



Radioenge

WebReceiver
Radioenge

Tutorial

Revisão - Julho de 2023

Sumário

1	Servidor de Monitoramento - WebReceiver	3
2	Instalação do Software WebReceiver	4
2.1	Requisitos para instalação	4
2.2	Instalação do WebReceiver	4
3	Inicialização do Software WebReceiver	7
3.1	Falha ao inicializar WebReceiver – Porta HTTP já utilizada	8
4	Login WebReceiver	11
5	Status do Software	13
6	Eventos	15
7	Centrais de alarme	16
7.1	Informações gerais	17
7.2	Comandos	18
7.2.1	Armar/desarmar partições	18
7.2.2	Anular zona	19
7.2.3	Ativar/desativar PGM	20
7.3	Configurações	20
7.3.1	Zonas	22
7.3.2	Zonas - Cadastro de sensores	23
7.3.3	Partições	24
7.3.4	Partições - Temporização	25
7.3.5	Partições - Auto arme	25
7.3.6	Usuários	25
7.3.7	Usuários - Cadastro de controle remoto	27
7.3.8	Usuários - Configuração do controle remoto	28
7.3.9	Usuários - Configuração do controle remoto - Função pânico através do controle remoto	28
7.3.10	Usuários - Configuração do controle remoto - Função coação através do controle remoto	29
7.3.11	Usuários - Dias e horário para permitir usuário	29
7.3.12	PGM	30
7.3.13	Sistema	31
7.3.14	Sistema - Intervalos de testes, keepalives e atraso de evento de falha	32
7.3.15	Sistema - Configuração de avisos sonoros	32
7.3.16	Sistema - Canais de operação	32
7.3.17	Sistema - Senha do usuário	32
7.3.18	Sistema - Calibração do teste da sirene	32
7.3.19	Horário	33
7.3.20	Atualização do firmware	34
7.3.21	Cloud	34
7.3.22	Cloud - Cadastro no aplicativo via token	34
7.3.23	Cloud - Vincular empresa de monitoramento na RadioengeCloud	34
8	Configurações	35
8.1	Rede	35
8.2	Central	38
8.2.1	Comunicação	39
8.2.2	Comunicação - Módulo IP	40
8.2.3	Configurador CWR-32 e CWR-128	42
8.3	Monitoramento	44
8.3.1	SIGMA	44
8.3.2	SIGMA - Configuração com WebReceiver	46

8.3.3	MONI	48
8.3.4	MONI - Configuração com o WebReceiver	51
8.4	Eventos	53
8.5	Cloud	55
9	Alterar Senha	56
10	Logout	57
11	Códigos de Eventos da Central	58
12	Contato	60

1 Servidor de Monitoramento - WebReceiver

O servidor de monitoramento e controle **WebReceiver** tem a função de se conectar com as centrais de alarme. Esta conexão é feita de forma direta com os modelos Radioenge e através do Módulo IP Alarme com os modelos Paradox e JFL. O WebReceiver recebe e envia eventos para os softwares de monitoramento (Sigma, Moni etc.), efetua os principais comandos disponíveis nas centrais, apresenta os estados das zonas, partições e PGM e disponibiliza a opção de configuração para as centrais de alarme Radioenge.

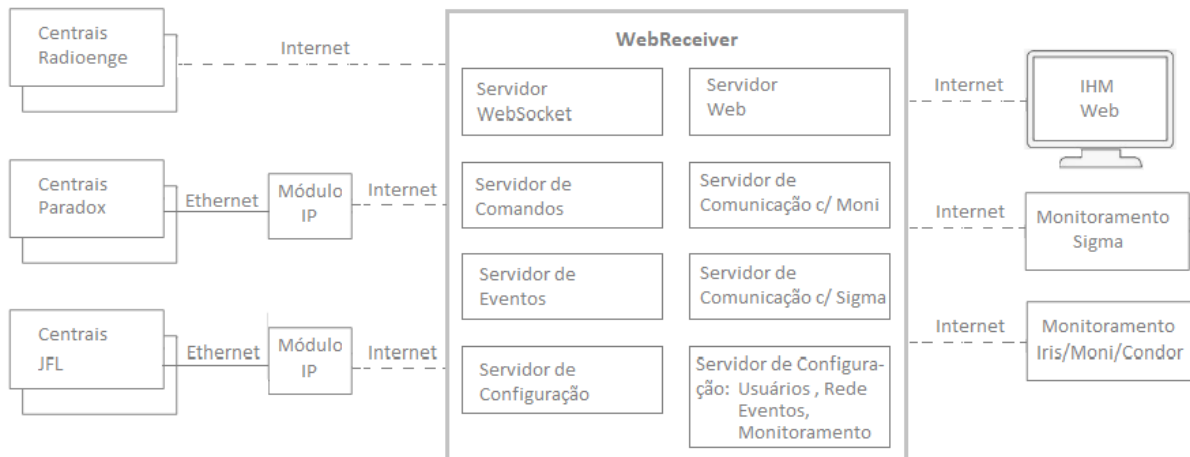


Figura 1: Diagrama de funcionamento do WebReceiver Radioenge

2 Instalação do Software WebReceiver

O software de instalação do WebReceiver está disponível para download no site da Radioenge. O nome do software acompanha sua versão, exemplo: Setup WebReceiver_V103, SetupWebReceiver_V106 etc.

2.1 Requisitos para instalação

Sua instalação pode ser feita no sistema operacional Windows nas seguintes versões:

- Windows Server – 2008 até o atual.
- Windows 7 até o atual.

O software utiliza o **.Net Framework 4.6.1** em diante. No momento da instalação, caso a versão do framework necessária não exista, será apresentada uma opção para que seja instalada.

2.2 Instalação do WebReceiver

Para instalar o software “Radioenge WebReceiver”, siga os seguintes passos:

- 1) Execute o software de instalação do WebReceiver;

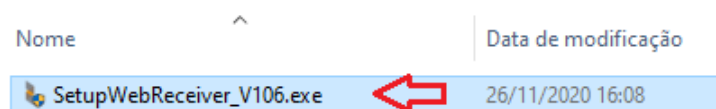


Figura 2: Executar o assistente de instalação

- 2) Selecione a pasta de instalação (é recomendado deixar esta opção como aparece). Em seguida, clique em **Instalar**;

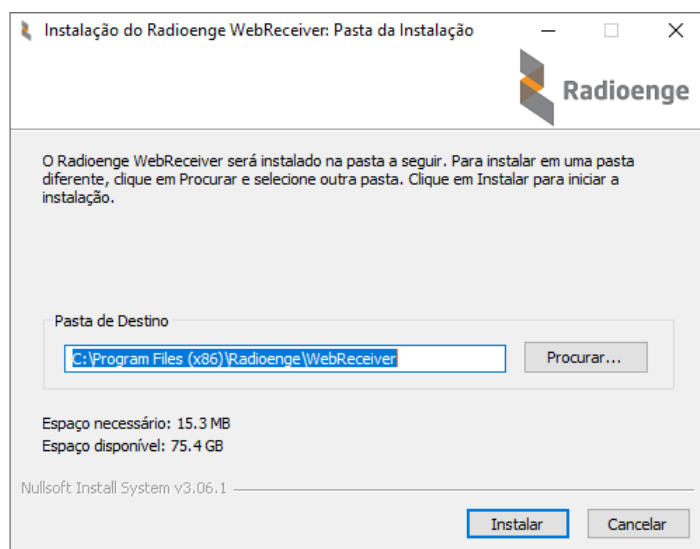


Figura 3: Selecionando a pasta de instalação dos arquivos

- 3) Caso já tenha o WebReceiver instalado, clique em “OK” para **remover** a versão anterior e instalar a nova;

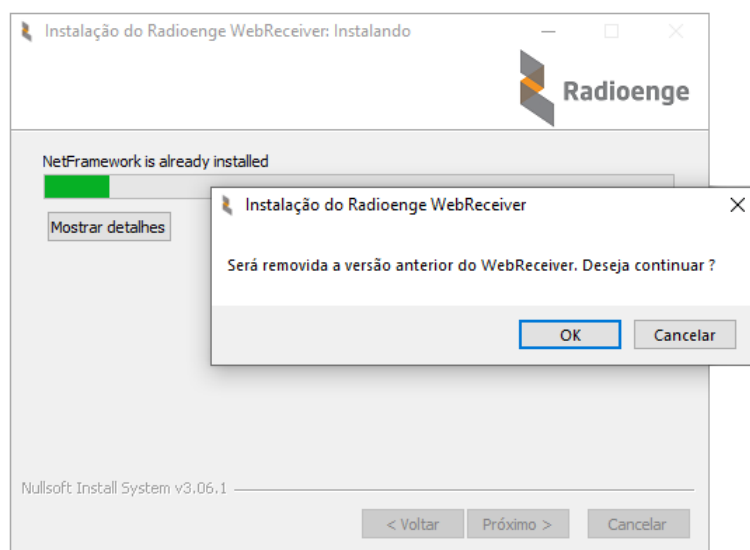


Figura 4: Remover a versão anterior do WebReceiver

4) **Aguarde** a instalação do WebReceiver;

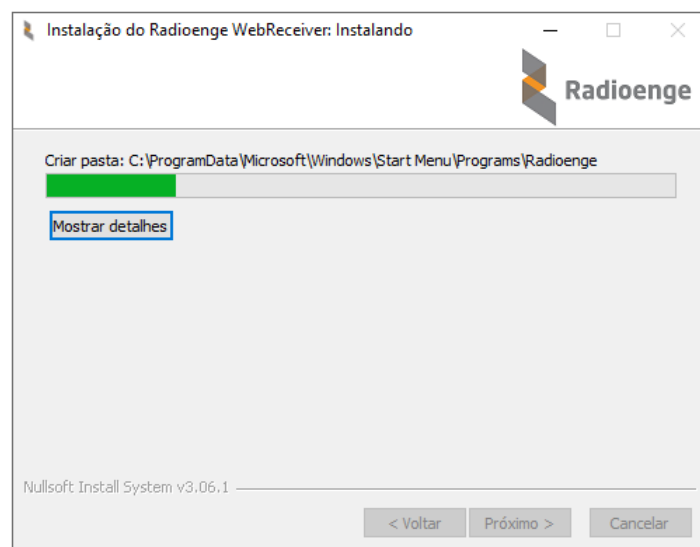


Figura 5: Instalando o WebReceiver

5) Clique em **Concluir** para finalizar a instalação.

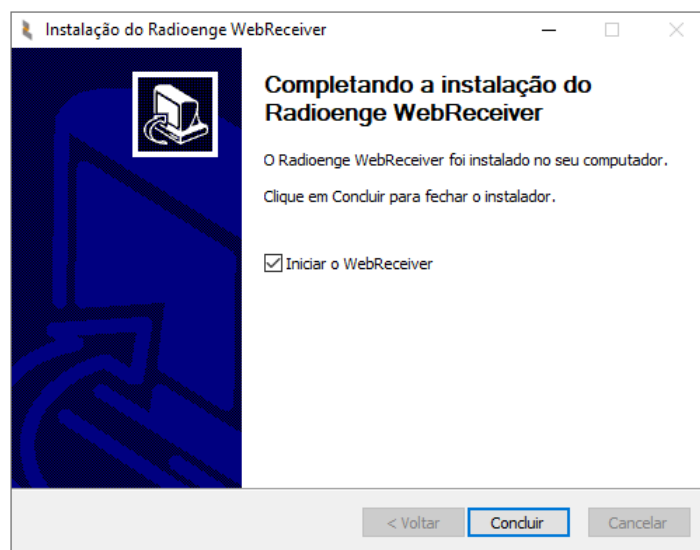


Figura 6: Concluir a instalação

3 Inicialização do Software WebReceiver

Após a instalação do WebReceiver, siga os seguintes passos para sua inicialização:

- 1) O ícone referente a inicialização do software WebReceiver, será apresentado na área de trabalho de sua máquina. Clique (duas vezes) sobre ele para que seja executado;



Figura 7: Ícone de inicialização do WebReceiver

- 2) Para verificar se o software **WebReceiver** está em execução, basta verificar no canto inferior direito de seu computador, em **Mostrar ícones ocultos**, onde deverá aparecer o ícone conforme figura abaixo:

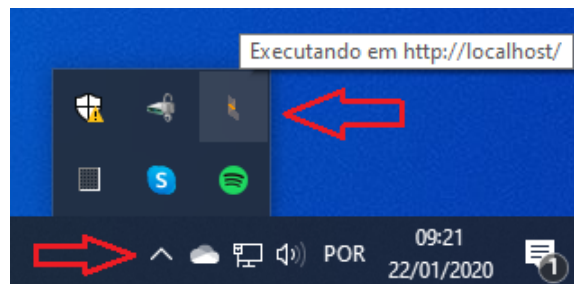


Figura 8: Software em execução

- 3) Para abrir a página web da IHM, no mesmo computador em que o WebReceiver está instalado, vá em **Mostrar ícones ocultos**, clique com o botão direito do mouse sobre o ícone **WebReceiver** e em seguida, escolha a opção **Configurações** para que a página seja aberta;

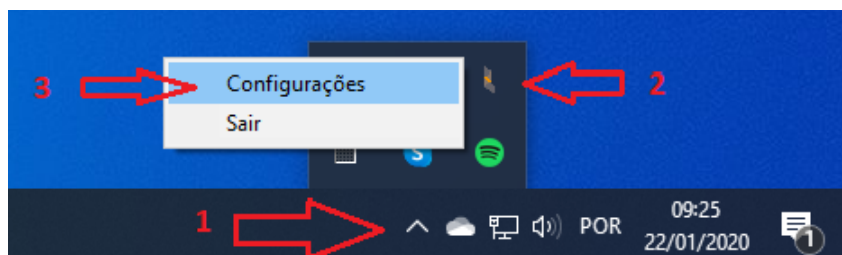


Figura 9: Abrir a página web

- 4) Outra opção seria abrir um navegador (Chrome, Mozilla Firefox etc.) e entrar com a URL e porta.
Exemplo: <http://localhost/login.html>, <http://localhost:8080/login.html>;
- 5) A tela de login será apresentada conforme a figura abaixo:

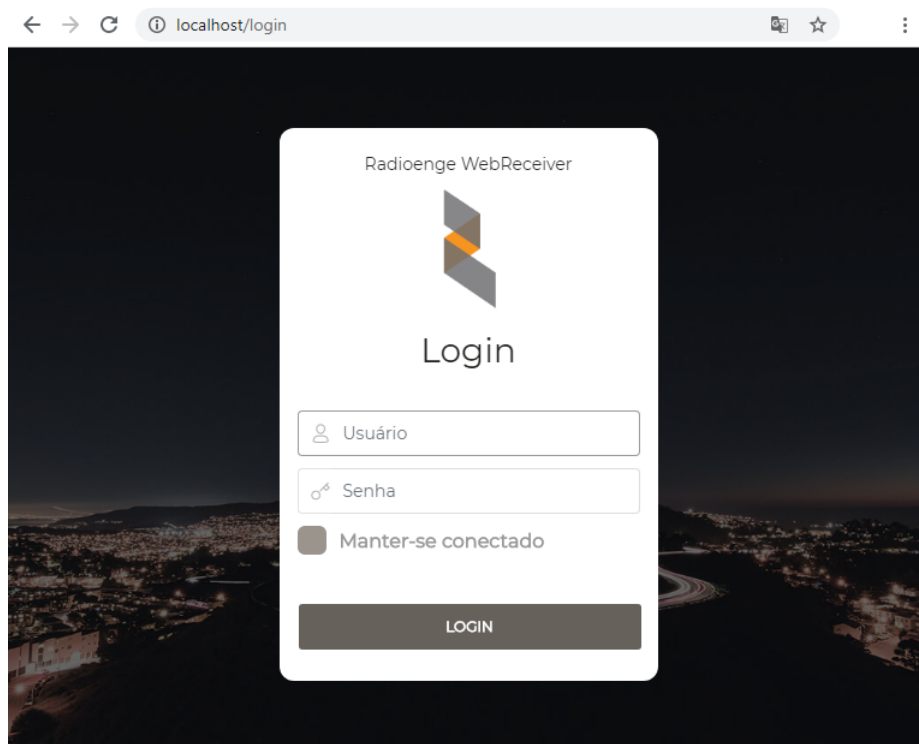


Figura 10: Login na página web

3.1 Falha ao inicializar WebReceiver – Porta HTTP já utilizada

Se a **porta HTTP** estiver sendo utilizada pelo WebReceiver (já inicializado) ou outro software qualquer, será apresentada a mensagem abaixo e a nova inicialização será interrompida.

