SDK: Software Development Kit (Kit de Desenvolvimento de Software)
API: Application Programming Interface (Interface de Programação de Aplicações)
WCF: Windows Communication Foundation
IIS: Internet Information Services (web server)

Introdução

O Salto é um sistema de AC que providencia um vasto leque de funcionalidades para gerir a operação de atividades e a integração de localizações no que concerne a infraestrutura de controlo de acessos.

Quanto ao Milestone XProtect, trata-se de um sistema de alta performance de supervisão de sistemas de vídeo vigilância. Esta plataforma de gestão inclui a capacidade de integração de sistemas de AC e consequente operação por intermédio das suas interfaces de utilizador (XProtect Management Client e XProtect Smart Client), através do seu MIP SDK, permitindo na prática a operadores no mercado com sistemas de segurança a interação dos seus sistemas AC com a plataforma XProtect.

Neste contexto, o plugin a que se refere este documento foi desenvolvido com o intuito de proporcionar o acesso à informação presente no sistema de controlo de acessos SALTO via a sua integração ou leitura por outros sistemas externos ao SALTO, no caso particular, a plataforma XProtect da Milestone. O objetivo principal prende-se com facilitar e tornar mais eficiente a operação destes sistemas, permitindo a realização desta através de um único interface de operador, em oposição à necessidade de operar várias interfaces em organizações com vários sistemas, sendo um deles o SALTO.

O SALTO disponibiliza uma API de comunicação com o exterior, sendo esta a única forma de comunicar com este, tratando-se de outra forma de um sistema fechado.

Em termos de blocos macro, o sistema na sua globalidade poderá ser descrito pela seguinte figura:





Existem essencialmente 3 workflows a considerar:

- a) Obtenção da configuração inicial, efetuado no sentido AC -> VMS em termos de passagem de informação, mas com pedidos de informação executados pelo plugin, o que implica comunicação no outro sentido. Neste workflow é transmitida informação de portas, tipos de eventos e cardholders;
- b) Obtenção de eventos (histórico e realtime), efetuado no sentido AC -> VMS, sendo que os pedidos de batchs de eventos são efetuados pelo plugin. Neste workflow é transmitida informação de ocorrência de eventos, como aberturas de portas, intrusões, etc;
- c) Envio de comandos, efetuado no sentido VMS -> AC. Neste workflow, o plugin envia comandos de, por exemplo, abertura de portas para o AC.

A comunicação e passagem de informação entre o VMS (plugin) e o AC nunca é efetuada diretamente, passa sempre pelo serviço de comunicação, que intermedeia toda a interação entre ambos os sistemas.

Salientar ainda que este plugin foi desenvolvido com vista à sua utilização em sistemas de variadas dimensões, desde sistemas de grandes dimensões, com o VMS distribuído por várias máquinas (ex, hierarquia federada) e a gerir centenas de câmeras (ver Fig.1), a sistemas de pequenas dimensões, com o VMS numa única máquina e a gerir um pequeno número de câmeras. Neste último caso, inclusivamente será possível considerar uma única máquina com ambos os sistemas AC e VMS, ainda que o desejável seja uma instalação distribuída, ou seja, cada sistema na sua máquina. Para efeito deste manual, será considerada esta última configuração.



Fig.1: esquema de infraestrutura de rede de um VMS com uma estrutura hierárquica de servidores Milestone ligados a câmaras



Requisitos

Este sistema de integração é composto por 3 componentes que comunicam entre si: o sistema AC Salto, o sistema VMS Milestone e um web service em tecnologia WCF que intermedeia a comunicação entre ambos. Conforme anteriormente assinalado, para efeito deste guia, considerar-se-ão instalados cada um na sua máquina.

Tipicamente, o sistema de AC Salto e o VMS Milestone estarão instalados em máquinas diferentes e localizados em diferentes zonas da rede de uma organização, pelo que se estará neste caso perante uma instalação distribuída. Não invalida que os mesmos princípios não possam ser aplicados a uma instalação local ou em menos máquinas. A figura 2 representa uma instalação distribuída, que servirá de referência para as informações que se seguirão.



Fig.2: esquema de exemplo de infraestrutura com instalação distribuída de sistema de vídeo vigilância e sistema de controlo de acessos, prevendo já servidor de comunicação para web service do plugin



Segue-se uma lista dos requisitos mínimos para integração de um sistema distribuído Salto – Milestone:

- Win 7, 8+ | Win Server 2010 2012+ (64bit): em qualquer uma das máquinas
- Framework .NET 4.0.0 / 4.5.0: em qualquer uma das máquinas
- SQL Server 2012 (poderá ser versão express): na máquina do web service WCF
 - O SQL Server deverá ser instalado em "Mixed Mode", de modo a permitir a autenticação de utilizadores criados no próprio SQL Server
- IIS 10.0: na máquina do web service WCF
- Salto 3.1.4.0 | SHIP 1.26c: na máquina do AC
- Milestone XProtect Corporate 2014: na máquina do VMS (<u>http://www.milestonesys.com/systemrequirements</u>)
- Milestone XProtect Smart Client 2016 R3: na máquina do VMS
- MIPSDK 2016 R2: na máquina do VMS

As máquinas são identificadas na rede através de IPs (xxx.xxx.xxx, conjunto de 4 números inteiros com no máximo 3 dígitos separados por '.') e portas (também um número inteiro). É desta forma que se "vêm" umas às outras e assim poderão comunicar entre si. Considerando a infraestrutura distribuída por 3 máquinas já descrita, o responsável pela instalação deverá também ter presente como requisito de instalação a seguinte informação:

- Endereço IP de rede e porta da máquina Milestone XProtect
- Endereço IP de rede e porta da máquina SALTO
- Endereço IP de rede e porta do web service WCF na máquina de comunicação

O plugin propriamente dito é instalado na máquina do sistema VMS. O plugin foi implementado com recurso à tecnologia MIP-AC Milestone, uma vertente do SDK específico para integração de sistemas AC. O plugin recebe a configuração do AC (portas, cardholders e tipos de eventos), bem como eventos (passados e realtime), e pode enviar para o Salto via SHIP comandos de ação sobre as portas.

O web service em arquitetura WCF tem, como indicado, o objetivo de servir de interface de comunicação Milestone – Salto, atuando como fila de comandos, bem como guardando os eventos localmente em base de dados SQL própria e sincronizar os eventos gerados pelo Salto / SHIP com todos os pontos licenciados e autorizados.

Finalmente, o servidor Salto, com base de dados própria, fechada atrás da interface / API SHIP, aceita comandos de ação sobre portas e envia, a pedido do plugin, a informação de configuração do AC e o stream de eventos.



É muito importante ainda como requisito que os relógios das máquinas envolvidas estejam acertados uns com os outros, isto é, todas com a mesma hora (ao segundo).



Conteúdo do pacote de instalação

O conteúdo do pacote de instalação, com diretório base MIPSaltoPuresecurity, encontra-se listado em seguida:

- MIPSaltoPuresecurity
 - \MIPSDK2016R2
 - MIPSDK_Installer_2016R2.msi
 - \Plugin
 - acplugin.def
 - clsJSONZip.dll
 - MIPSALTOPuresecurity.dll
 - MIPSALTOPuresecurity.dll.config
 - Newtonsoft.Json.dll
 - \WebserviceWCF
 - isystemsSaltoShipWS.isystemsSaltoSHIP.svc
 - Web.config
 - \WebserviceWCF\bin
 - BLayer.dll
 - BLayer.pdb
 - isystemsSaltoShipWS.dll
 - isystemsSaltoShipWS.pdb
 - Newtonsoft.Json.dll
 - \WebserviceWCF\DB
 - 2017-05-22-isystems_Salto_MIP.bak
 - milestone_salto_plugin_guide_byPuresecurity.pdf

Descrição dos ficheiros do plugin

acplugin.def: ficheiro de configuração geral do plugin, necessário para reconhecimento do plugin pelo sistema XProtect

clsJSONZip.dll: libraria de funções de compressão e descompressão de mensagens JSON, tecnologia usada nas mensagens de comunicação entre o plugin, o serviço de comunicação e o AC Salto (via SHIP)

MIPSALTOPuresecurity.dll: lógica relativa a toda a operação específica do plugin, como

MIPSALTOPuresecurity.dll.config: ficheiro xml de configuração específica desta implementação de plugin

Newtonsoft.Json.dll: libraria pública de funções relativas a operações sobre a tecnologia JSON, como conversões "de" e "para" JSON



Descrição dos ficheiros do web service WCF

isystemsSaltoShipWS.isystemsSaltoSHIP.svc: ficheiro de acesso ao web service

Web.config: ficheiro de configuração ao web service

bin\BLayer.dll e BLayer.pdb: regras de negócio do serviço de comunicação

bin\isystemsSaltoShipWS.dll e isystemsSaltoShipWS.pdb: lógica relativa a restante operação específica do web service, nomeadamente métodos de acesso

bin\Newtonsoft.Json.dll: (ver em cima)

DB\2017-05-22-isystems_Salto_MIP.bak: ficheiro de backup para efetuar restore no SQL Server da base de dados usada para registo de informação pelo web service



Procedimento de instalação do plugin

Nesta secção deste guia, serão indicados os passos necessários para a instalação do plugin e do web service WCF de comunicação. É assumida a instalação num sistema no qual já estarão instalados o VMS e o AC.

