



BRAVAS
TECNOLOGIA

PRD0028

Módulo Acesso

Manual de Integração com Sigma Cloud

(versão de Documento V1.00.1)



Bravas – PRD0028 Módulo Acesso

Nenhuma parte desta publicação pode ser reproduzida, armazenada ou transmitida sob qualquer forma (mecânica, fotocopiada, gravada), sem permissão escrita da Bravas Tecnologia.

A Bravas Tecnologia não assume qualquer responsabilidade por erros ou omissões contidos neste manual. As aplicações, softwares, protocolos, etc. aqui reproduzidos são de propriedade da Bravas Tecnologia que permite ao usuário realizar cópias de proteção ("backup") e/ou transferir este documento para uso próprio.

Todas as marcas e nomes de produtos de outros fabricantes citados neste manual são marcas ou marcas registradas de seus respectivos proprietários.

A Bravas Tecnologia não se responsabiliza pelas aplicações que fazem uso das APIs e protocolos de comunicação descritos neste documento. O usuário pode reproduzi-los apenas para seu próprio uso, sendo vedado sua comercialização sem a permissão expressa da empresa.



1 Tabela de Conteúdos

1 Tabela de Conteúdos.....	3
2 Introdução.....	4
3 Configurando o Módulo Acesso.....	4
3.1 Envio de Eventos para o SigmaCloud.....	4
3.2 Configurando os Códigos de Eventos.....	8
3.3 Configurando Estado de Porta e Envio de comandos.....	8
4 Controle de Versão de Documento de API.....	15

2 Introdução

Este documento descreve os passos necessários para configurar o Módulo Acesso (PRD0028) para operar em conjunto com a plataforma de monitoramento Sigma Cloud, no que tange recebimento de eventos na plataforma e envio de comandos.

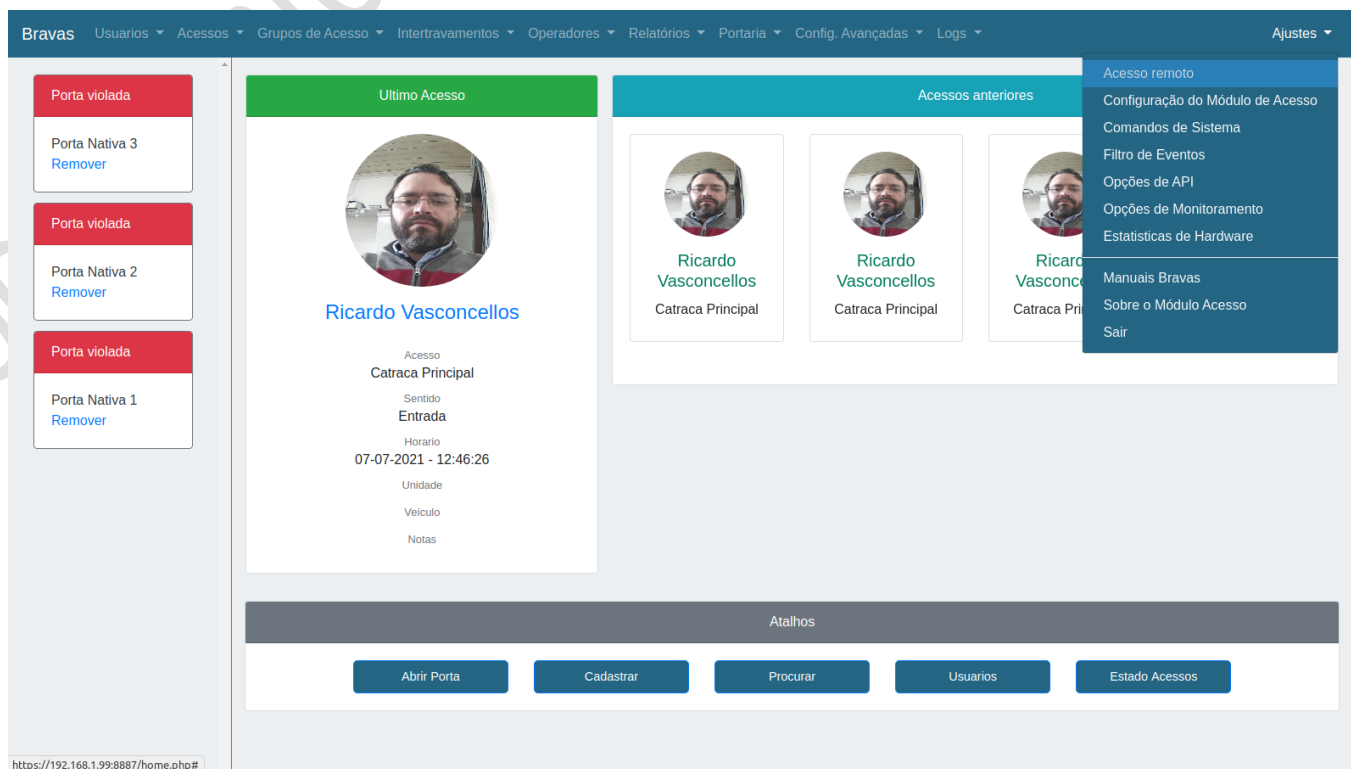
O Módulo Acesso é o hardware que será instalado nas dependências da Conta monitorada no SigmaCloud e requer acesso a internet para o envio dos eventos. Para recebimento de comandos, a infraestrutura de rede no local (instalação do Módulo Acesso) deverá permitir que o acesso externo, via internet por exemplo, consiga estabelecer conexão com o Módulo Acesso,

O Módulo Acesso Bravas (PRD0028) deve estar operando com versão de firmware no mínimo 1.10.1.