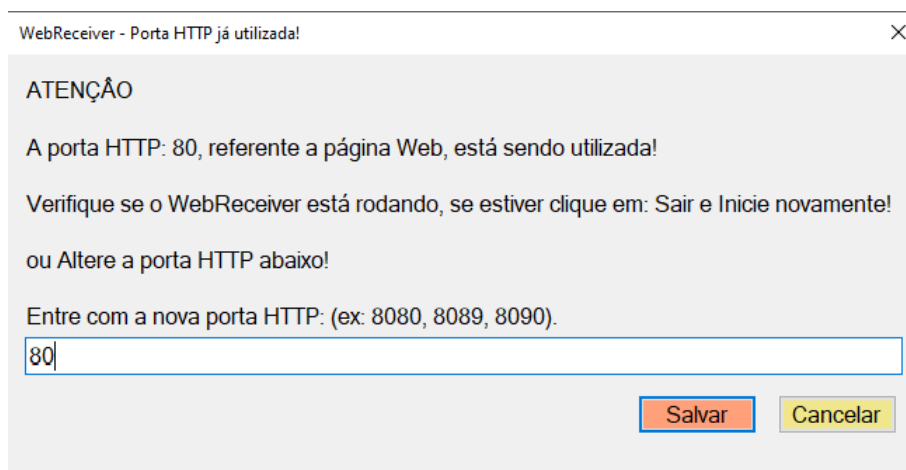


Figura 11: Redefinição da porta HTTP

Para corrigir o problema de porta HTTP já utilizada, verifique as seguintes condições:

► Verificar se o WebReceiver está executando (versão antiga)

Para verificar se o WebReceiver está em operação (rodando) e encerrar o sistema, utilize uma das maneiras abaixo:

A) Encerrar o WebReceiver pelo ícone

Quando o WebReceiver estiver em operação, o ícone da Radioenge estará disponível no canto inferior direito de sua tela, em ícones ocultos. Para encerrar, execute os passos abaixo:

- 1) Clique em ícones ocultos, localizado na parte inferior direita de sua tela;
- 2) Com o botão direito do mouse, clique sobre o ícone da Radioenge (referente ao WebReceiver);
- 3) Clique na opção **Sair** (isto irá encerrar o sistema).

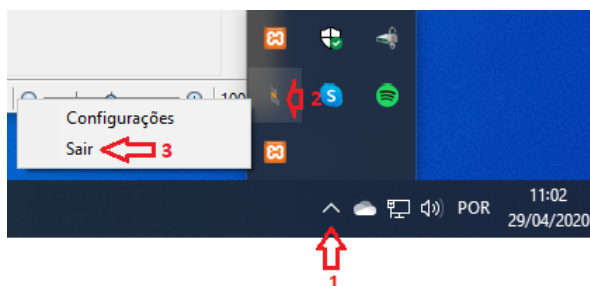


Figura 12: Encerrando o software através do ícone

B) Encerrar o WebReceiver pelo Gerenciador de Tarefas

Abra o **Gerenciador de Tarefas** do windows (clique com o botão direito do mouse sobre a barra inferior e escolha: Gerenciador de Tarefas).

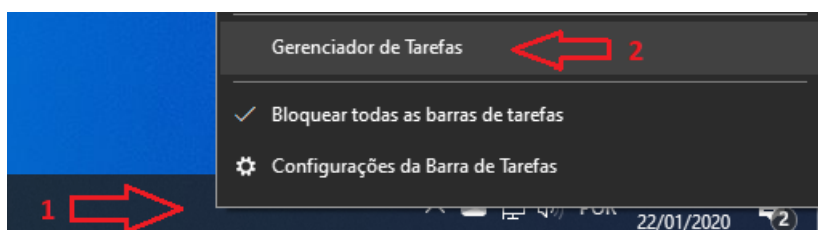


Figura 13: Encerrando o software pelo gerenciador de tarefas

Em **Processos**, verifique se o **WebReceiver** está em uso. Se estiver, clique sobre ele com o botão direito do mouse e escolha a opção **Finalizar tarefa**. Esta operação interrompe a execução de uma versão que esteja executando, possibilitando assim que a nova versão execute sobre a porta HTTP configurada anteriormente.

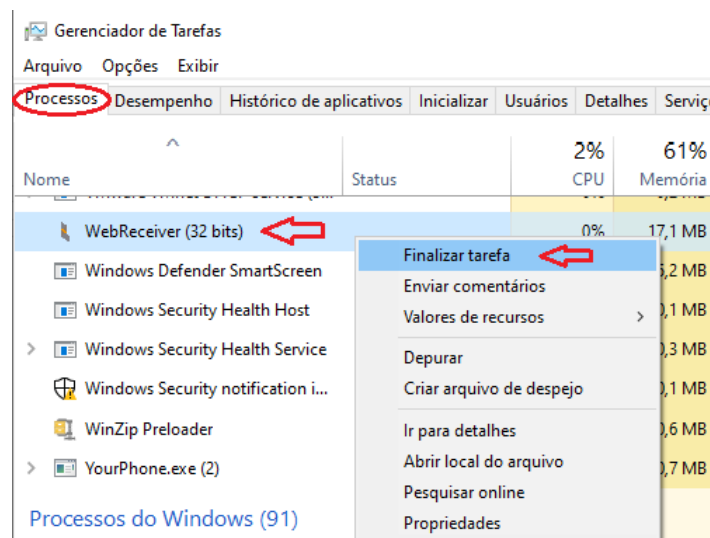


Figura 14: Processos - finalizar tarefa

Agora basta clicar (2 vezes) sobre o ícone de atalho de inicialização do WebReceiver para que seja executado.



Figura 15: Ícone de inicialização do WebReceiver

► **O WebReceiver não está rodando e a porta HTTP está sendo utilizada por outro software**

Caso a porta HTTP já esteja sendo utilizada por outro software, será necessário alterar a porta HTTP do WebReceiver para que ele funcione normalmente. Para isto siga os seguintes passos:

- 1) Altere a porta HTTP por outra que esteja livre;
- 2) Salve a alteração da porta.

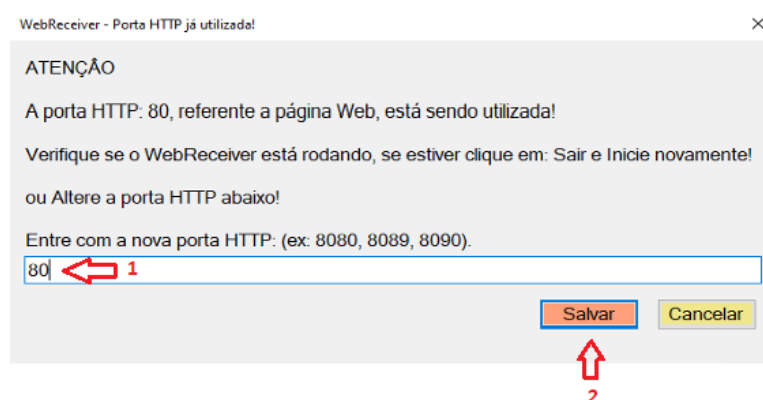


Figura 16: Redefinição da porta HTTP

OBS.: Ao clicar sobre o botão “Salvar”, a nova porta HTTP será gravada nas configurações e o WebReceiver irá reiniciar, retornando com a porta alterada.

4 Login WebReceiver

Abra o browser (Chrome, Mozilla Firefox etc.) e digite a url:porta referente ao ip:porta onde o software está instalado.

Exemplos: <http://localhost>, <http://localhost:8080>, <http://192.168.1.50>, <http://192.168.1.50:8080>

Entre com o **usuário** e **senha** cadastrados. Caso não existam usuários cadastrados, entre com o usuário **admin** e senha **1234**.

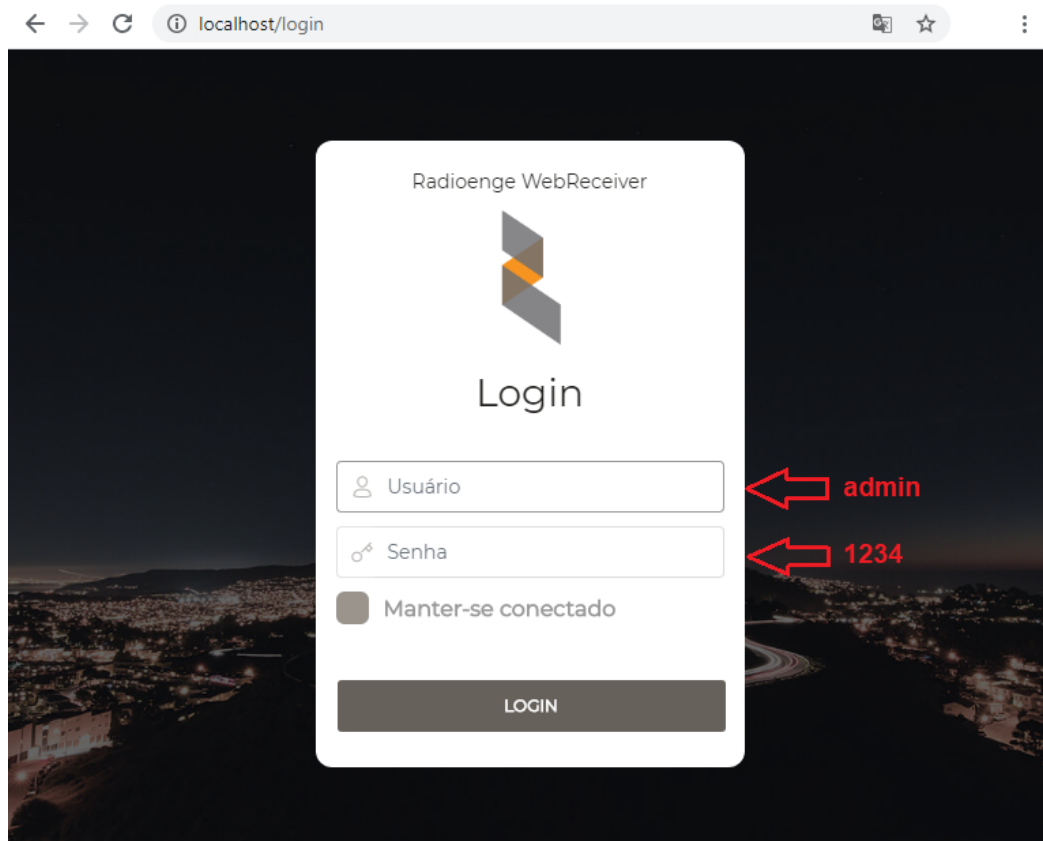


Figura 17: Login na página Web


Se o login do usuário e senha forem válidos, será apresentada a tela de “Status do Software”:



Figura 18: WebReceiver - Página web

Na tela acima, temos a IHM do WebReceiver, sendo disponibilizadas, conforme as permissões do usuário logado, as seguintes opções:

- Status do software
- Eventos
- Centrais de alarme

Além disso, o ícone  localizado no canto superior direito da página, permite acessar as seguintes opções:

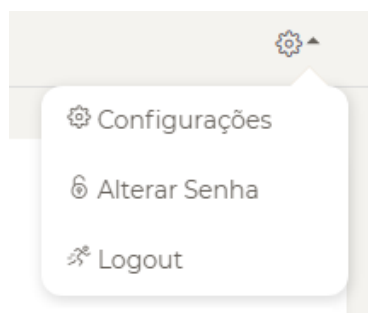


Figura 19: Menu de opções

- Configurações
- Alterar senha
- Logout

5 Status do Software

Nesta página estão apresentadas as informações gerais e de maior relevância, resumindo o estado geral do sistema, conforme mostra a Figura 20.



Figura 20: Página de status do software

Parâmetros gerais

- **SW de Monitoramento:** indica se o WebReceiver está conectado com o software de monitoramento. Quando estiver desconectado, esse campo será marcado com um “-”.
- **Centrais Cadastradas:** centrais que já se cadastraram no WebReceiver (Online e Offline).
- **Centrais Online:** centrais conectadas com o WebReceiver.
- **Centrais Offline:** centrais cadastradas que não estão conectadas com o WebReceiver.

Status da Comunicação

- **IP do Software de Comunicação:** endereço IP do monitoramento.
- **Conectado em:** data e hora na qual o WebReceiver conectou-se ao software de monitoramento (dd/mm/aaaa hh:mm:ss).
- **Eventos Pendentes:** eventos que não foram enviados para o software de monitoramento (Sigma, Moni).
- **Transmissões sem ACK:** número de tentativas de envio de evento ou keepalive sem confirmação de que o software de monitoramento tenha recebido.

Eventos e Keep Alive

- **Evento Enviado em:** último evento que o WebReceiver recebeu de uma central (dd/mm/aaaa hh:mm:ss).

- **Evento Confirmado em:** último evento que foi confirmado pelo software de monitoramento (dd/mm/aaaa hh:mm:ss).
- **Keep Alive Enviado em:** último keepalive enviado e confirmado pelo monitoramento (dd/mm/aaaa hh:mm:ss).
- **Keep Alive Recebido em:** último keepalive recebido e confirmado pelo monitoramento (dd/mm/aaaa hh:mm:ss).

6 Eventos

Nesta página são apresentados todos os eventos recebidos das centrais de alarmes. Os eventos são apresentados em ordem decrescente de data (eventos mais recentes até os eventos mais antigos). O campo **Entregue** indica se o evento foi enviado e confirmado pelo software de monitoramento.

CENTRAL	APELIDO	CONTA	EVENTO	PARTIÇÃO	ZONA	HORÁRIO	ENTREGUE
4		03D9	R361	1	0	18/11/2020 10:11:02	✓
4		03D9	E602	1	0	18/11/2020 10:11:01	✓
4		03D9	E602	1	0	18/11/2020 10:11:01	✓
4		03D9	E602	1	0	18/11/2020 10:11:01	✓
4		03D9	E602	1	0	18/11/2020 10:11:00	✓
4		03D9	E602	1	0	18/11/2020 10:11:00	✓
4		03D9	E602	1	0	18/11/2020 10:11:00	✓
4		03D9	E602	1	0	18/11/2020 10:10:59	✓
4		03D9	E602	1	0	18/11/2020 10:10:59	✓
4		03D9	E602	1	0	18/11/2020 10:10:59	✓

Mostrando De 1 Até 10 De 100 Elementos

« 1 2 3 4 5 »

Figura 21: Página de eventos

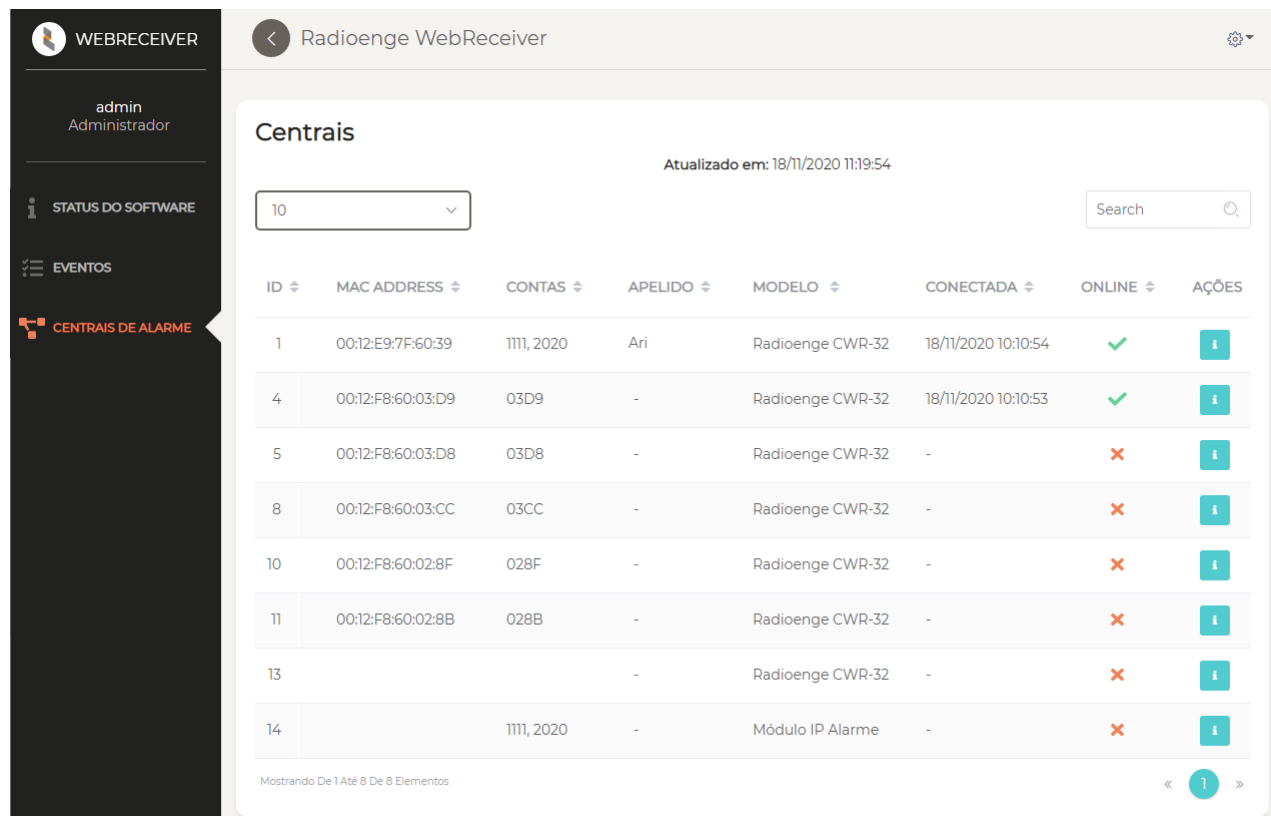
Descrição dos campos

- **Central:** indica o ID da central.
- **Apelido:** apresenta a descrição, opcional, dada ao cliente (apelido configurado para a central).
- **Conta:** identificação do número da conta configurada na central.
- **Evento:** código e descrição do evento.
- **Partição:** identificação da partição referente ao evento.
- **Zona:** identificação da zona referente ao evento.
- **Horário:** data e hora de ocorrência do evento (dd/mm/aaaa hh:mm:ss).
- **Entregue:** indica se o evento foi recebido pelo monitoramento:
 - ✓ - sim
 - ✗ - não.