Para a execução da instalação e configuração que se segue poderá ser útil o apoio do administrador de redes da empresa.

Instalação do Web service WCF

É considerada na 1ª fase a instalação do web service WCF. Este é instalado com recurso às ferramentas Microsoft SQL Server para colocação da base de dados e web server IIS para instanciação do web service com referência aos ficheiros em \WebserviceWCF e \WebserviceWCF\bin.

O web service é instalado na máquina destinada para o web service de comunicação e tem como pré-requisitos, portanto, o SQL Server e o IIS.

Passo 1 Restore do ficheiro de base de dados

Efetuar o restore do ficheiro 2017-05-22-isystems_Salto_MIP.bak referente à base de dados. Para tal, abrir a ferramenta de gestão de base de dados da Microsoft SQL Server Management Studio.

1.1 Clicar em "databases" com o botão direito do rato -> "Restore Database...":



1.2 Surgirá a janela de diálogo referente ao restauro de uma base de dados. Nesta, deverá ser selecionada em "Source" a opção "Device" e clicado o botão "..." no alinhamento.

Surgirá outra janela de dialogo sobreposta à primeira ("Select backup devices") na qual deverão ser efetuadas as seguintes escolhas e ações:

1.2.1 Em "Backup media type" -> "File"

1.2.2 Clicar em "Add"

1.2.3 Selecionar o ficheiro .bak fornecido nos ficheiros de instalação em \WebserviceWCF\DB (a escolha efetuada surgirá na janela "Backup media")

1.2.4 Clicar em "OK":

😓 Restore Database -	- 0	×
🐼 No backupset selected to be res	tored.	
Select a page	Script - 📑 Help	
I General I Files I Options	Source Database:	~
	Select backup devices — — X	~
	Specify the backup media and its location for your restore operation.	~
	Backup media type: File V Timeline	e
	Backup media: Add Remove LSN Contents Add	Full L
Connection DESKTOP-3LRVCST\SQLEXPRI SS [DESKTOP-3LRVCST\az]	OK Cancel Help	
View connection properties		
Progress Ready	<	> edia
	OK Go to Settings to activate	Window



Surgirá na primeira janela de dialogo em "Destinaton" e "Restore plan", o resumo resultante das escolhas efetuadas, referente ao ficheiro de base de dados que irá ser restaurado.

1.2.5	Clicar em	"OK"	novamente:
-------	-----------	------	------------

😼 Restore Database - isystems_Sal	to_MIP				- 0	×
🕕 Ready						
Select a page	🔄 Script 👻 📑 Help					
Select a page	Script - Check Help Source Database: Device: Database: Destination Database: Restore to: Restore plan Backup sets to restor Restore Name Systems_S	C:\Program Files\ isystems_Salto_M isystems_Salto_M The last backup t re: Salto_MIP-Full Database Back	Microsoft SQL Server IP IP aken (13 de junho de j Component Type rup Database Full	MSSQL11.SQLEXPRESS 2017 11:11:20) Server DESKTOP-3LRVCST	\MSSQL'	 Databa isysten
Connection DESKTOP-3LRVCST\SQLEXPRE SS [DESKTOP-3LRVCST\az]						
View connection properties						
Progress	4					>
One Done					Verify Backup	Media
				ок _{Gojto} setance	Vindows Is to activat	e 만Wind or

A base de dados restaurada surgirá colocada no SQL Server Management Studio, em "Databases":





Passo 2 Remoção do utilizador 'default'

Remover utilizador "saltomipuser" da base de dados restaurada.

2.1 Verificar a sua existência expandindo a base de dados criada (nome default: isystems_Salto_MIP) e clicando em "Security" -> "Users".

2.2 Remover o utilizador clicando em "saltomipuser" com botão direito do rato, seguido de "Delete".





Passo 3 Criação de utilizador

Criar utilizador para acesso à base de dados.

3.1 Expandir o servidor SQL local no SQL Server Management Studio e clicar em "Security" -> "Logins".

Clicar depois com o botão direito do rato em "Logins" -> "New Login..."



3.2 Preencher os campos necessários para a configuração do utilizador.

3.2.1 No separador "General", preencher "Login name" com "saltomipuser" e "Password"/"Confirm password" com palavra-passe pretendida:

Jser			-		×
🔄 Script 🔻 🛐 Help					
Login name: Windows authentication SQL Server authentication Password: Confirm password: Specify old password Old password: Enforce password policy Enforce password expira User must change passw Mapped to certificate	saltomipuser			Search	h
 Mapped to asymmetric key 			\sim		
Map to Credential			\sim		
Mapped Credentials	Credential	Provider			
					ve
Default database:	master		~		
	Sorpt Fight Help Login name: Windows authentication SQL Server authentication SQL Server authentication Password: Confirm password: Specify old password Old password: Enforce password expira User must change passw Mapped to casymmetric key Mapped to asymmetric key Mapped to credential Mapped Credentials	Soript Vindows authentication SOL Server authentication SOL Server authentication Solut Server authentication Password: Solut Server authentication Solut password: Solution	Soript ▼ Image: Baltomipuse: Windows authentication ● SQL Server authentication ● SQL Server authentication ● eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	Sortet Help Login name: Satomipuser Windows authentication SQL Server authentication Password: SQL Server authentication Password: Software password experiments Old password: Friforce password policy Friforce password policy Griforce password experiments Mapped to certificate Mapped to certificate Mapped to asymmetric key Map to Credential Mapped Credential Credential Provider	Sorpt Vindows authentication Searce Vindows authentication Solut Server authentication Solut Server authentication Password: Confirm password Old password Old password Old password Old password policy Enforce password policy Discriment change password at next login Mapped to certificate Mapped to asymmetric key Mapped to certificate Add Mapped Credential Credential Provider Remo



3.2.2 No separador "User Mapping", selecionar base de dados restaurada em "Users mapped to this login" e as permissões assinaladas na imagem em "Database role membership":

🚦 Login Properties - saltomipu	Iser		-		×			
Select a page Page General	🔄 Script 🔻 📑 Help							
Server Roles	Users mapped to this login:							
Securables	Map Database	User	Default Schema	1				
E Status	isystems_Salto_MIP	saltomipuser	dbo					
	master							
	model							
	msdb							
	tempdb							
	Guest account enabled for: CES/	AE_Salto_MIP						
	Database role membership for: CESA	AE_Salto_MIP						
Connection	db. accessadmin							
Server: DESKTOP-3LRVCST\SQLEXPRE	db_backupoperator db_datareader							
Connection: DESKTOP-3LRVCST\az	db_datawriter db_ddladmin							
View connection properties	db_denydatareader							
Progress	db_securityadmin							
Ready	D public							

3.2.3 No separador "Securables", garantir que está selecionada a permissão "Grant" na opção "Connect SQL" em "Permissions":

🚦 Login Properties - saltomipu	ser			-	\Box ×
Select a page	🔄 Script 🔻 🛐 Help				
Server Roles	Login name: saltomipus	er			
Status	Securables:			Se	arch
	Name			Туре	
	DESKTOP-3LRVCS	T\SQLEXPRESS		Server	
Connection	Parmingings for DESKTOP				
Connection	Femilisions for DESKTOP-	SERVEST (SQLEAPRESS)			
DESKTOP-3LRVCST\SQLEXPRE	Daminian	Constan	Creat	Wah Count	Deeu
Connection:	Connect SQL	Grantor	Grant	With Grant	
DESKTOP-3LRVCST\az	Connect SQL	sa			
View connection properties	Control server				
	Create any database				
Progress	Create availability group				
Ready	Create DDL event noti				
	Carda andreida				— ~



3.2.4 No separador "Status", garantir a seleção de "Grant" e "Enabled" conforme a imagem, seguido de "OK":

🔒 Login Properties - saltomip	user
Select a page	🔄 Script 🔻 🎼 Help
Server Roles User Mapping Securables	Settings Permission to connect to database engine: Grant Deny Login: Enabled Disabled
	Status
	SQL Server authentication:
	Login is locked out
Connection	
Server: DESKTOP-3LRVCST\SQLEXPRE	



Como já indicado nos requisitos do sistema, o SQL Server deverá permitir a autenticação de utilizadores criados no próprio SQL Server, como é o caso do utilizador "saltomipuser".

