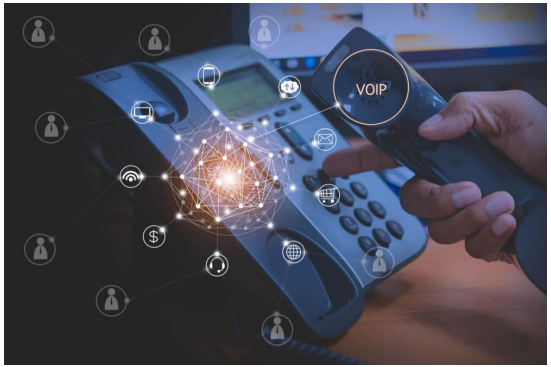
Prova de Conceito

Defensoria Pública do Estado do Rio de Janeiro

DEFENSORIA PÚBLICA
DO ESTADO DO RIO DE JANEIRO

CAM TECNOLOGIA



Empresa nascida no Laboratório de Pesquisa no NCE/UFRJ, criada a partir de um grupo de trabalho da RNP (Rede Nacional de Ensino e Pesquisa) com foco em VoIP e tecnologias de integração, participando no desenvolvimento da solução VoIP4ALL que hoje é conhecido como fone@RNP e está presente em mais de 400 instituições no Brasil.

ÁREA DE ATUAÇÃO

Atuamos em todo o Brasil, com suporte remoto ou local, contando com uma equipe especializada e certificada, garantindo o melhor atendimento.

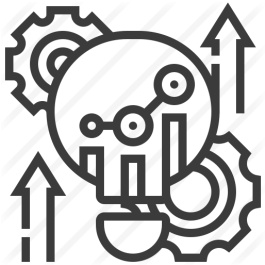
dCAP
Digium-Certified
Asterisk Professional

CISCO
CERTIFIED
CCNA

ITIL®

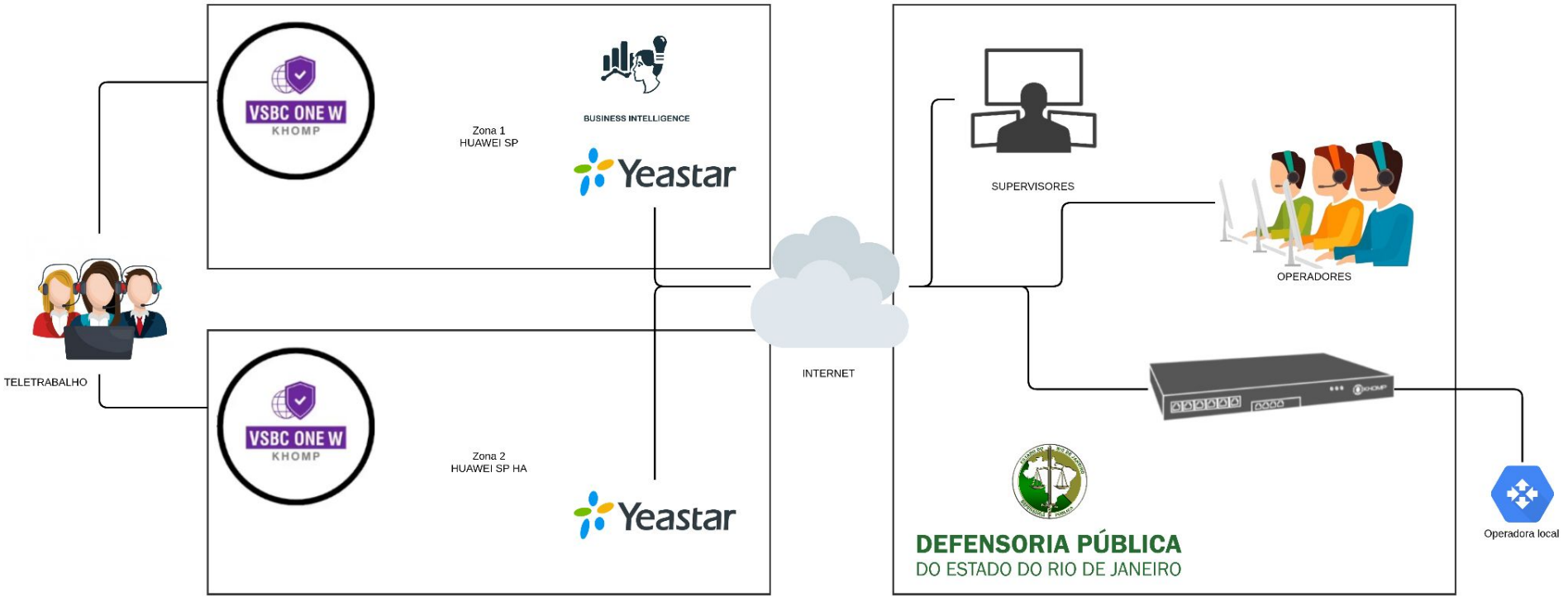
DESTAQUES:

Equipe especializada.
Equipe multidisciplinar, especialistas e técnicos, executam um atendimento rápido de forma a reduzir perdas com tempo de inatividade;



Desenvolvimento contínuo
Sempre com as necessidades dos clientes em foco, desenvolvendo novas ferramentas que facilitam o trabalho de nossos clientes, para que tenham tempo de pensar somente em seu negócio.

TOPOLOGIA


VSBC ONE W
KHOMP
Zona 1
HUAWEI SP
BUSINESS INTELLIGENCE
Yeastar
VSBC ONE W
KHOMP
Zona 2
HUAWEI SP HA
Yeastar
TELETRABALHO
INTERNET
SUPERVISORES
OPERADORES
DEFENSORIA PÚBLICA
DO ESTADO DO RIO DE JANEIRO
Operadora local

Responsabilidades da CAM

Ambiente de Cloud
Servidores com alta disponibilidade, 24 horas por dia 7 dias por semana, em ambientes controlados sem risco de queda de energia ou falha física, ampliação de ramais de forma simples e rápida e em qualquer lugar.

Equipamentos em Comodato
Fornecimento, substituição e manutenção dos Headsets e Gateway E1/SIP ou SIP/SIP para us pela equipe da Defensoria Pública do Estado do RJ

Atualização e insights contínuos
Apoiar a equipe da Defensoria Pública com insights de dados e avaliações do serviço e realizar atualizações do servidores continuamente conforme alinhamento.

Suporte remoto e presencial
Fornecer canais de atendimento remotos e presenciais para equipe da Defensoria Pública.

PRINCIPAIS FUNCIONALIDADES:

Filas de atendimento e call center
Funcionalidades que facilitam o atendimento de suporte e equipes de televendas.

Softphones para celular
Integração com sistema móveis permitindo a utilização de aplicativos SIP para utilizar os ramais nos smartphones.

Voice Mail
Receba as mensagens de áudio deixadas diretamente em seu email.

Video chamadas
Integração completa com sistemas de videoconferência e webconferência, suportando diversos dispositivos, garantindo qualidade nas vídeo chamadas.

PRINCIPAIS FUNCIONALIDADES:

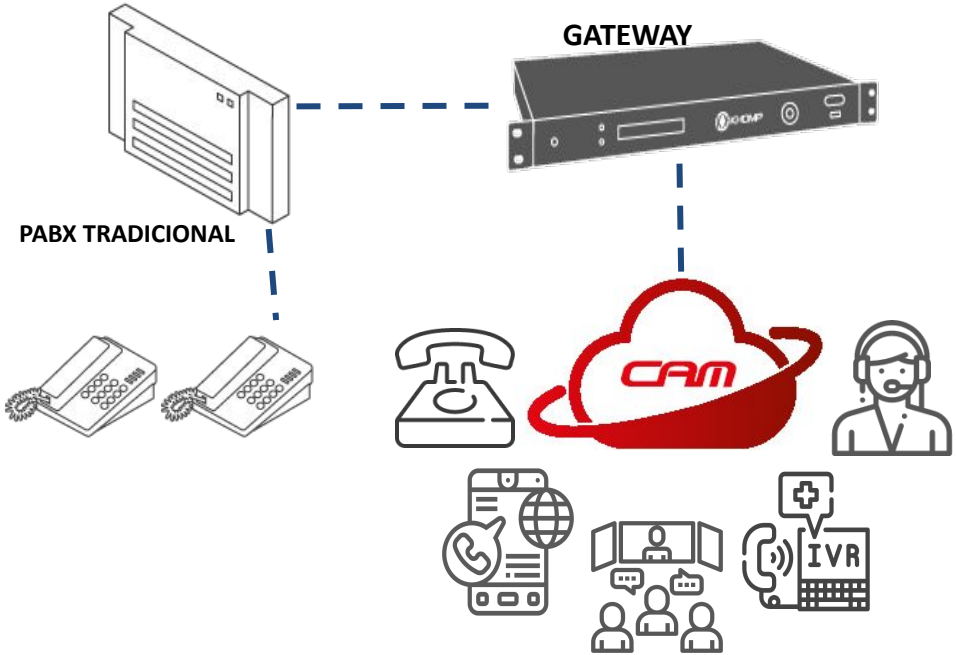
Callcenter Ativo
Criação de campanhas e processos de automação de chamadas ativo. Com Atendimento humanizado ou robotizado.

URA Inteligente
Atendimento automático com direcionamento para os ramais remotos, permitindo a criação de grupos de atendimento.

Gravação de chamadas
Gravação das chamadas originadas e recebidas pelos ramais, garantindo a segurança e qualidade dos atendimentos.

Relatórios de chamadas
Controle total das ligações, com relatórios personalizados e bilhetagem, por centros de custos e usuários.

INTEGRAÇÃO / CENÁRIOS HÍBRIDOS:



Através de Gateways SIP/SIP ou SIP/TDM permite a integração com sistemas de PABX analógicos, mantendo a estrutura atual e integrando com novas funcionalidades, possibilitando a migração gradual.