7 Centrais de alarme

Nesta página são apresentadas todas as centrais cadastradas (Offline e Online) e suas informações mais significativas como: contas, cliente, modelo, conexão etc.


Ao selecionar uma central **Online**, o usuário terá acesso a opções específicas a ela como: estados e comandos.




ID	MAC ADDRESS	CONTAS	APELIDO	MODELO	CONECTADA	ONLINE	AÇÕES
1	00:12:E9:7F:60:39	1111, 2020	Ari	Radioenge CWR-32	18/11/2020 10:10:54	✓	
4	00:12:F8:60:03:D9	03D9	-	Radioenge CWR-32	18/11/2020 10:10:53	✓	
5	00:12:F8:60:03:D8	03D8	-	Radioenge CWR-32	-	✗	
8	00:12:F8:60:03:CC	03CC	-	Radioenge CWR-32	-	✗	
10	00:12:F8:60:02:8F	028F	-	Radioenge CWR-32	-	✗	
11	00:12:F8:60:02:8B	028B	-	Radioenge CWR-32	-	✗	
13			-	Radioenge CWR-32	-	✗	
14		1111, 2020	-	Módulo IP Alarme	-	✗	

Figura 22: Página de centrais de alarme

Descrição dos campos:

- **ID:** identificador da central.
- **MAC Address:** endereço físico da central.
- **Contas:** contas referentes a central.
- **Apelido:** identificador do cliente configurado na central.
- **Modelo:** indica o modelo da central: Módulo-Paradox, Módulo-JFL, Radioenge CWR-32, Radioenge CWR-128.
- **Conectada:** indica desde quando a central está conectada ao WebReceiver (dd/mm/aaaa hh:mm:ss).
- **Online:** identifica o status da conexão da central com o WebReceiver:
 - ✓ - conectada
 - ✗ - desconectada.
- **Ações:** ao clicar sobre o ícone  é possível acessar as informações gerais da central e a aba de comandos.

7.1 Informações gerais


Para acessar as informações gerais da central, clique sobre o ícone  exibido na página de centrais de alarme e selecione a aba **Informações Gerais**.

Esta aba permite visualizar as informações da central e as informações de conexão com o monitoramento.




Figura 23: Informações gerais da central

Informações da Central

- **ID:** identificador da central.
- **MAC Address:** endereço físico da central.
- **Apelido:** identificador do cliente configurado na central. Para modificar o apelido, clique em .
- **Modelo:** indica o modelo da central: Módulo-Paradox, Módulo-JFL, Radioenge CWR-32 e Radioenge CWR-128.
- **Contas:** contas referentes a central.
- **Versão do Hardware:** indica a versão de hardware da central ou Módulo IP.

Informações de Conexão

- **Status:** indica se a central está conectada ou desconectada do WebReceiver.
- **Último KeepAlive:** indica o último keepalive enviado e confirmado pela central (dd/mm/aaaa hh:mm:ss).
- **Último Evento:** indica o último evento recebido da central (dd/mm/aaaa hh:mm:ss).
- **Tipo de conexão:** indica se a central está conectada via WebReceiver 1 (IP 1), WebReceiver 2 (IP 2) ou GPRS.

Para deletar a central, clique em .

7.2 Comandos

Para acessar a aba de comandos da central, clique sobre o ícone ⓘ exibido na página de centrais de alarme e selecione a aba **Comandos**.

Esta aba permite consultar os estados e enviar comandos para partições, zonas e PGMs. Para isso, clique em **Atualizar Status** e insira a **senha** da central. Para centrais Radioenge, é a senha do usuário cadastrado na central. Para centrais Paradox e JFL, corresponde à senha remota cadastrada.

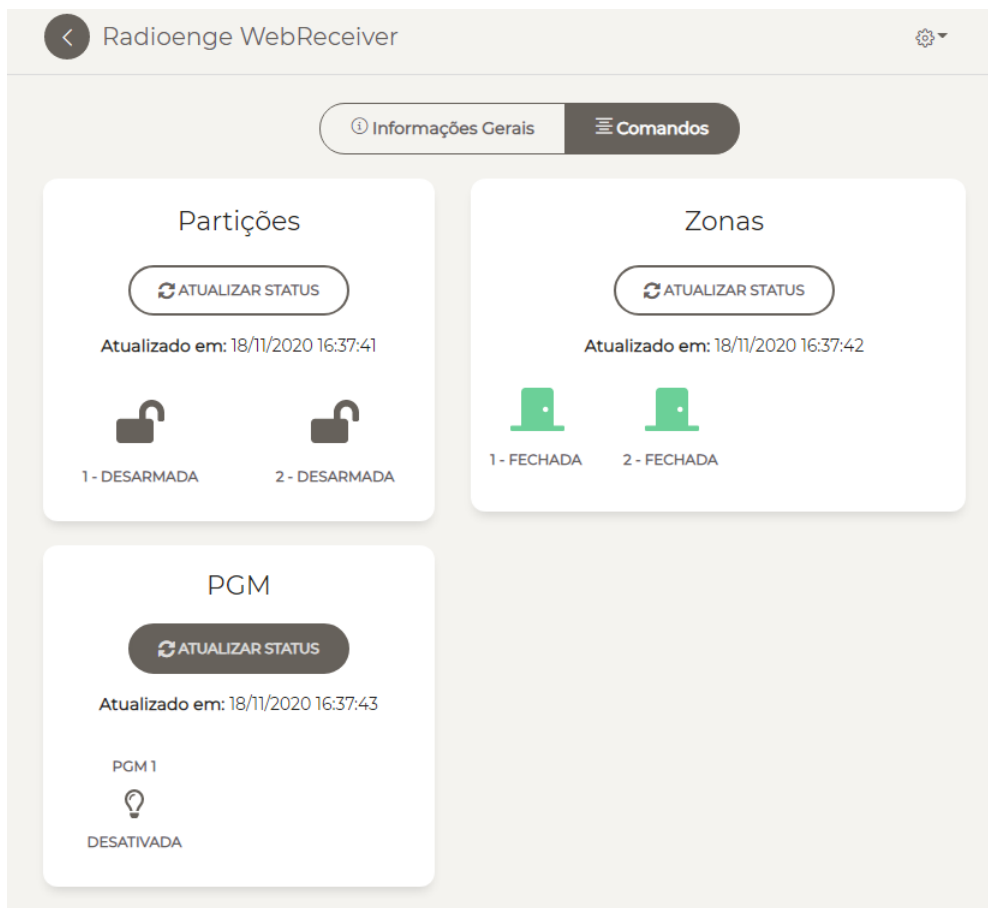


Figura 24: Informações gerais da central

Após carregar os estados, clique sobre os símbolos das partições, zonas e PGM para selecionar o comando desejado.

7.2.1 Armar/desarmar partições

Para enviar comandos para a partição, clique sobre o ícone da partição desejada e selecione um comando, conforme mostram as Figuras 25 e 26.

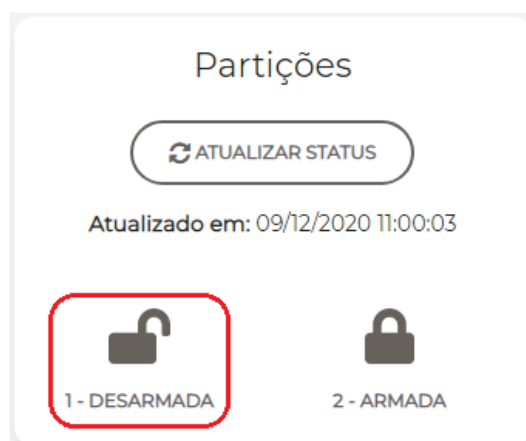


Figura 25: Ícones das partições



Figura 26: Comandos para a partição selecionada

7.2.2 Anular zona

Para anular a zona, clique sobre o ícone da zona desejada e ative a opção **Anular Zona**, conforme mostram as Figuras 27 e 28



Figura 27: ícones das zonas

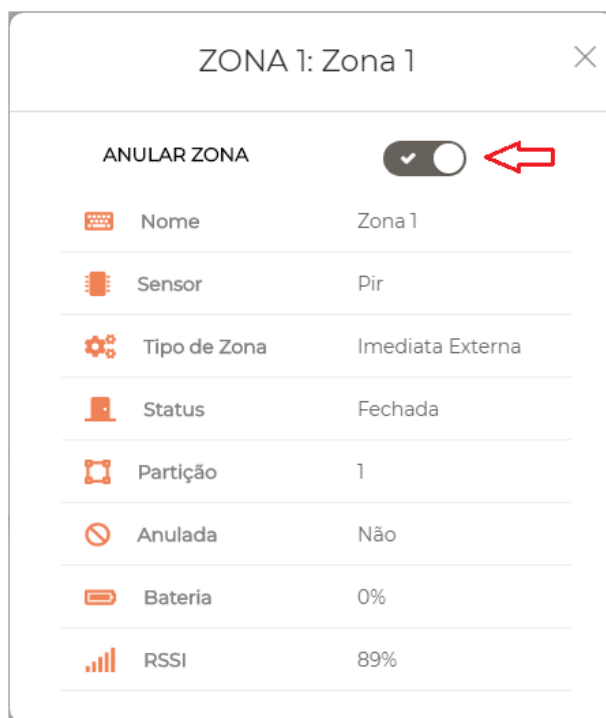


Figura 28: Informações da zona


7.2.3 Ativar/desativar PGM

Ao clicar sobre o símbolo da PGM, o comando de ativar/desativar será enviado.



Figura 29: PGMs e seus respectivos estados

7.3 Configurações

Para acessar o menu de configurações da central, clique sobre o ícone  exibido na página de centrais de alarme e selecione a aba **Configurações**.

Esta aba permite configurar a central de alarme. Para isso, é necessário inserir a senha do usuário que irá configurar a central. A senha inserida deve ser a de um usuário **Mestre** ou **Instalador**.

As senhas padrão e permissões de configuração são apresentadas abaixo:

- **Usuário Mestre** (Senha Padrão 1234): permite incluir, excluir e alterar usuários e controle remoto. Permite gerar o token necessário para incluir a central no aplicativo Radioenge App.
- **Usuário Instalador** (Senha Padrão 0000): permite configurar zonas, partições, PGM, parâmetros do sistema, monitoramento, teclados, sirenes, configuração de rede e Cloud na central de alarme.

Opções de configuração para usuários com permissão: **Mestre**

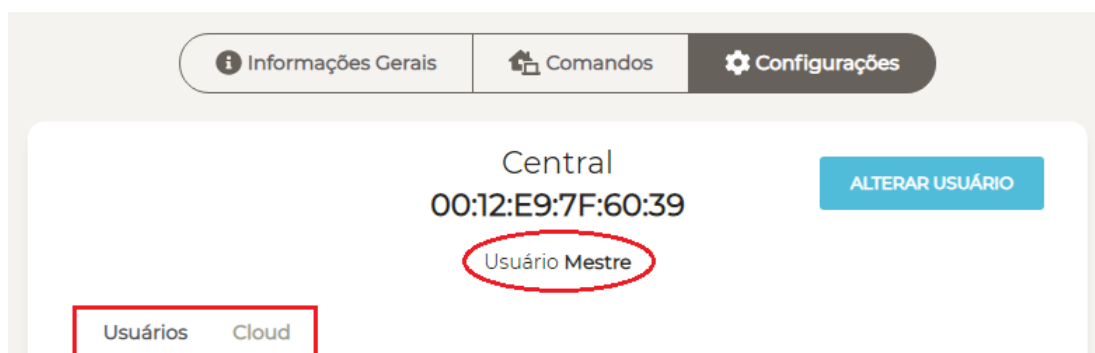


Figura 30: Permissões de configuração para o usuário mestre

Opções de configuração para usuários com permissão: **Instalador**

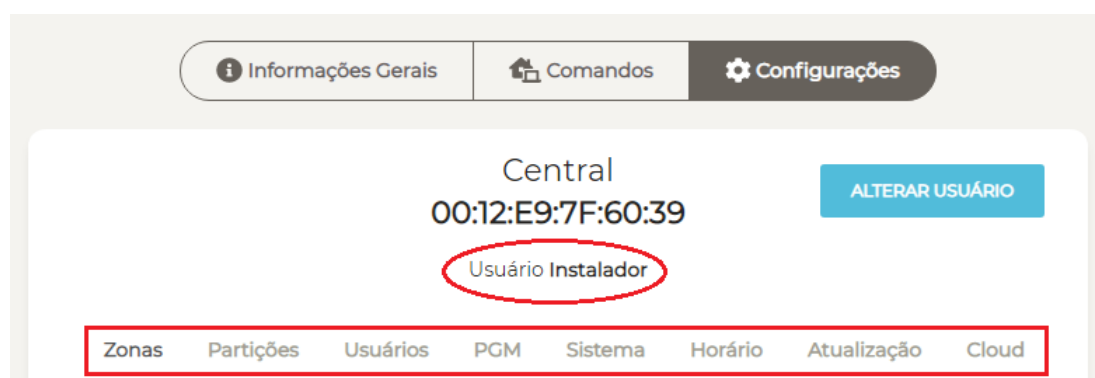


Figura 31: Permissões de configuração para o usuário instalador

Para acessar as configurações da central utilizando outra senha de usuário, clique em **Alterar Usuário**.

7.3.1 Zonas

Selecione a zona que deseja configurar e clique em **Atualizar**.

Zona 1

ATUALIZAR

RESETAR ZONA

CONFIGURAÇÕES DE ZONAS

Tipo de Zona: Imediata Externa

Partição: 1

Nome: Zona 1

Anulável: Sim

Intelizone: Não

Forçável: Sim

Auto-Anulável: Não

Modo de Alarme: Audível

INFORMAÇÕES DO SENSOR

Tipo de Sensor: Sensor PIR

Sensor ID: 2546

RSSI Rx: -69 dBm

RSSI Tx: -78 dBm

Bateria: 97%

CADASTRAR SENSOR

DESCADASTRAR SENSOR

SALVAR

CANCELAR

Figura 32: Configurações de zonas

Para alterar a configuração da zona para os valores padrão, clique em **Resetar zona**.

Parâmetros da zona

- **Tipo de zona:** condição de funcionamento da zona.
- **Partição:** partição a qual a zona pertence.
- **Nome:** campo para personalizar o nome da zona.
- **Anulável:** permite realizar o anulamento da zona. Selecione “Sim” para permitir ou “Não” para não permitir que a zona seja anulada pelo usuário.
- **Intelizone:** a intelizone (ou zona inteligente) dispara com a detecção de pelo menos 2 eventos dentro do tempo de intelizone configurado na aba partições. Selecione “Sim” para ativar ou “Não” para desativar a intelizone.
- **Forçável:** força a zona a armar mesmo se estiver aberta. Na prática, ao armar a zona forçável, ocorre o mesmo efeito de anular e em seguida armar. Selecione “Sim” para ativar ou “Não” para desativar a zona forçável.
- **Auto-anulável:** a zona é anulada automaticamente após um determinado número de disparos dentro do mesmo arme. Este número de disparos é configurado na aba partições. Selecione “Sim” para permitir ou “Não” para que a zona não seja auto-anulável.