A forma de testar se este utilizador, criado para acesso do web service à sua base de dados, tem realmente acesso à base de dados, é testar o seu login através da aplicação SQL Server Management Studio. Nesta, depois de aberta, deverá ser clicado 'File' -> 'Connect Object Explorer' e na janela seguinte escolhido o nome do servidor SQL onde está a base de dados e 'SQL Server Authentication', bem como preenchidos os campos 'Login' e 'Password' com "saltomipuser" e a sua palavra-passe. Após clique no botão 'Connect', não deverá ocorrer qualquer erro e do lado esquerdo deverá surgir uma janela 'Object Explorer' que permitirá aceder às bases de dados do servidor SQL escolhido, no qual deverá estar incluída a base de dados "isystems_Salto_MIP".

Se eventualmente ocorrer algum erro nesta operação, muito provavelmente significa que o servidor SQL não estará a permitir o acesso a utilizadores sql e que terá sido erroneamente instalado em modo 'Windows Authentication". Neste caso, deverá ser corrigida esta configuração do SQL Server antes de prosseguir. Tal deverá ser efetuado novamente através da aplicação SQL Server Management Studio. Na janela 'Object Explorer', normalmente situada do lado esquerdo, clicar com o botão direito do rato no nome do servidor SQL em questão, e em seguida 'Properties'. Na janela que se abrirá, clicar no separador 'Security' e selecionar 'SQL Server and Windows Authentication mode' na secção 'Server Authentication', seguido de clique em OK, e novo clique em OK para confirmar a mudança. Finalmente, deverá ser clicado novamente o nome do servidor SQL com o botão direito do



rato, seguido de clique em 'Restart'. O re-arranque do SQL Server é necessário para que a mudança se torne efetiva.

Passo 4 Instalação de ficheiros

Instalar os ficheiros do web service WCF.

4.1 Criar pasta no diretório C:/ da máquina escolhida para alojar o serviço. Poderá ser na raiz ou em qualquer subpasta que seja conveniente conforme a organização da estrutura de pastas ali existente. A título de exemplo, na imagem seguinte foi-lhe dado o nome "WCF".



4.2 Copiar ficheiros do serviço WCF presentes no bundle de instalação (aqueles na raiz da pasta \WebserviceWCF, incluindo a subpasta \WebserviceWCF\bin e respetivos ficheiros) para a pasta criada especificamente para o efeito no ponto anterior.

4.3 Criar website no IIS, associado aos ficheiros do web service colocados na pasta "WCF".

4.3.1 Abrir a aplicação Windows IIS através de "Windows Administrative Tools" -> "Internet Information Services"

4.3.2 Como tarefa preparatória, criar "application pool" para o website que posteriormente irá ser criado através de "<web server name>" (no caso do exemplo da figura em baixo "DESKTOP-3LRVCST") -> "Application Pools" -> "Add Application Pool":



Internet Information Services (IIS) Manage	r						
← → DESKTOP-3LRVCST →	Application Pools						
File View Help							
Connections	Applicat	ion Poo	DIS age the list of ap ations.	pplication pools on	the server. Application	pools are associated	l with worker
> 🚯 Default We 🔯 Refresh		- 9	🖉 Go 👒 🕁 Sho	w All Group by:	No Grouping	•	
> 😌 SaltoService	Name	Status	.NET CLR V	Managed Pipel	Identity	Applications	
	.NET v2.0	Started	v2.0	Integrated	ApplicationPoolld	0	
	.NET v2.0 Classic	Started	v2.0	Classic	ApplicationPoolld	0	
	INET v4.5	Started	v4.0	Integrated	ApplicationPoolld	0	
	.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolld	0	
	🕼 Classic .NET Ap	Started	v2.0	Classic	ApplicationPoolld	0	
	DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolld	1	
	SaltoService	Started	v4.0	Integrated	ApplicationPoolld	1	

4.3.3 Preencher os campos necessários para a criação da "pool", "Name" com "SaltoService" (este campo fica ao critério, não é obrigatório que seja o exemplo fornecido), ".NET CLR Version" com ".NET CLR Version v4.0.30319" e "Managed pipeline mode" com "Integrated".

Clicar em "OK".

Add Application Pool		?	×
Name:			
.NET CLR version:			
.NET CLR Version v4.0.303	19		\sim
Managed pipeline mode:			
Integrated N	+		
Start application pool	mmediate	ly	
OK		Cancel	

4.3.4 Verificar que o campo "Identity" da pool criada é "ApplicationPoolIdentity":



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker p isolation among different applications.

Filter:	- 3	Go 🕞 👾 Sho	w All Group by:	No Grouping	-
Name	Status	.NET CLR V	Managed Pipel	Identity	Applications
INET v2.0	Started	v2.0	Integrated	ApplicationPoolIdentity	0
.NET v2.0 Classic	Started	v2.0	Classic	ApplicationPoolIdentity	0
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0
🔊 Classic .NET Ap	Started	v2.0	Classic	ApplicationPoolIdentity	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	1
SaltoService	Started	v4.0	Integrated	ApplicationPoolldentity	1
					ApplicationPoolldentity

Se não for este o caso, então deverão ser acedidas as definições avançadas da "pool" por clique no botão direito do rato nesta, e ajustar o campo "Identity" na secção "Process Model" por clique em "…", seguido da configuração apropriada em "Built-in account".

4.3.5 Criar website propriamente dito para o web service, através de "<web server name>" -> "Sites" -> "Add Website":

💱 Internet Information Services (IIS) Manage	er				
← → DESKTOP-3LRVCST →	Sites 🕨				
File View Help					
Connections	Sites		Ch Shawa A		
Application Pools	Filter:	+ ♥ Go	- Show A	Group by: No Grouping •	
Add Website	Default Web Site	1D	Status Stopped (Binding *:80 (http);808:* (net.tcp);localhos	Path %SystemDrive%\inetpub\www.root
> 💐 🔯 Refresh	SaltoService	2	Started (ht	*:8100 (http)	C:\WCF
Switch to Content View					

4.3.6 No formulário que se abrirá subsequentemente, preencher os campos "Site name" (por exemplo, com "SaltoService", o mesmo nome que foi dado à pool criada em 4.3.3), "Application pool", que deverá ser preenchido automaticamente com a pool criada anteriormente (senão, esta deverá ser selecionada recorrendo ao botão "Select... " ao lado), "Physical path" com o caminho para a pasta do web service, selecionando-o por intermédio do botão "..." (ex, "C:\WCF"), e "Host name" com "*:<nº de porta do web service>".

<nº de porta do web service> é, conforme já indicado nos requisitos, um número inteiro representativo da porta a partir da qual o web service irá responder na máquina em que está colocado (ex, 8100, 9000, ...). Todos os sistemas que tentarem comunicar com este, terão que ter na sua configuração esta porta identificada (ex, o plugin).



Add Website					?	×
Site name:		Application pool: DefaultAppPool		Select		
Content Directory Physical path:			1			
Pass-through authentio	cation est Settings					
Binding Type:	IP address:		Port:			
http ~ Host name:	All Unassigned	4 v	80			
Example: www.contoso	o.com or marke	ting.contoso.com				
☑ Start Website immedia	tely		OK		Cancel	

A checkbox "Start Website immediately" poderá ser deixada selecionada, pois deste modo o web service será iniciado imediatamente após clique em "OK".

De outro modo, terá que ser dada ordem de arranque posteriormente através de clique em "Sites" -> SaltoService" (botão direito do rato) -> "Manage Website" -> "Start":

🍓 Internet Inform	atio	n Services (IIS) Manage	er						
$\leftrightarrow \rightarrow$	۲I	DESKTOP-3LRVCST							
File View H	lelp								
Connections				DE	SKTOP-3	LRVCST F	Home		
DESKTOP-3	LRV	CST (DESKTOP-3LRV Pools	Filter:	NET		• 🐺 Go 🕞	Show All	Group by: Ar	ea
✓ Sites Sites Sites Sala	ault '	Web Site	ASP.			404	٢		*
	2	Edit Permissions		.T izat	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Trust Levels	Application Settings
l E	(*) (*)	Add Application Add Virtual Directory						Cer.	3
		Edit Bindings		ntic	Default	Handler	HTTP	ISAPI and	ISAPI Filters
		Manage Website	•	\$	Restart		Kespon	COI Kestii	
	60 X	Refresh Remove			Start Stop				
		Rename		•	Browse				
6		Switch to Content Vi	ew		Advanced Set	tings			



Passo 5 Configuração do web service

Para que o web service fique funcional é necessário um passo final de configuração. Trata-se de configurar o ficheiro xml "Web.Config", presente na pasta de ficheiros do web service colocada na raiz da máquina ("C:\WCF" ou noutra localização na estrutura de pastas da máquina conforme a preferência na instalação).