CAM TECNOLOGIA

PARCEIROS

Yealink

KHOMP

Asterisk™

Issabel

GRANDSTREAM

ALIGERA

Yeastar

CAM TECNOLOGIA

Alguns clientes

UFLA
UNIVERSIDADE FEDERAL DE LAVRAS

prodam

PREFEITURA DE BOTUCATU

POLÍCIA FEDERAL

UFGD
Universidade Federal da Grande Dourados

UFMT

DETRAN.RJ

INMETRO

JFCE

PREFEITURA DE Coronel Fabriciano

RNP

PORTO DE VITÓRIA
CODESA - AUTORIDADE PORTUÁRIA

TJAP
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ

AGUDOS 1897 1898

UNIFEI
UNIVERSIDADE FEDERAL DE ITAJUBÁ

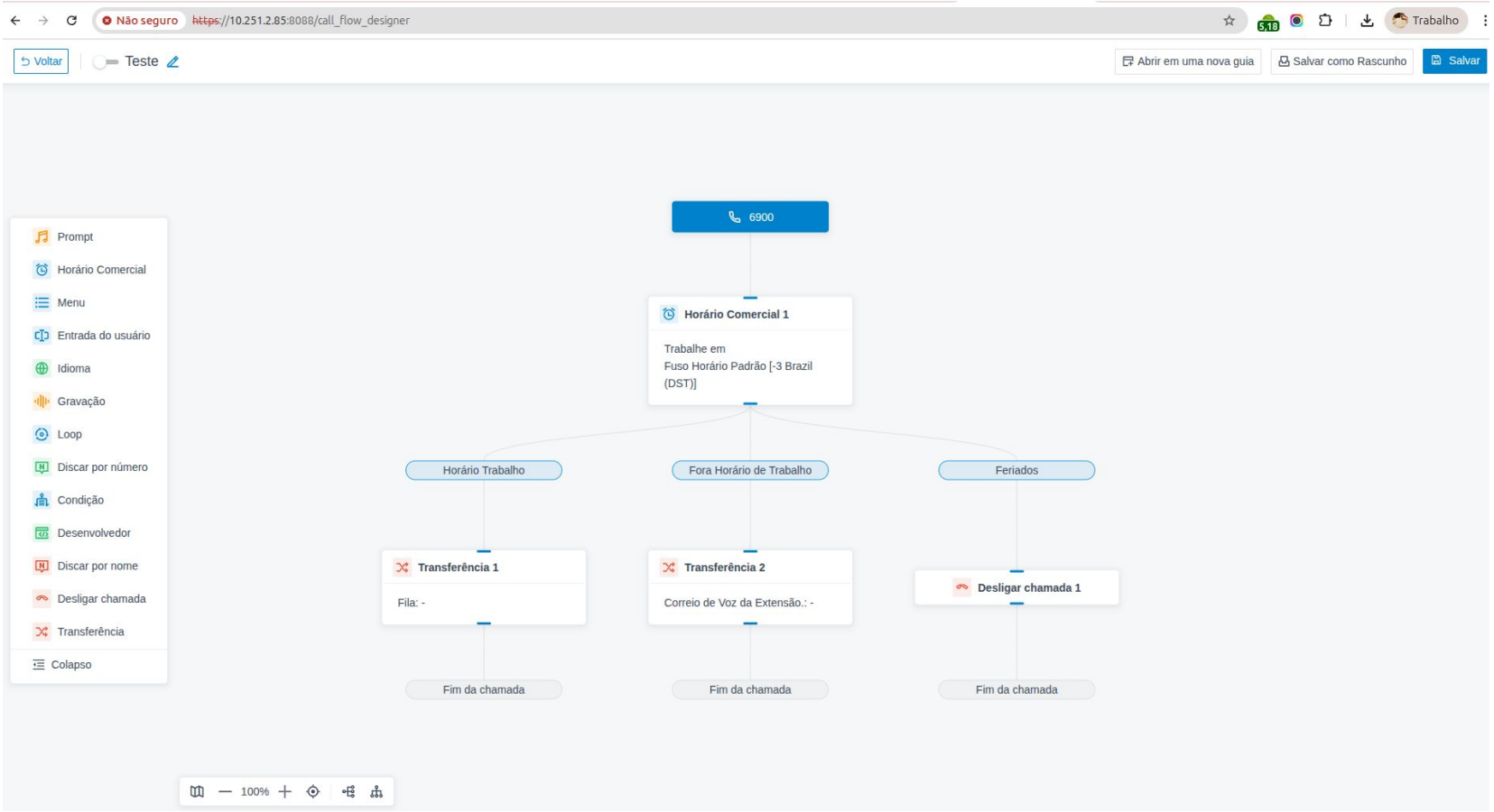
Senac

Embrapa

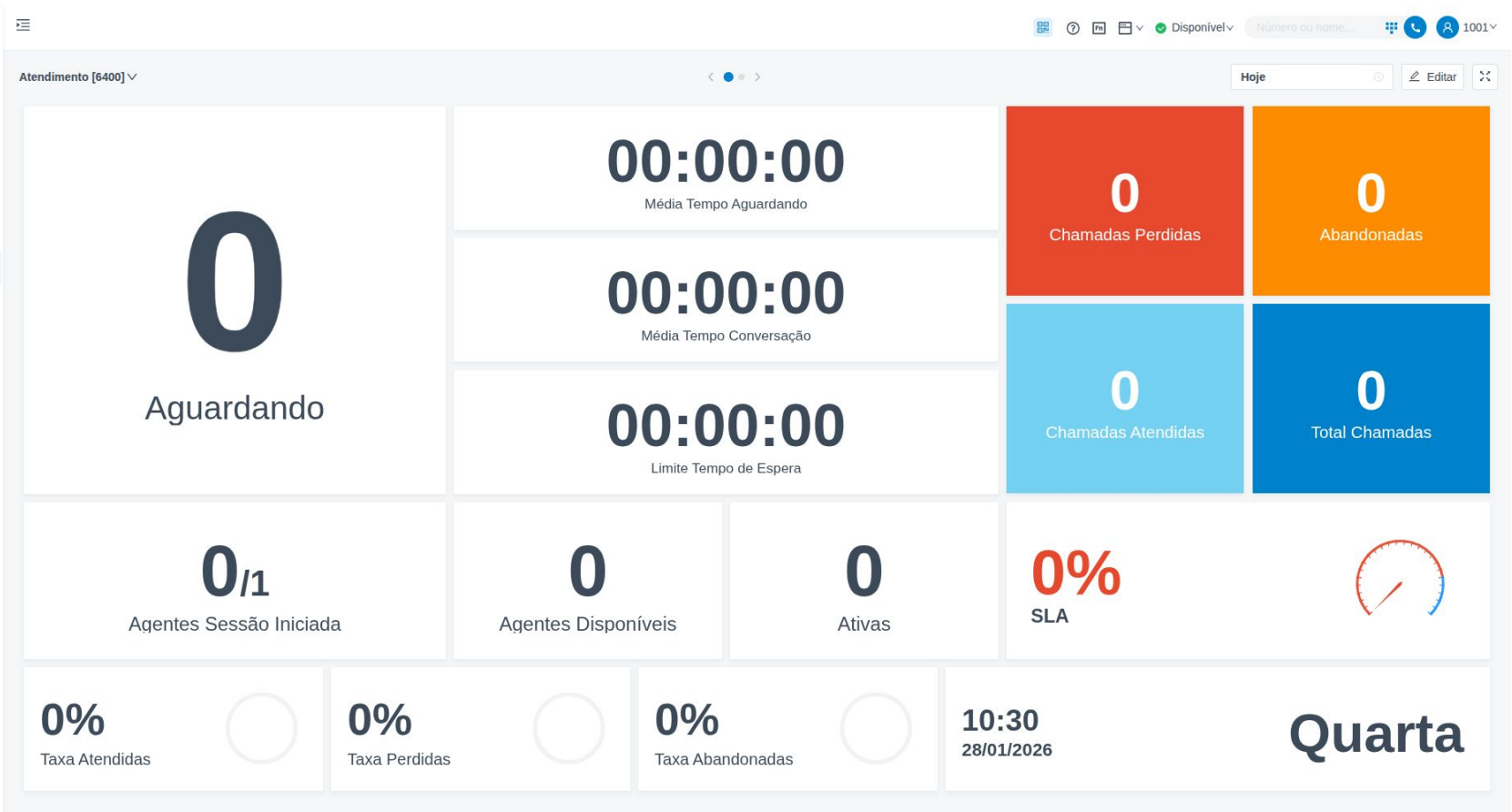
INTERFACES

CAM TECNOLOGIA

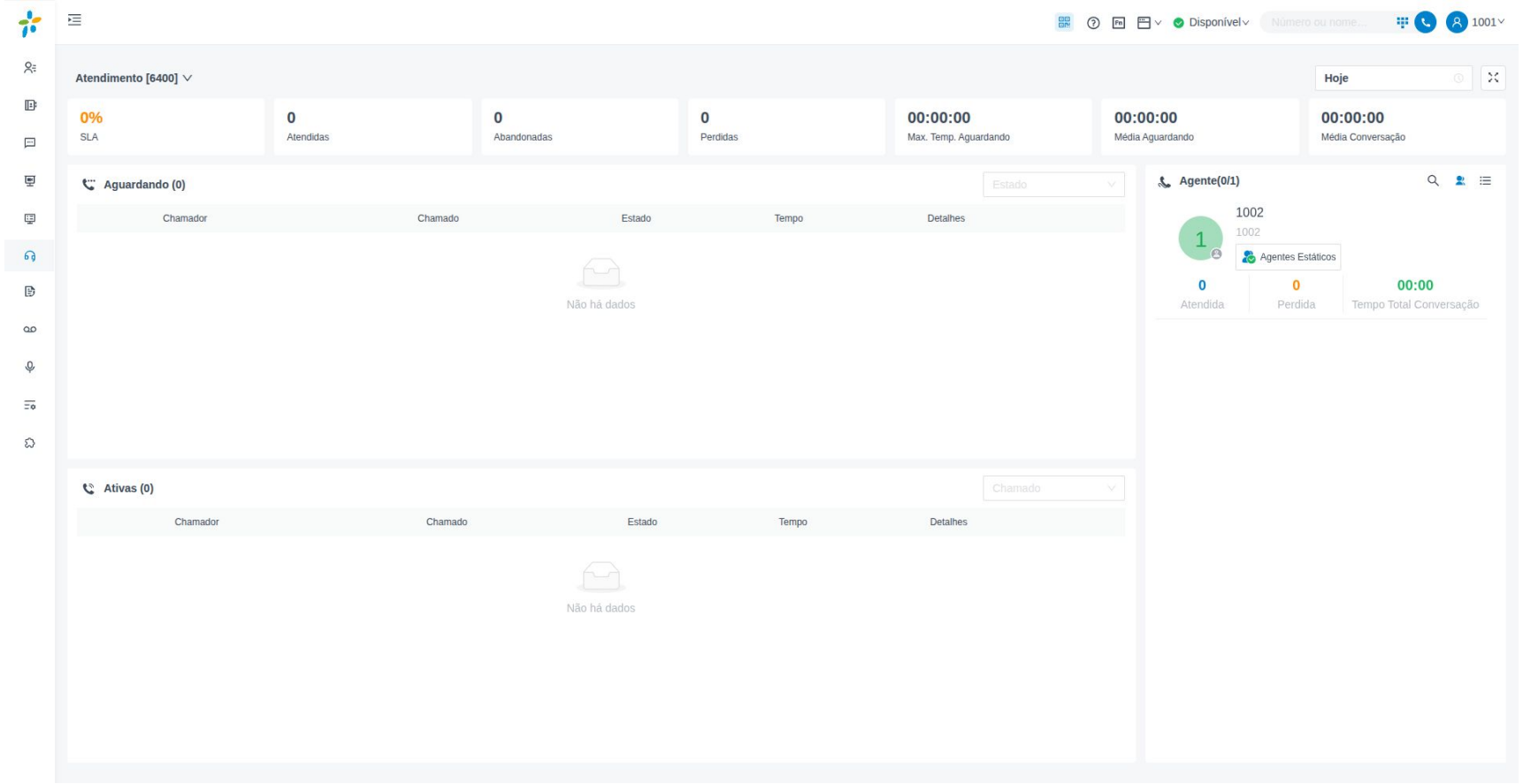
Administração da URA



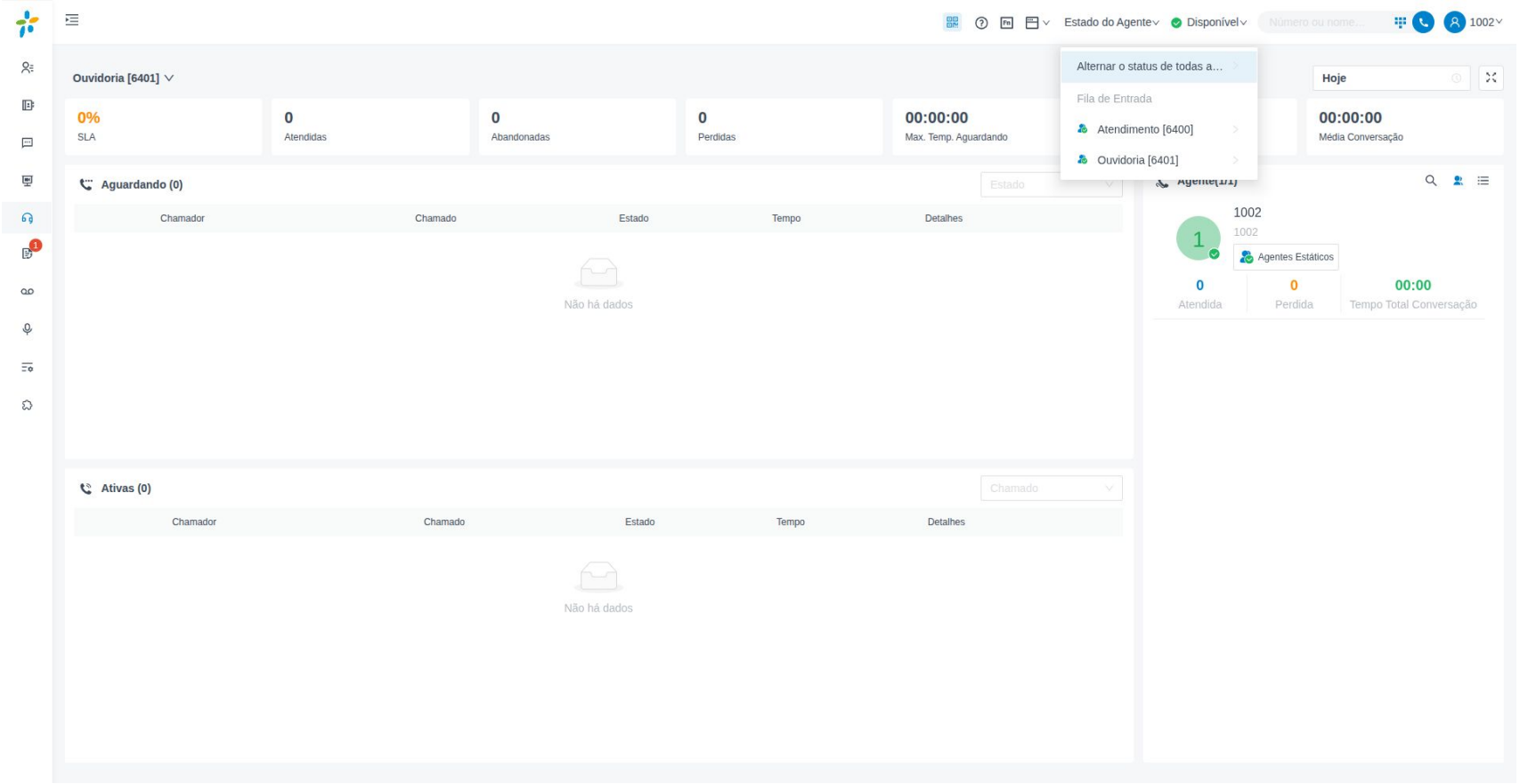
Dashboard da Fila



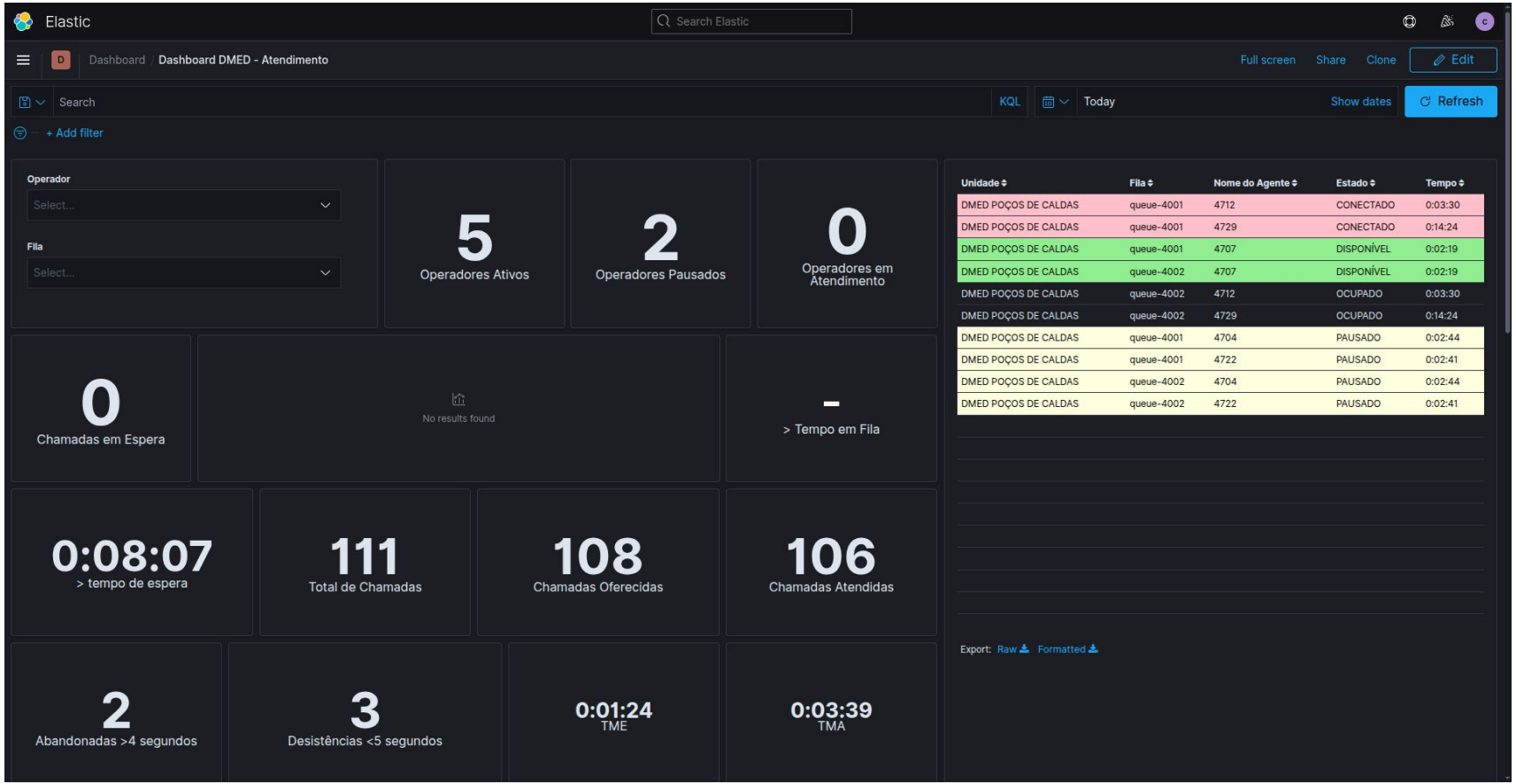
Supervisão da Fila



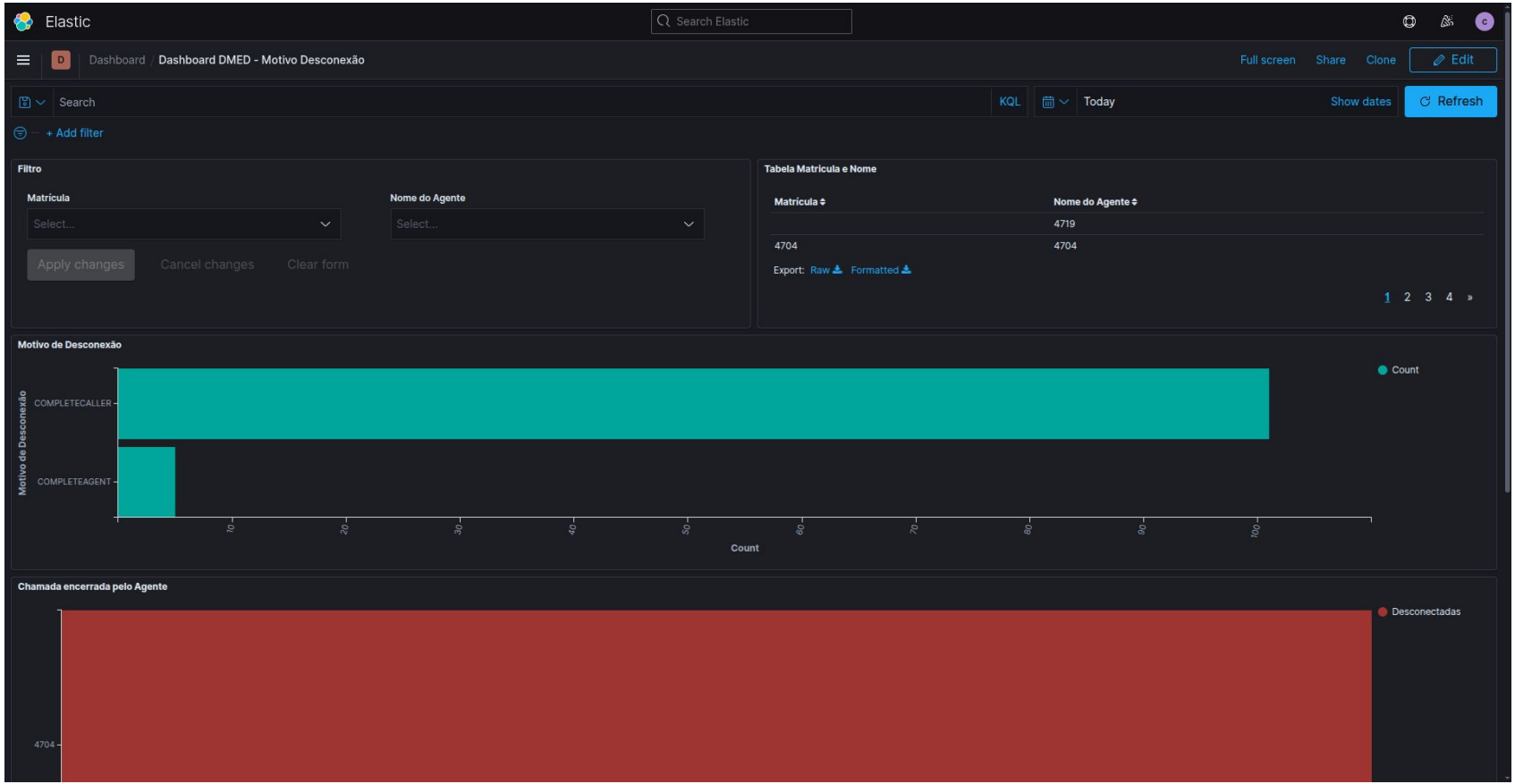
Operador


Estado do Agente
Disponível
1002
Alternar o status de todas a...
Fila de Entrada
Atendimento [6400]
Ouvidoria [6401]
Ouvidoria [6401]
Hoje
0%
SLA
0
Atendidas
0
Abandonadas
0
Perdidas
00:00:00
Max. Temp. Aguardando
00:00:00
Média Conversação
Aguardando (0)
Estado
Chamador
Chamado
Estado
Tempo
Detalhes
Não há dados
Agente(1/1)
1002
1002
Agentes Estáticos
0
Atendida
0
Perdida
00:00
Tempo Total Conversação
Ativas (0)
Chamado
Chamador
Chamado
Estado
Tempo
Detalhes
Não há dados

BI


Elastic
Search Elastic
Dashboard / Dashboard DMED - Atendimento
Full screen
Share
Clone
Edit
Search
KQL
Today
Show dates
Refresh
+ Add filter
Operador
Select...
Fila
Select...
5
Operadores Ativos
2
Operadores Pausados
0
Operadores em Atendimento
0
Chamadas em Espera
No results found
-
> Tempo em Fila
0:08:07
> tempo de espera
111
Total de Chamadas
108
Chamadas Oferecidas
106
Chamadas Atendidas
2
Abandonadas >4 segundos
3
Desistências <5 segundos
0:01:24
TME
0:03:39
TMA
Unidade
Fila
Nome do Agente
Estado
Tempo
DMED POÇOS DE CALDAS queue-4001 4712 CONECTADO 0:03:30
DMED POÇOS DE CALDAS queue-4001 4729 CONECTADO 0:14:24
DMED POÇOS DE CALDAS queue-4001 4707 DISPONÍVEL 0:02:19
DMED POÇOS DE CALDAS queue-4002 4707 DISPONÍVEL 0:02:19
DMED POÇOS DE CALDAS queue-4002 4712 OCUPADO 0:03:30
DMED POÇOS DE CALDAS queue-4002 4729 OCUPADO 0:14:24
DMED POÇOS DE CALDAS queue-4001 4704 PAUSADO 0:02:44
DMED POÇOS DE CALDAS queue-4001 4722 PAUSADO 0:02:41
DMED POÇOS DE CALDAS queue-4002 4704 PAUSADO 0:02:44
DMED POÇOS DE CALDAS queue-4002 4722 PAUSADO 0:02:41
Export: Raw Formatted

BI


Elastic
Search Elastic
Dashboard / Dashboard DMED - Motivo Desconexão
Full screen
Share
Clone
Edit
Search
KQL
Today
Show dates
Refresh
+ Add filter
Filtro
Matrícula
Select...
Nome do Agente
Select...
Apply changes
Cancel changes
Clear form
Tabela Matrícula e Nome
Matrícula
Nome do Agente
4719
4704
4704
Export: Raw Formatted
1 2 3 4 »
Motivo de Desconexão
COMPLETECALLER
COMPLETEAGENT
Motivo de Desconexão
Count
10 20 30 40 50 60 70 80 90 100
Count
Chamada encerrada pelo Agente
Desconectadas
4704

Siga-nos

@camtecnologiavoip

cam tecnologia

CAM TECNOLOGIA

OBRIGADO

Thiago Maluf Resende
CEO

(21) 99700-9113
thiago@camtecnologia.com.br

Av. Pastor Martin Luther King Jr, 126 Nova América Offices, Torre 2000,
Sala 408 Del Castilho | Rio de Janeiro | RJ

CAM TECNOLOGIA

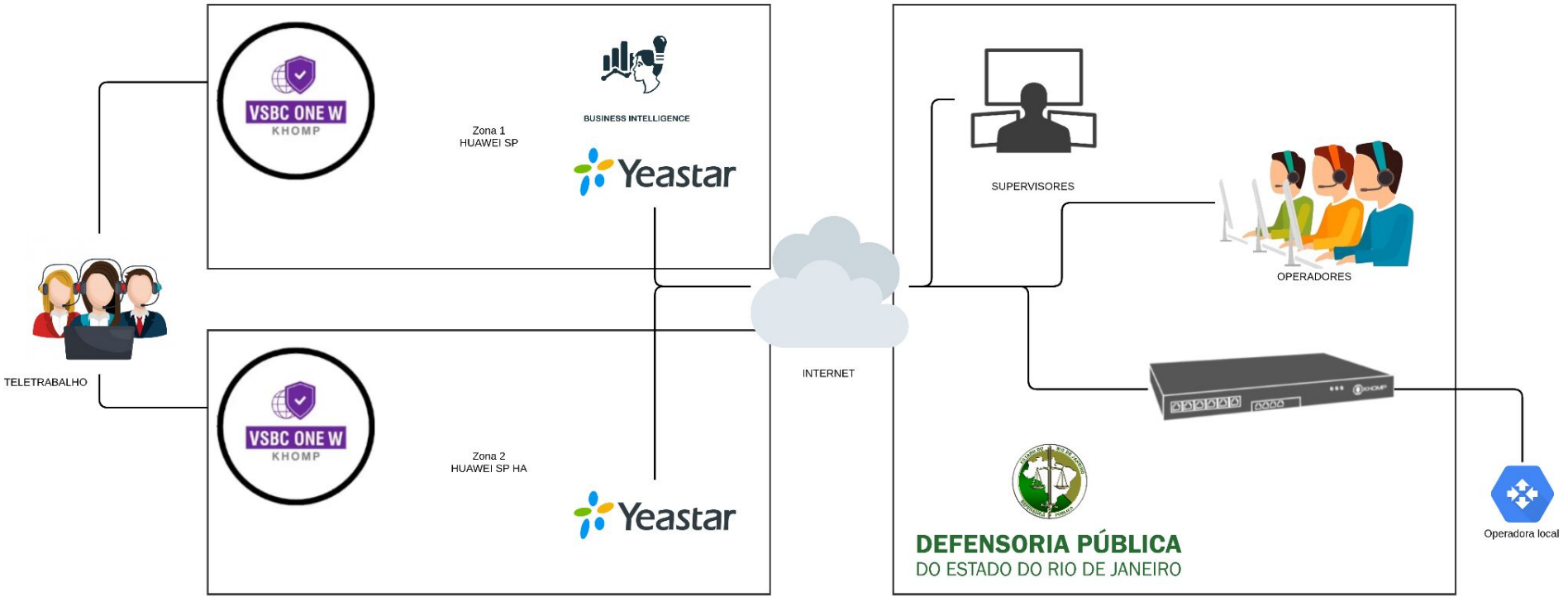
ANEXO II
Evidências da Prova de Conceito
Defensoria Pública do Estado do Rio de Janeiro

DEFENSORIA PÚBLICA
DO ESTADO DO RIO DE JANEIRO

CAM TECNOLOGIA

PARTE I
APRESENTAÇÃO DA SOLUÇÃO

1.1 Apresentação da Solução



1.1 Apresentação da Solução

Ambiente de Cloud
Ambiente em Alta disponibilidade sediado em DataCenter no território brasileiro em Zonas geograficamente distintas.

Equipamentos em Comodato
Headsets USB com teclas de gerenciamento no cabo e aplicativo de validação de serviços
Gateway E1/SIP ou SIP/SIP para integração com a Operadora

Solução Cloud
SBC para integração com parceiros via SIP Internet. PBX Yeastar para fornecimento da solução de comunicação em nuvem. BI para gestão dos dados.

1.2 Apresentação da Documentação Solução

vSBC One W
Anexo III - Manual vSBC-W

BI
https://www.elastic.co/docs/explore-analyze

YEASTAR
https://help.yeastar.com/en/p-series-software-edition/index.html

Gateway KMG 400 One
Anexo IV - Manual KMG One

1.3 Apresentação da Infraestrutura da Solução

Ambiente de Cloud
Ambiente em Alta disponibilidade sediado em DataCenter no território brasileiro em Zonas geograficamente distintas.

Equipamentos em Comodato
Headsets USB com teclas de gerenciamento no cabo e aplicativo de validação de serviços
Gateway E1/SIP ou SIP/SIP para integraçaõ com a Operadora

Integração de Infraestrutura
Ampliando a segurança e a disponibilidade do serviço, Integração da infraestrutura local com a Cloud via IPSEC/VPN.

1.4 Apresentação da Política de Segurança e Backup

Segurança da Informação
Servidores dedicados a infraestrutura da Defensoria Pública, não sendo compartilhado com outros clientes.