- **Modo de Alarme:** define o modo como a sirene irá se comportar quando a central receber comandos ou disparar.
 - Audível: a sirene irá emitir sons audíveis.
 - Silencioso: a sirene entrará no modo silencioso, não emitindo sons.
 - Apenas Reportar: equivalente ao modo silencioso.
- **Anular Tamper:** o evento de tamper ocorre quando o gabinete de um sensor PIR é violado (aberto). Se o tamper estiver anulado a central não irá enviar eventos de tamper. Nesse caso, é possível armar a central mesmo se o tamper estiver violado. Selecione “Sim” para anular ou “Não” para que o tamper não seja anulado.

Caso a zona tenha um sensor MAG cadastrado, os parâmetros da Figura 33 serão exibidos.



SENSOR MAG	
Anular Reedswitch	Não
Anular Borne Externo	Não
Contato Borne Externo	NA

Figura 33: Parâmetros do sensor MAG

- **Anular Reedswitch:** caso seja utilizado somente o borne externo, deve-se anular o reedswitch. Selecione “Sim” para anular ou “Não” para manter seu funcionamento normal.
- **Anular Borne Externo:** caso seja utilizado somente o reedswitch, deve-se anular o borne externo. Selecione “Sim” para anular ou “Não” para manter seu funcionamento normal.
- **Contato Borne Externo:** tipo de contato no borne externo. Selecione “NF” para definir como normalmente fechado ou “NA” para normalmente aberto.

7.3.2 Zonas - Cadastro de sensores

Para cada zona, deve-se cadastrar um sensor com um ID diferente, ou seja, não é possível cadastrar o mesmo sensor em mais de uma zona.

Clique em **Cadastrar** e realize o procedimento de cadastro do sensor em até 30 segundos. Caso o tempo esgotar, é necessário clicar novamente em “Cadastrar”.

Procedimento de cadastro para os sensores MAG-915 e PIR-915

- **MAG-915:** Pressione PAR até o LED acender. Após isso, solte o botão.
- **PIR-915:** Pressione PROG até o LED acender. Após isso, solte o botão.

Caso o cadastro seja bem sucedido, o LED do dispositivo irá piscar rapidamente antes de apagar.

Após realizar o cadastro, os campos de **Informações do sensor**, mostrados na Figura 32, serão preenchidos:

- **Tipo Sensor:** tipo do sensor cadastrado.
- **Sensor ID:** código ID do sensor cadastrado.
- **RSSI Rx:** intensidade do sinal recebido pelo sensor.
- **RSSI Tx:** intensidade do sinal transmitido pelo sensor.

Para descadastrar, clique em **Descadastrar sensor**.

Após realizar as configurações, clique em **Salvar**.

7.3.3 Partições

Selecione a partição que deseja configurar e clique em **Atualizar**.

Zonas Partições Usuários PGM Sistema Horário Atualização Cloud

Partição 1 ATUALIZAR RESETAR PARTIÇÃO

CONFIGURAÇÕES DE PARTIÇÕES

Habilitada Sim

Conta 0001

Nome Particao 1

Tempo de Entrada 1 300

Tempo de Entrada 2 600

Tempo de Saída 300

Tempo de Intelizone 60

Disparos para Auto-Anular a Zona 5

AUTO ARME POR HORÁRIO

Horário do Auto Arme 00:00

Modo de Auto-Arme Desativado

☒ dom ☒ seg ☒ ter ☒ qua ☒ qui ☒ sex ☒ sab

AUTO ARME POR INATIVIDADE

Início do Auto-Arme 00:00

Término do Auto-Arme 23:59

Período de Inatividade para o Auto-Arme 30

Modo de Auto-Arme Desativado

☒ dom ☒ seg ☒ ter ☒ qua ☒ qui ☒ sex ☒ sab

✓ SALVAR ✗ CANCELAR

Figura 34: Configuração de partições

Para alterar a configuração da partição para os valores padrão, clique em **Resetar partição**.

Parâmetros da partição

- **Habilitada:** selecione “Sim” para ativar ou “Não” para desativar a partição.
- **Conta:** número da conta do monitoramento da partição. Esta informação é cadastrada pelo técnico instalador da empresa de monitoramento, caso seja utilizada.
- **Nome:** campo para personalizar o nome da partição.
- **Número de disparos para auto-anular zona:** número de vezes que a zona deverá disparar dentro do mesmo arme para que ela seja anulada automaticamente. Válido para zonas configuradas como auto-anuláveis.

7.3.4 Partições - Temporização

- **Tempo de Entrada 1:** tempo limite para desarmar a central ao entrar no ambiente. Válido para zonas configuradas como temporizada 1 e para seguidoras, caso o usuário entre primeiro pela zona temporizada.
- **Tempo de Entrada 2:** tempo limite para desarmar a central ao entrar no ambiente. Válido para zonas configuradas como temporizada 2 e para seguidoras, caso o usuário entre primeiro pela zona temporizada.
- **Tempo de Saída:** tempo limite para deixar o ambiente após armar a central.
- **Tempo de Intelizona:** intervalo de tempo limite, desde a primeira detecção do evento, dentro do qual uma nova detecção irá gerar o disparo. Ou seja, uma intelizona só gera um evento de disparo caso neste intervalo de tempo haja mais de uma violação.

7.3.5 Partições - Auto arme

- **Auto arme por horário:** nesta opção, a central irá armar automaticamente em um horário específico.
- **Auto arme por inatividade:** nesta opção a central irá armar automaticamente caso nenhum evento seja detectado dentro de um determinado período de tempo (período de inatividade) entre os horários de início e término do auto arme.
- **Dom/Seg/Ter/Qua/Qui/Sex/Sab:** dias da semana em que o auto arme irá funcionar. Ambos os modos de auto arme possuem esta opção.

Após realizar as configurações, clique em **Salvar**.

7.3.6 Usuários

A configuração de usuários da central depende das permissões referentes ao tipo do usuário, identificado pela senha, podendo ser:

- **Mestre:** pode cadastrar controle remoto, adicionar e alterar todos os usuários, exceto o instalador. Não pode configurar partições, zonas e sensores.
- **Instalador:** não pode configurar os outros usuários. É permitido a ele alterar apenas o próprio nome e senha. O instalador é o técnico usuário que pode configurar partições, zonas e cadastrar sensores.

Por padrão de fábrica, os usuários 1 e 2 já vem definidos como Mestre e Instalador, respectivamente.

Opções de configuração para usuários com permissão: **Instalador**

Zonas Partições **Usuários** PGM Sistema Horário Atualização Cloud

Usuário 2

CONFIGURAÇÕES DE USUÁRIO

Privêlégio

Senha

Nome

Figura 35: Permissão de configuração para usuário tipo instalador

Opções de configuração para usuários com permissão: **Mestre**

Usuários Cloud

Usuário 1

CONFIGURAÇÕES DE USUÁRIO

Privêlégio

Senha

Nome

CONTROLE REMOTO

Tipo de Controle Remoto

Controle Remoto ID

PARTIÇÕES

☒ P-1 ☒ P-2

PERMISSÕES

☒ Arme ☒ Desarme

☒ Pânico ☒ Anular

☒ PGM 1 ☐ PGM 2

☐ PGM 3 ☐ PGM 4

Figura 36: Permissão de configuração para usuário tipo mestre

Selecione o usuário que deseja configurar e clique em **Atualizar**.

Para alterar a configuração do usuário para os valores padrão, clique em **Resetar usuário**.

Parâmetros do usuário

- **Partições:** partições às quais o usuário terá acesso.
- **Permissão:** funções da central que o usuário poderá utilizar.
- **Privilégio:** tipo de privilégio do usuário no sistema.
- **Senha:** senha do usuário.
- **Nome:** campo para personalizar o nome do usuário.

7.3.7 Usuários - Cadastro de controle remoto



Cada usuário pode ter um controle remoto associado. Com ele é possível armar/desarmar a central, utilizar como pânico, coação, entre outras funções.



Figura 37: Controle remoto cadastrado

Clique em **Cadastrar controle** e realize o procedimento de cadastro do controle em até 30 segundos. Caso o tempo esgotar, é necessário clicar novamente em “Cadastrar controle”.

Procedimento de cadastro dos controles

◦ **CR-915:** Pressione ao mesmo tempo os botões desarme e sleep ( e  respectivamente) do controle. Quando o LED acender, pressione qualquer botão para finalizar. Caso o cadastro seja bem sucedido, o LED do dispositivo irá piscar rapidamente antes de apagar.

◦ **433 MHz Code-learning:** Pressione qualquer botão do controle até que a mensagem de cadastro realizado com sucesso seja exibida na tela.

Após realizar o cadastro, os campos mostrados pela Figura 37 serão preenchidos:

- **Tipo de controle remoto:** 433 MHz ou Radioenge.
- **Controle remoto ID:** código ID do controle remoto cadastrado.

Para descadastrar o controle clique em “Descadastrar controle”.

7.3.8 Usuários - Configuração do controle remoto

Após cadastrar o controle remoto, é possível configurar as funções de cada botão e as partições nas quais irá funcionar. Estas configurações podem ser feitas somente pelo usuário Mestre.

Botão 4	Pânico	<input checked="" type="checkbox"/> P-1	<input checked="" type="checkbox"/> P-2
Botão 3	Arme Sleep	<input checked="" type="checkbox"/> P-1	<input checked="" type="checkbox"/> P-2
Botão 2	Desarme	<input checked="" type="checkbox"/> P-1	<input checked="" type="checkbox"/> P-2
Botão 1	Arme Total	<input checked="" type="checkbox"/> P-1	<input checked="" type="checkbox"/> P-2

Figura 38: Configuração do controle remoto

7.3.9 Usuários - Configuração do controle remoto - Função pânico através do controle remoto

A função de pânico através do botão do controle remoto poderá ser no modo silencioso ou audível. As notificações irão aparecer no aplicativo e na aba de eventos da página web da central.

Tabela 1: Função pânico através do controle remoto

Versão de firmware	Evento Alarme de Pânico
Até 0.3.11	<p>► Botão configurado com função de Pânico: Segurar o botão por cerca de 5 segundos. O clique curto no botão não terá efeito.</p> <p>► Demais botões: Segurar o botão por cerca de 5 segundos. O clique curto no botão irá realizar a função principal configurada.</p>
0.3.12 ou superior	<p>► Botão configurado com função de Pânico: Segurar o botão por cerca de 5 segundos. O clique curto no botão não terá efeito.</p> <p>► Demais botões: Não é possível realizar a função de pânico, apenas a função principal configurada.</p>

7.3.10 Usuários - Configuração do controle remoto - Função coação através do controle remoto

O modo coação realiza a função de arme ou desarme normalmente com um clique curto. Com um clique longo (segurando o botão cerca de 5 segundos) ele faz a mesma coisa, gerando também um evento de coação.

Configure o botão do controle remoto com uma das seguintes funções:

- Desarme com coação
- Arme/desarme com coação

7.3.11 Usuários - Dias e horário para permitir usuário

É permitido ao usuário Mestre configurar os dias e horário em que cada usuário poderá operar a central (exceto usuário Instalador).

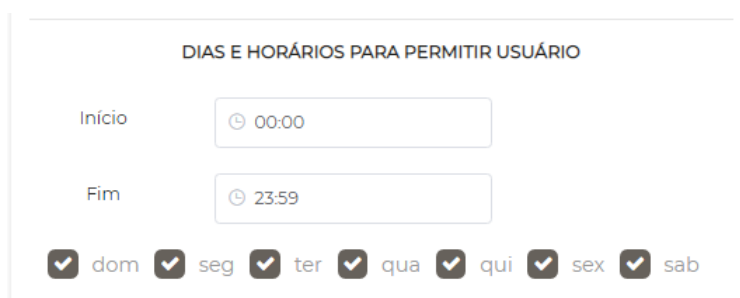


Figura 39: Configuração de dias e horário para permitir o usuário

Insira o horário de início e fim e selecione os dias da semana em que o usuário terá permissão para realizar as ações configuradas para ele nesta aba.

OBS.: Usuários do tipo mestre sempre têm permissão.

Após realizar as configurações, clique em **Salvar**.

7.3.12 PGM

A aba **PGM** permite configurar o acionamento da PGM. Selecione a PGM que deseja configurar e clique em **Atualizar**.

Figura 40: Configuração de PGM

Para alterar a configuração da PGM para os valores padrão, clique em **Resetar PGM**.

Parâmetros da PGM

- **Tipo de Contato:** selecione “NA” para definir o contato como normalmente aberto ou “NF” para definir como normalmente fechado.
- **Duração do Pulso:** intervalo de tempo em segundos no qual a PGM permanecerá acionada após seu disparo.
 - Zero: retenção.
 - Maior que zero: pulsado.
- **Modo de operação:**
 - Desativado: desativa a PGM.
 - Eventos/comandos: a PGM irá acionar na ocorrência de eventos (Evento 1 e Evento 2).
 - Seguir sirene: a PGM irá acionar toda vez que a sirene disparar.
 - Indicar armado/desarmado: a PGM irá acionar quando a central estiver armada (para contato tipo NA) ou desarmada (para contato tipo NF).

- **Vinculado a:**

- PGM Onboard: a PGM acionará um dispositivo conectado fisicamente à central.
- Sirenes sem fio: a PGM irá acionar uma sirene sem fio.

Caso o modo de operação “Eventos/Comandos” seja selecionado, os campos Evento 1 e Evento 2 devem ser configurados:

- **Código do Evento:** código do evento que ao ser gerado, deverá acionar a PGM. A saída PGM é vinculada a um evento da central.
- **Zona/Usuário:** zona ou usuário ao qual a PGM está associada.
- **Partição:** partição à qual a PGM está associada.
- **Ativar com:** condições de ativação da PGM
 - Evento: ocorrência de eventos.
 - Restauro: ocorrência de restauro.
 - Ambos: ocorrência de eventos e restauros.

Após realizar as configurações, clique em **Salvar**.

7.3.13 Sistema

A aba **Sistema** permite realizar as configurações gerais da central.

ZonasPartiçõesUsuáriosPGMSistemaHorárioAtualizaçãoCloud

ATUALIZAR

RESETAR CONFIGURAÇÕES

CONFIGURAÇÕES DE SISTEMA

Tempo de Alarme da Sirene

— 5 +

Tempo de Teste da Sirene

— 0 +

Intervalo de Keepalive quando Armado

— 15 +

Intervalo de Keepalive quando Desarmado

— 5 +

Intervalo entre eventos de teste periódico (E602)

— 60 +

Atraso para a geração de evento de falha de AC

— 1 +

Atraso para a geração de evento de falha de ETH

— 10 +

Canal de operação 915 MHz

— 2 +

CONFIGURAÇÕES DE SISTEMA

Alarme Sonoro com Tamper do Sensor

Não ▾

Alarme Sonoro com Falha de Supervisão de Zona

Não ▾

Tamanho da Senha

4 Dígitos ▾

BIPE DE ARME/DESARME NA SIRENE

☐ Teclado

☒ Controle

☐ App

CALIBRAR SIRENE

CALIBRAR TESTE DA SIRENE

SALVAR

CANCELAR

Figura 41: Configurações do sistema

Para retornar os parâmetros do sistema para a configuração padrão, clique em **Resetar configurações**.

7.3.14 Sistema - Intervalos de testes, keepalives e atraso de evento de falha

- **Intervalo de Teste da Sirene:** intervalo de tempo entre os testes periódicos da sirene.
- **Intervalo de Keepalive quando Armado:** intervalo de tempo entre transmissões de keepalives dos sensores quando a central estiver armada.
- **Intervalo de Keepalive quando Desarmado:** intervalo de tempo entre transmissões de keepalives dos sensores quando a central estiver desarmada.
- **Intervalo entre eventos de teste periódico (E602):** tempo para reportar os testes periódicos da central à empresa de monitoramento.
- **Atraso para geração de evento de falha AC:** intervalo de tempo contado desde a queda de energia para que seja reportado à empresa de monitoramento.
- **Atraso para geração de evento de falha de ETH:** intervalo de tempo contado desde a queda da conexão via ethernet para que seja reportado à empresa de monitoramento

7.3.15 Sistema - Configuração de avisos sonoros

- **Tempo de Alarme da Sirene:** tempo de duração do efeito sonoro da sirene caso não haja evento de restauro.
- **Alarme sonoro com Tamper do Sensor:** se o tamper do sensor for aberto, o alarme irá disparar caso a opção “Sim” esteja marcada. Se a opção “Não” for marcada, o alarme não irá disparar.
- **Alarme sonoro com Falha de Supervisão de Zona:** a falha de supervisão acontece quando a central fica 3,5 vezes o tempo de keepalive configurado sem receber informações do sensor. Nesse caso, quando o evento de falha for gerado o alarme irá disparar caso a opção “Sim” esteja marcada. Se a opção “Não” for marcada, o alarme não irá disparar.
- **Bipe de arme/desarme na sirene:** a central poderá emitir bipes ao ser armada/desarmada via teclado, controle ou app. Selecione uma ou mais opções.