O ficheiro "Web.Config" poderá ser aberto com um simples editor de texto do tipo "notepad". É um simples ficheiro xml/texto.

5.1 Configuração da ligação à base de dados

Depois de aberto, deverá ser localizada a seguinte entrada numa das suas linhas: key="ADDRESSDB"

Nesta linha deverá ser configurada a ligação do web service à base de dados própria e, neste sentido, deverá ser atualizado o atributo 'value'.

Exemplo: <add key="ADDRESSDB" value="server=192.168.254.40; database=isystems_SALTO_MIP; uid=saltomipuser; pwd=saltomipuser" />

Esta linha de configuração representa a conexão do web service à base de dados que se configurou anteriormente (passo 1). O atributo value possui neste caso 4 subatributos (server, database, uid e pwd).

O nome da base de dados (database=isystems_SALTO_MIP), tendo sido seguidas as instruções de restore fornecidas no passo 1, será o mesmo, pelo que não necessita atualização, bem como o nome do utilizador (uid=saltomipuser).

Terá que ser configurado o IP do servidor de base de dados (server=192.168.254.40), substituindo o IP "192.168.254.40" (indicado a título de exemplo) pelo IP da máquina em que está colocada a base de dados do web service, idealmente, a mesma em que está o próprio web service.

Terá também que ser configurada a password do utilizador usado para aceder à base de dados (pwd=saltomipuser), criado anteriormente neste procedimento (passo 3), substituindo a password "saltomipuser" por aquela criada na criação do utilizador.

5.2 Configuração da comunicação com o sistema AC Salto

De recordar ainda que o web service serve de comunicação entre o plugin (no VMS Milestone XProtect) e o sistema AC Salto, através da interface SHIP deste último. Por conseguinte, o web service terá que ter configurada a sua ligação ao SHIP.

Como na configuração da ligação à base de dados vista em cima, deverão ser localizadas as seguintes entradas no ficheiro de configuração "Web.Config":

key="ComandosIP" e key="ComandosPort"

Também nestes casos deverão ser atualizados os respetivos atributos 'value'.

Exemplo:



<add key="ComandosIP" value="192.168.254.50" />

<add key="ComandosPort" value="9100" />

Estas duas linhas de configuração representam o IP da máquina em que se encontra o AC Salto, nomeadamente a API SHIP, e a porta dessa máquina que permite a entrada de pedidos de comunicação com o SHIP.

Terá, por conseguinte, que ser configurado o IP da máquina onde se localiza o SHIP (value="192.168.254.50"), substituindo o IP "192.168.254.50" (indicado a título de exemplo) pelo IP correto.

Terá também que ser configurada a porta de acesso à maquina onde se localiza o SHIP (value="9100") substituindo o valor "9100" (indicado a título de exemplo) pelo valor correto.

5.3 Outras configurações

Um dos fatores a considerar na instalação desta integração é o desempenho das comunicações. Numa instalação distribuída poder-se-ão ter o sistema VMS Milestone numa máquina, o web service de comunicação noutra máquina, e ainda o sistema AC Salto numa outra máquina. A troca de informação entre estes diversos elementos gera tráfego na rede em cima de outro tráfego que já possa existir. Tal pode acarretar problemas de desempenho da rede, afetando por sua vez o desempenho e bom funcionamento das comunicações entre os componentes da integração.

Existem neste ficheiro de configuração do web service duas linhas relativas à configuração da regularidade com que o web service efetua a sincronização de eventos e a consulta da fila de comandos, que podem ser identificadas, respetivamente, pelas entradas: key="syncEventTimeIntervalSecs" e key="syncCmdQueueTimeIntervalSecs".

Exemplo: <add key="syncEventTimeIntervalSecs" value="10" />

O atributo 'value' deverá ser usado para configurar a regularidade da sincronização de eventos. Quanto mais baixo o valor, maior a regularidade da sincronização de eventos, ou seja, os eventos surgirão mais rapidamente e mais próximos do "tempo-real" no cliente Milestone.

Exemplo: <add key="syncCmdQueueTimeIntervalSecs" value="10" />

O atributo 'value' deverá ser usado para configurar a regularidade da consulta da fila de comandos. Quanto mais baixo o valor, maior a regularidade da consulta da fila, ou seja, os comandos sobre portas serão executados mais rapidamente.

Deverão ser tidas em conta as seguintes orientações nesta configuração:

 A configuração destes valores deverá ser efetuada caso-a-caso e de acordo com o desempenho verificado após instalação da integração numa qualquer rede. Verificando-se um bom desempenho do sistema na rede, podem-se diminuir os valores;



 Os valores não deverão ser colocados a zero, deverá antes ser encontrado um equilíbrio entre o desempenho funcional pela diminuição dos valores e o desempenho do sistema na rede.

Sempre que qualquer configuração neste ficheiro de configuração (web.config) seja alterada, o web service deverá ser reiniciado por execução no web server IIS do comando "Sites" -> SaltoService" (botão direito do rato) -> "Manage Website" -> "Restart".

Instalação do plugin

Após a instalação do web service WCF, na 2ª fase é necessário instalar o plugin propriamente dito.

Este será instalado na máquina onde se encontra o VMS Milestone XProtect, pois foi implementado recorrendo a tecnologia Milestone, precisamente com o intuito da sua incorporação neste tipo de sistemas.

A instalação do plugin necessita de 2 passos, a colocação dos ficheiros do plugin (presentes na pasta "\Plugin" no bundle de instalação) em determinada localização da estrutura de pastas do Milestone XProtect, e a sua configuração no XProtect.

Passo 1 Instalação dos ficheiros

Colocação dos ficheiros do plugin na localização correta.

Relativamente a este passo, um aspeto que é necessário mencionar é que o plugin está fortemente interligado com o "event server" do Milestone XProtect. Quer isto dizer que uma das, senão a finalidade principal do plugin é a receção de eventos do sistema de AC em realtime e o registo destes no VMS. Assim, é natural que seja incorporado no XProtect com relação ao "event server". Outro aspeto a mencionar é que a localização do plugin no XProtect poderá variar consoante a versão deste software, no caso, para efeito deste manual, trata-se da versão 2014.

1.1 Copiar a pasta do plugin para a pasta de plugins do Event Server Milestone.

Para tal deverá ser localizada em primeiro lugar a pasta de plugins do Event Server, recorrendo ao Windows Explorer. Conforme referido, na versão 2014 do software XProtect, esta pasta estará localizada em "C:\Program Files (x86)\Milestone\XProtect Event Server\MIPPlugins".

Depois de localizada esta pasta numa janela de Windows Explorer, bastará fazer uma operação de copiar a pasta "\Plugin" situada no pacote de instalação e colar na janela aberta situada na localização destino.

O resultado será o que se pode observar na figura seguinte. A pasta "\Plugin" deverá ser renomeada para um nome significativo (ex, MIPSalto, PluginMIPSalto, etc). A título de exemplo, na figura a pasta "\Plugin" foi renomeada para "\MIPSALTOPuresecurity".



📙 🛃 📕 🖛 MIPPlugins				_	
Ficheiro Base Partilhar	Ver				
← → × ↑ 🔤 « Progr	amas (x86) > Milestone > XProtec	t Event Server > MIPPlugins >	√ Č	Procurar em MIPPIu	igins
🕂 Transferência 🖈 🔨	Nome	Data de modificaç	Tipo	Tamanho	
🚆 Documentos 🖈	MIPSALTOPuresecurity	29/09/2017 11:38	Pasta de ficheiros		
📰 Imagens 🛛 🖈	VideoOS.Analytics.Events	29/09/2017 10:21	Pasta de ficheiros		
📙 Dash	VideoOS.LicenseService	29/09/2017 10:21	Pasta de ficheiros		
👌 Música					
Vídeos					
🗥 OneDrive					

1.2 Preparar ficheiro de configuração do plugin.

Dentro da pasta do plugin copiada para a estrutura do Milestone XProtect encontrar-se-á um ficheiro de configuração, "MIPSALTOPuresecurity.dll.config". Este ficheiro deverá ser aberto para edição e para tal poderá ser usado o Notepad, dado tratar-se de um simples ficheiro de texto XML.

Após aberto, deverão ser localizadas as linhas assinaladas na figura seguinte:



Estas linhas referem-se ao "endpoint" referente ao web service de comunicação, ou seja, na prática, contêm a informação que o plugin necessita para invocar o web service. O atributo "address" do endpoint deverá ser atualizado da seguinte forma:

- Substituir o IP "192.168.254.40", dado como exemplo, pelo endereço IP de rede do web service WCF na máquina de comunicação;
- Substituir a porta "8100", dada como exemplo, pela porta do web service WCF na máquina de comunicação.