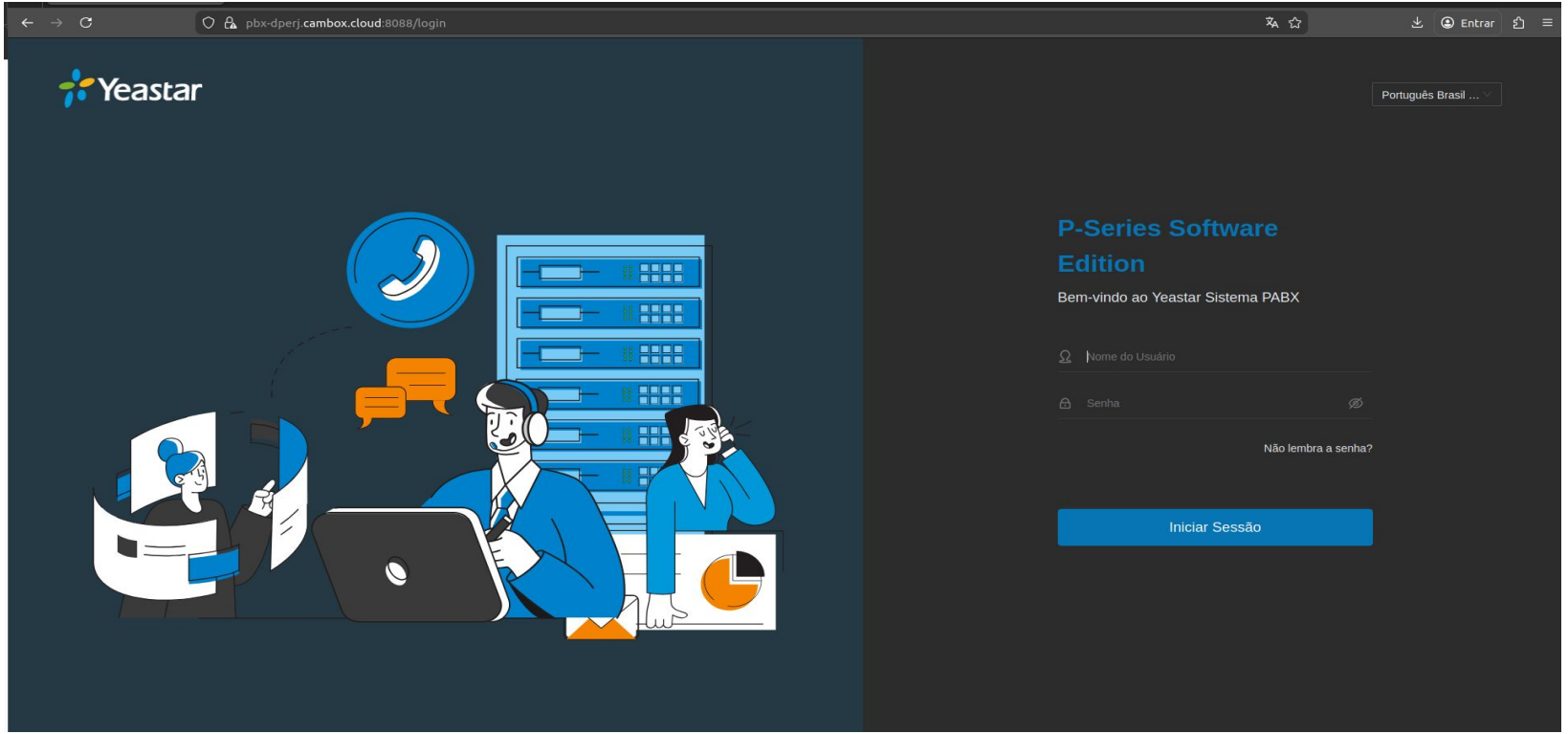
Alta disponibilidade
Equipamentos ativos espelhados em zonas distintas

Backup
Backup das gravações e dados realizados em horários pré-determinados.
Backup completo do ambiente de virtualização realizado diariamente.

PARTE II
DEMONSTRAÇÃO DO CALLCENTER

CAM TECNOLOGIA

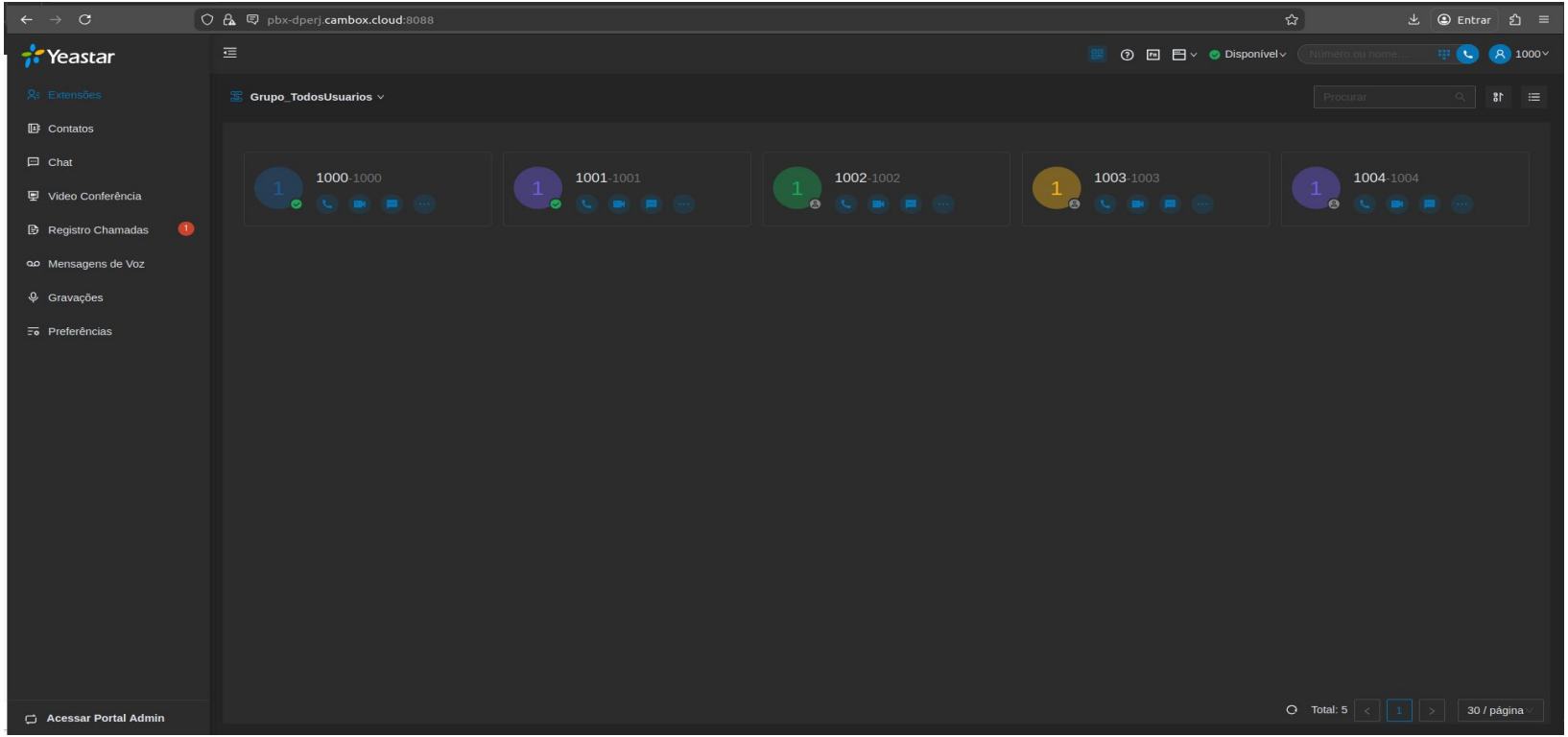
2.1 Apresentação do Ambiente da Demonstração



Tela de Login

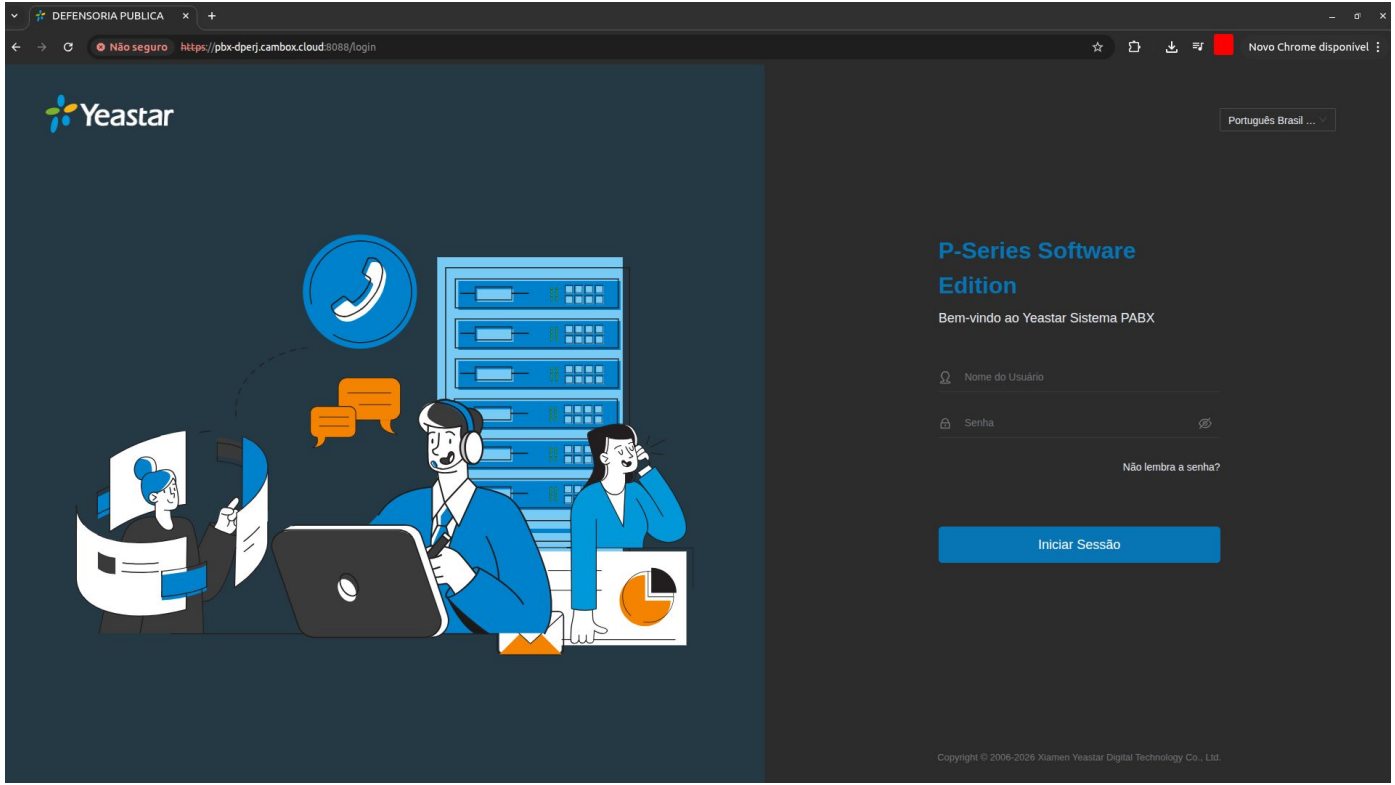
2.1 Apresentação do Ambiente da Demonstração

Tela de Início - Pós-login



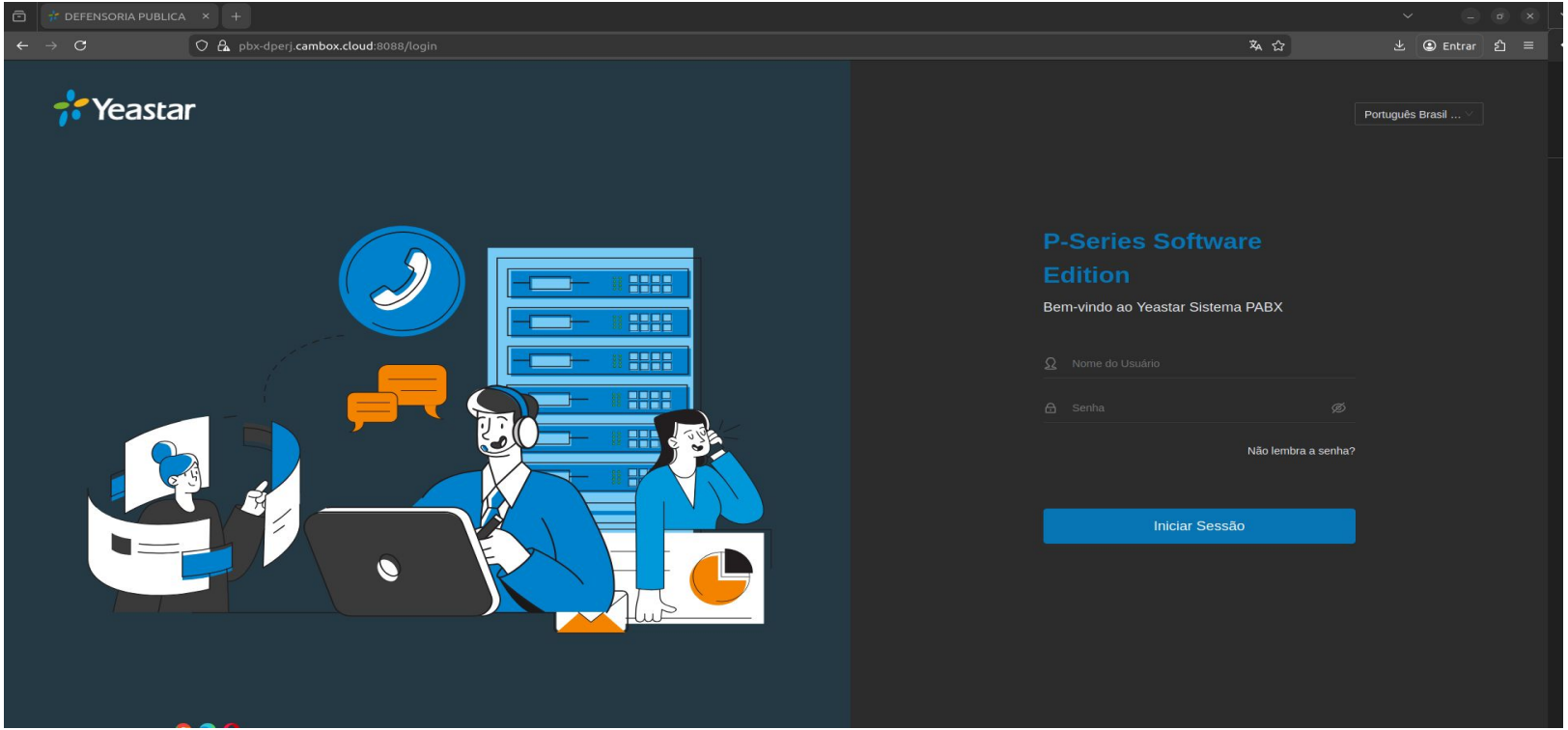
Uso do Serviço com Chrome

2.2 Compatibilidade (3 navegadores padrão de mercado)



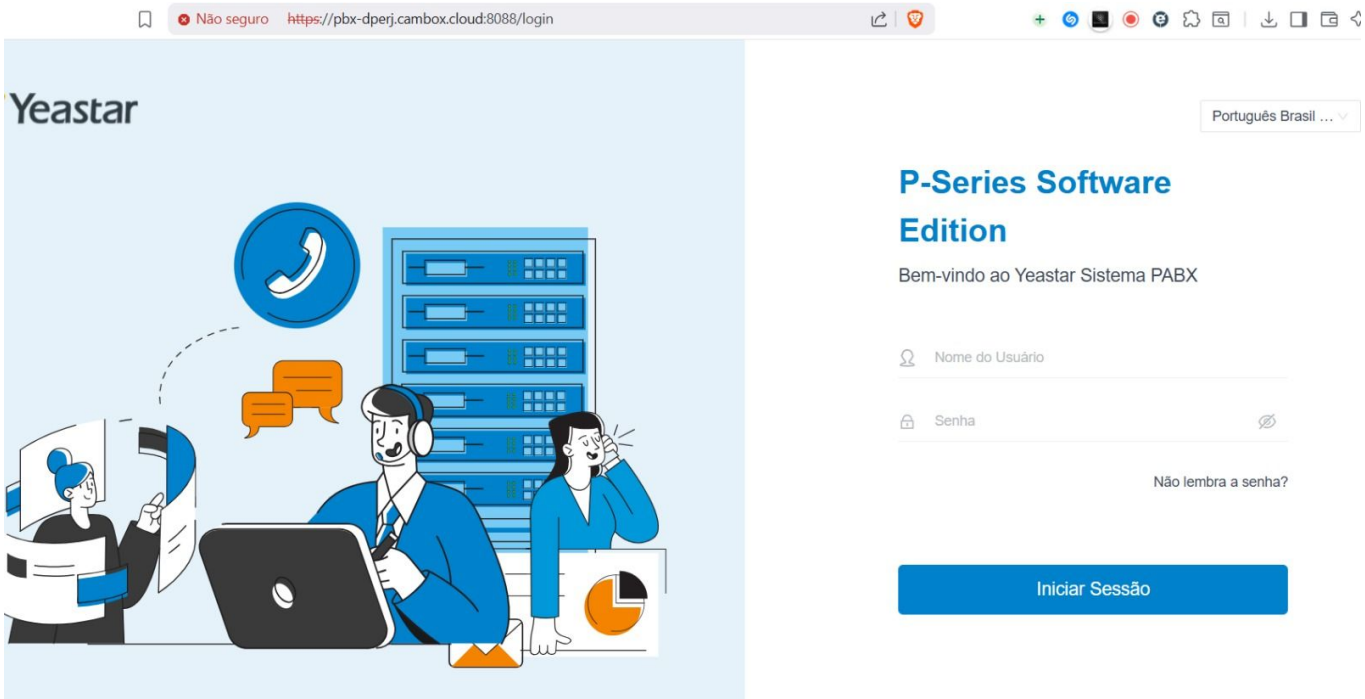
2.2 Compatibilidade (3 navegadores padrão de mercado)

Uso do Serviço com Firefox



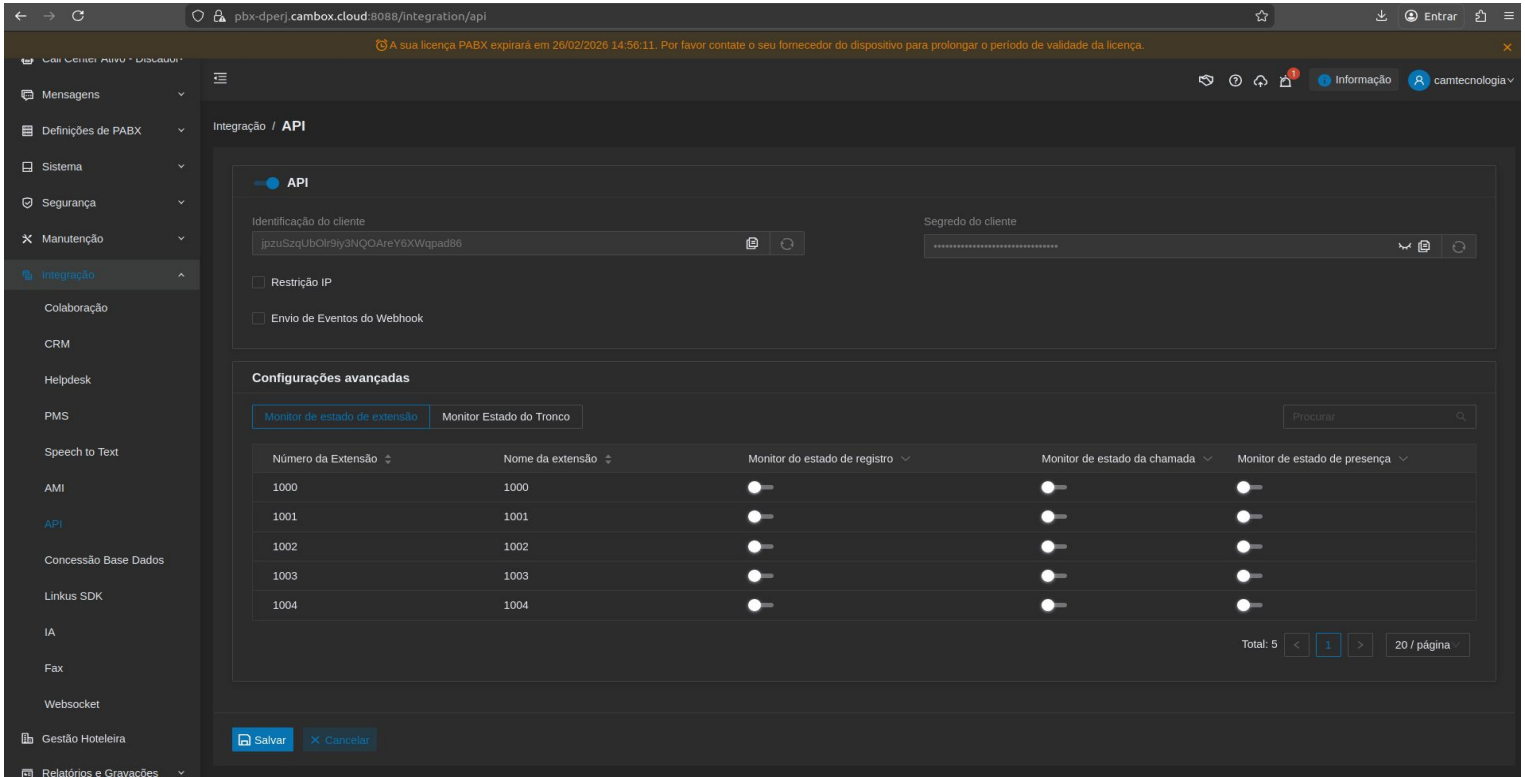
2.2 Compatibilidade (3 navegadores padrão de mercado)