7.3.16 Sistema - Canais de operação

- **Canal de operação 915 MHz:** número do canal de operação na faixa de 915 MHz.



Se o canal for alterado, todos os sensores e controles remotos deverão ser pareados novamente.

7.3.17 Sistema - Senha do usuário

- **Tamanho da Senha:** quantidade de dígitos que as senhas de usuário deverão conter.

7.3.18 Sistema - Calibração do teste da sirene

A calibração do teste da sirene serve para encontrar o valor de referência que será utilizado no teste periódico da sirene. Ela deve ser feita com a sirene instalada ou com o cabo de comprimento igual ao que será utilizado na instalação final.

Para realizar a calibração, clique em “Calibrar teste da sirene”. Após verificar a instalação da sirene, clique em “Sim” e aguarde 1 minuto até a finalização da calibração.



A calibração do teste da sirene é importante para que os testes periódicos da sirene sejam realizados corretamente. Durante o minuto de espera da calibração, ela não deve ser armada nem desarmada.

Após realizar as configurações, clique em “Salvar”.

7.3.19 Horário

Na aba **Horário** é possível fazer a escolha do servidor NTP e do fuso horário no qual a central estará sincronizada ou configurar o horário manualmente. É possível também ativar a opção de horário de verão.

Zonas Partições Usuários PGM Sistema **Horário** Atualização Cloud

ATUALIZAR RESETAR CONFIGURAÇÕES

CONFIGURAÇÕES DE HORÁRIO

Servidor NTP

✓ SALVAR NTP

FUSO HORÁRIO

Fuso Horário

☐ Habilitar Horário de Verão

✓ SALVAR FUSO HORÁRIO

HORÁRIO MANUAL

✓ SALVAR

Figura 42: Configuração de horário

Para retornar os parâmetros de horário para a configuração padrão, clique em **Resetar configurações**.

Parâmetros de horário

- **Servidor NTP:** URL do servidor utilizado pela central para sincronização de horário com a internet.
- **Fuso Horário:** fuso horário no qual a central será sincronizada através do servidor NTP.
- **Horário de Verão:** habilita ou desabilita o horário de verão.

Após realizar as configurações, clique em **Salvar**.

7.3.20 Atualização do firmware

Na aba de **Atualização** é possível atualizar a versão de firmware da central.



Figura 43: Atualização de firmware

Clique em **Selecione o arquivo de Firmware** e selecione ou arraste o arquivo desejado até este campo. Em seguida clique em **Atualizar firmware**.

7.3.21 Cloud

A aba **Cloud** permite gerar o token para cadastrar a central no aplicativo **Radioenge App** e realizar a vinculação da central com a **RadioengeCloud**.



Figura 44: Configuração do serviço em cloud

7.3.22 Cloud - Cadastro no aplicativo via token

- **Cadastro no aplicativo via Token:** clique em **Gerar Token** para obter o código token necessário para cadastrar a central no aplicativo **Radioenge App**.

7.3.23 Cloud - Vincular empresa de monitoramento na RadioengeCloud

Para vincular uma central a empresa de monitoramento, é necessário entrar em contato com a Radioenge para obter o email e senha de vinculação. Esta senha de vinculação é gerada apenas na primeira instalação, e normalmente é feita na instalação do WebReceiver junto a empresa de monitoramento.

- **Email:** email da empresa de monitoramento.
- **Senha:** senha de vinculação da empresa de monitoramento.

Em seguida, clique em **Vincular central com a cloud**.

8 Configurações

Para acessar o menu de configurações do WebReceiver, clique sobre o ícone  e selecione a opção **Configurações**.



Figura 45: Opção de configuração

Esta opção permite configurar parâmetros e funcionalidades do sistema como:

- **Rede:** porta HTTP e HTTPS da página web;
- **Central:** porta de comunicação com centrais, tempo para gerar evento de falha de conexão e senha de comunicação com centrais;
- **Monitoramento:** software utilizado no monitoramento, versão de keepalive e porta de conexão com o monitoramento;
- **Eventos:** permite remover eventos.

8.1 Rede

A página de **Rede** permite que o usuário **Administrador** configure a porta HTTP ou HTTPS utilizadas na página web da IHM. Esta porta deverá estar disponível e livre para uso exclusivo do WebReceiver.

Para alterar a porta HTTP:



- 1) Clique no ícone  e selecione a opção **Configurações**;
- 2) Selecione a aba **Rede**;
- 3) Altere a porta HTTP para uma porta disponível e livre. O valor escolhido deve estar compreendido entre 1 e 65535;
- 4) Salve a configuração.



Figura 46: Configuração porta HTTP

Para habilitar e alterar a porta HTTPS:

- 1) Clique no ícone  e selecione a opção **Configurações**;
- 2) Selecione a aba **Rede**;
- 3) Selecione **Habilitar HTTPS**;
- 4) Altere a porta HTTPS para uma porta disponível e livre (padrão: 443);
- 5) Selecione a opção **Redirecionar HTTPS** (opcional);
- 6) Salve a configuração.

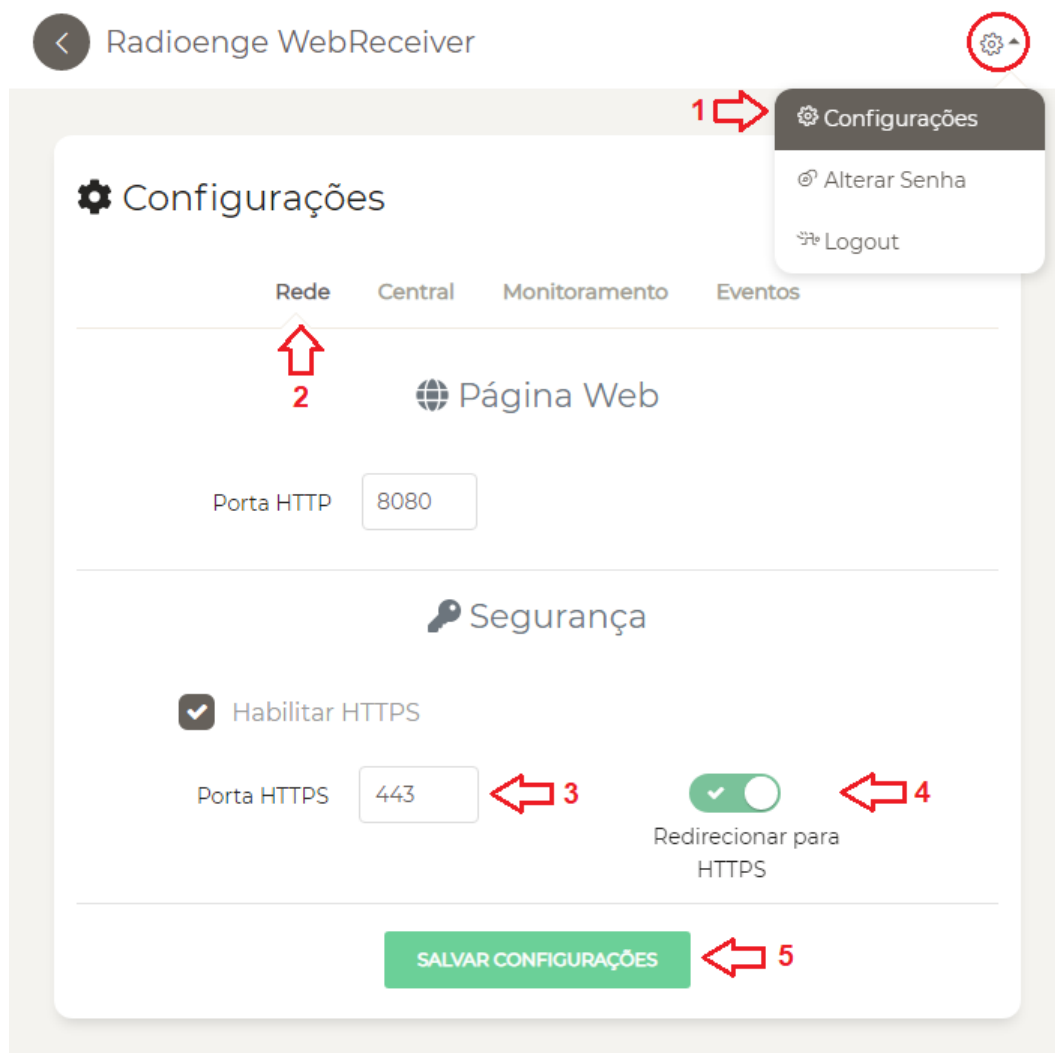


Figura 47: Configuração porta HTTP

OBS.: Após **salvar** as informações, o sistema **WebReceiver** irá **reinicializar**, carregando a nova configuração. Será necessário efetuar o login novamente para continuar na IHM do sistema.

Arquivo de configuração alterado: app.json (C:\Radioenge\WebReceiver)

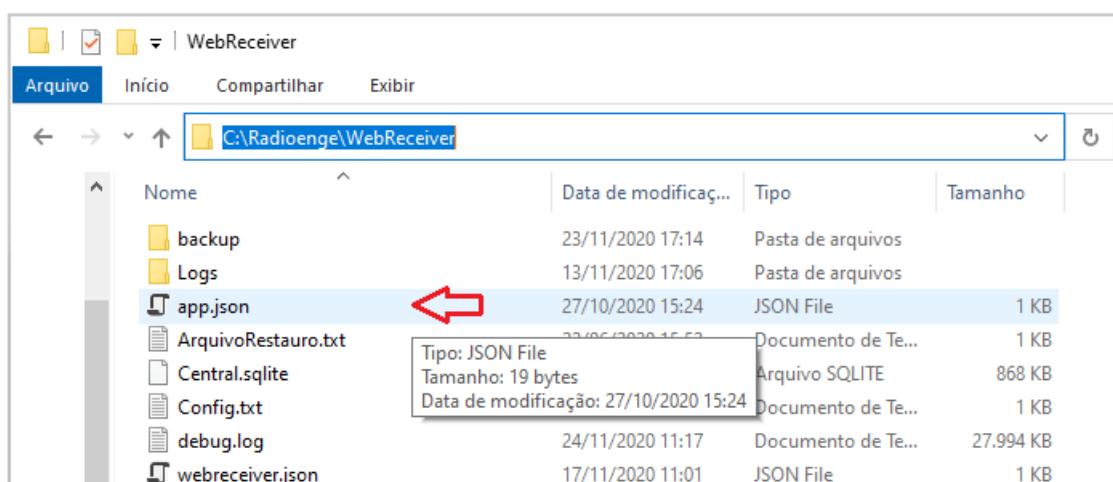


Figura 48: Arquivo de configuração alterado

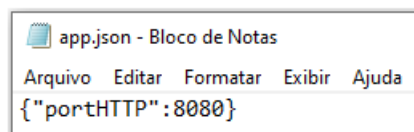
Conteúdo do arquivo app.json alterado:

Figura 49: Arquivo de configuração alterado com o novo valor da porta HTTP

Para acessar a página web será necessário alterar a URL do sistema, corrigindo a porta alterada. Para isso, clique em **Mostrar ícones ocultos** (localizado no canto inferior direito da tela), clique com o botão direito e escolha a opção **Configurações**. Dessa maneira, a página web será aberta já com o novo valor de porta.

Pode-se também alterar a URL diretamente no navegador, inserindo a nova porta no formato ip:porta. Exemplos: <http://localhost>, <http://localhost:8080>, <http://192.168.1.50>, <http://192.168.1.50:8080>

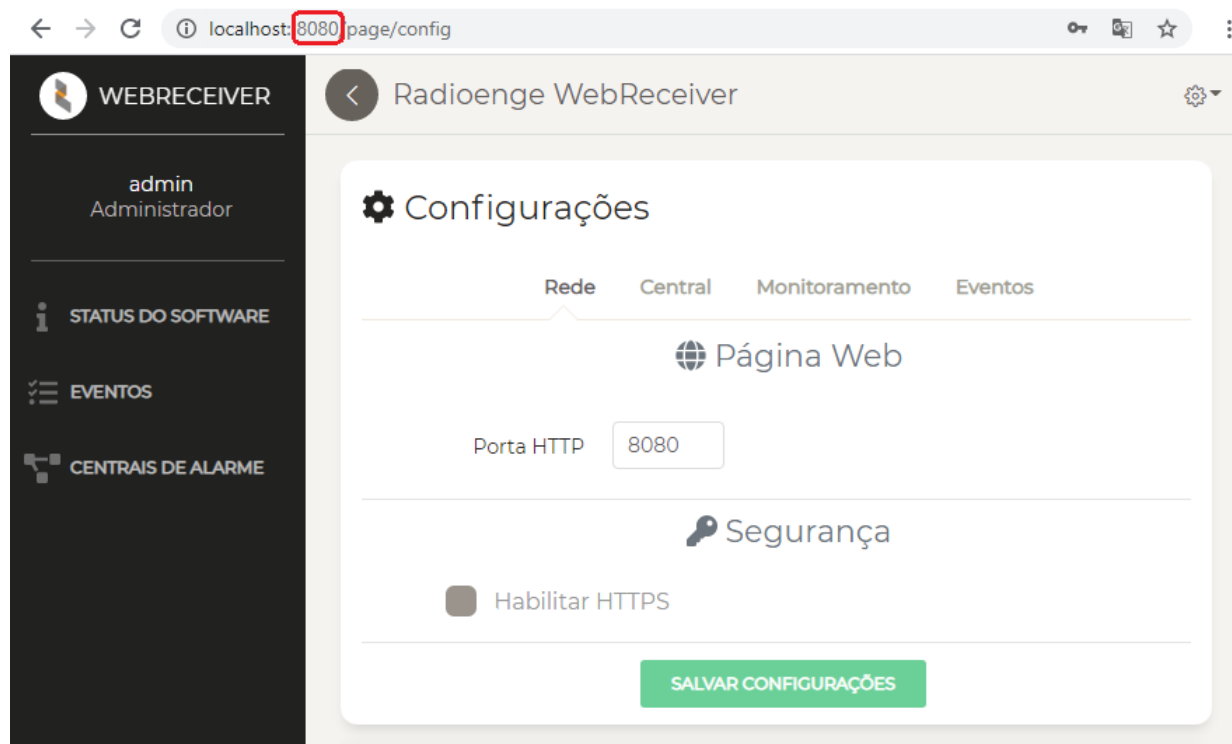


Figura 50: Endereço (URL) com a porta HTTP configurada

8.2 Central

A aba **Central** permite que o usuário **Administrador** configure a porta de comunicação utilizada pelo websocket, a senha de comunicação com as centrais. Além disso, é possível configurar o tempo de atraso para gerar o evento de falha de conexão com o WebReceiver.

A senha configurada será gravada no sistema de forma criptografada, assim, não é possível recuperá-la utilizando a informação salva, garantindo segurança no processo.

Radioenge WebReceiver

Configurações

Rede Central Monitoramento Eventos

Comunicação com a Central

Porta TCP 8085

Falha de desconexão - 2 + Minutos

SALVAR CONFIGURAÇÕES

Senha de Comunicação Senha

SALVAR SENHA DE COMUNICAÇÃO

Figura 51: Aba de centrais


8.2.1 Comunicação

Para que uma central, ligada na rede, estabeleça a comunicação com o sistema WebReceiver, é necessário que sejam configurados ambos os lados (centrais e WebReceiver) com informações consistentes.

Neste exemplo, iremos mostrar a configuração dos dois lados para um maior entendimento.

No **WebReceiver**, configuramos a **porta de comunicação** como: **8085** (porta utilizada na comunicação websocket entre centrais e WebReceiver).

É possível também configurar o tempo em minutos para gerar o evento de **Falha de desconexão** caso a conexão com a central seja perdida.

 Comunicação com a Central

Porta TCP  **8085**

Falha de desconexão Minutos

SALVAR CONFIGURAÇÕES

Figura 52: Configuração de porta TCP e tempo para gerar falha de desconexão

Após realizar as alterações, clique em “Salvar Configurações”.

Em seguida, configuramos a **senha de comunicação** como: **S955431**.

Senha de Comunicação  **S955431**

SALVAR SENHA DE COMUNICAÇÃO

Figura 53: Configuração de senha de comunicação com centrais

Após inserir a senha, clique em “Salvar Senha de Comunicação”.

Os campos: Porta: **8085** e Senha: **S955431**, deverão fazer parte da configuração das centrais. Utilizando a página web de configuração do Módulo IP, ou um dos softwares de configuração da Central CWR-32 ou CWR-128, iremos configurar o lado da central.