Ainda no mesmo ficheiro, localizar as linhas assinaladas na figura seguinte:



Situam-se no fim do ficheiro, logo abaixo da definição do "endpoint".

Esta linha contem informação relativa ao utilizador usado para fazer login na máquina do web service, na definição de "identity". Nesta, deverão ser atualizados os atributos "userName" e "password" para o nome de utilizador, e respetiva password, a ser utilizado para aceder à máquina do web service.

Passo 2 Configuração do plugin

Configuração do plugin no software Milestone XProtect.

2.1 Registar a existência do novo plugin no XProtect.

Depois da colocação dos ficheiros do plugin na localização correta, o XProtect terá que reconhecer o plugin. Para tal, é necessário reiniciar o serviço do Event Server do XProtect.

Deverá abrir-se o "management client" do XProtect, a aplicação de gestão deste software, tipicamente colocada na estrutura de aplicações do Windows em "Milestone" -> "XProtect Management Application". Após esta aplicação aberta, na árvore de opções à esquerda, deverá ser estendida a opção "Advanced Configuration" e clicar em "Services".



Do lado direito surgirão as ações de gestão relativamente aos serviços do XProtect. O serviço que se deve reiniciar é o "Event Server service", conforme assinalado na figura que se segue. A



ação de reiniciar poderá ser efetuada por clique no botão "Restart" ou por clique em "Stop" seguido de "Start" (após o estado do serviço passar a parado).

mlestone			C
Service Control:			
Service Name	Status	Service Start/Stop	Service Restart
Recording Server service	Stopped	Start	Restart
Image Server service	Started	Stop	Restart
Image Import service	Started	Stop	Restart
Log Check service	Started	Stop	Restart
Event Server service	Started	Stop	Restart
Notification Server service	Started	Stop	Restart

Este passo permitirá executarem-se os passos seguintes. De outra forma não seria possível.

2.2 Criar uma instância do plugin.

2.2.1 Após o registo de plugin pelo sistema VMS, tem que se, de alguma forma, torna-lo visível na interface do XProtect. Para tal, dever-se-á clicar com o botão direito do rato na opção "Access Control" na árvore de opções e depois clicar em "Create new...".



2.2.2 Preencher os campos na primeira janela do wizard de criação do plugin que, entretanto, terá surgido no ecrã, "Name" com alguma designação significativa para o plugin (no exemplo da figura, "MIPSalto"), e escolher na lista de plugins "Integration plug-in" aquele que se pretende instanciar, no caso, "MIP SALTO Puresecurity", seguido de clique no botão "Next":



Create Access Contro	I System Integration	×
Create access Name the access con	control system integration trol system integration, select the integration plug-in and enter the connection details.	
Name:	MIPSalto	
Integration plug-in:	~	
	MIP SALTO Puresecurity	
	Next Car	icel

2.2.3 Surgirá a segunda parte do wizard de criação do plugin, na qual se deverão preencher todos os campos integrantes adicionais, "Address" com o endereço IP da máquina do web service WCF (no exemplo da figura, 192.168.254.40), "Port" com a porta a partir da qual responde o web service na respetiva máquina (no exemplo da figura, 8100), "Username" com o nome de utilizador para autenticação na máquina do web service (no exemplo da figura, edp1) e respetiva password, e, finalmente, "Event polling start date".

Quanto a este último, um parágrafo aparte para explicar: conforme indicado anteriormente, o plugin tem uma componente essencial de obtenção de eventos do AC em realtime. No entanto, a obtenção de eventos poderá ser configurada neste ponto para começar, não somente no momento imediato, mas antes "ir ao passado" obter eventos em histórico no AC até ao momento atual, a partir do qual "engatará" na obtenção realtime. Este último campo serve para indicar a data "para trás" a partir da qual se pretende obter esse tal histórico de eventos, no formato "aa/mm/dd" (2 dígitos para ano, seguidos de 2 dígitos para mês e 2 dígitos para dia, todos estes pares de dígitos separados por barra). No exemplo da figura que se segue está-se a indicar a pretensão de obtenção de todos os eventos a partir do dia 1 de setembro de 2017.

Este passo prosseguirá com clique no botão "Next", após o qual se entrará na fase automática do wizard, assinalada pelo título "Connecting to the access control system..." e uma barra verde de progresso (conforme poderá ser observado na figura após a seguinte).



Create Access Control System Integra	tion		×
Create access control sys Name the access control system integ	stem integration gration, select the integration plug-in ar	d enter the connection de	tails.
Name:	MIPSalto		
Integration plug-in:	MIP SALTO Puresecurity	Ŷ	
Address:	192.168.254.40		
Port:	8100		
Username:	edp1		
Password:	•••••		
Event polling start date (aa/mm/dd):	17/09/01		
]	Next Cancel
· · ·			
Create Access Control System Integr	ration		
Connecting to the acces	ss control system		
Collecting configuration data			

Sendo o procedimento anterior executado corretamente, o resultado deverá ser um ecrã similar à figura seguinte, no qual se poderá encontrar um resumo da informação obtida pelo plugin ao integrar com o AC. De maior relevância, a informação relativa a portas do AC ("Doors"), tipificação de eventos ("Events"), tipos de comandos permitidos ("Commands") e estados de portas ("States").

Connecting to the access control syste	em	
Collecting configuration data		
Configuration successfully received from access control s	system.	
Added:		
Doors (4)		-
Units (4)		•
Servers (1)		-
Events (82)		-
Commands (2)		-
States (13)		-



O ecrã anterior poderá servir desde logo para o operador/administrador avaliar a informação do AC integrado recebida pelo plugin.

Para prosseguir, deverá ser clicado o botão "Next".

2.2.4 O wizard prosseguirá com um ecrã idêntico ao da figura seguinte, com o título "Associated cameras". Nesta fase da configuração do plugin, pode-se encontrar uma lista das portas obtidas do AC do lado esquerdo e do lado direito uma lista das câmeras já registadas pelo VMS (Milestone XProtect).

Create Access Control System Integration			\times
Associated cameras Drag cameras to the access points for each do Client when access control events related to or	or in the list. The associated c ne of the door's access points	ameras are used in the XProtect Smart are triggered.	
Doors:		Cameras:	
Name	Enabled License 🤏	▲ 된 Server	
Cilindro Electronico	✓ Pending	All Cameras (Server)	
Access point: Cilindro Electronico access p Drop camera here to associate it with the ac Escudo XS4 Wireles Porta Especial Cãó	oint ccess point. Pending	Ali Slaves (Server)	
Porta OnLine Act.	Pending		
		Previous Next Can	cel

Um dos intuitos desta integração VMS Milestone <-> AC Salto é também permitir associar estas câmeras a portas, de modo a criar posteriormente automatismos de, por exemplo, gravação vídeo por intermédio das câmeras na ocorrência de eventos em portas.

Assim, neste ponto da configuração do plugin, é já possível encetar esta associação de câmeras a portas, através de operações de "drag-and-drop", pegando nas câmeras do lado direito e arrastando-as para o lado esquerdo. Conforme as portas a que se pretendam associar as câmeras, estas devem ser arrastadas para as zonas identificadas com "Drop camera here..." das respetivas portas. Na figura seguinte poderá ser observada, relativamente à anterior, a subtil diferença resultante da associação da "Camera 1" à porta "Cilindro Electronico", na qual acima da expressão "Drop camera here..." se encontrará a designação da câmera associada à porta, com um botão de remoção ("Remove") alinhado, usado para remover a associação, caso assim seja pretendido.

Para prosseguir, deverá ser clicado o botão "Next".



Create Access Control System Integration					×
Associated cameras Drag cameras to the access points for each do Client when access control events related to or	or in the li ne of the c	ist. The ass door's acce	ociated ss point	cameras are used in the XProtect Smart is are triggered.	
Doors:				Cameras:	
Name	Enabled	License	9	▲ ↓ Server	
Cilindro Electronico	 Image: A start of the start of	Pending	\checkmark	A 🚞 All Cameras (Server)	
Access point: Cilindro Electronico access p	oint			All Slaves (Server)	
Camera 1 Drop camera here to associate it with the a	ccess poin	<u>Re</u> t.	move		
Escudo XS4 Wireles	✓	Pending			
Porta Especial Çãó					
Porta OnLine Act.	~	Pending			
				Previous Next Can	ice

2.2.5 Finalizados os passos anteriores, surgirá o ecrã de finalização do wizard de configuração do plugin.

Create Access Control System Integration	×
You have successfully completed the access control system integration Your XProtect Smart Client users can now monitor access control events. See the help system for how to optimize the XProtect Smart Client for access control system integration.	
You can edit the integration settings in the access control system properties, if you, for example, update the access control system.	
Ck	ose



A atualização do plugin com uma nova versão (novos ficheiros) requer sempre a repetição do passo 1 da secção "Plugin" deste guia, com uma nuance: dado tratar-se de uma atualização, antes de copiar os ficheiros novos para cima dos antigos, será necessário parar ("Stop") o "Event Server service", conforme exemplificado no passo 2.1, para desbloquear os ficheiros do plugin registados no Milestone XProtect. Depois sim, poderão ser copiados os ficheiros da nova versão para cima dos ficheiros da versão em uso, nunca esquecendo a necessidade de, no fim do procedimento de atualização, iniciar ("Start") novamente o "Event Server service".