Uso do Serviço com Edge



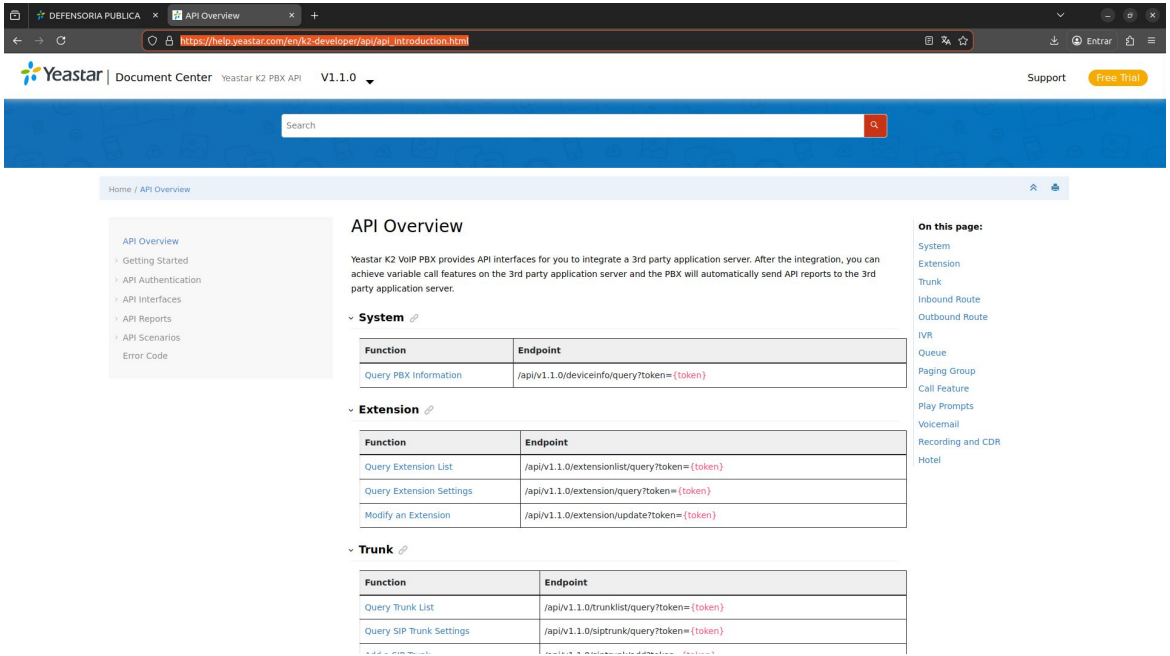
2.3 Avaliação da API

Administração da API



2.3 Avaliação da API

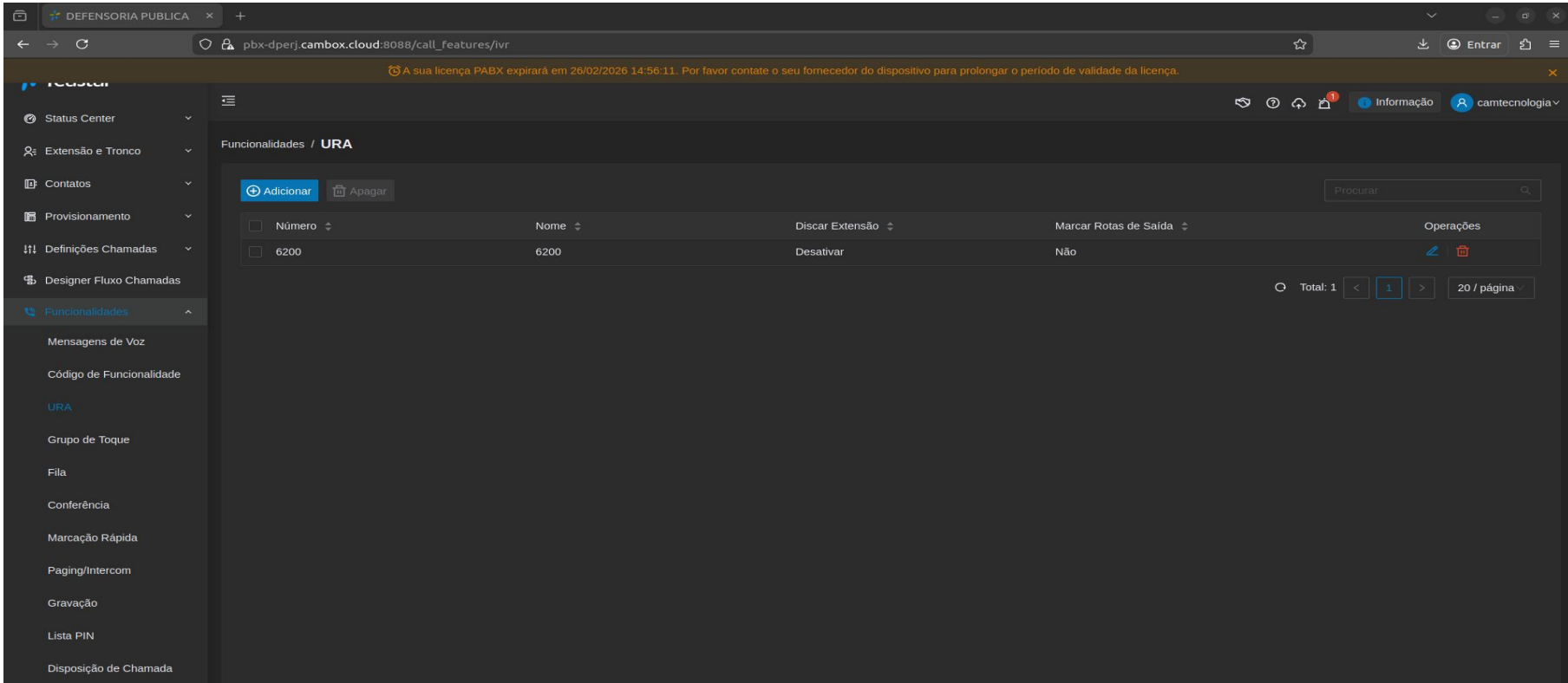
Documentação da API



https://help.yeastar.com/en/k2-developer/api/api_introduction.html

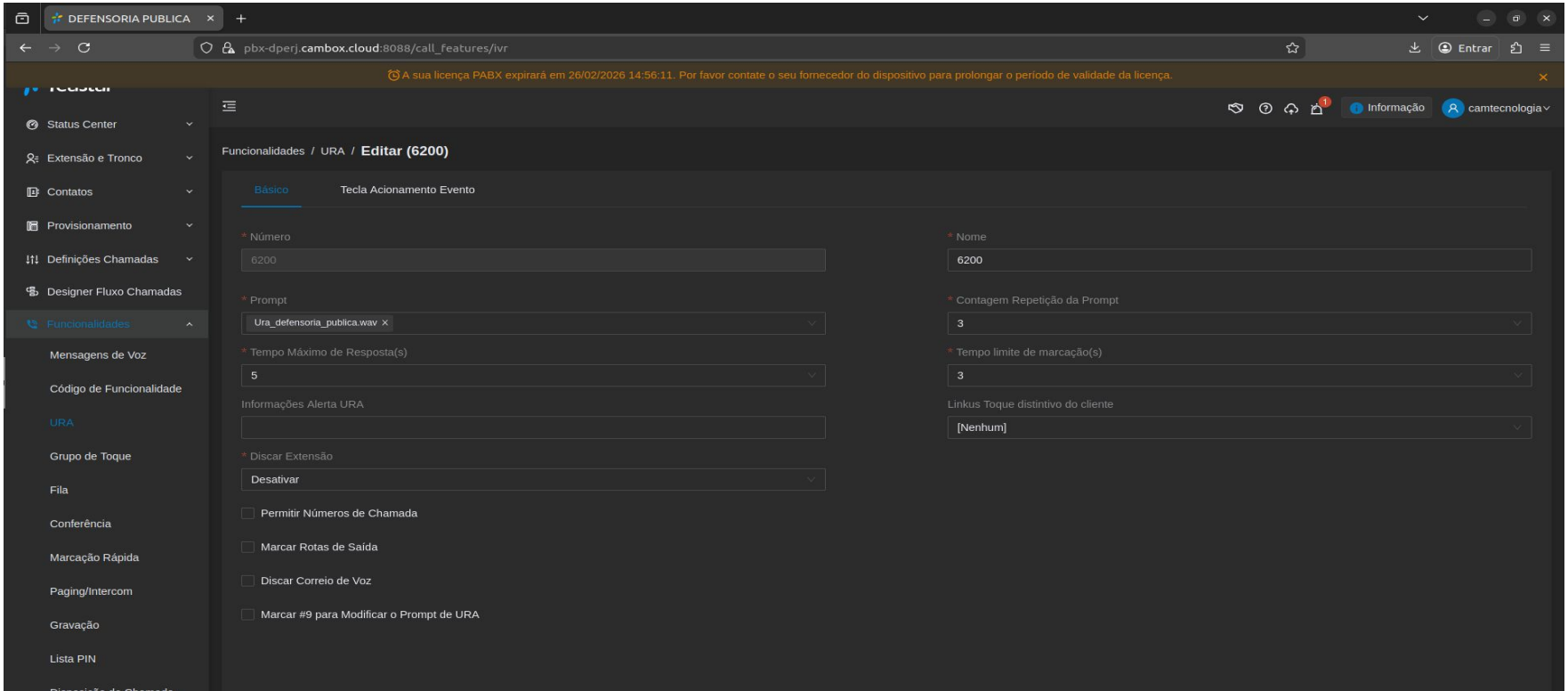
2.4 Avaliação da URA

Listagem das URAs



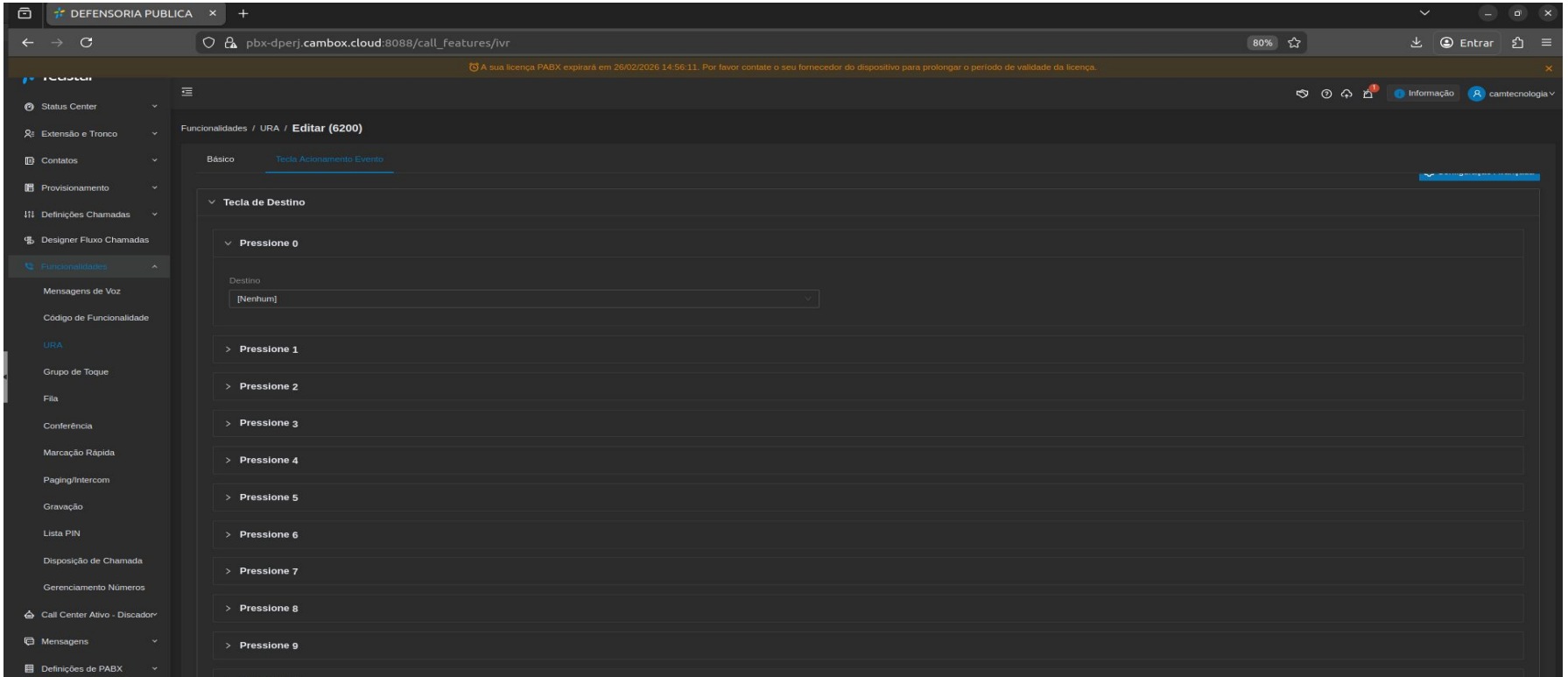
2.4 Avaliação da URA

Edição da URA



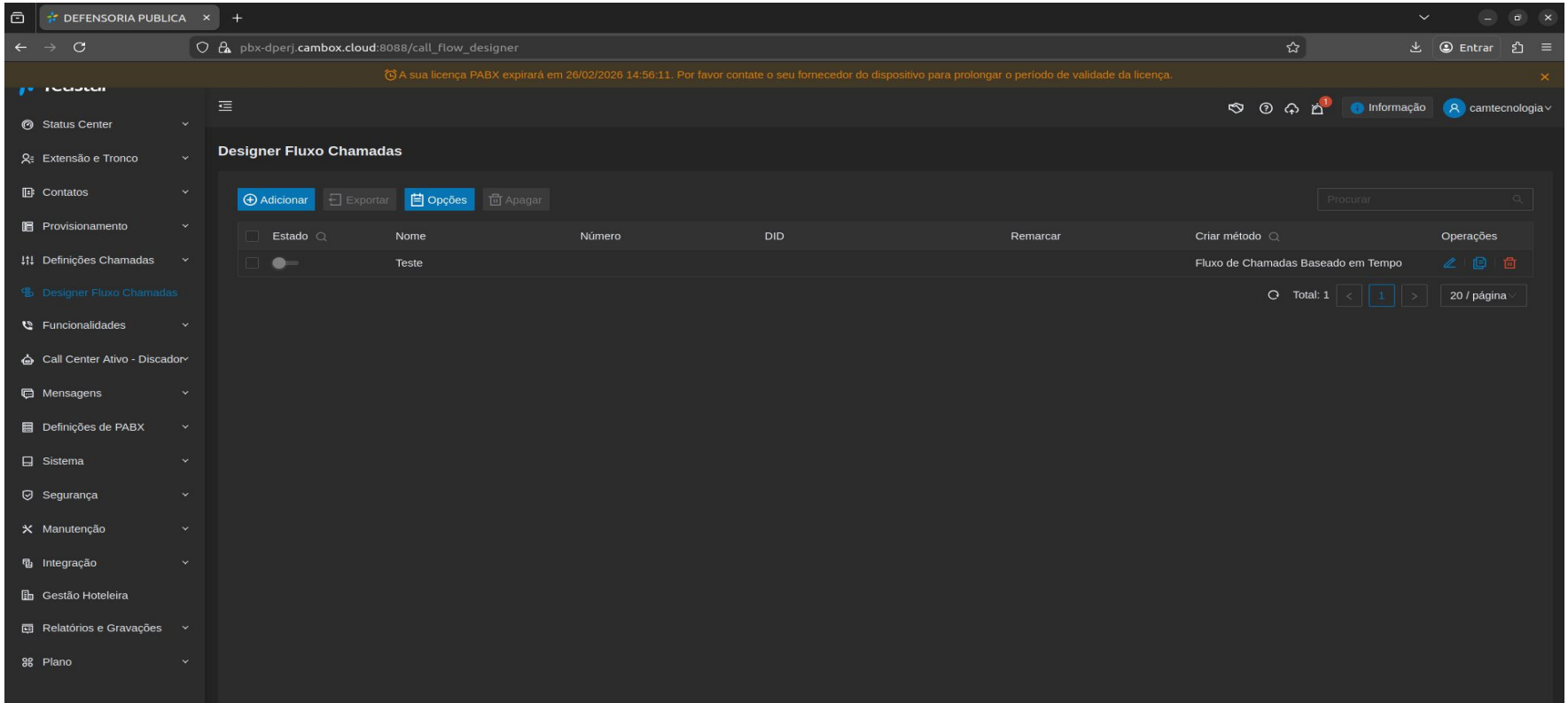
2.4 Avaliação da URA

Edição da URA (2)