3 Configurando o Módulo Acesso

3.1 Envio de Eventos para o SigmaCloud

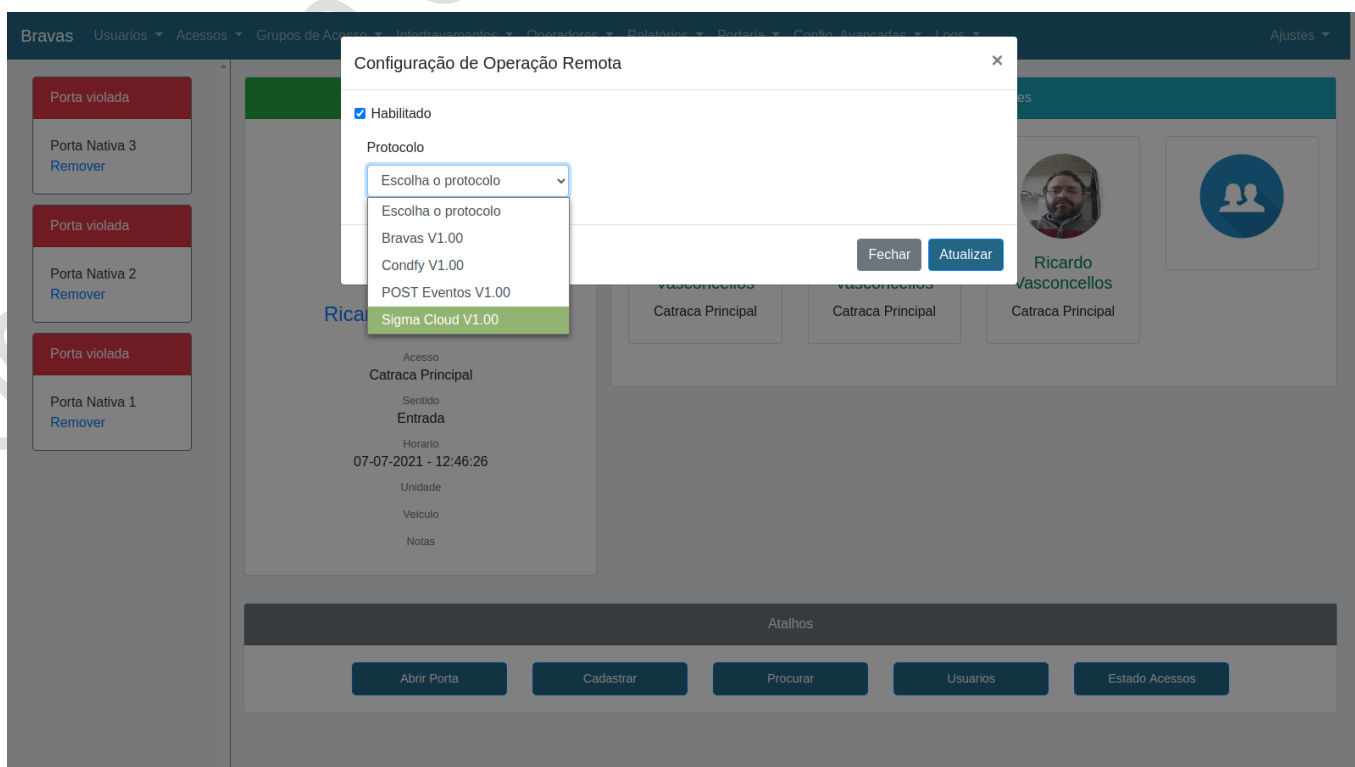
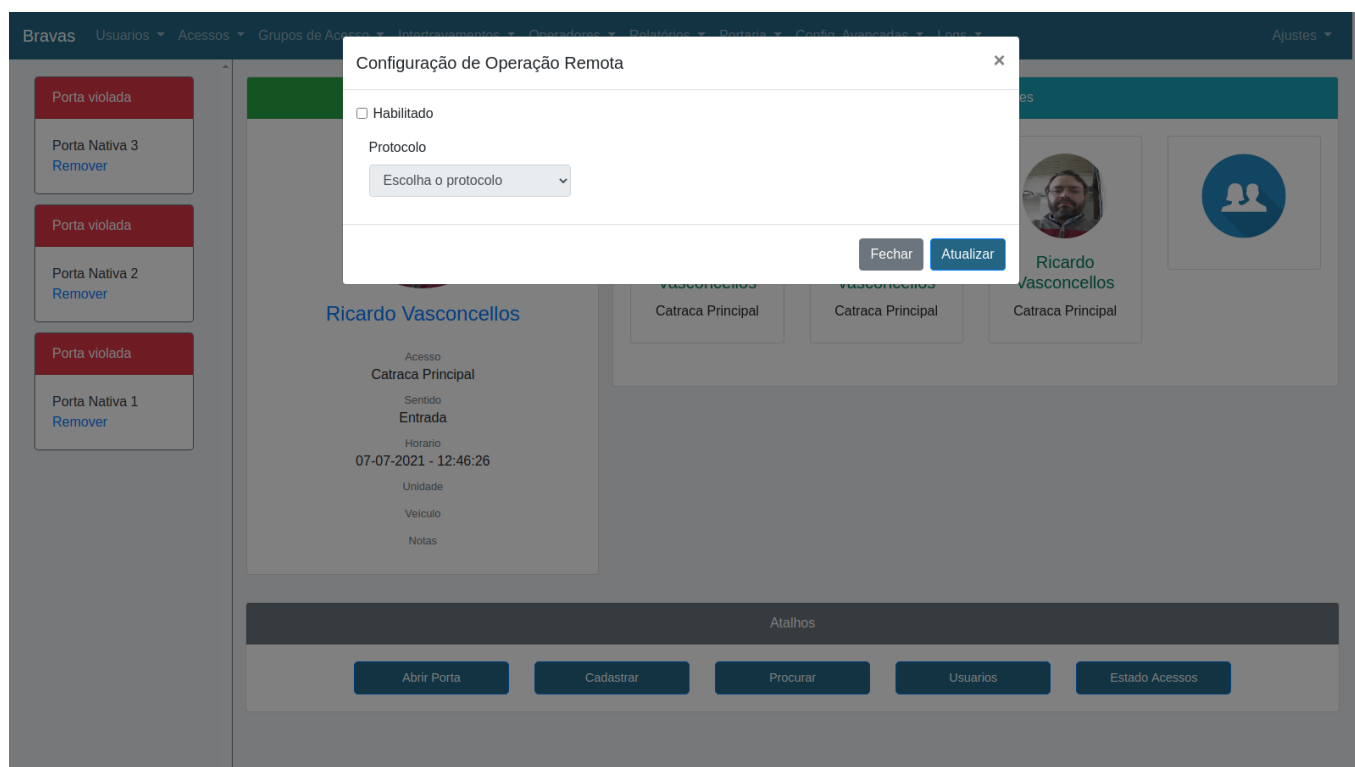
Para o envio de eventos (ex. Porta Aberta) para a plataforma Sigma Cloud é necessário configurar o acesso remoto no Módulo Acesso. Isto é feito selecionando a opção “Acesso Remoto” no menu “Ajustes” na interface de configuração do Módulo Acesso:



A seguir será apresentada a tela de configurações de acesso remoto. Habilite o acesso remoto e selecione a opção SigmaCloud V1.00:



O



Agora é necessário entrar com os parâmetros registrados no Sigma para a correta operação.

O primeiro passo é adicionar o Token. O Token é um item disponibilizado pela Segware para permitir que o equipamento estabeleça comunicação com a plataforma Sigma Cloud. Se você já possui o Token de acesso basta preencher este campo.



Se você não possui o Token de acesso, é necessário fazer a solicitação para a Segware, enviando um e-mail para suporte@segware.com, informando os dados de sua empresa e solicitando o Token para integração via API do Módulo Acesso Bravas (PRD0028).

Uma vez inserido o Token é necessário preencher o nome da sua empresa, a qual será responsável pelo monitoramento da Conta do cliente final. Para facilitar é possível clicar no botão “VERIFICAR”. O Sistema apresentará uma nova tela com os Nomes das empresas associados a este Token, para que você possa fazer a seleção:

Configuração de Relação de Empresas

☒ Habilitado

Protocolo: Seleção
Bravas Monitoramento

Sigma Cloud V...

Fechar Selecionar

Token de Empresa
eyJhb...

Nome da Empresa
Verificar

Nome da Conta

Porta TCP (local)

Fechar Atualizar

Complete os demais campos:

Nome da Conta: é o nome da Conta (dentro do SigmaCloud) do cliente final onde será feito o monitoramento:



Condominio Bela Vista (Bela Vista)

Contas **+ Adicionar**

COND0001
Bela Vista (Condominio Bela Vista)
Virtoz (Bravas Monitoramento)

Alarme Controle de acesso

Informações

Razão social
Condominio Bela Vista
Permitido no máximo 100 caracteres

Nome fantasia
Bela Vista
Permitido no máximo 100 caracteres

Tipo
Pessoa jurídica

CPF/CNPJ
1231231234
Permitido no máximo 100 caracteres

Telefone 1
Permitido no máximo 20 caracteres

Telefone 2
Permitido no máximo 20 caracteres

Nextel
Permitido no máximo 20 caracteres

E-mail
Permitido no máximo 100 caracteres

Website
Permitido no máximo 100 caracteres

Coordenadas Excluir Cancelar Salvar

Porta TCP (local): é a porta TCP que o Módulo Acesso “escutará” para receber comando vindos do SigmaCloud, como abrir porta. Esta porta deve ser selecionada de forma que não tenha impacto sobre as demais portas usadas pelo sistema. Por exemplo, definir porta 9080.

Configuração de Operação Remota

☒ Habilitado

Protocolo
Sigma Cloud V1.00 **Ajustar Códigos**

Token de Empresa
eyJ... (redacted)

Nome da Empresa
Bravas Monitoramento **Verificar**

Nome da Conta
COND0001

Porta TCP (local)
9080

Fechar Atualizar



Ao clicar em “Atualizar” o sistema estará pronto para enviar os eventos para o SigmaCloud.

3.2 Configurando os Códigos de Eventos

É possível ajustar o código “ContactID” de cada um dos eventos originados pelo Módulo Acesso. Isso permite ajustar os eventos padronizados dentro do Módulo Acesso a sincronizar com as CUCs já definidas pelo cliente dentro do SigmaCloud.