Licenciamento

Não havendo licenciamento para o plugin, este exibirá uma mensagem "Licence invalid" na sua informação de conexão:

milestone		

Access Control:

Enable	Name	Connection Status	Connection Information
<	teste	Not connected	Licence invalid

Para licenciar o plugin, é necessário obter um ficheiro de licenciamento ("licenca.kws") e coloca-lo em local específico na máquina do web service WCF, conforme parametrização. Esta parametrização encontra-se no ficheiro xml de configuração do web service, "Web.Config". Neste deverá ser localizada a seguinte linha:

<add key="licencePath" value="c:\wcf\" />, onde key é a identificação do parâmetro e value o seu valor, sendo que é este segundo que deve ser ajustado conforme a localização pretendida para o ficheiro de licenciamento.

Este parâmetro não é mais, portanto, do que a indicação da localização do ficheiro de licenciamento, para que o web service e o plugin saibam onde este está, o verifiquem e ajam de acordo com a validade da licença.

No exemplo em cima, é indicada a pasta do próprio web service para colocação do ficheiro da licença, pasta onde foram colocados os ficheiros do web service conforme indicado no passo 4 da secção de instalação do web service deste manual. No entanto, poderá ser escolhida qualquer outra localização na mesma máquina. Aconselha-se, contudo, por uma questão de organização e eficiência, a colocação do ficheiro de licenciamento juntamente com os ficheiros do web service.

Como passo final, e essencial, para ativar a licença é necessário reiniciar o web service no IIS (web server do Windows), pelo que se terão que executar os seguintes passos:



- Abrir a aplicação Windows IIS através de "Windows Administrative Tools" -> "Internet Information Services"
- Dar ordem de reinicio do web service posteriormente através de clique em "Sites" -> SaltoService" (botão direito do rato) -> "Manage Website" -> "Restart" (conforme imagem em baixo)



Quando se tratar de uma renovação de licença, bastará copiar o novo ficheiro de licenciamento atualizado para cima do anterior, na mesma localização, e executar novamente os dois passos de reinicialização do web service.

O licenciamento tem duas vertentes: limitação do nº máximo de portas a gerir pelo plugin e prazo de validade, limitado por uma data de expiração, pelo que a sua expiração ou perda de validade poderá estar relacionada com a introdução de novas portas no sistema AC Salto, que poderão, depois de importadas pelo plugin, originar o ultrapassar do limite máximo permitido pela licença ou, simplesmente, com o ultrapassar da data de expiração.

A funcionalidade do plugin relativa ao licenciamento gera automaticamente na própria máquina Milestone, onde está instalado o plugin, um ficheiro de configuração encriptado ("configuration.txt"), na pasta pública

"C:\Users\Public\Documents\MIPSaltoiSystems" do sistema operativo Windows. Este ficheiro só tem utilidade para a operação interna do plugin, pelo que não é necessário abri-lo, editá-lo ou movê-lo.



Operação do plugin

Após a instalação, o plugin instalado ("MIPSalto" na figura) surgirá na lista de plugins relativos a integrações com sistemas AC (separador "Access Control" na interface da aplicação de gestão "XProtect Management Application").

Milestone XProtect Enterprise 2014 Management App



MIPSalto

Selecionando o plugin neste separador, surgirá do lado direito informação relativa ao estado do plugin. Estando tudo a funcionar corretamente, o estado deverá estar "Connected" e "Server connected".



Para aceder à interface de operação de backoffice do plugin, dever-se-á clicar com o botão direito do rato na designação do plugin, seguido de clique em "Properties":

Connected

Server connected



Milestone XProtect Enterprise 2014 Management App



Surgirá posteriormente a janela que permite operações de gestão do plugin em backoffice.

Access Control			_		×
				1	C
General Settings Associated Cameras Access Control Events Access ControlActions Cardholders	General settings Enable: Name: Description: Integration plug-in: Last configuration refresh: Address: Port: Username: Password: Event polling period (ms): Event polling max count: Event polling start date (aa/mm/dd):	✓ MIP Salto MIP SALTO Puresecurity (Version: 1.0.0 29/09/2017 12:20 192.168.254.40 8100 edp1 ••••••••••••••••••••••••••••••••••••	Refresh Configura	tion	
			ОК	Cano	cel



Gestão do plugin em backoffice

1 General Settings

Na figura de cima pode-se ver o conteúdo do separador de gestão do plugin relativo a configurações gerais. Este é também o separador que abre inicialmente quando se clica em "Properties" no plugin.

Neste separador, além da informação de configuração inicialmente introduzida na instalação ("Name", "Integration plug-in", "Address", "Port", "Username", "Password" e "Event polling start date"), podem-se encontrar os seguintes campos de configuração do plugin:

- "Enable", que serve para ativar/desativar o plugin;
- "Description", no qual se pode registar uma pequena descrição do plugin, ou algumas notas referentes ao mesmo que se considerem pertinentes e necessárias;
- "Last configuration refresh", que indica a data da última sincronização de informação efetuada com o sistema AC (Salto). Este campo tem associado um botão para se efetuar nova sincronização manual sempre que desejável;
- "Event polling period" e "Event polling max count". Relativamente a estes dois campos de configuração, são emparelhados pois estão ambos associados à obtenção dos eventos, o primeiro tratando-se de "quanto em quanto tempo se pedem eventos ao web service" (em milissegundos) e o segundo, "quantos eventos são puxados de cada vez". Assim, no exemplo da figura de cima, estarão a ser puxados 10 eventos de 10 em 10 segundos (10000 milissegundos). Assinalar ainda relativamente a estes parâmetros de configuração, a importância da sua afinação consoante as condições da rede em que o plugin está a ser instalado. De cada vez que são puxados eventos, é gerado tráfego na rede.

Em qualquer momento se pode usar este separador para editar e ajustar todos estes campos de configuração do plugin.

2 Associated Cameras

Este separador refere-se à associação de portas a câmeras, exatamente da mesma forma conforme surgia em determinado momento no wizard de instalação. As câmeras poderão ser associadas a portas por arrastamento da direita (câmeras) para esquerda (portas). As câmeras poderão ser desassociadas de portas por clique no respetivo botão "Remove". Todas as associações efetuadas durante a instalação estão aqui refletidas e poderão ser alteradas.

Na figura em baixo pode ser observado o conteúdo deste separador:



Access Control							×
						1	C
🍪 General Settings	Associated cameras						
👒 Associated Cameras	Drag and drop to associate camer	as with do	or access points.				
🎨 Access Control Events	Doors:				Cameras:		
📖 Access Control Actions	Name	Enabled	License	3	▲ 🗐 Server		
🧘 Cardholders	Cilindro Electronico	~	Expires in 30 days	~	🔺 🧰 All Can	neras (Sei	rver)
	Access point: Cilindro Electron Camera 1 Drop camera here to associa	ico acces te it with th	s point e access point.	Remove	All Slav	ves (Serve	er)
	Escudo XS4 Wireles	~	Expires in 30 days				
	Porta Especial Çãó						
	Porta OnLine Act.	✓	Expires in 30 days				
					ОК	Can	cel

3 Access Control Events

Neste separador reside a informação referente aos tipos de eventos existentes no AC, importados durante a instalação do plugin para o VMS. Estes tipos de eventos servem essencialmente para tipificar os eventos e eventualmente agrupar eventos semelhantes por categorias, uma vez que se podem agrupar vários tipos de eventos (coluna "Access Control Event") numa mesma categoria de evento (coluna "Event Category"), simplificando a observação e análise dos tipos de eventos recebidos, pois poderão estar agrupados por categorias mais significativas e de mais simples compreensão imediata.

Adicionalmente, a coluna "Select" permite selecionar quais os tipos de eventos que se pretendem monitorizar e, em oposição, aqueles que não se pretendem monitorizar. Pode acontecer que em determinados sistemas ocorram muitos eventos no AC de um determinado tipo que não interessa de todo monitorizar do lado do VMS. Neste caso, poder-se-á desmarcar na coluna "Select" este tipo de evento, não surgindo depois os eventos deste tipo nas listas de eventos.