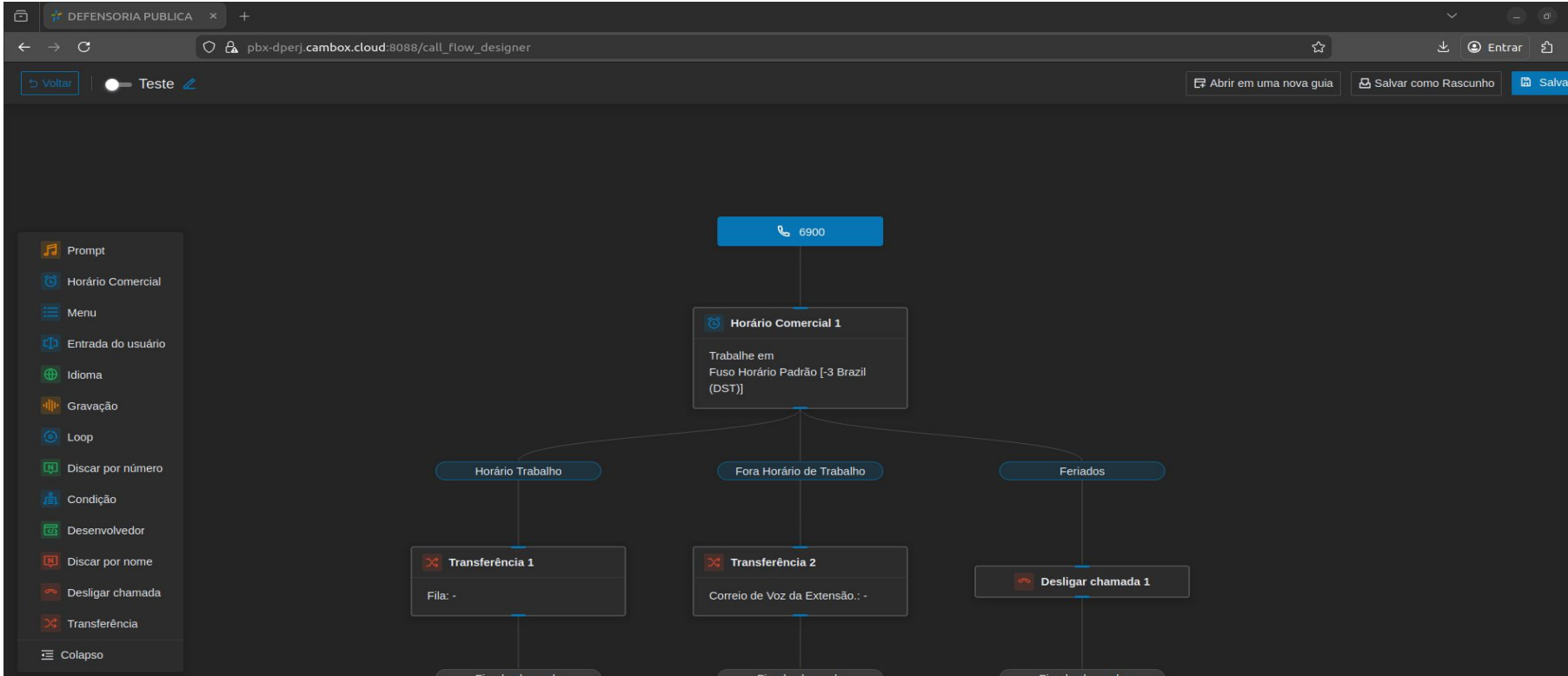
2.4 Avaliação da URA

Listar Designer de Chamadas



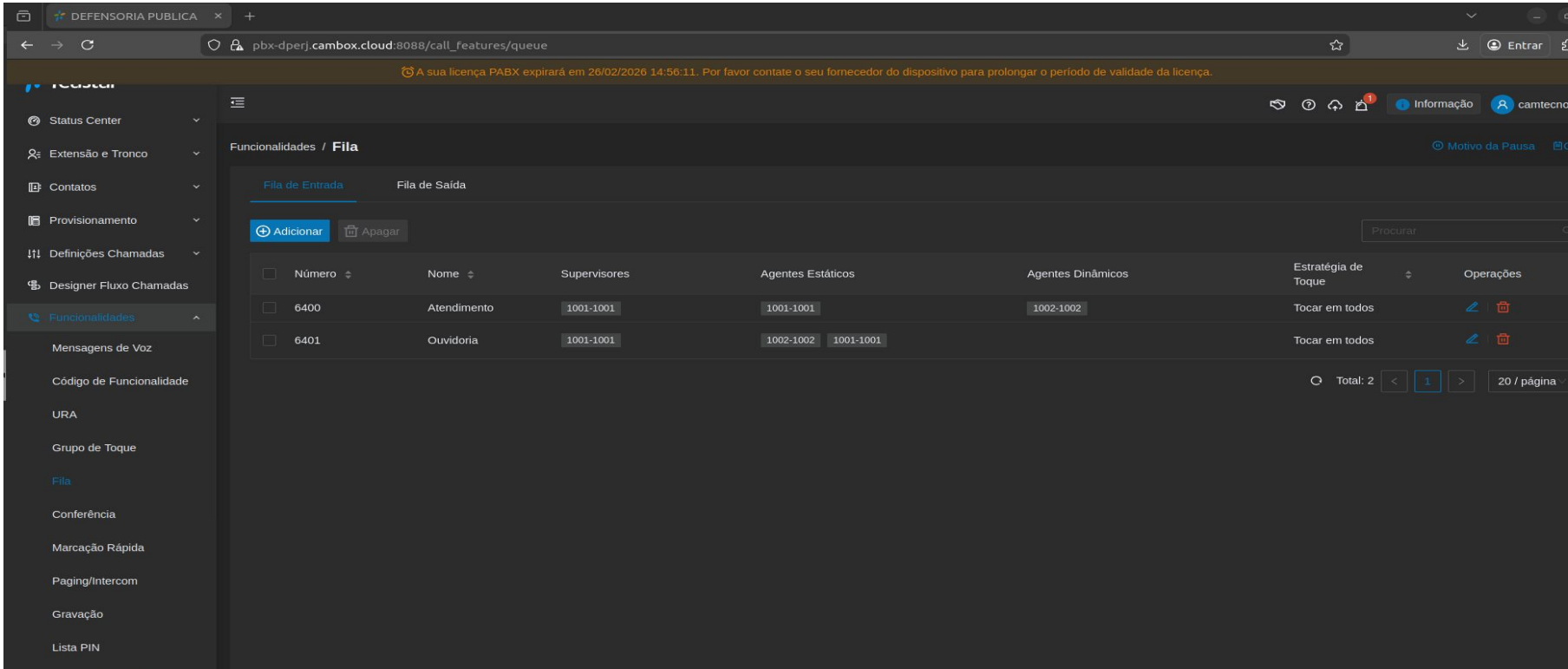
2.4 Avaliação da URA

Designer de Chamadas



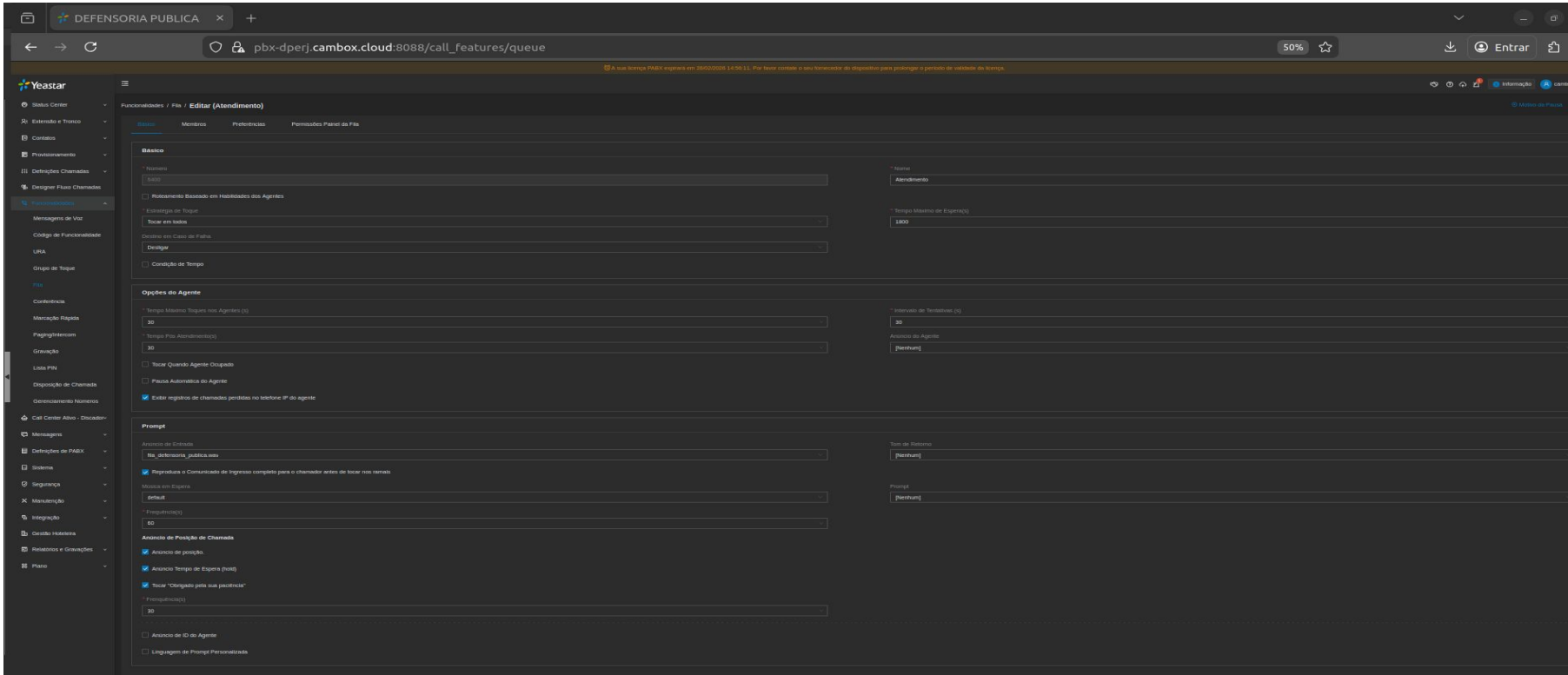
2.5 Avaliação da DAC e Filas

Listar Filas de Chamadas



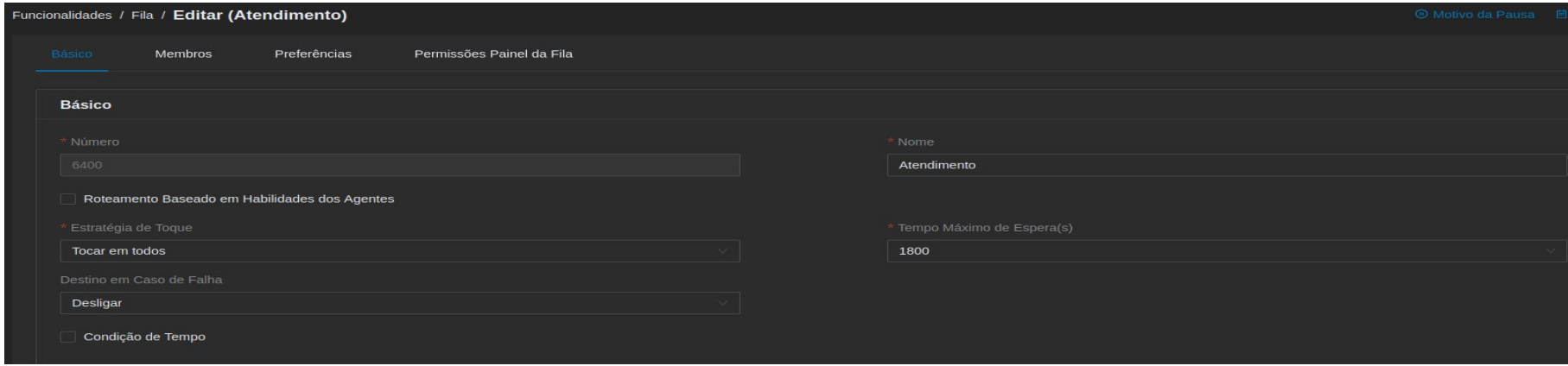
2.5 Avaliação da DAC e Filas

Editar Filas de Chamadas



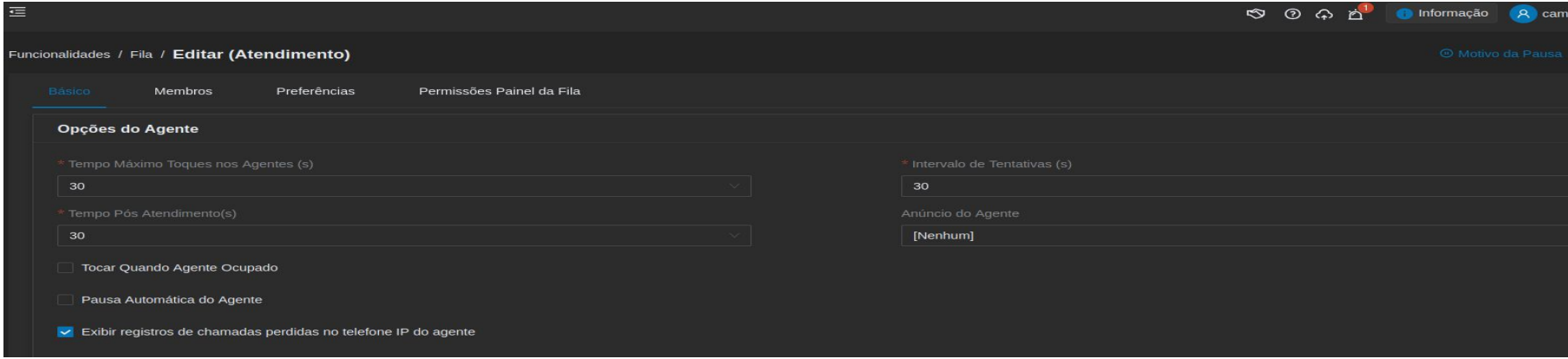
2.5 Avaliação da DAC e Filas

Editar Filas de Chamadas (2)



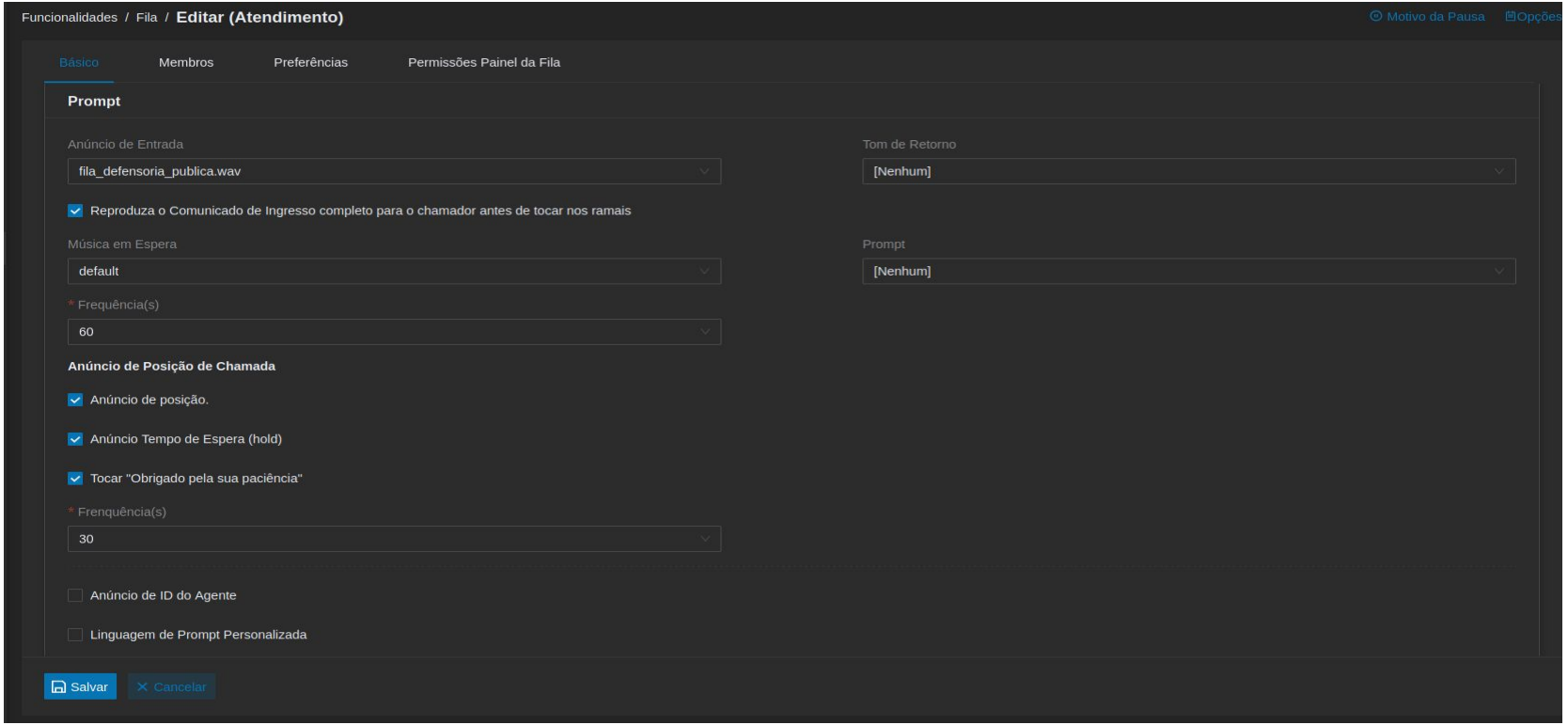
2.5 Avaliação da DAC e Filas

Editar Filas de Chamadas (3)



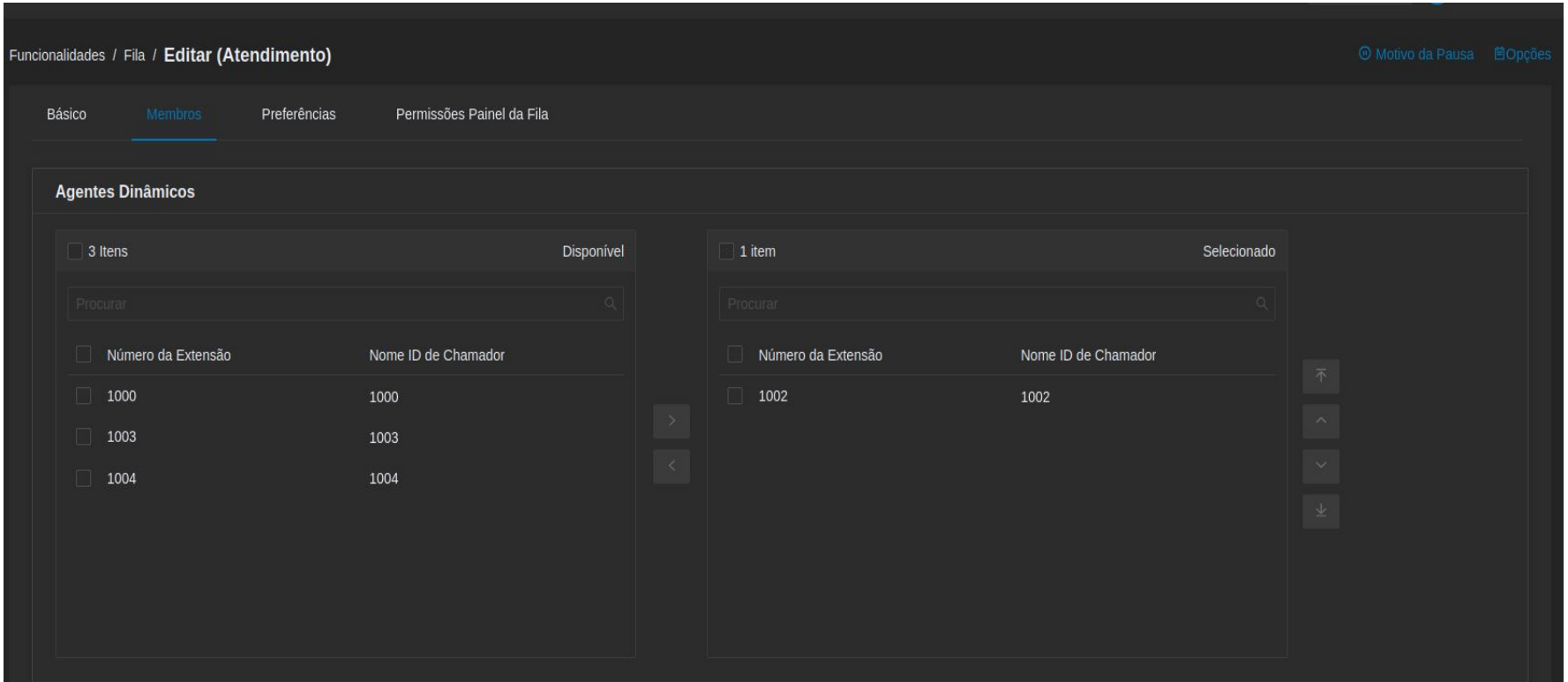
2.5 Avaliação da DAC e Filas

Editar Filas de Chamadas (4)