8.2.2 Comunicação - Módulo IP

Para as centrais **Paradox** e **JFL** estabelecerem a conexão e comunicação com o sistema WebReceiver, é necessário a utilização do Módulo IP, que irá realizar a ponte de transferência de eventos, estados e comandos.

No exemplo abaixo, será configurado o Módulo IP (IP: 192.168.1.141) ligado a uma central Paradox.

Para configurar o Módulo IP, conectado a rede e central, siga os seguintes passos:

- 1) Abra seu **navegador web** (Chrome, Firefox etc.), entre com o **IP** referente ao módulo e clique em **Configuração**.

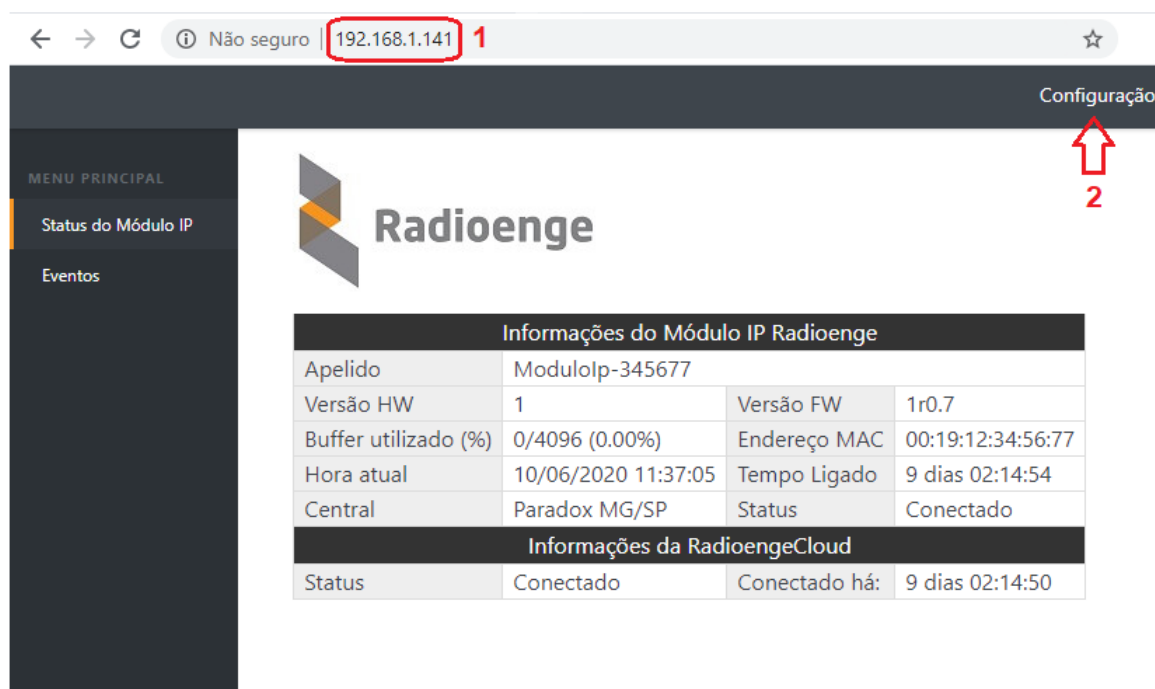


Figura 54: Página web do Módulo IP Radioenge

2) A tela de login será apresentada. Insira o **Nome do usuário** e **Senha** e clique em **Fazer login**.

Fazer login

http://192.168.1.141

Sua conexão a este site não é particular

Nome de usuário: admin

Senha:

Fazer login Cancelar

Figura 55: Login na página de configurações do módulo IP

3) Acesse a aba **Monitoramento** e siga os seguintes passos:

- Em **Monitoramento 1** ou **Monitoramento 2** selecione: **Habilitar monitoramento**;
- Insira o endereço **IP/URL**, **Porta de comunicação** e **Senha de comunicação**;
- Clique em **Salvar Configurações de Monitoramento**.

Página Inicial

CONFIGURAÇÃO

- Rede
- Central
- Monitoramento**
- Cloud
- Sistema

Logout

Radioenge

Comunicação com o monitoramento

Modo de operação

☒ Duplo
☐ Backup

Monitoramento 1

☒ Habilitar monitoramento

IP / URL do monitoramento

192.168.1.3

Porta de Comunicação

8085

Senha de Comunicação

S955431

Monitoramento 2

☐ Habilitar monitoramento

Salvar Configurações de Monitoramento

Figura 56: Aba de configuração da comunicação com o monitoramento

Descrição dos campos

- **IP/URL de monitoramento:** IP ou URL referente a máquina onde o WebReceiver está instalado e executando.
- **Porta de comunicação:** porta de comunicação configurada no WebReceiver. (No exemplo, porta: 8085)
- **Senha de comunicação:** senha de comunicação configurada no WebReceiver. (No exemplo, senha: S955431)

8.2.3 Configurador CWR-32 e CWR-128

Para as centrais **Radioenge** modelos **CWR-32** e **CWR-128** estabelecerem conexão e comunicação com o sistema WebReceiver, é necessário configurá-las utilizando um dos softwares disponíveis.

Para configurar uma central Radioenge utilizando o software **Configurador de Centrais**, siga os seguintes passos:

- 1) Abra o software configurador **ConfigCentral_Vxxx.exe**;
- 2) Clique no botão **Buscar Centrais** para que as centrais ligadas à rede sejam listadas;
- 3) Entre com a senha de usuário **Instalador** e clique sobre a linha correspondente à central que deseja configurar; (Exemplo: IP 192.168.1.118)

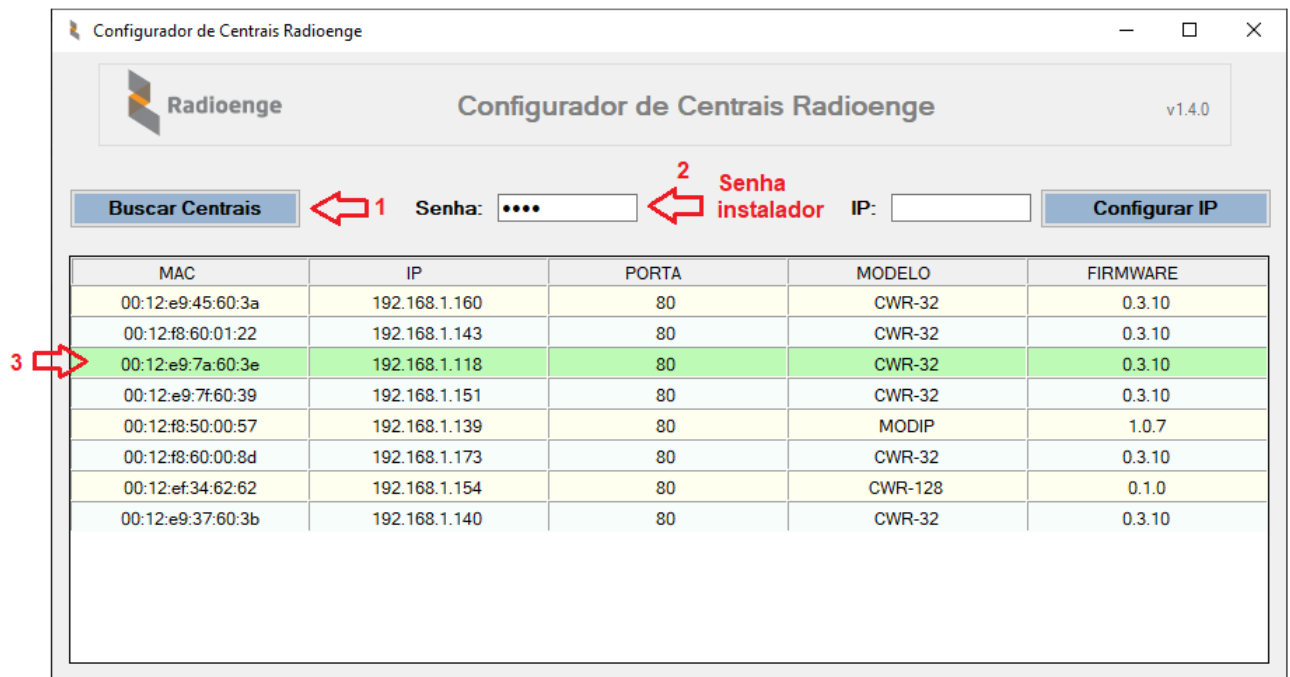


Figura 57: Realizar login no software configurador de centrais

- 4) Selecione a aba **Monitoramento** para habilitar e fazer a configuração do WebReceiver (pode ser configurado até 2 softwares WebReceiver);

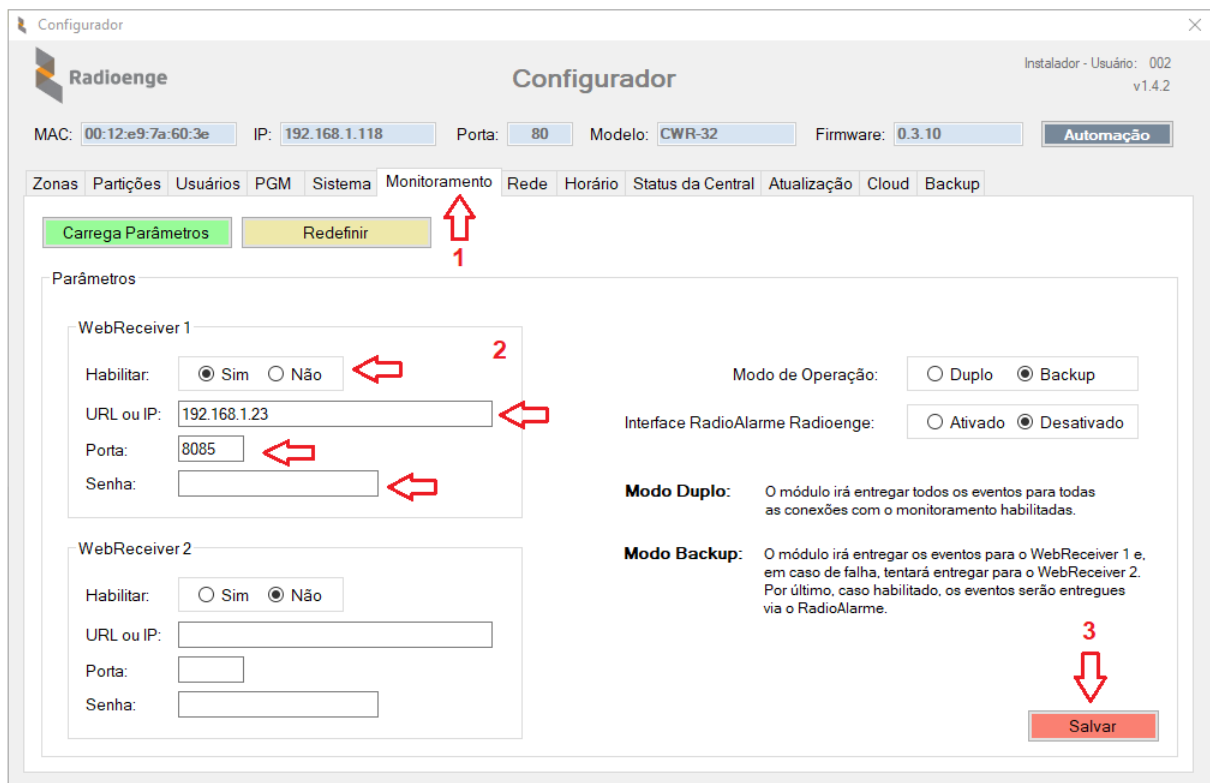


Figura 58: Aba de configuração da comunicação com o monitoramento

Descrição dos campos (WebReceiver 1 ou WebReceiver 2):

- **Habilitar:** habilita a central para se conectar com o WebReceiver.
- **URL ou IP:** URL ou IP do computador onde o WebReceiver está Instalado e executando.
- **Porta:** porta de comunicação configurada no WebReceiver. (No exemplo, porta: 8085)
- **Senha:** senha de comunicação configurada no WebReceiver. (No exemplo, senha: S955431)

5) Clique em **Salvar** para que a central recarregue a nova configuração e estabeleça a conexão com o WebReceiver.

8.3 Monitoramento

A aba **Monitoramento** permite configurar o sistema WebReceiver para enviar eventos para o software de monitoramento: **Sigma** ou **Moni/Condor/Iris**.

O WebReceiver controla o envio de eventos recebidos das centrais e sinaliza a confirmação de que o software de monitoramento recebeu cada evento. Quando não houver eventos na fila de envio, o WebReceiver envia constantemente a mensagem de KeepAlive para o monitoramento, o qual, confirma seu recebimento. Este processo de envio e confirmação garante a funcionalidade de comunicação entre WebReceiver e Monitoramento.

8.3.1 SIGMA

Neste exemplo iremos configurar o WebReceiver para se conectar com o software de monitoramento **SIGMA**.

Para efetuar a configuração do WebReceiver – Monitoramento, siga os seguintes passos:

- 1) No menu principal do WebReceiver, selecione a página de **Configurações**;

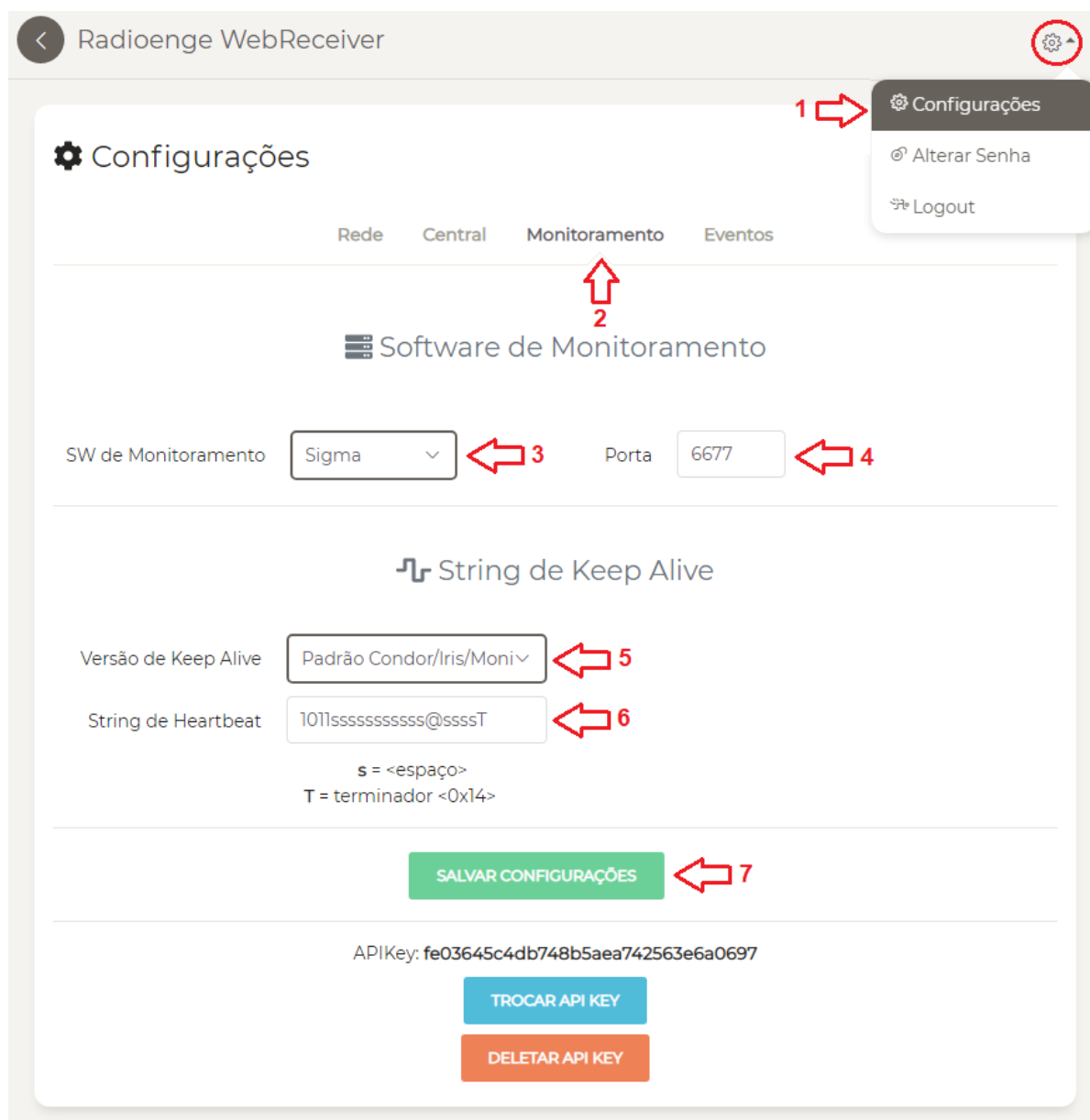


Figura 59: Configuração da conexão com o monitoramento - SIGMA

- 2) Selecione, no submenu, a aba **Monitoramento**;
- 3) Selecione o software utilizado: **Sigma**;

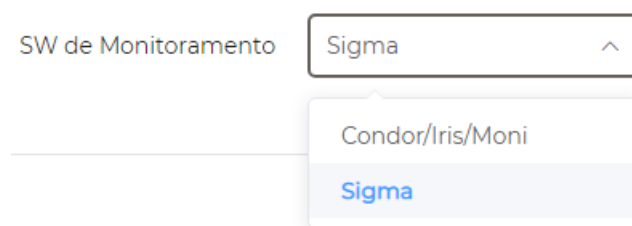


Figura 60: Seleção do software SIGMA

- 4) Defina a **porta** que será utilizada;

Porta 6677

Figura 61: Porta de conexão com o Sigma

- 5) Selecione a versão de **KeepAlive** que será utilizado;

Versão de Keep Alive

Padrão Sigma

Padrão Condor/Iris/Moni

Padrão Sigma

Personalizado

Figura 62: Configuração da versão de keepalive

- 6) Defina a string de **HeartBeat** (string de envio na mensagem de KeepAlive). Para Sigma e Iris/Moni/Condor esta string já vem preenchida, porém é possível alterá-la;

String de Heartbeat

101000ssssssssss@ssssT

s = <espaço>

T = terminador <0x14>

Figura 63: Definição da string de heartbeat

- 7) **Salve** a configuração referente ao monitoramento. O WebReceiver irá reinicializar carregando os novos parâmetros.