A funcionalidade referente a este separador pode ser observada na figura em baixo:



Access Control				- 0	×
				1	C
🍘 General Settings	Acce	ss control events			
👒 Associated Cameras	Calanti			in the first life of a second state of the	
🔁 Access Control Events	Select tr	e events you want to monitor in AP	rotect Smart Client. Use categor	les to simplify the use of triggering	events.
Access Control Actions	Select	Access Control Évent	Source Type	Event Category	
	✓	Alarm: intrusion (online)	Door Unit	Alarm, Warning	× ^
Cardholders	✓	Alarm: tamper (online)	Door Unit	Alarm, Warning	v
	~	Automatic change.	Door Unit		~
	~	Blacklisted key deleted	Door Unit		v
	✓	Closing not allowed: door in em	Door Unit	Access denied, Access requ	× .
	✓	Communication with Salto Esta	Door Unit		~
	✓	Communication with Salto Lost.	Door Unit		~
	✓	Door Closed: key and keyboard.	Door Unit		~
	✓	Door Closed: key.	Door Unit		~
	✓	Door Closed: keyboard.	Door Unit		~
	~	Door Closed: switch.	Door Unit		~
	~	Door left opened (DLO)	Door Unit	Alarm, Warning	~
	~	Door most probably opened: ke	Door Unit		~
	✓	Door opened after second doub	Door Unit		~
	~	Door Opened: mechanical key.	Door Unit		~
	✓	Door Opened: inside handle	Door Unit		~
	~	Door Opened: key and keyboar	Door Unit		~
	✓	Door Opened: key.	Door Unit		v
	✓	Door Opened: keyboard.	Door Unit		~
	✓	Door Opened: multiple guest k	Door Unit		~
	✓	Door Opened: online command.	Door Unit		× ~
	User-o	lefined Categories			
				OK Car	ncel

Finalmente, assinale-se ainda a existência do botão "User-defined Categories…" (categorias definidas pelo operador). Este botão serve precisamente para criar categorias adicionais, ajustadas às necessidades e contexto da empresa e do sistema em que foi instalado o plugin. Estas categorias "extra" poderão depois ser usadas para agrupar tipos de eventos através da sua escolha, após criação, na coluna "Event Category".

A janela de criação de uma nova categoria pode ser verificada no exemplo da figura seguinte:

User-defined Categories		×
Name		Add
Categoria criada por utilizador		Remove
	ОК	Cancel



4 Access Control Actions

Neste separador de gestão do plugin, podem ser criadas ações de variados tipos de acordo com vários parâmetros, ou seja, permite configurar a ocorrência de ações (como notificações) consoante a ocorrência de eventos de determinado tipo ou de determinada maneira. No exemplo da figura de baixo, está criada uma ação ("Action") que se trata do lançamento de uma notificação ("Display (...) notification") quando ocorrerem eventos de natureza de pedido de acesso ("Triggering Event") a qualquer tipo de porta ("Source") em qualquer momento ("Time Profile").

Segue uma descrição dos vários aspetos funcionais deste separador:

- Botão "Add Access Control Action", serve para criar uma nova ação e, na prática, adiciona uma nova linha à lista de ações acima do botão;
- Na nova linha de criação de ação:
 - Coluna "Enable", serve para ativar/desativar a ação depois de criada (pode deixar de ter utilidade num determinado momento ou durante ou determinado período);
 - Coluna "Triggering Event", serve para escolher o tipo de evento que irá espoletar a ação;
 - Coluna "Source", serve para escolher a fonte na qual poderá ocorrer o evento que espoletará a ação, no caso, a porta (ou portas);
 - Coluna "Time Profile", serve para escolher o momento ou período durante o qual a ação poderá ocorrer;

Access Control						×
					1	C
General Settings	Access control actio	ons				
Associated Cameras	Specify the settings for each acti	ion you define.				
Control Events	Enable Triggering Event S	Source	Time Profile	Action		
Access ControlActions	Access request V A	All doors V	Always v	Display access request notification	v	X
🛓 Cardholders						
						>
	Add Access Control Action					

• Coluna "X", serve para apagar completamente a ação do sistema.

Adicionalmente, algumas ações poderão ter algum tipo de detalhe mais "fino" a definir. Será o caso das notificações e, por conseguinte, do exemplo na figura acima. Neste caso, selecionando a ação na lista, surgirão na zona por baixo do botão de criação das ações os dados cuja definição é necessária para concluir a configuração da ação (exceto se o pretendido for o 'default').

No exemplo fornecido, este detalhe poderá ser observado na figura seguinte, correspondente ao detalhe originado pela ação escolhida na figura anterior.



Add Acces	s Control Action				
Configure the	access request notification behavior.				
Camera:	Related camera	~	Commands:		
Speaker:	Camera speaker	~	Command		
Microphone:	Camera microphone	Ŷ	Related access request commands		v X
Sound alert:		~			
			Add Command		
				ОК	Cancel

O detalhe para esta ação, do tipo notificação, inclui, do lado esquerdo, a definição da câmera que poderá ser acionada pela ação, e de outros aspetos como o altifalante, o microfone e o alerta sonoro.

Do lado direito, situa-se a definição dos comandos permitidos para esta ação do tipo notificação, no caso, estão definidos os comandos 'default' para as caraterísticas da ação em questão ("lock" e "unlock").

Poderá ser adicionado um novo comando por clique no botão "Add Command" ou então alterado o comando já existente, clicando no próprio. Imagine-se que se pretende que na notificação gerada só seja permitido um dos comandos "Lock" ou "Unlock": dever-se-á neste caso selecionar a linha do comando criado e depois, dado não se pretenderem todos os comandos disponíveis, mas tão-somente um deles, optar por "Access control command" -> "Lock" ou "Unlock" (conforme o comando que se pretenda disponibilizar na janela da notificação) -> "[source]" (significando a fonte da notificação, no caso, provavelmente, uma porta para a qual foi pedido acesso por um cardholder).

Add Acces Action d Configure the	is Control Action			
Camera:	Related camera	Ŷ	Commands:	
Speaker:	Camera speaker	~	Command	
Microphone:	Camera microphone	~	Related access request commands v X	
Sound alert:		~	Related access request commands All related commands	
			Access control command	[source]
			System command Unlock	Other
			Add Command	
			OK Cancel	12

Esta sequência de opções pode ser confirmada na figura seguinte:

5 Cardholders

Este último separador da interface de gestão do plugin inclui informação relativa aos cardholders (utentes de cartões, isto é, as pessoas com acesso às instalações/portas registadas no sistema).



Trata-se de uma simples lista dos cardholders importados do AC para o VMS.

Access Control				— 🗆	×
				- 7	C
 General Settings Associated Cameras Access Control Events Access Control Actions Carcholders 	Cardholders Search for cardholders to vie when an access control even Search cardholder	ew, add or delete a picture of the cardh nt has been registered. Q	older. The cardholder picture is used in the	XProtect Smart Client	t,
	Name Alice Martins Carlos Silva Ferreira Castro Gedeão Murillo João Çidhs João Çidhs João Qidhs Jose Henrique Raul Rimni Rita Fonseca Romeu Fernandes Tita Carvalho Vasco Zacarias Zelian Zaza Gabor Zé Manel	Type			
				OK Cance	el

Clicar no nome de cada cardholder dá acesso a informação mais detalhada que surgirá no espaço à direita. No exemplo da figura que se segue, pode-se observar o detalhe do cardholder fictício "Carlos Silva":

Cardholders

Search for cardholders to view, add or delete a picture of the cardholder. The cardholder picture is used in the XProtect Smart Client, when an access control event has been registered.

Search cardholder	Q	
Name	Туре	Carlos Silva
Alice Martins		
António Simões Dias		Select picture
Carlos Silva		Delete picture
Fernando Leal		
Ferreira Castro		3
Gedeão Murillo		5
Joana Freitas		Cardholder ID: A274F531DE4FCECE818008D4C2EEAF7C
João Çjdhs		Expiry date: 2000-01-01T00:00:00
Joaquim		
1 11 1 1		1

Em grandes sistemas, esta lista de cardholders poderá atingir uma dimensão muito grande, pelo que o plugin disponibiliza ainda uma funcionalidade de pesquisa de cardholders, bastando para tal colocar a string de texto que se pretende pesquisar na caixa de texto com a lupa,



sendo o resultado da pesquisa imediato e refletido na lista, conforme se pode observar na figura seguinte:

Cardholders			
Search for cardholders to when an access control ev	view, add or delete a pi vent has been registere	cture of the cardl d.	holder. The cardholder picture is used in the XProtect Smart Client,
Car	8		
Name	Туре		
Carlos Silva			
Tita Carvalho			
Zacarias Zelian			

5.1 Fotografias de cardholders

É possível associar fotografias aos respetivos cardholders.