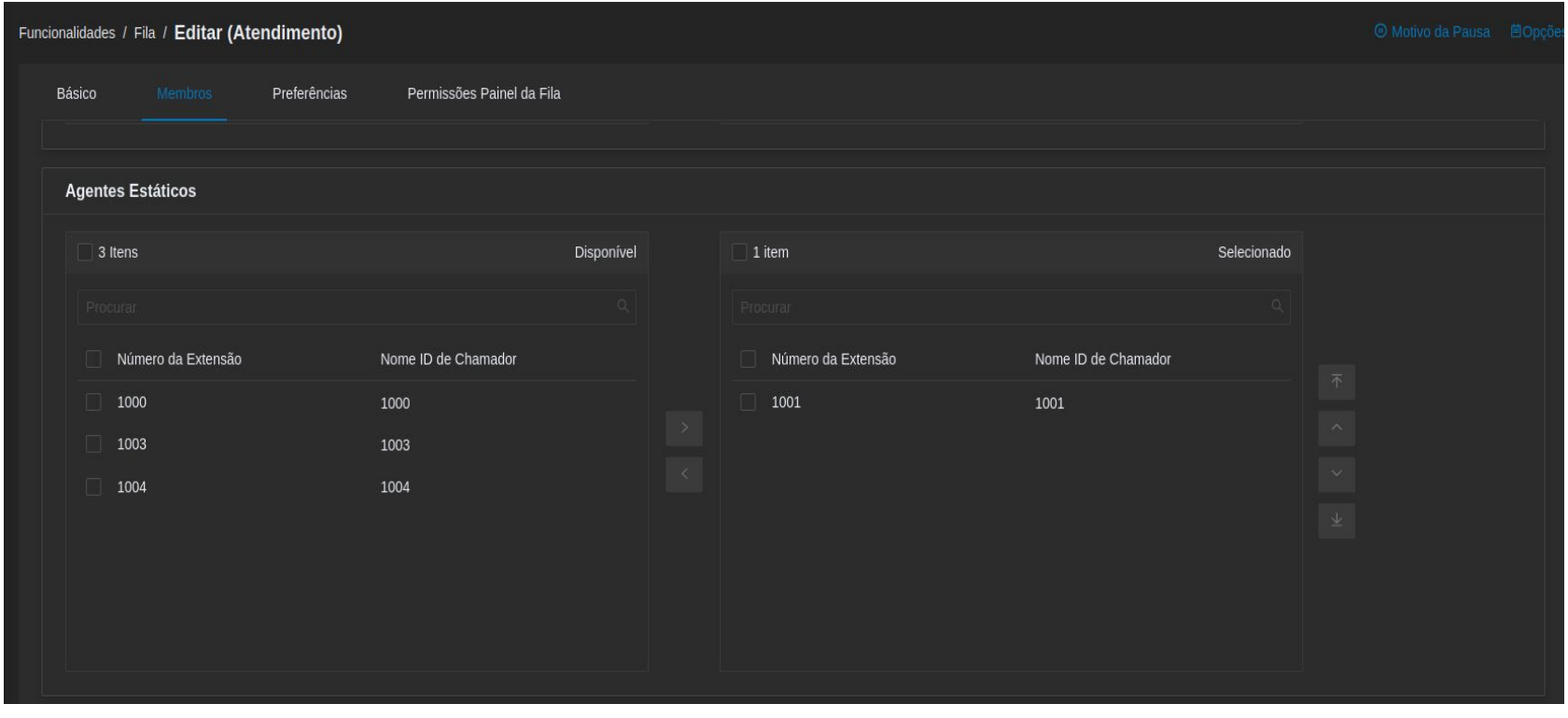
2.5 Avaliação da DAC e Filas

Operadores Dinâmicos



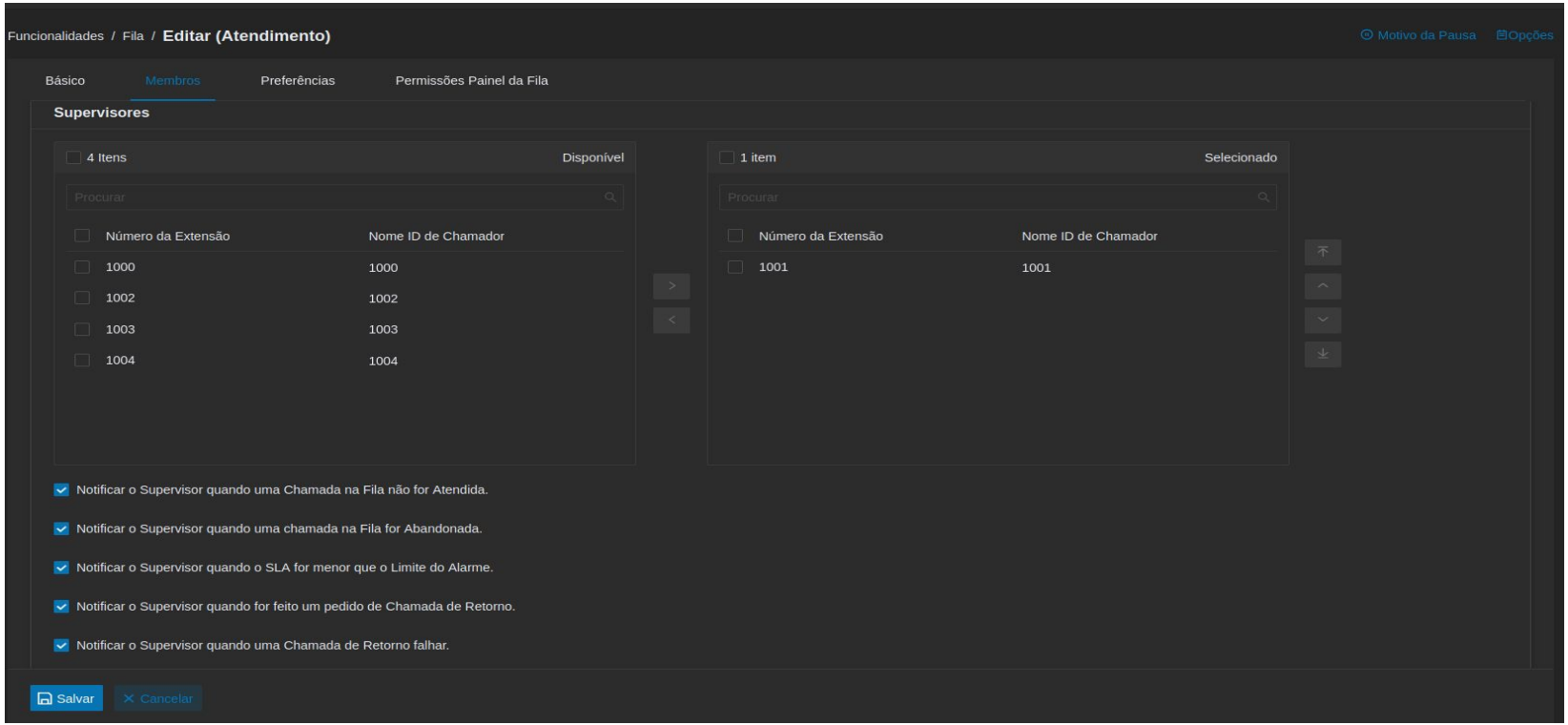
2.5 Avaliação da DAC e Filas

Operadores Estáticos



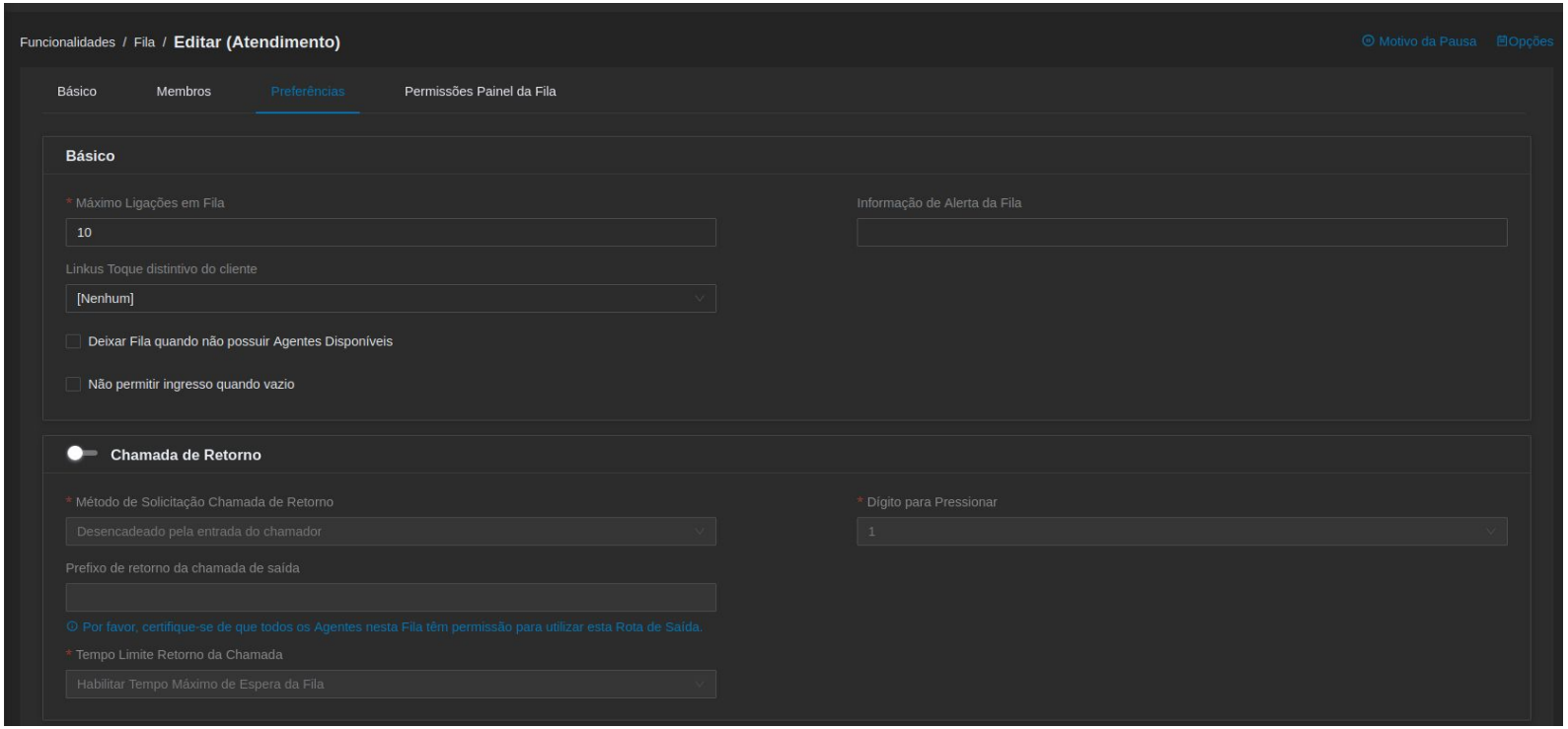
2.5 Avaliação da DAC e Filas

Supervisores e Notificações



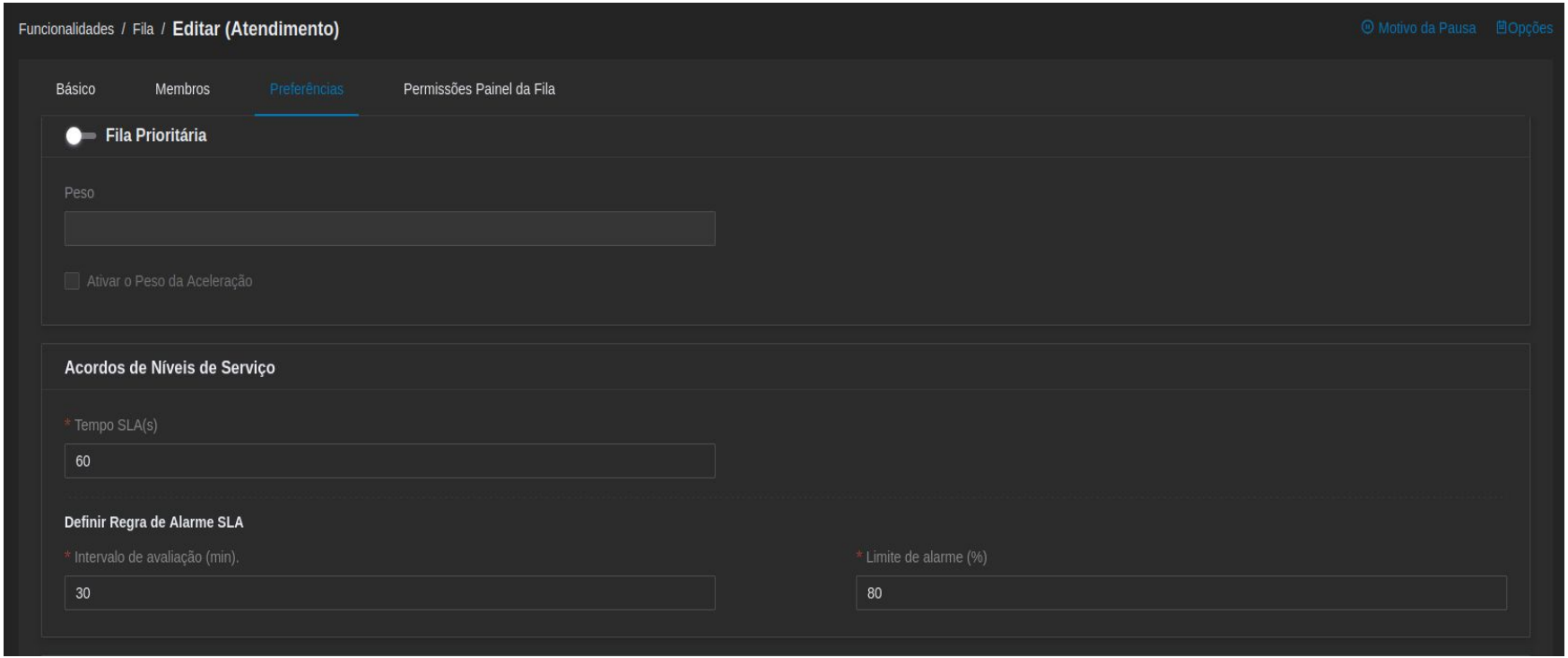
2.5 Avaliação da DAC e Filas

Preferências do Atendimento



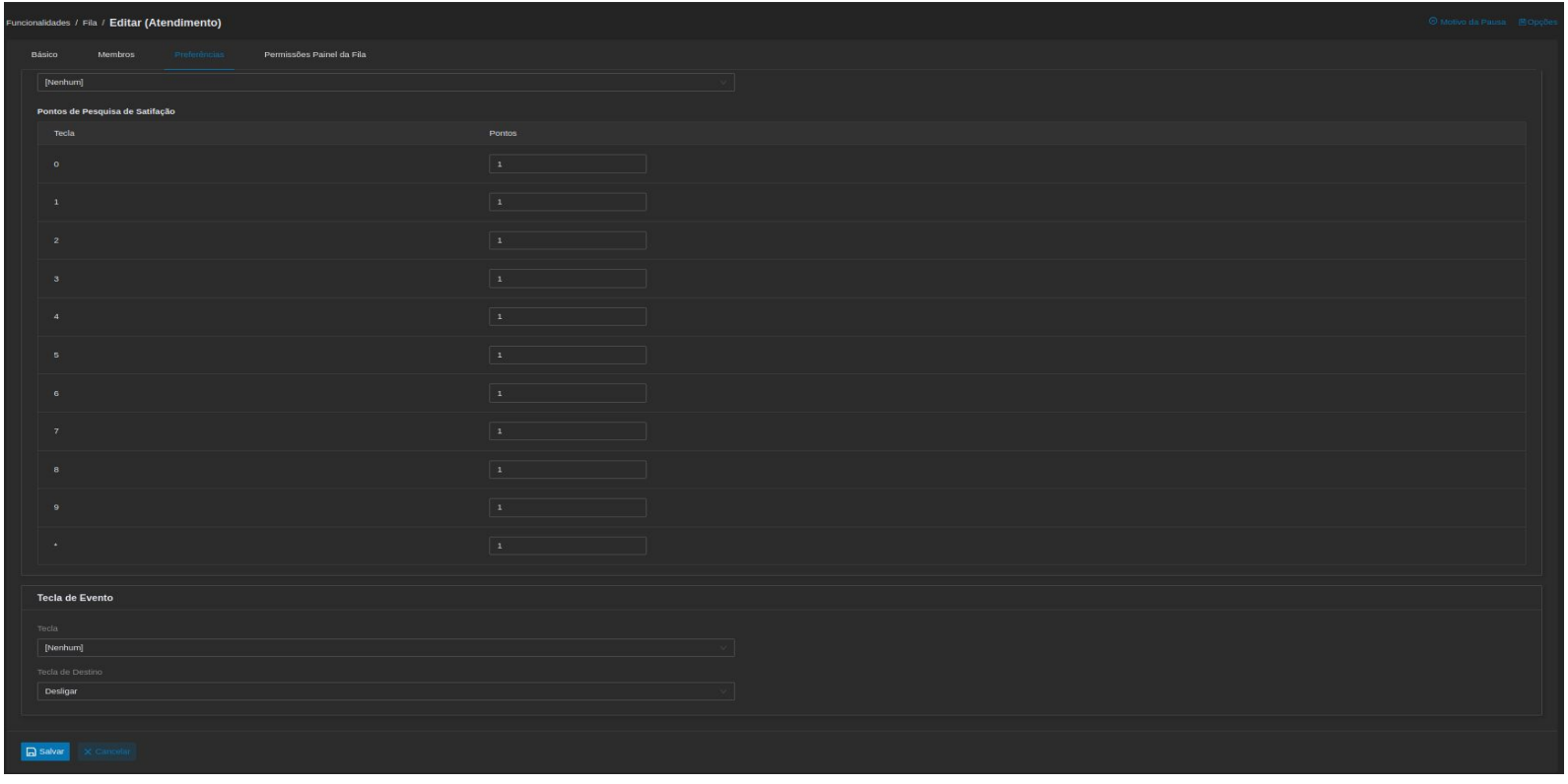
2.5 Avaliação da DAC e Filas

SLA - Nível de Serviço

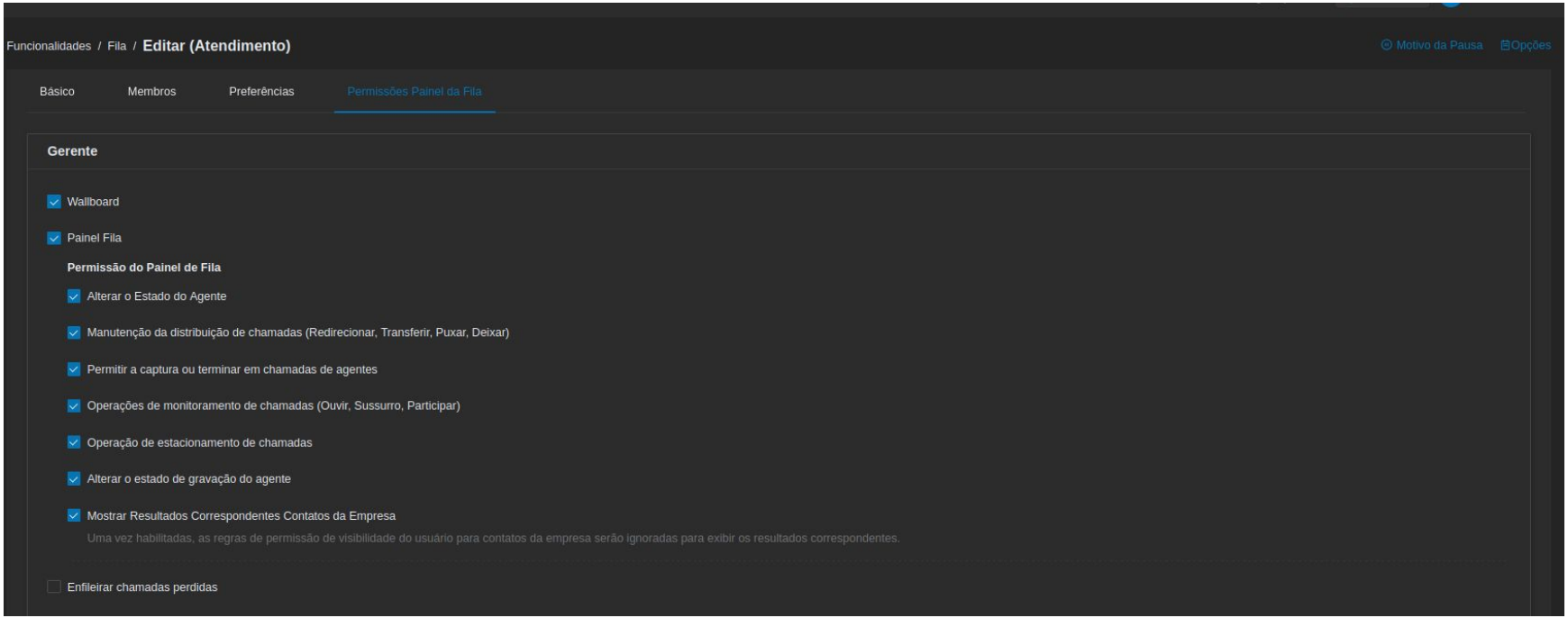


2.5 Avaliação da DAC e Filas

Pesquisa de Satisfação



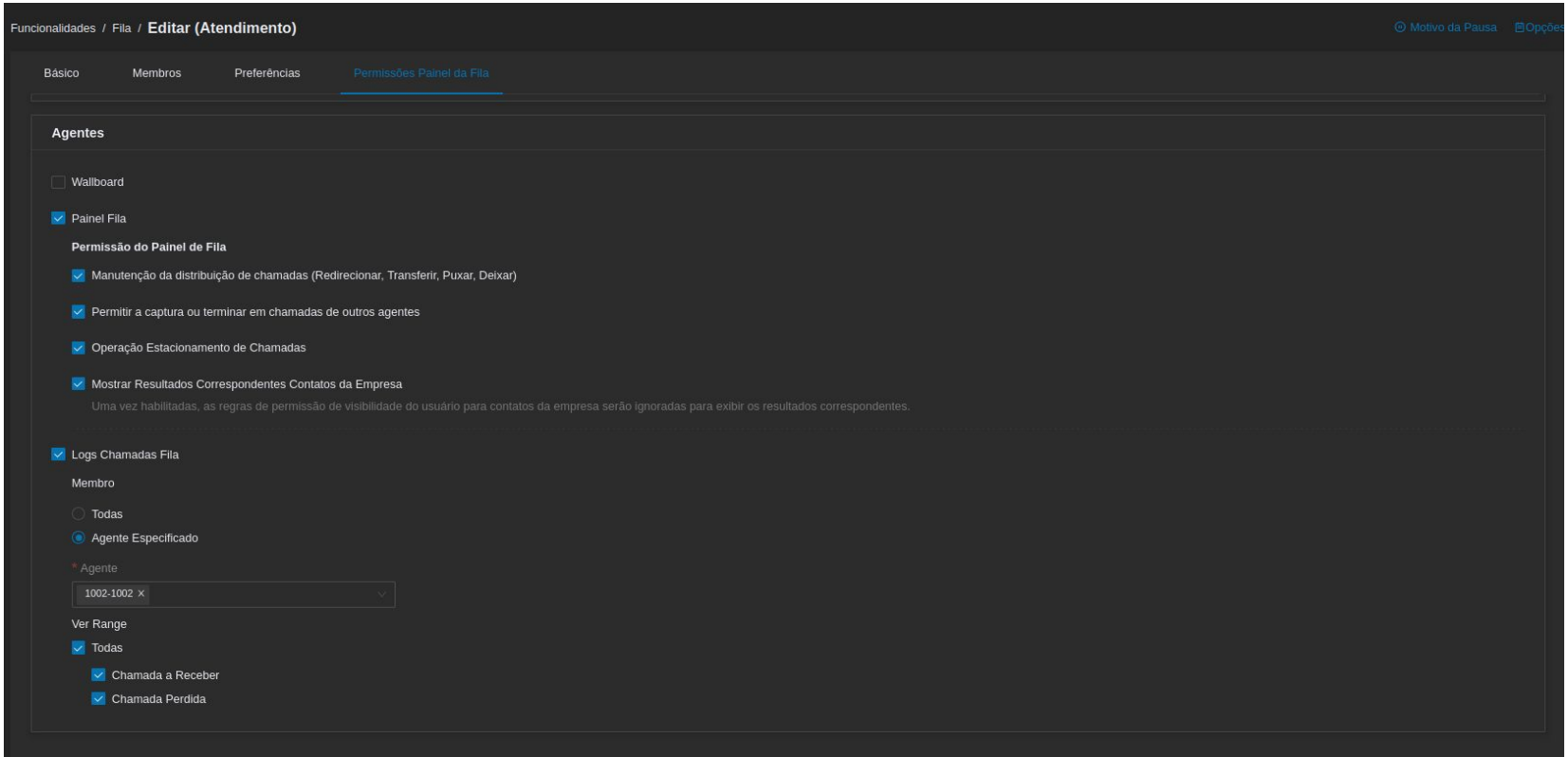