SALVAR CONFIGURAÇÕES

Figura 64: Salvar as configurações

8.3.2 SIGMA - Configuração com WebReceiver

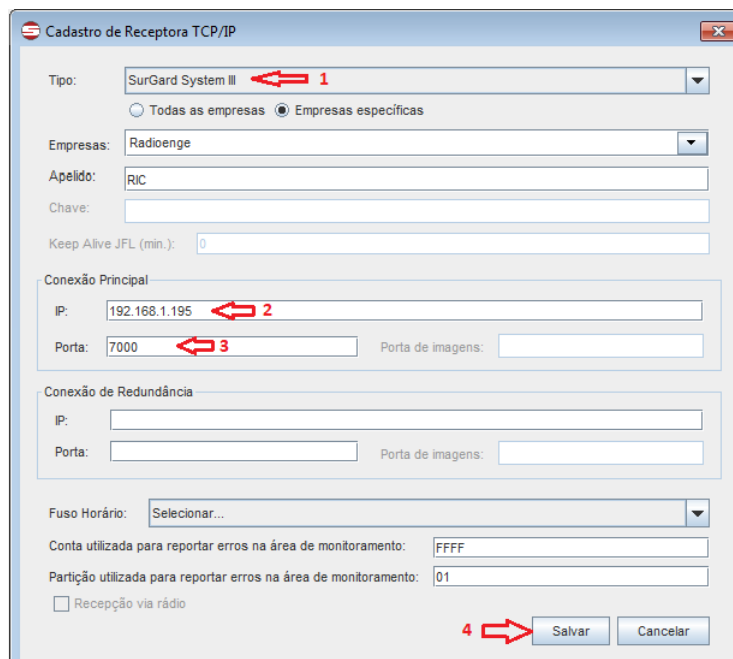
Neste exemplo iremos configurar o software de monitoramento **SIGMA** para se conectar com o WebReceiver e receber os eventos das centrais.

- 1) Abra o software Sigma, selecione a aba **Recepção via Porta TCP/IP** e pressione o botão **Incluir**;



Figura 65: Software SIGMA

2) A tela de configuração abaixo será apresentada. Preencha os campos necessários:



Cadastro de Receptora TCP/IP

Tipo: SurGard System III

☐ Todas as empresas ☒ Empresas específicas

Empresas: Radioenge

Apelido: RIC

Chave:

Keep Alive JFL (min.): 0

Conexão Principal

IP: 192.168.1.195

Porta: 7000

Porta de imagens:

Conexão de Redundância

IP:

Porta:

Porta de imagens:

Fuso Horário: Selecionar...

Conta utilizada para reportar erros na área de monitoramento: FFFF

Partição utilizada para reportar erros na área de monitoramento: 01

☐ Recepção via rádio

Salvar Cancelar

Figura 66: Configuração de conexão com o SIGMA

Campos necessários para a conexão com WebReceiver:

- 1 - **Tipo:** SurGard System III
- 2 - **IP:** 192.168.1.195 (IP do pc onde o WebReceiver está executando)
- 3 - **Porta:** 7000 (porta de comunicação configurada no monitoramento do WebReceiver)

3) Pressione o botão **Salvar** para que as novas configurações sejam válidas.

Após salvar, as novas configurações serão apresentadas conforme tela abaixo:

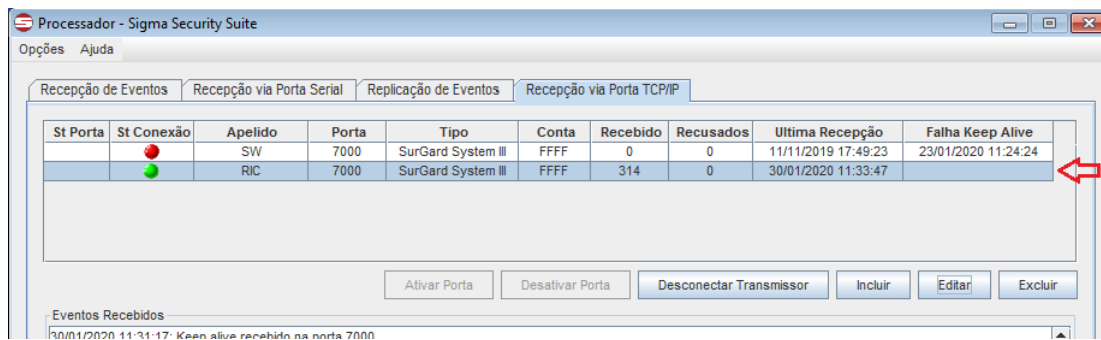


Figura 67: Configuração de conexão com o SIGMA

Para verificar se o **WebReceiver** está conectado ou não ao software de monitoramento, acesse a página de **Status do Software**.

- A figura abaixo indica que o monitoramento está **Desconectado (-)**.



Figura 68: WebReceiver desconectado do software de monitoramento

- A figura abaixo indica que o monitoramento está **Conectado**.



Figura 69: WebReceiver conectado ao software de monitoramento

8.3.3 MONI

Neste exemplo iremos configurar o WebReceiver para se conectar com o software de monitoramento **MONI**.

Neste padrão de conexão: **Iris / Moni / Condor**, podemos configurar o WebReceiver para 2 servidores com software de monitoramento, sendo:

- Servidor principal - Software de monitoramento 1.
- Servidor de redundância - Software de monitoramento 2.

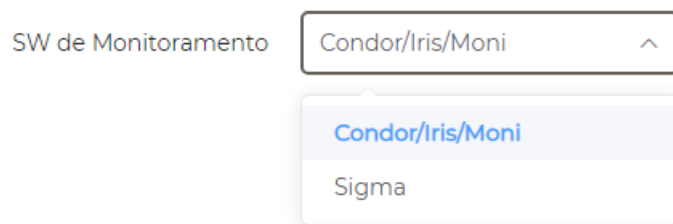
O WebReceiver tenta estabelecer a conexão com o servidor 1. Caso não consiga, faz a tentativa de conexão com o servidor 2. A empresa de monitoramento pode disponibilizar 1 ou 2 servidores com o software. Caso tenha apenas 1, basta configurar o primeiro.

Para efetuar a configuração do WebReceiver – Monitoramento, siga os seguintes passos:

- 1) No menu principal do WebReceiver, selecione a página de **Configurações**;

Figura 70: Configuração da conexão com o monitoramento - Iris/Moni/Condor

- 2) Selecione, no submenu, a aba **Monitoramento**;
- 3) Selecione o software utilizado: **Iris / Moni / Condor**;



SW de Monitoramento

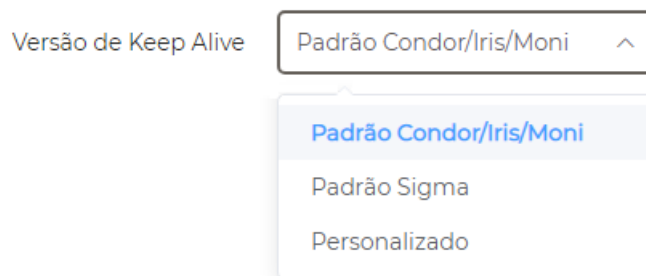
Condor/Iris/Moni

Condor/Iris/Moni

Sigma

Figura 71: Seleção do software Iris/Moni/Condor

- 4) Selecione a versão de **KeepAlive** que será utilizado;



Versão de Keep Alive

Padrão Condor/Iris/Moni

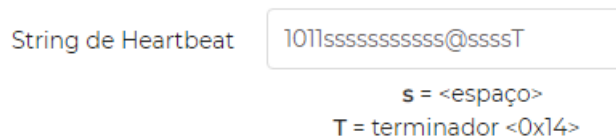
Padrão Condor/Iris/Moni

Padrão Sigma

Personalizado

Figura 72: Configuração da versão do keepalive

- 5) Defina a string de **HeartBeat** (string de envio na mensagem de KeepAlive). Para Sigma e Iris/Moni/Condor, esta string vem preenchida, porém o usuário pode alterá-la;



String de Heartbeat

1011ssssssssss@ssssT

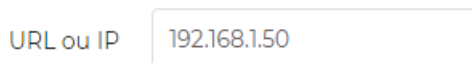
s = <espaço>

T = terminador <0x14>

Figura 73: Configuração da string de heartbeat

- 6) Defina o **Servidor principal – Software de monitoramento 1:**

- **URL ou IP:** onde o software MONI está instalado.



URL ou IP

192.168.1.50

Figura 74: Endereço IP/URL de conexão com o Moni

- **Porta:** porta de comunicação configurada no **MONI**:



Porta

7000

Figura 75: Porta de conexão com o Moni

- 7) Defina o **Servidor secundário – Software de monitoramento 2 (Redundância):**

- **URL ou IP:** onde o software **MONI** está instalado (redundância).

URL ou IP (Backup) 192.168.1.135

Figura 76: Endereço IP/URL de conexão com o Moni (redundância)

- **Porta:** porta de comunicação configurada no **MONI**.

Porta 5000

Figura 77: Porta de conexão com o Moni

- 8) **Salve** a configuração referente ao monitoramento. O WebReceiver irá reinicializar carregando os novos parâmetros.

SALVAR CONFIGURAÇÕES

Figura 78: Salvar as configurações

8.3.4 MONI - Configuração com o WebReceiver

Neste exemplo iremos configurar o software de monitoramento **MONI** para receber a conexão do WebReceiver.

- 1) Abra o software de monitoramento **Moni** e selecione as abas: **Utilitários**, **Configurar** e **Sistema**;

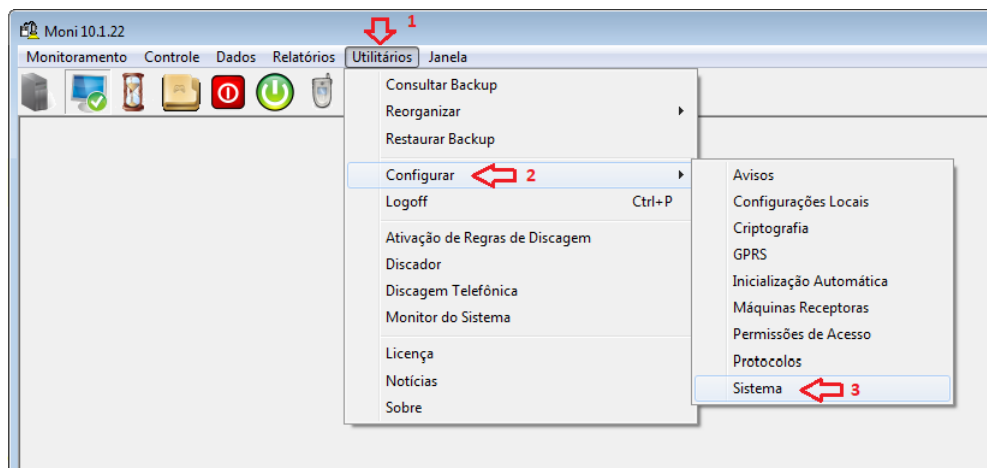


Figura 79: Software MONI

- 2) Será apresentada a tela de configuração abaixo. Selecione a aba **Máquinas Receptoras**, e em seguida pressione o botão **Incluir** (para uma nova conexão);

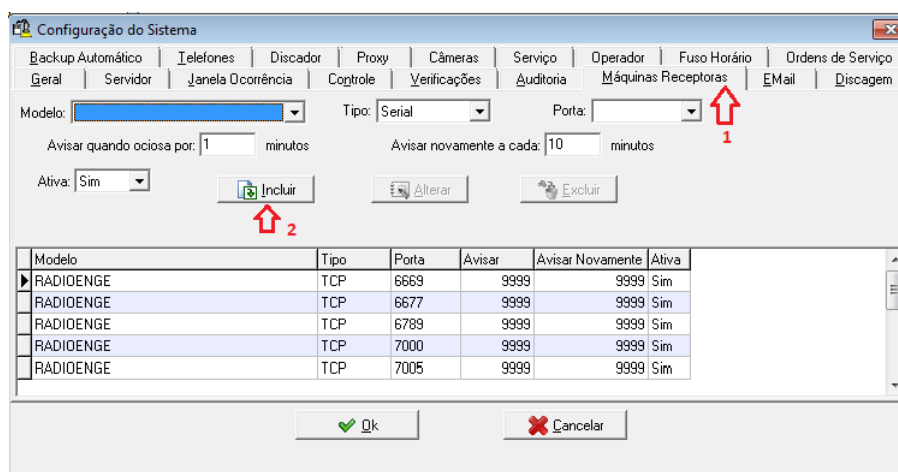


Figura 80: Configuração do software MONI

3) Após pressionar o botão incluir, entre com os campos abaixo:

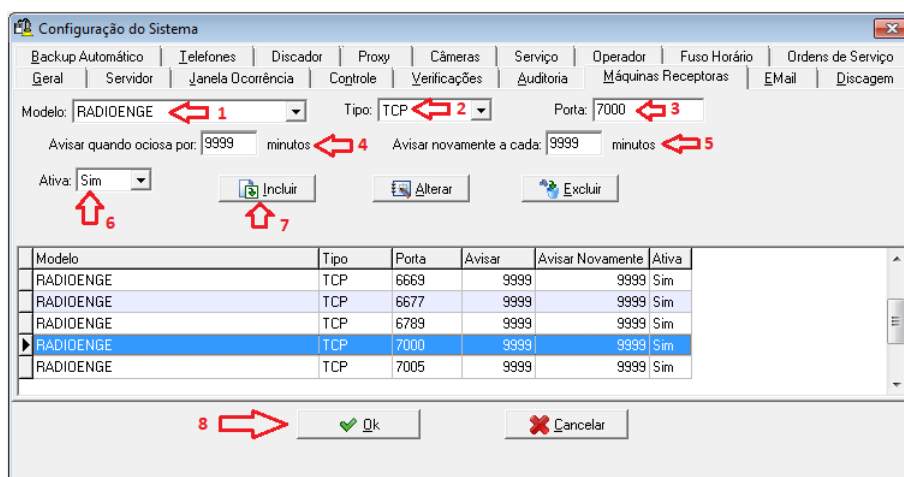


Figura 81: Configuração de conexão com o MONI

Campos necessários:

- 1 - **Modelo**: Selecione o modelo;
 - 2 - **Tipo**: TCP (defina a conexão TCP);
 - 3 - **Porta**: 7000 (a mesma porta configurada no WebReceiver);
 - Defina os tempos 4 e 5;
 - 6 - **Ativa**: Sim (defina a configuração de conexão como ativa);
- 4) Após entrar com os campos acima, pressione o botão **Incluir**, novamente, para que seja incluído na lista;
- 5) Clique no botão **Ok** para finalizar a configuração.

Para verificar se o **WebReceiver** está conectado ou não ao software de monitoramento, acesse a página de **Status do Software**.

- A figura abaixo indica que o monitoramento está: **Desconectado (-)**.