Após a instalação inicial e consequente obtenção inicial da lista de cardholders, é gerado no sistema um ficheiro de texto com informação dos cardholders (nome e ID). Sempre que ocorrer alguma alteração na lista de cardholders no sistema, e esta for consultada através do backoffice de gestão do plugin, este ficheiro será atualizado.

O ficheiro gerado não é mais do que um ficheiro de suporte cujo objetivo é facilitar a operação de atribuição de fotografias aos cardholders e que se descreverá em seguida.

Este ficheiro, conforme indicado, é gerado de forma automática e estará localizado numa pasta pública do sistema operativo Windows, na máquina Milestone, onde foi instalado o plugin:

"C:\Users\Public\Documents\MIPSaltoiSystems"

A pasta "MIPSaltoiSystems" (caso ainda não exista) é gerada também automaticamente na estrutura pública de pastas já existente no sistema operativo. Nesta pasta poderão ser então encontrados todos os ficheiros que o plugin gera de forma automática, como suporte à sua operação. Um deles é o ficheiro "cardholderList_forPictures.txt", usado como suporte à operação de atribuição de fotografias a cardholders:





Tratando-se de um simples ficheiro de texto, poderá ser aberto com um editor de texto simples, como o acessório Windows notepad. Na figura seguinte pode ser visto a título de exemplo o conteúdo deste ficheiro, referente a uma lista de cardholders fictícios:

CardholderList_forPictures.txt - Bloco de notas
Ficheiro Editar Formatar Ver Ajuda
Romeu Fernandes 0EA80BC0F9AD14CFDB0008D4C2EE2F58
Fernando Leal 29DA7F661EADBFCC818008D559DD185F
Raul Rimni 35C174A9E23A92CA020008D4C2EF9473
Jose Henrique 3C212593FC55CA115E2108D2F0196909
Joana Freitas 3E4F03EF8285EFC4E70008D4C7CBBD5F
Gedeão Murillo 66254DA6FEDB5AC45E8008D4C84A4CF2
Joaquim 751F611D556AC852A73A08D2F0182DA7
António Simões Dias 7A630D75DACB90CB050008D559DD2BF4
Ferreira Castro 7A633C3C7A9993CC110008D4C8535A88
Zé Manel 8463DE3503E9C83444DC08D4A9BF6692
Rita Fonseca 8E0FC851ECC887CE6D0008D4C2EEA78B
Carlos Silva A274F531DE4FCECE818008D4C2EEAF7C
João Çjdhs AB556E82503DCD619E8E08D2F01933BB
Alice Martins C6EF5EA90AB862CDC58008D4C7CA0E66
Vasco D90460B2EFCEC8E57DF008D2F019152B
Zaza Gabor E622E74F1172F9C7CF0008D4C2EFA959
Tita Carvalho EDBE80230A35B6C95B8008D4C2EE9FC7
Zacarias Zelian F92B891152CE2BCD708008D4C2EE97FA

O conteúdo não é mais do que a informação de nome e ID de cardholder por cada linha. Desta forma, tem-se fácil acesso a esta informação, ao invés de fazê-lo através do backoffice de gestão e clicando em cada cardholder um-a-um.

O passo seguinte para atribuição de fotografias aos cardholders é criar a pasta "cardholders_pictures" na pasta em que foi instalado o plugin, isto é, na pasta em que foram colocados os ficheiros do plugin, na máquina Milestone, conforme procedimento indicado na secção "Instalação do plugin – Passo 1":

퉲 🛃 🚮 🛨		Ferramentas de Imagem	MIPSALTOPu	resecurity	
Ficheiro Base Partilha	r Ver	Gerir			
(c) → ↑ 🦉 « MIPPlugins → MIPSALTOPuresecurity v C Pro					
🔆 Favoritos	Nome	*	Data de modificaç	Тіро	
🔜 Ambiente de trabalh	퉬 cardh	olders_pictures	15/03/2018 17:31	Pasta de fick	
🔚 Locais recentes	🖹 acplu	gin.def	13/03/2018 17:31	Export Defin	
🗼 Transferências	🚳 clsJSC	DNZip.dll	01/03/2017 11:17	Extensão da	
쑦 Favoritos - Atalho	🚳 MIPS	ALTOPuresecurity.dll	27/03/2018 17:51	Extensão da	
	MIPS	ALTOPuresecurity.dll.confi	g 14/03/2018 12:24	Ficheiro COI	
🤣 Grupo Doméstico	🚳 Newt	onsoft.Json.dll	08/11/2016 11:23	Extensão da	

"C:\Program Files (x86)\Milestone\XProtect Event Server\MIPPlugins\MIPSALTOPuresecurity"

Dentro desta pasta ("cardholders_pictures") deverão ser colocadas as fotografias dos cardholders, quando existentes, no formato de ficheiros de imagem JPG, e com tamanhos de



ficheiro que poderão ir desde os poucos KB (ex, ~10KB), até algumas dezenas de KB, mas evitando ultrapassar 150-200KB, por questões de eficiência.

No passo que se segue, é quando o ficheiro de texto "cardholderList_forPictures.txt" de suporte mencionado atrás se tornará útil. O nome a atribuir a cada ficheiro de fotografia de cardholder deverá ser o ID do respetivo cardholder. Esta informação estará facilmente disponível no tal ficheiro de suporte. Para um determinado cardholder, bastará encontrar o seu nome no conteúdo do ficheiro e, na mesma linha, após o carater "|" poderá ser encontrado o seu ID, que deverá ser selecionado, copiado e colado na renomeação do ficheiro de imagem JPG respetivo. No final desta operação, todos os ficheiros de fotografias de cardholders deverão ter como nome de ficheiro o ID do respetivo cardholder, conforme figura que se segue:

鷆 💽 🛄 🛨		Ferramentas de Imagem		cardholders_pictu	ures	- 🗆 🗙	
Ficheiro Base Partilhar	Ver	Gerir				~ (
() ▼ ↑) ≪ MIPSALTOPuresecurity → cardholders_pictures				~ Č	Procurar em cardholders_pict 🔎		
🔆 Favoritos	Nome	*		Data de modificaç	Тіро	Tamanho	
📃 Ambiente de trabalk	🔛 0EA80	BC0F9AD14CFDB0008D4C	2EE2F58.jpg	15/03/2018 15:16	Imagem JPEG	54 KB	
🖳 Locais recentes	SC212593FC55CA115E2108D2F0196909.jpg			15/03/2018 15:17	Imagem JPEG	74 KB	
🗼 Transferências	🚬 3E4F0	3EF8285EFC4E70008D4C70	BBD5F.jpg	15/03/2018 15:18	Imagem JPEG	18 KB	
쑦 Favoritos - Atalho	🚬 7A633	C3C7A9993CC110008D4C	8535A88.jpg	14/03/2018 17:31	Imagem JPEG	184 KB	
	🚬 8E0FC	851ECC887CE6D0008D4C2	EEA78B.jpg	15/03/2018 15:19	Imagem JPEG	35 KB	
🝓 Grupo Doméstico	🚬 29DA	7F661EADBFCC818008D55	DD185F.jpg	15/03/2018 15:17	Imagem JPEG	103 KB	
	🚬 35C17	4A9E23A92CA020008D4C2	EF9473.jpg	15/03/2018 15:17	Imagem JPEG	35 KB	
👰 Este PC	C6EF5	EA90AB862CDC58008D4C	7CA0E66.jpg	13/03/2018 18:08	Imagem JPEG	10 KB	

O reconhecimento dos ficheiros de fotografia novos pela parte do plugin requer como passo final que se faça o "Restart" do "Event Server service", no backoffice de gestão Milestone XProtect, conforme exemplificado no passo 2.1, na secção de instalação do plugin.

Tal permitirá ao plugin associar a cada cardholder a sua fotografia automaticamente através do campo chave ID. O efeito será o aparecimento da fotografia do cardholder no seu detalhe, em oposição ao aparecimento de uma imagem genérica:

em oposição ao apare	cimento de uma image	m genérica:	
Cardholders			
Search for cardholders to view, a when an access control event ha	add or delete a picture of the cardł as been registered.	holder. The cardho	older picture is used in the XProtect Smart Clien
Search cardholder	Q		
Name	Туре	Carlos Si	lva
Alice Martins		1	
António Simões Dias			Select picture
Carlos Silva		a 🖘 🖥	Delete picture
Fernando Leal			Delete picture
Ferreira Castro			
Gedeão Murillo			
Joana Freitas		Cardbolder ID:	A274E531DE4ECECE818008D4C2EEAE7C
João Çjdhs		Expiny date:	2000-01-01T00-00-00
Joaquim		Expiry date.	2000-01-01100.00.00