2.5 Avaliação da DAC e Filas



Permissões

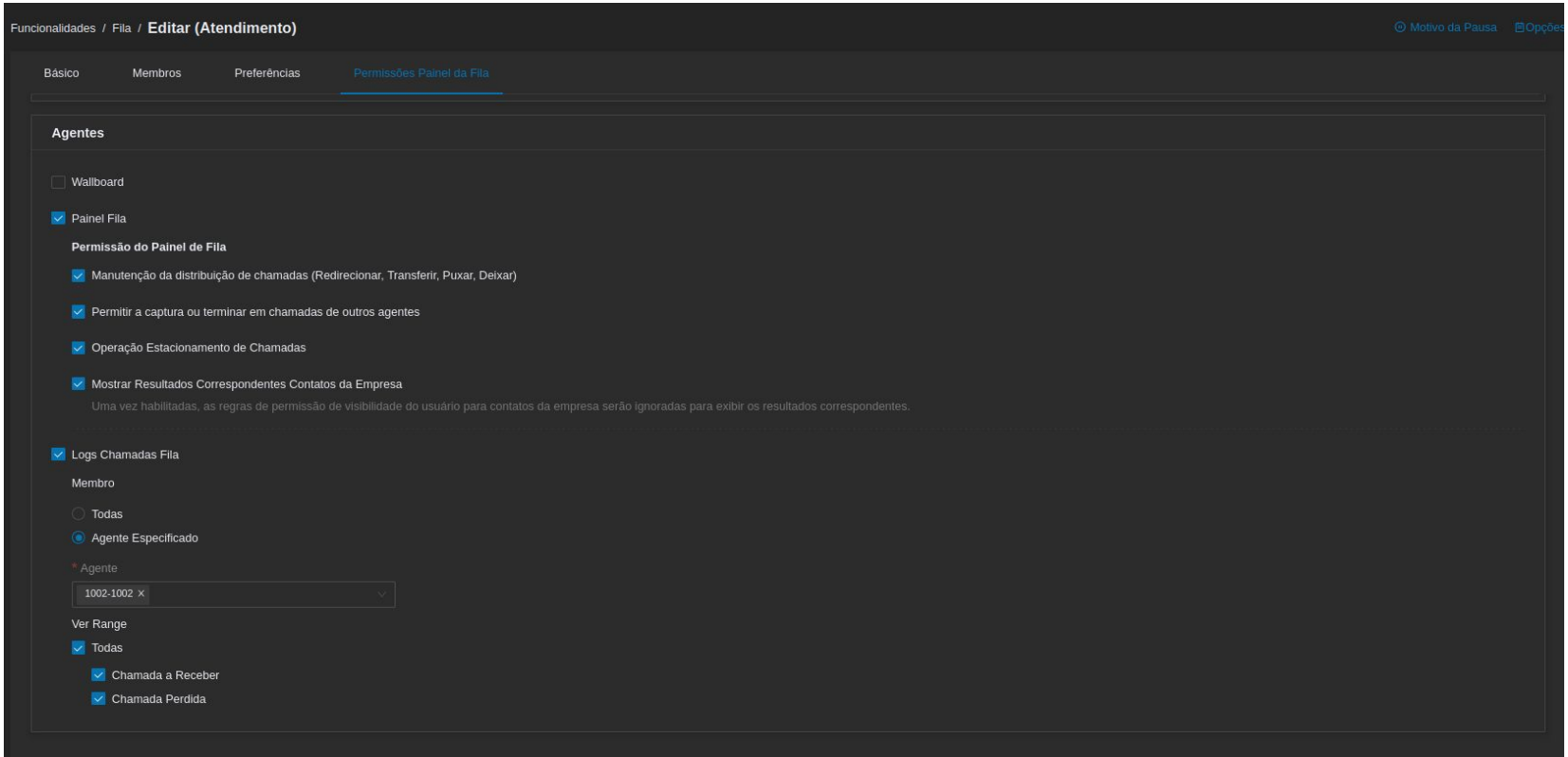
2.5 Avaliação da DAC e Filas

Permissões (2)

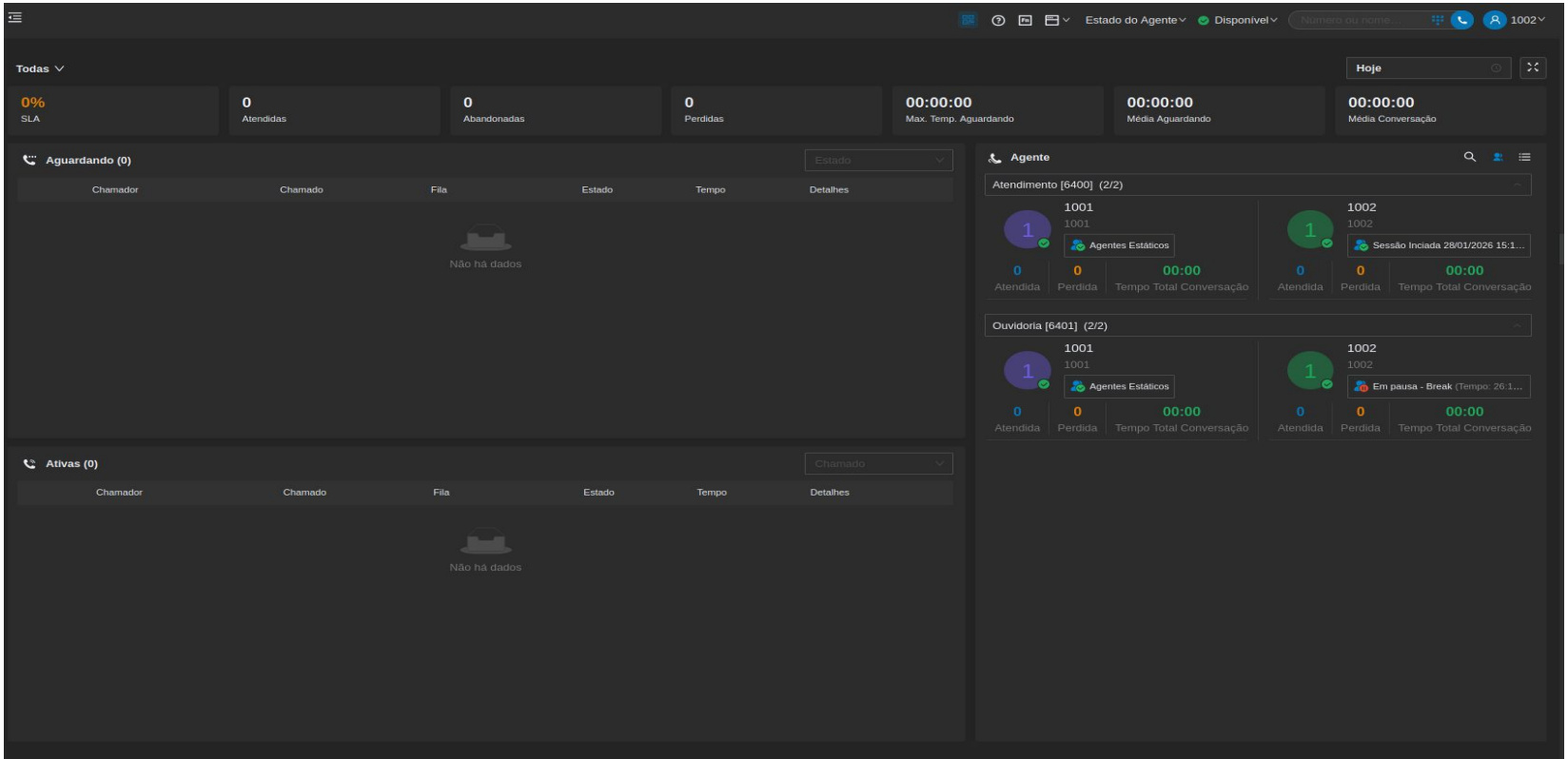


2.5 Avaliação da DAC e Filas

Permissões (2)



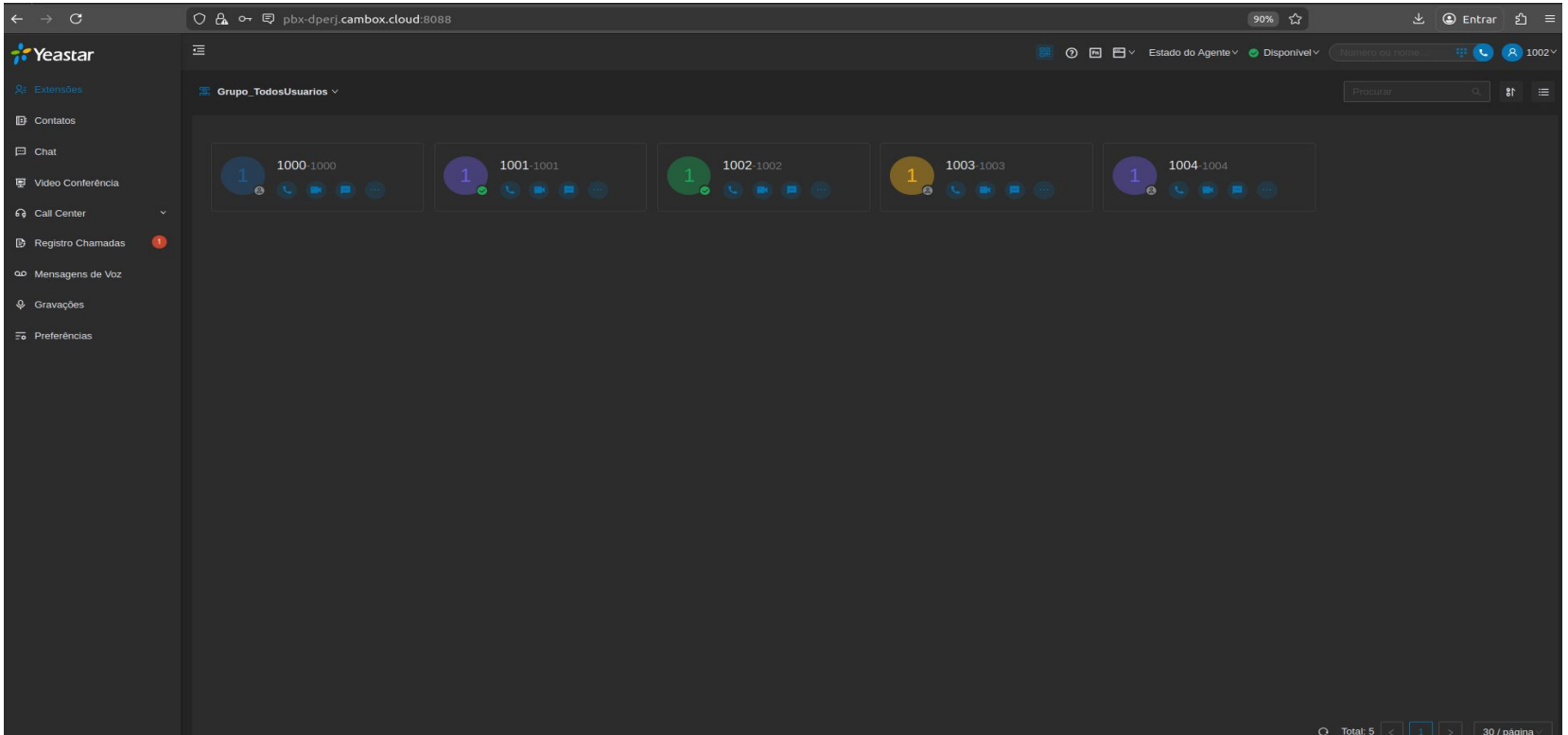
2.5 Avaliação da DAC e Filas



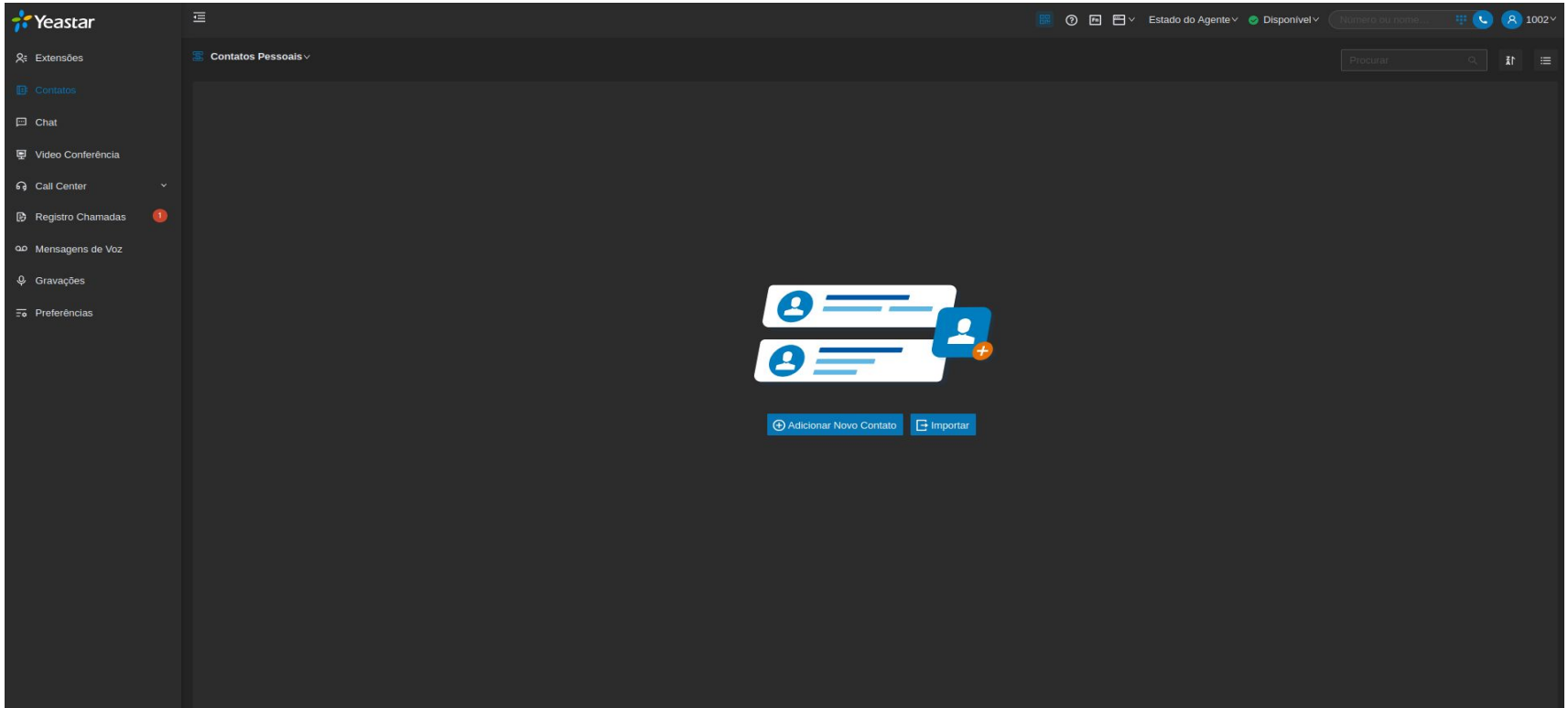
Operação

2.6 Avaliação do Ambiente do Atendente

Tela de Início



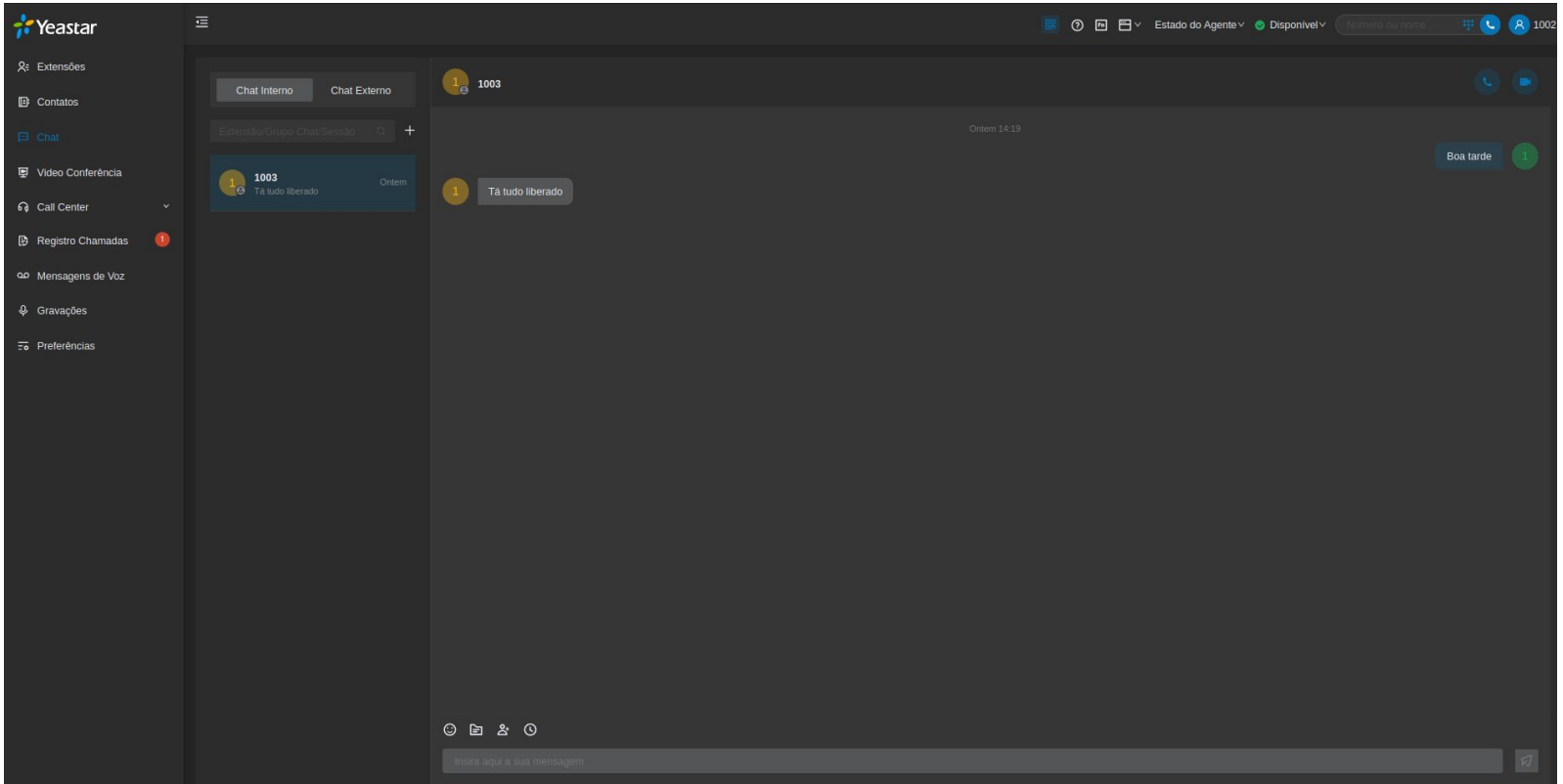
2.6 Avaliação do Ambiente do Atendente



Contatos

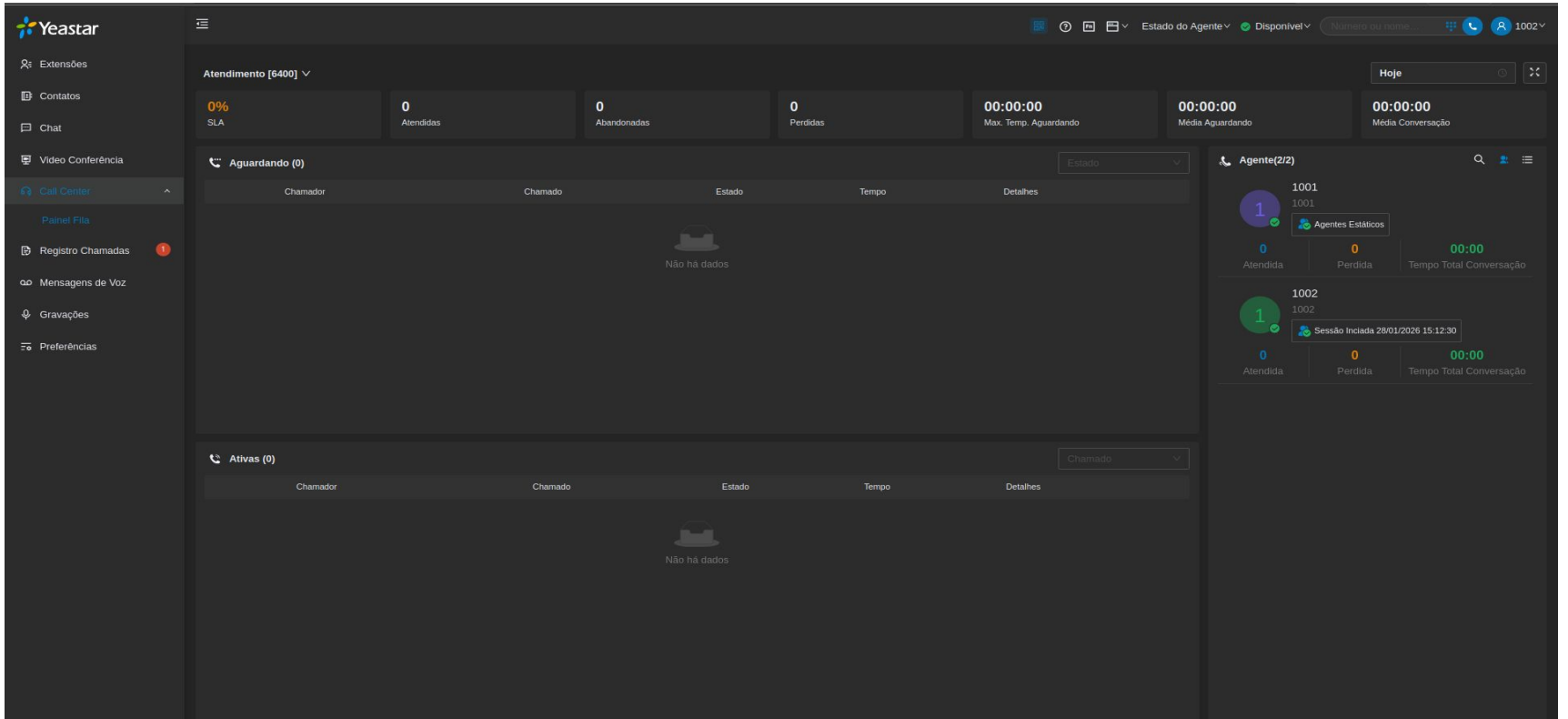
2.6 Avaliação do Ambiente do Atendente

Chat (Interno e Externo)