Para realizar esse procedimento, na mesma janela de configuração do acesso remoto (Item 3.1 desde documento), clique na opção “Ajustar Códigos”. Será apresentada a janela com todos os Eventos que o Bravas pode enviar para o SigmaCloud no momento e, clicando sobre algum deles, é possível ajustar o código:

Nome		Código
Porta aberta		BV01
Porta fechada	Acesso	BV02
Porta violada	Alarme	BV03
Botao pressionado	Acesso	BV04
Credencial tag	Acesso	BV05
Credencial senha	Acesso	BV06
Credencial panico	Alarme	BV07
Credencial biometria	Acesso	BV08
Credencial controle	Acesso	BV09
Credencial desconhecida	Acesso	BV10
Comando remoto	Acesso	BV14
Credencial de API	Acesso	BV26
Acao de automacao	Automacao	BV27
Evento de automacao	Automacao	BV28
Solicitado travar porta	Acesso	BV29
Solicitado destravar porta	Acesso	BV30
Usuario desabilitado	Acesso	BV31
Solicitado abrir porta	Acesso	BV32
Credencial QRCode	Acesso	BV33

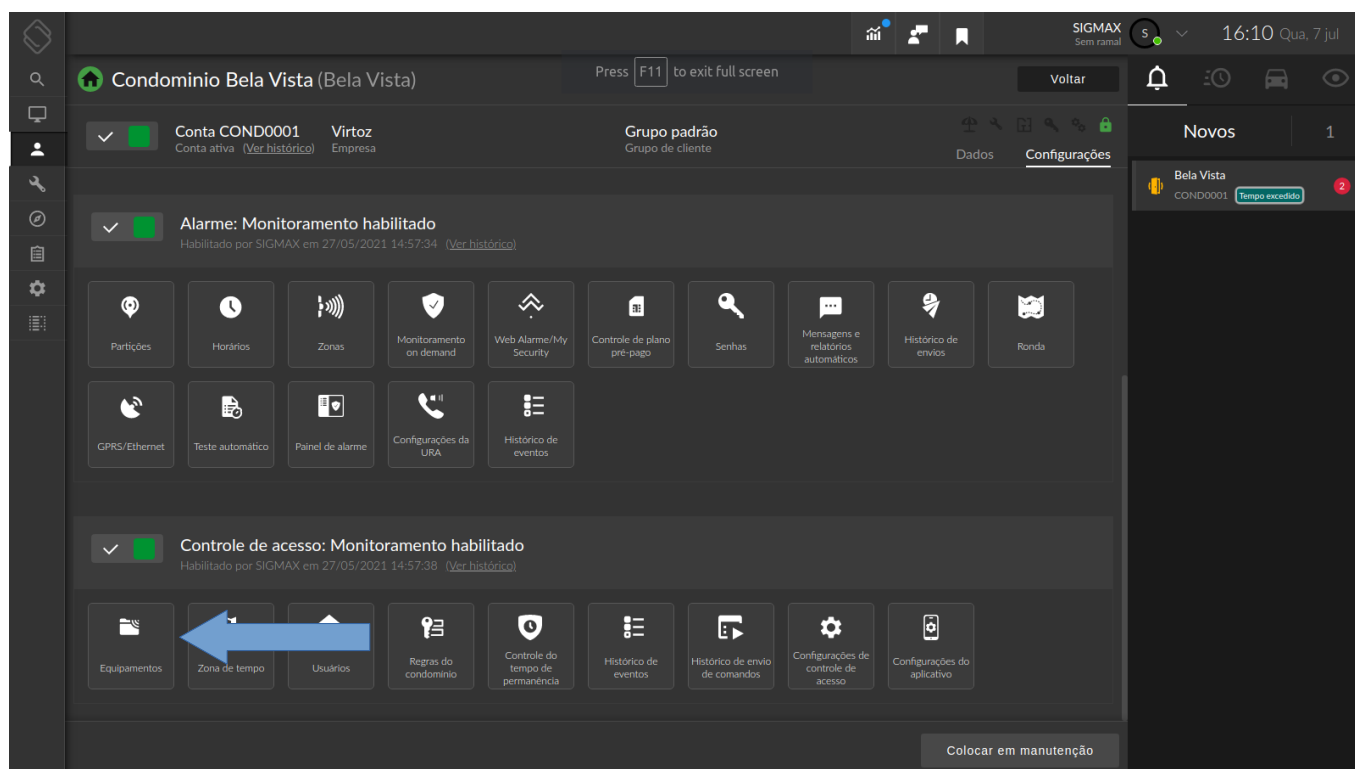
Após realizar as alterações desejadas clique em Gravar. Ao fechar a tela, clique novamente em Atualizar para ajustar os códigos no Módulo Acesso.