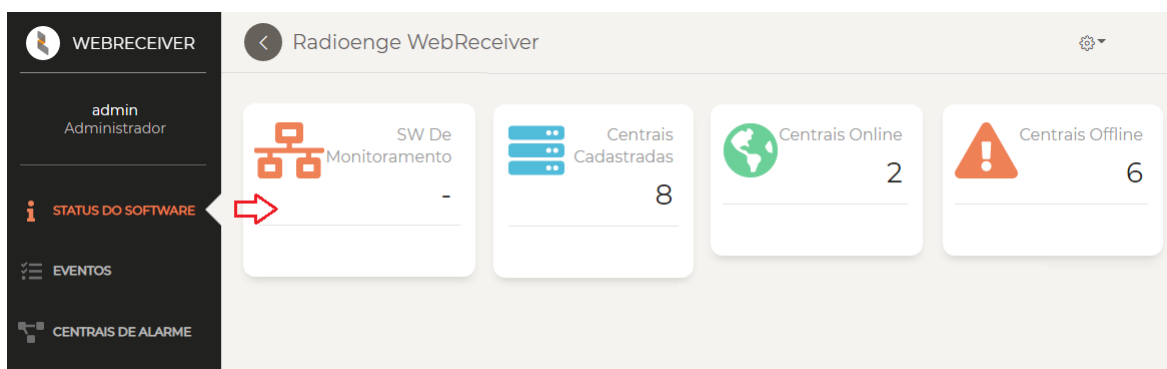


Figura 82: WebReceiver desconectado do software de monitoramento

- A figura abaixo indica que o monitoramento está: **Conectado**.



Figura 83: WebReceiver conectado ao software de monitoramento

8.4 Eventos

A página **Eventos** permite que um usuário **Administrador** delete os eventos gravados na base de dados, anteriores a uma dada específica. Este processo irá gravar todos os eventos das centrais que possuam eventos anteriores a data, em um arquivo .log.

Este procedimento exclui todos os eventos das centrais até a data especificada pelo usuário, aliviando o processamento do sistema e aumentando o espaço livre em disco.

Para realizar a exclusão dos eventos anteriores a uma determinada data, siga os seguintes passos:

- 1) Selecione a data desejada através do campo **Remover eventos anteriores ao dia**. Neste exemplo, serão removidos os eventos anteriores ao dia 23/11/2020;

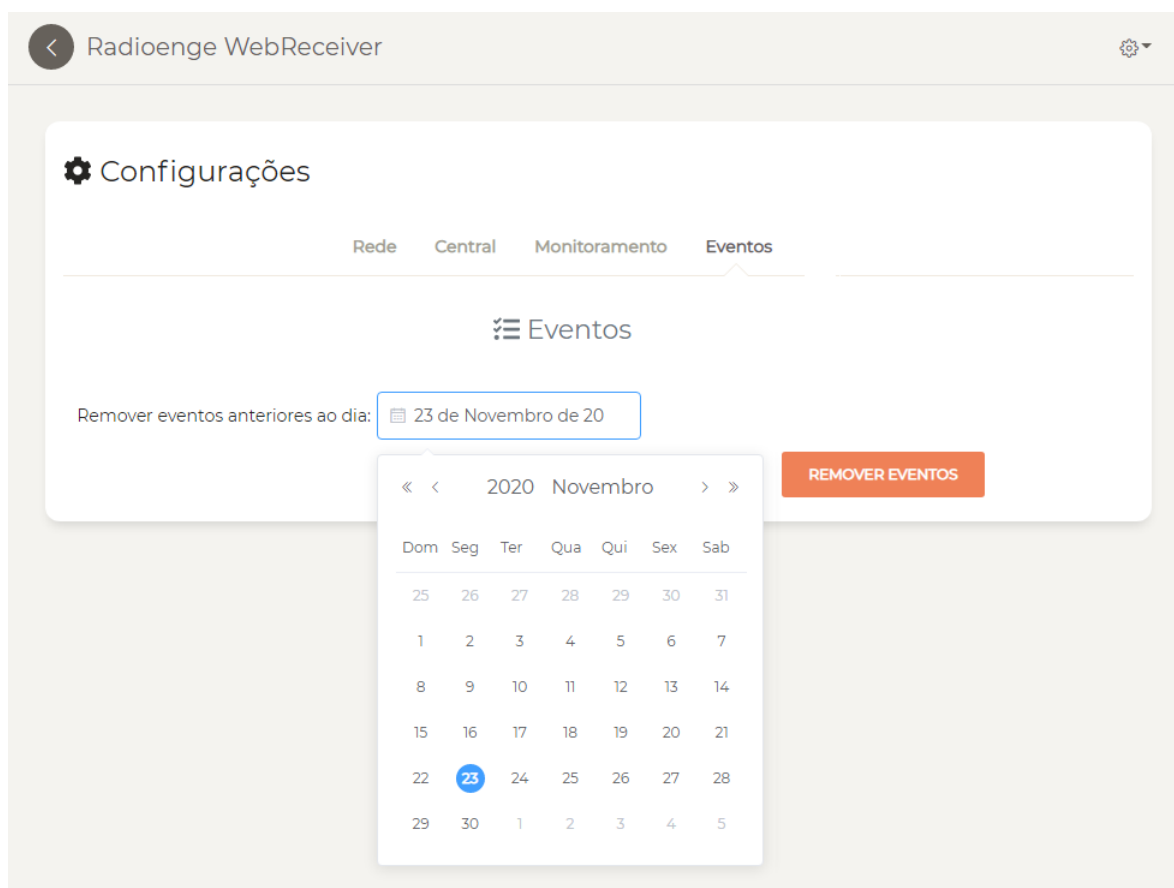


Figura 84: Deletar eventos anteriores à uma data específica

2) Após selecionar a data, clique em **Remover Eventos**.

Em seguida, tela de confirmação dos eventos removidos será mostrada.

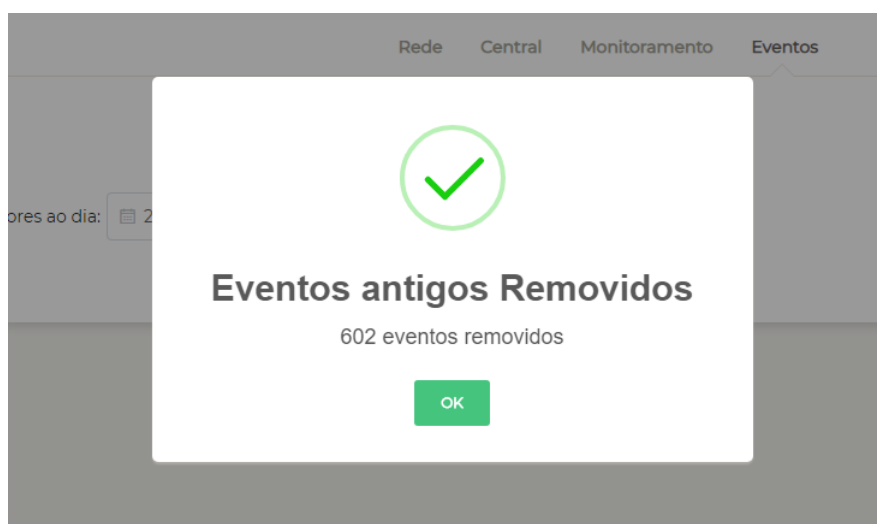


Figura 85: Janela de confirmação exclusão dos eventos

Durante o processo de exclusão, será disparada uma função para que sejam gravados todos os eventos das centrais, anteriores a data fornecida, em um arquivo no formato .log.

Para verificar o arquivo salvo, abra a pasta: C:\Radioenge\WebReceiver\backup, e observe sua existência, o nome do arquivo está no seguinte formato: eventos YYYY-MM-DD.log, onde: YYYY-MM-DD se refere a data fornecida.

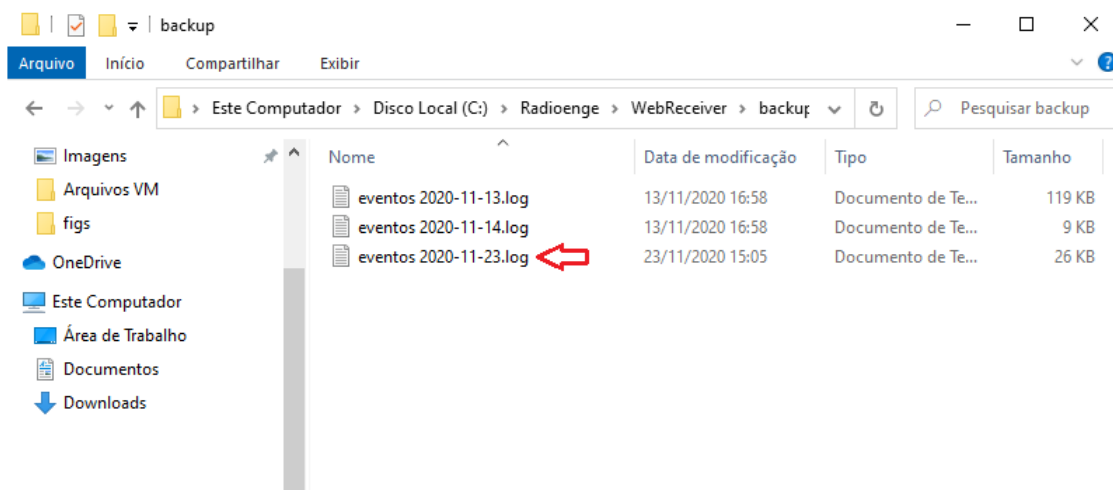


Figura 86: Arquivo contendo os eventos deletados da central

8.5 Cloud

A página **Cloud** permite realizar a integração com a Radioenge Cloud.

Insira o email e a senha referentes à empresa de monitoramento já cadastrada na Radioenge Cloud, e clique em “Salvar configuração”.

⚙️ Configurações

Rede Central Monitoramento Eventos Cloud

Integração com a Radioenge Cloud


Email

Senha

SALVAR CONFIGURAÇÃO

Figura 87: Integração com a Radioenge Cloud

9 Alterar Senha

Para acessar o menu que permite alterar a senha da página web, clique sobre o ícone  e selecione a opção **Alterar Senha**.

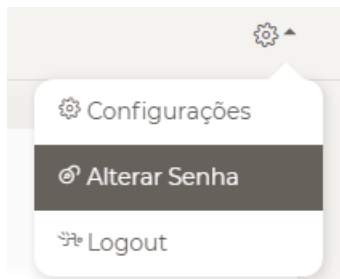


Figura 88: Opção de alterar a senha

Em seguida, a janela de alteração de senha do usuário será exibida.

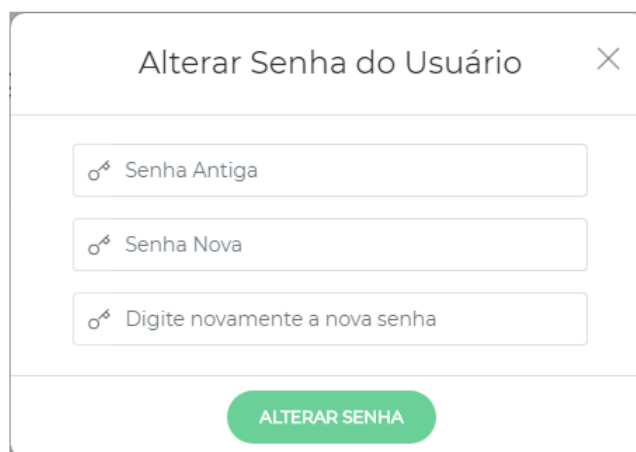



Figura 89: Janela de alteração da senha do usuário

Forneça a senha antiga no campo “Senha Antiga”, digite a nova senha nos campos “Senha Nova” e “Digite novamente a nova senha” e clique em **Alterar Senha**.

10 Logout

Para realizar o logout na página web, clique sobre o ícone  e selecione a opção **Logout**.

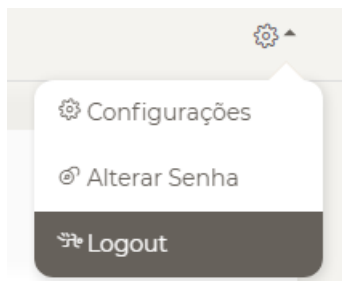


Figura 90: Opção de realizar logout

Após o logout, o usuário será redirecionado para a tela de login.

11 Códigos de Eventos da Central

Tabela 2: Códigos de alarmes 24h e alarme de furto

Alarme	Código	Descrição	Tipo
Alarme médico	E100	Sinaliza eventos do alarme 24h médico	Zona
Alarme incêndio	E110	Sinaliza eventos do alarme 24h incêndio	Zona
Alarme 24h pânico	E120	Sinaliza eventos do alarme 24h pânico	Zona
Alarme 24h hold up	E126	Sinaliza eventos do alarme 24h hold up	Zona
Alarme de furto	E130	Evento gerado quando o alarme de furto é disparado	Zona
	R130	Restauração do disparo do alarme de furto	Zona
Alarme 24h furto	E133	Sinaliza eventos do alarme 24h furto	Zona
Alarme 24h gás	E151	Sinaliza eventos do alarme 24h gás	Zona
Alarme 24h refrigeração	E152	Sinaliza eventos do alarme 24h refrigeração	Zona
Alarme 24h aquecimento	E153	Sinaliza eventos do alarme 24h aquecimento	Zona
Alarme 24h água	E154	Sinaliza eventos do alarme 24h água	Zona

Tabela 3: Códigos de arme/desarme, anulação e configuração remota


Evento	Código	Descrição	Tipo
Desarme com coação	E121	Sinaliza que o alarme foi desarmado utilizando a função de coação	Usuário
Arme/desarme partição	R401	Restauração gerado ao armar a partição	Usuário
	E401	Evento gerado ao desarmar a partição	
Arme/desarme via keyswitch	R409	Restauração gerado ao armar via keyswitch	Zona
	E409	Evento gerado ao desarmar via keyswitch	
Configuração remota	E410	Evento de configuração remota	Usuário
	R410	Restauração de configuração remota	
Ativação parcial	R456	Restauração gerado ao realizar um arme parcial (sleep/stay)	Usuário
	E456	Evento gerado ao desarmar a partição que estava armada parcialmente	
Bypass de zona	E570	Evento gerado ao anular a zona	Zona
	R570	Restauração gerado ao ativar a zona	

Tabela 4: Códigos de eventos de status da central

Status	Código	Descrição	Tipo
Falha na alimentação	E301	Evento gerado quando a central está desconectada da rede elétrica	000
Bateria baixa	E302	Evento gerado quando a bateria de alimentação está baixa	000
Reset do sistema	R305	Sinaliza a ocorrência de reset do sistema	000
Falha na bateria	E309	Evento gerado quando a bateria LiPo está desconectada	000
Bateria ausente	E311	Evento gerado quando a bateria LiPo está desconectada	000
Reset de fábrica	E313	Evento gerado quando a central é restaurada para o padrão de fábrica	000
Sirene em curto	E321	Evento gerado quando as saídas da sirene estão em curto	000
	R321	Restauração gerado quando as saídas deixam de estar em curto	
Sirene aberta	E322	Evento gerado quando as saídas da sirene estão em aberto	000
	R322	Restauração gerado quando as saídas deixam de estar em aberto	
Falha de comunicação ethernet	E361	Evento de falha de conexão com o WebReceiver 1 (000), WebReceiver 2 (001) ou via internet com a cloud (002)	000 001
	R361	Restauração da conexão	002
Conexão/Desconexão de dispositivo	E899	Evento gerado pelo WebReceiver. Indica desconexão da central com o WebReceiver ou central offline	000
	R899	Reconexão da central com o WebReceiver	
Falha de supervisão	E381	Evento de falha de comunicação do sensor com a central	Zona
	R381	Restauração da comunicação do sensor com a central	
Tamper de zona	E383	Evento gerado ao abrir o tamper	Zona
	R383	Restauração gerado ao fechar o tamper	
Bateria baixa sensor	E384	Evento gerado quando a bateria do sensor está baixa	Zona
Teste periódico da central	E602	Envio do teste periódico da central à empresa de monitoramento	000
Buffer de eventos 50% cheio	E622	Evento gerado ao atingir 50% da capacidade de armazenamento do buffer da central	000
	R622	Restauração gerado quando a taxa de utilização do buffer diminuir para um valor inferior a 50%	
Buffer de eventos 90% cheio	E623	Evento gerado ao atingir 90% da capacidade de armazenamento do buffer da central	000
	R623	Restauração gerado quando a taxa de utilização do buffer diminuir para um valor inferior a 90%	
Buffer de eventos cheio	E624	Evento gerado ao atingir a capacidade máxima de armazenamento do buffer da central	000
	R624	Restauração gerado quando a taxa de utilização do buffer diminuir para um valor inferior à capacidade máxima	

12 Contato

- **WhatsApp:**

 +55 (41) 3052-9444

- **Site:** <https://www.radioenge.com.br/contato/>