3.3 Configurando Estado de Porta e Envio de comandos

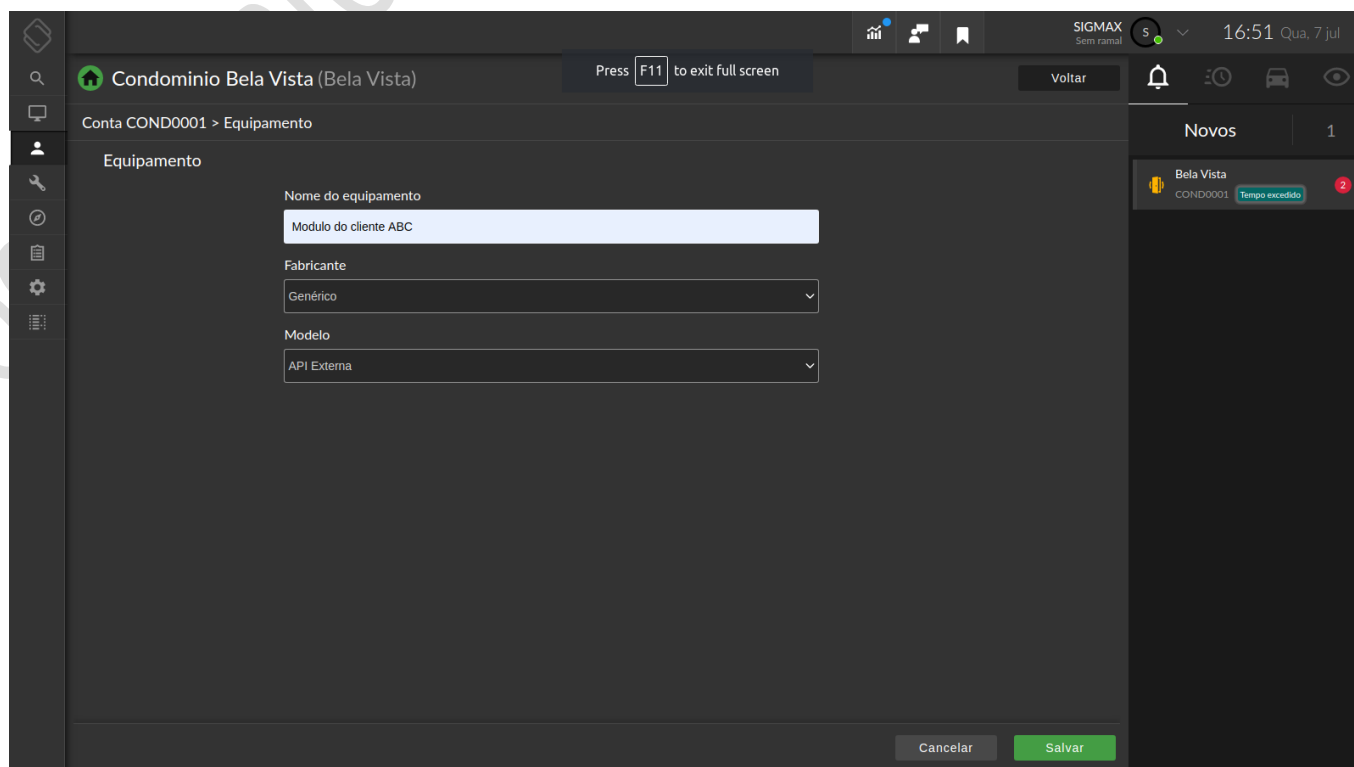
Para enviar comandos para o Módulo Acesso é preciso adicionar um equipamento a Conta do cliente no Sigma Cloud. Nas configurações da Conta, vá em “Controle de Acesso” => “Equipamentos”:



O

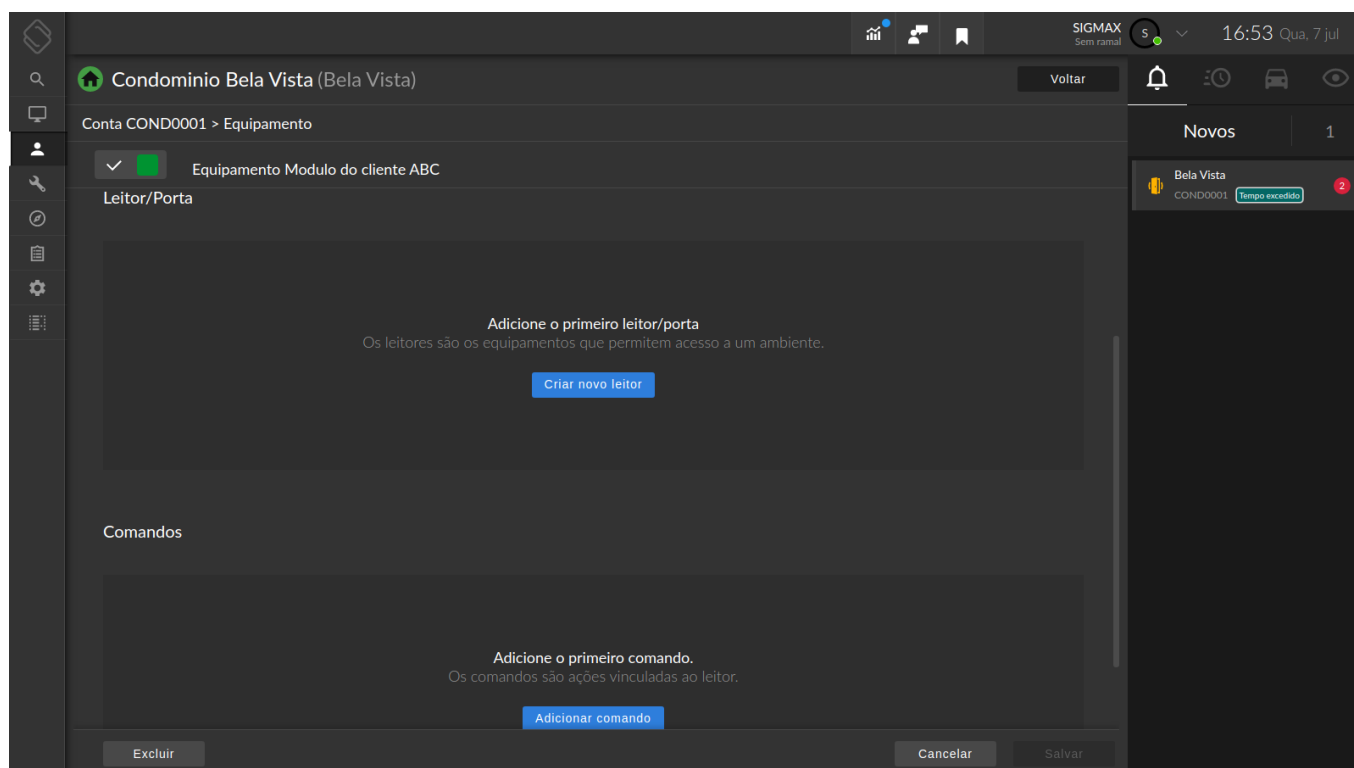


Ao clicar em Equipamento, na tela seguinte, deve ser adicionado um equipamento com fabricante do tipo “Genérico” e modelo “API Externa”:





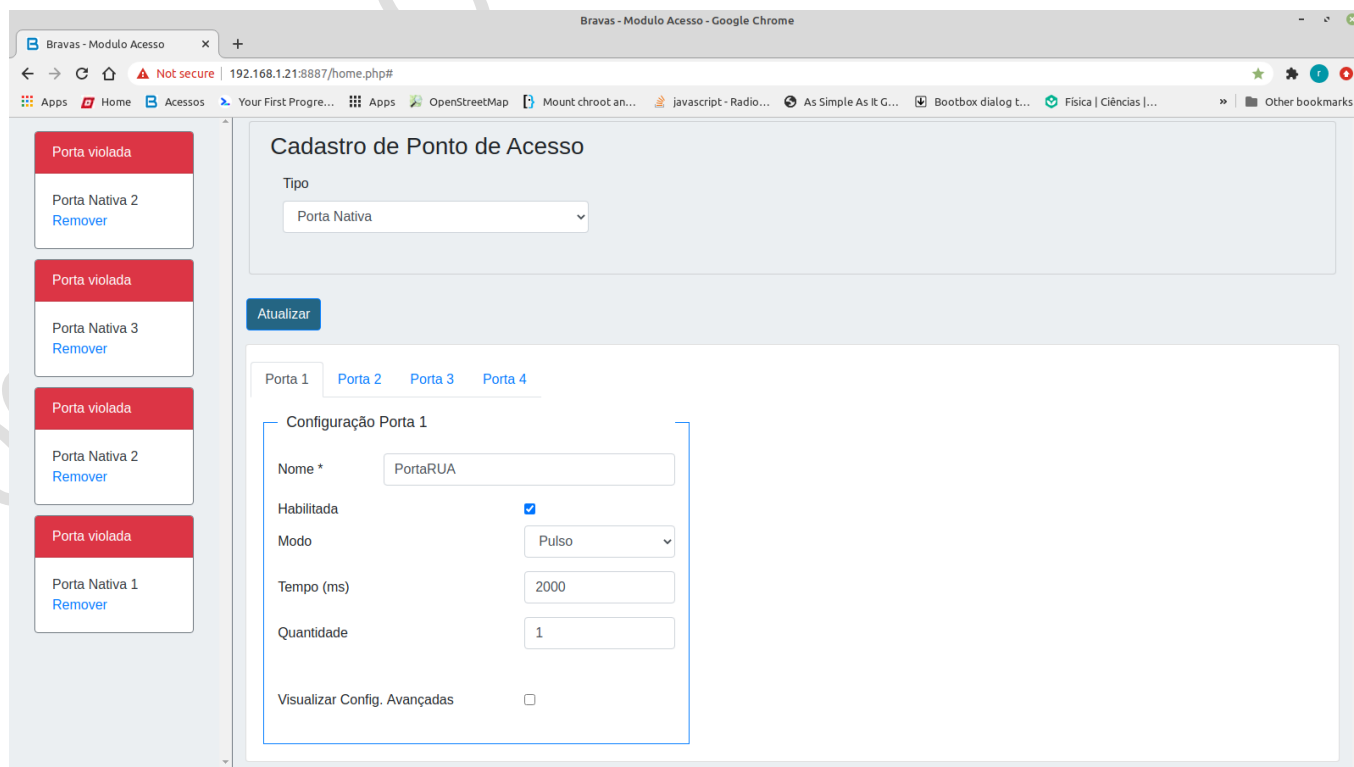
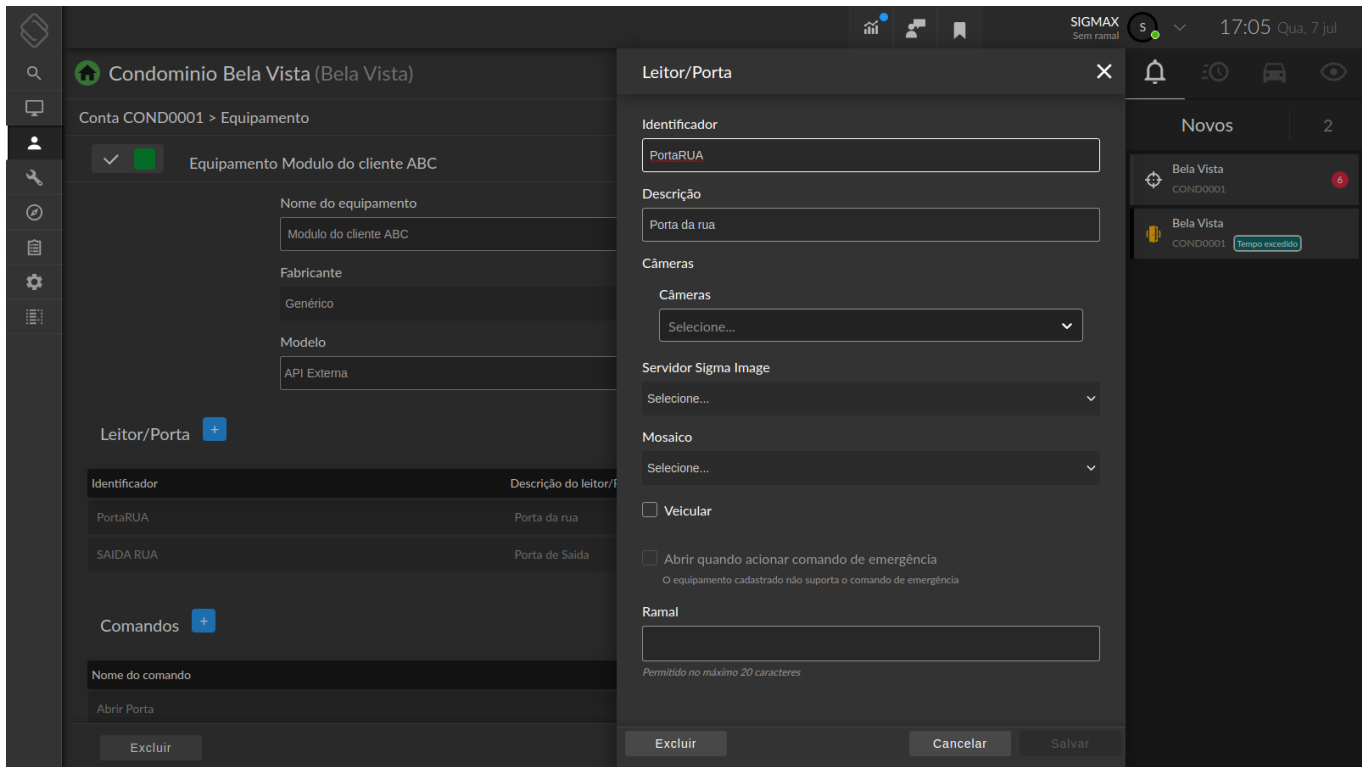
Logo em seguida a interface do SigmaCloud disponibilizará dois campos: Um para inserir as Portas (os acessos que você cadastrou previamente no Módulo Acesso) e também um campo para cadastro de Comandos:



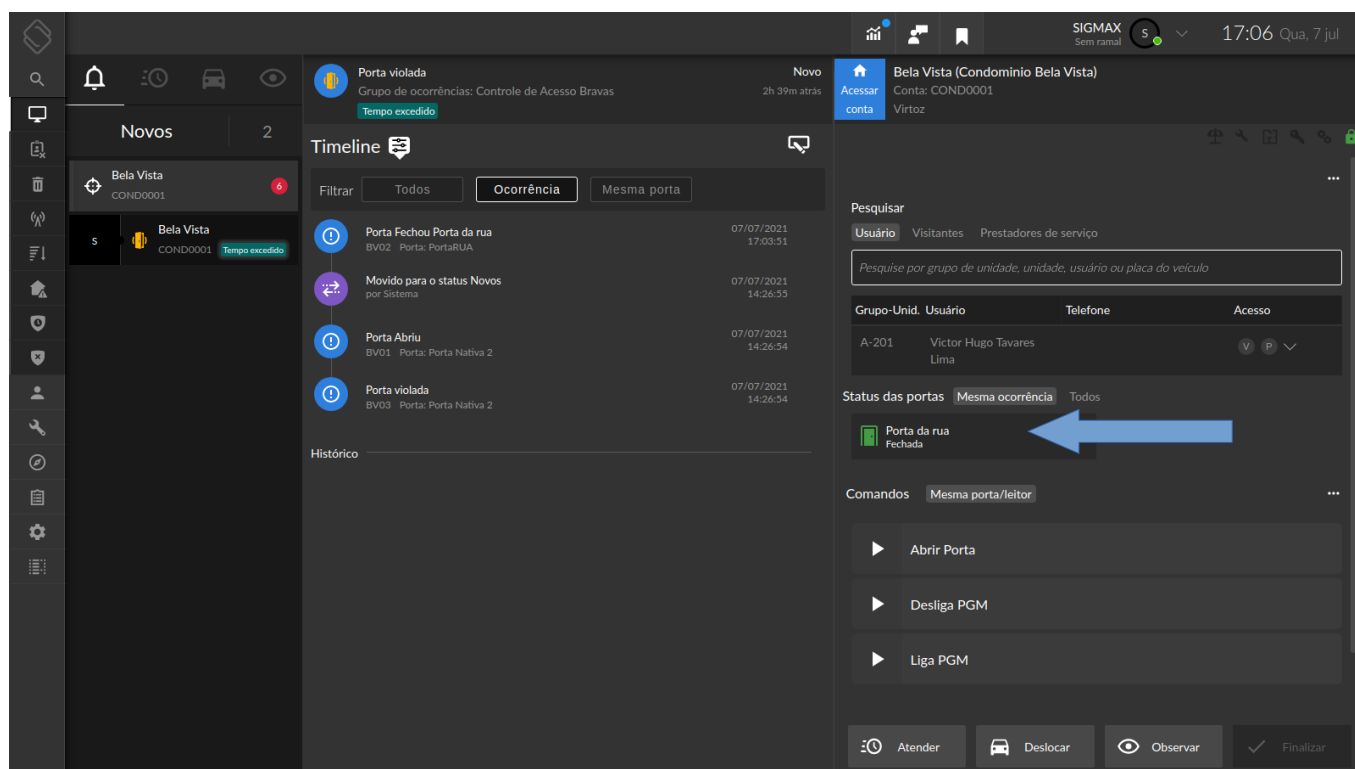
Para cadastrar as Portas o importante é que o campo “Identificador” contenha o mesmo nome que foi utilizado no cadastro do acesso no Módulo Acesso Bravas. Isto permitirá indicar, na interface do Sigma Cloud, o estado da porta (Aberta/Fechada).

Obs.: O estado de porta aberta ou fechada, no caso do Módulo Acesso, não é uma informação em tempo real. O SigmaCloud recebe do Módulo Acesso os eventos na medida que o estado na porta é modificado e armazena este estado para apresentar a condição na tela.

Para fins específicos de integração apenas os campos “Identificador” e “Descrição” são necessários.



Bravas Tecnologia
Porto Alegre – RS – Brasil
51 30294004 www.bravas.ind.br



Com relação aos comandos, clique, na tela que foi apresentada logo após criarmos o equipamento, em Adicionar Comando.

O envio de Comandos de Abertura de Porta ou acionamento de PGMs é um comando HTTP do tipo POST. Para isso basta escolher um acesso (esse campo pode selecionar qualquer acesso uma vez que o alvo real é indicado no corpo do comando HTTP), adicione um nome para este comando (ex. "Abrir porta") e insira o comando HTTP selecionando a opção POST.

Ex. de URL:

Abertura de porta

<http://bravastecnologia.dtdns.org:9080/command?token=14543435424434&type=door&action=open&name=PortaRUA&rules=false&direction=0>

Acionamento PGM

<http://bravastecnologia.dtdns.org:9080/command?token=14543435424434&type=automation&action=setPgm&address=1&position=1&value=1>

A estrutura de um comando para abertura de um acesso cadastrado no Módulo Acesso obedece o seguinte padrão:

Endereço

http://IP:PORTA

Onde:

IP: endereço IP associado ao Módulo Acesso



PORTA: Porta TCP Local configurada durante o ajuste de acesso remoto no Módulo Acesso

URI:
command?

Parâmetros (formato nome do parâmetro=valor do parametro), separados por &:

token: token de API configurado no Módulo Acesso. Se não estiver usando token mantenha o parâmetro zerado (ex. Token=&....);

type: tipo de comando. As opções atuais são “**door**” (para abertura de portas) e “**automation**” para acionamento de PGMS;

action: tipo de acionamento. No caso de portas o valor deve ser “**open**”. No caso de PGMS o valor deverá ser “**setPgm**”;

rules: Obedecer ou não as regras locais do controle de acesso (ex. Intertravamento) durante abertura de portas (**true**) ou ignorar e abrir (**false**). Essa parâmetro não é enviado para acionamento de PGM;

direction: Indica a direção que o acesso esta sendo realizado. Isso serve para reportar posteriormente através de eventos que foi um acesso de entrada ou saída. Para entrada usamos valor “0” e para saída o valor “1”;

address: Endereço físico configurado na PGM (dips). Essa parâmetro não é enviado para abertura de portas;

position: Posição do rele a ser acionado na PGM (1 a 4). Essa parâmetro não é enviado para abertura de portas;

value: Ligar ou desligar o rele da PGM. Valor “0” para desligar o rele. Valor “1” para ligar o rele. Essa parâmetro não é enviado para abertura de portas.

Exemplos:

Considerando que o Módulo acesso está instalado em local com endereço bravastecnologia.dyndns.org e a porta tcp local configurada como 9080:

Ex. 1: Abrindo Porta chamada de “Garagem 1” com Módulo Acesso configurado sem o token
[http://bravastecnologia.dyndns.org:9080/command?
token=&type=door&action=open&name=Garagem%201&rules=false&direction=0](http://bravastecnologia.dyndns.org:9080/command?token=&type=door&action=open&name=Garagem%201&rules=false&direction=0)

Obs.: Para usarmos nomes com espaços devemos substituir o espaço por %20

Ex. 2: Ligando o Rele 3 do Módulo PGM 5 com Módulo Acesso com Token de API =

[http://bravastecnologia.dyndns.org:9080/command?
token=ABCDEDED123&type=automation&action=setPgm&address=5&position=3&value=1](http://bravastecnologia.dyndns.org:9080/command?token=ABCDEDED123&type=automation&action=setPgm&address=5&position=3&value=1)



Ex. 3: Desligando o Rele 3 do Módulo PGM 5 com Módulo Acesso com Token de API =

[http://bravastecnologia.dyndns.org:9080/command?](http://bravastecnologia.dyndns.org:9080/command?token=ABCDEDED123&type=automation&action=setPgm&address=5&position=3&value=0)

[token=ABCDEDED123&type=automation&action=setPgm&address=5&position=3&value=0](http://bravastecnologia.dyndns.org:9080/command?token=ABCDEDED123&type=automation&action=setPgm&address=5&position=3&value=0)

Documento Confidencial

4 Controle de Versão de Documento de API

V1.00.0	07/07/2021	Versão Inicial
V1.00.1	08/07/2021	Adicionado informação sobre versão de firmware Bravas

Documento Confidencial