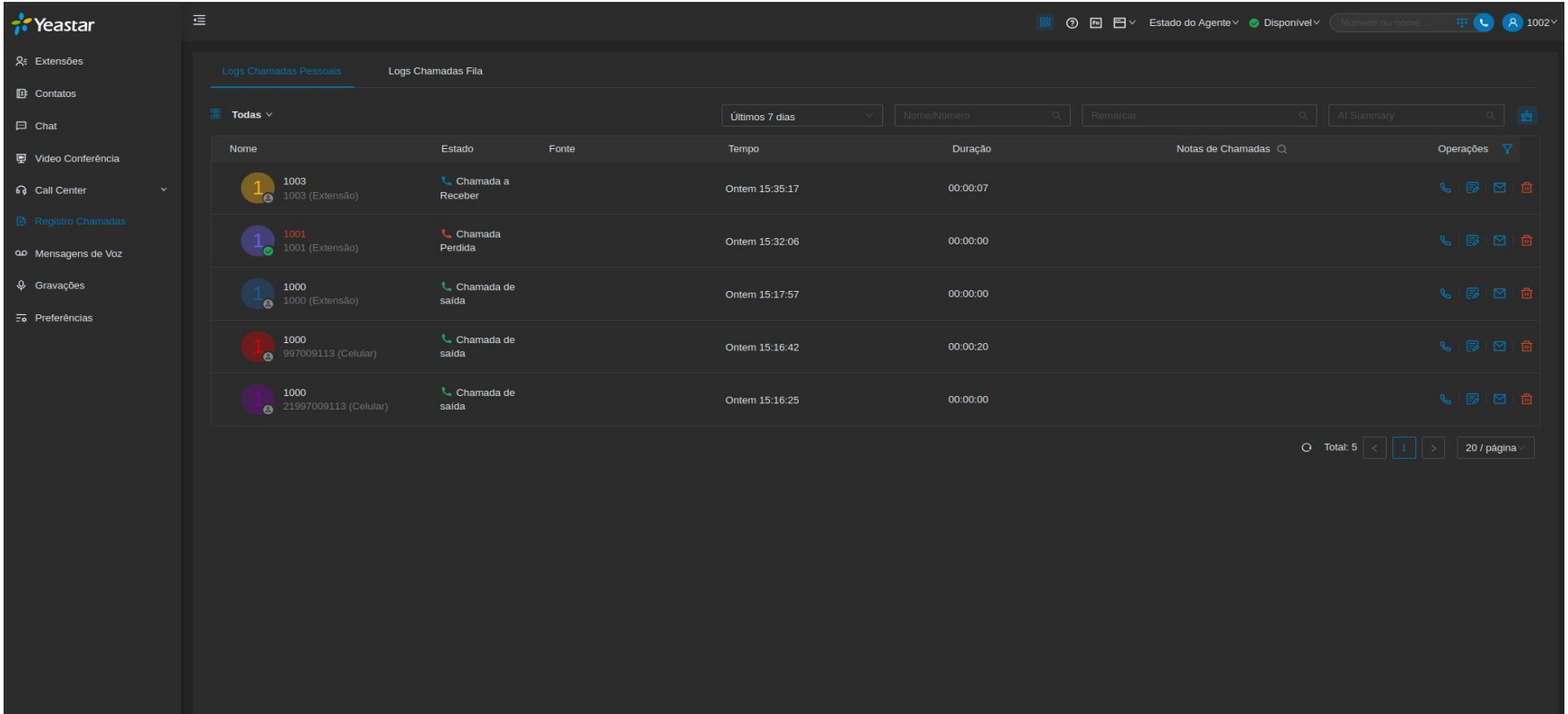
2.6 Avaliação do Ambiente do Atendente

Operação da Fila



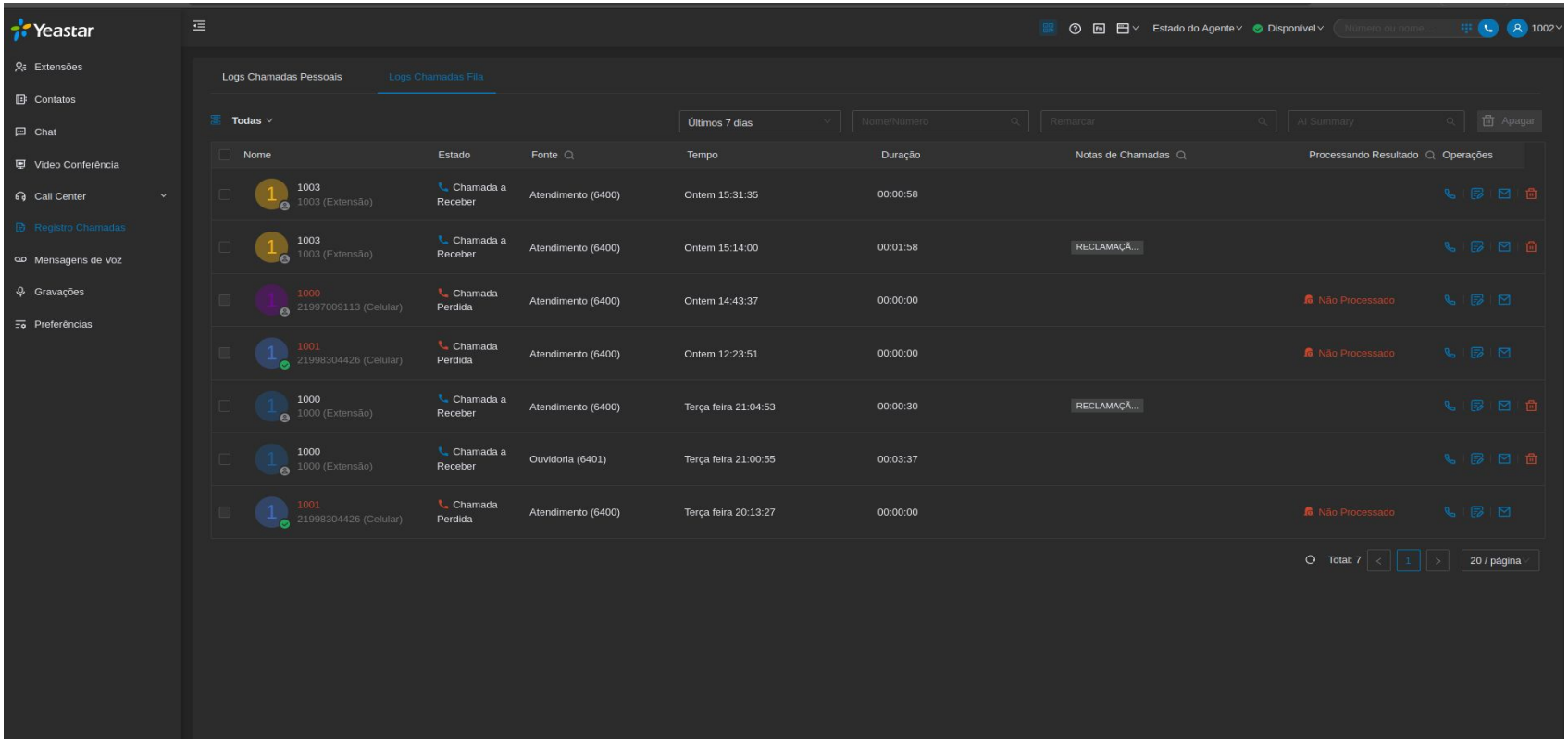
2.6 Avaliação do Ambiente do Atendente

Registros de Chamadas



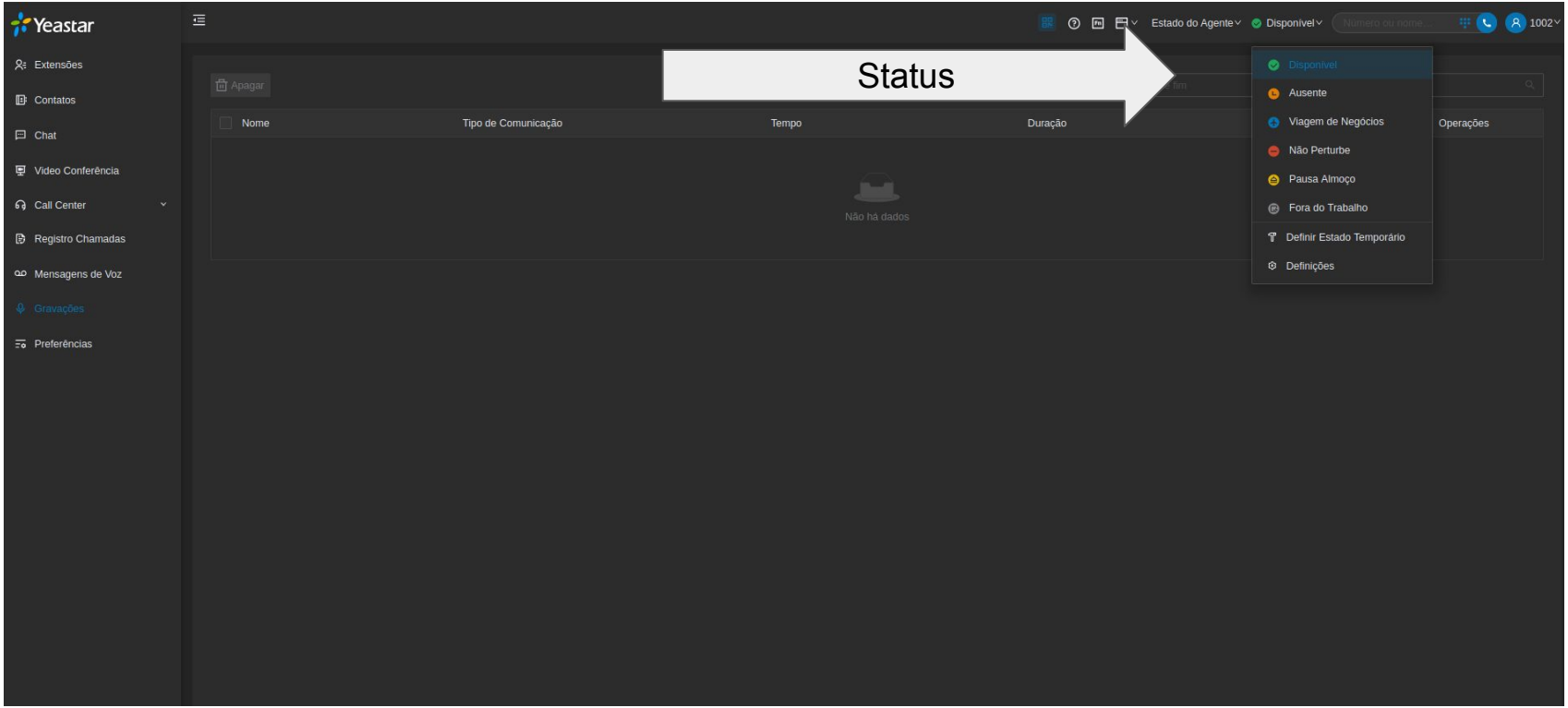
2.6 Avaliação do Ambiente do Atendente

Registros de Atendimento Fila



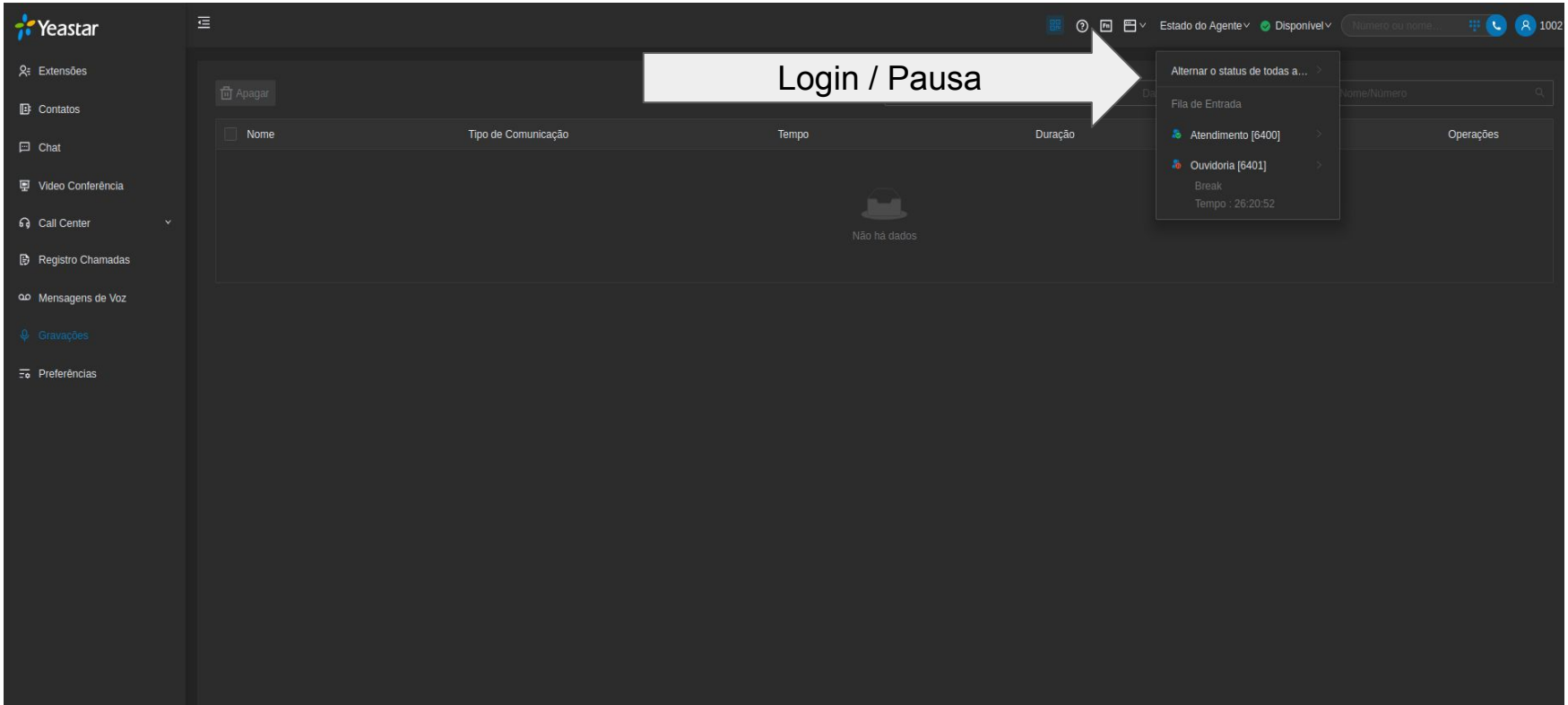
2.6 Avaliação do Ambiente do Atendente

Administração de Status

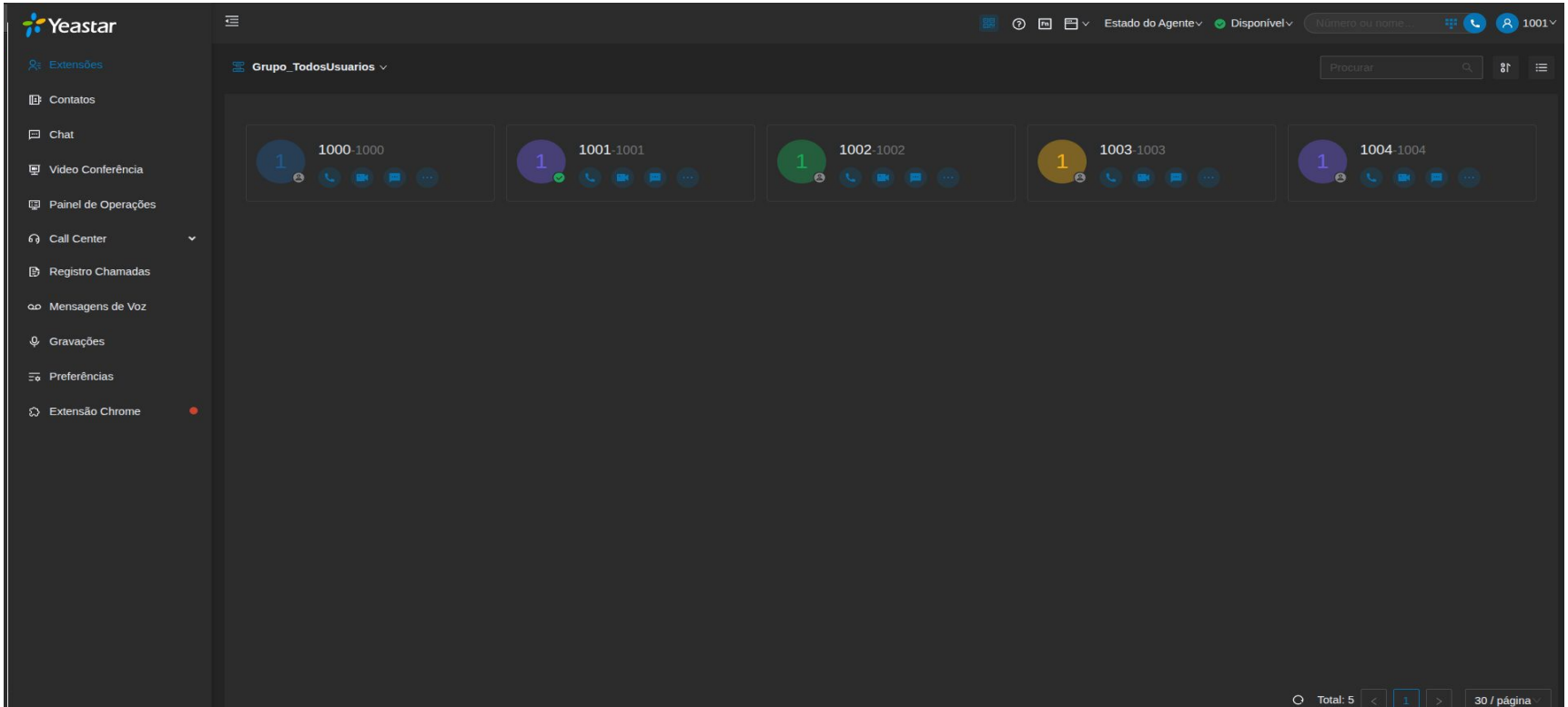


2.6 Avaliação do Ambiente do Atendente

Gestão de Status em Fila

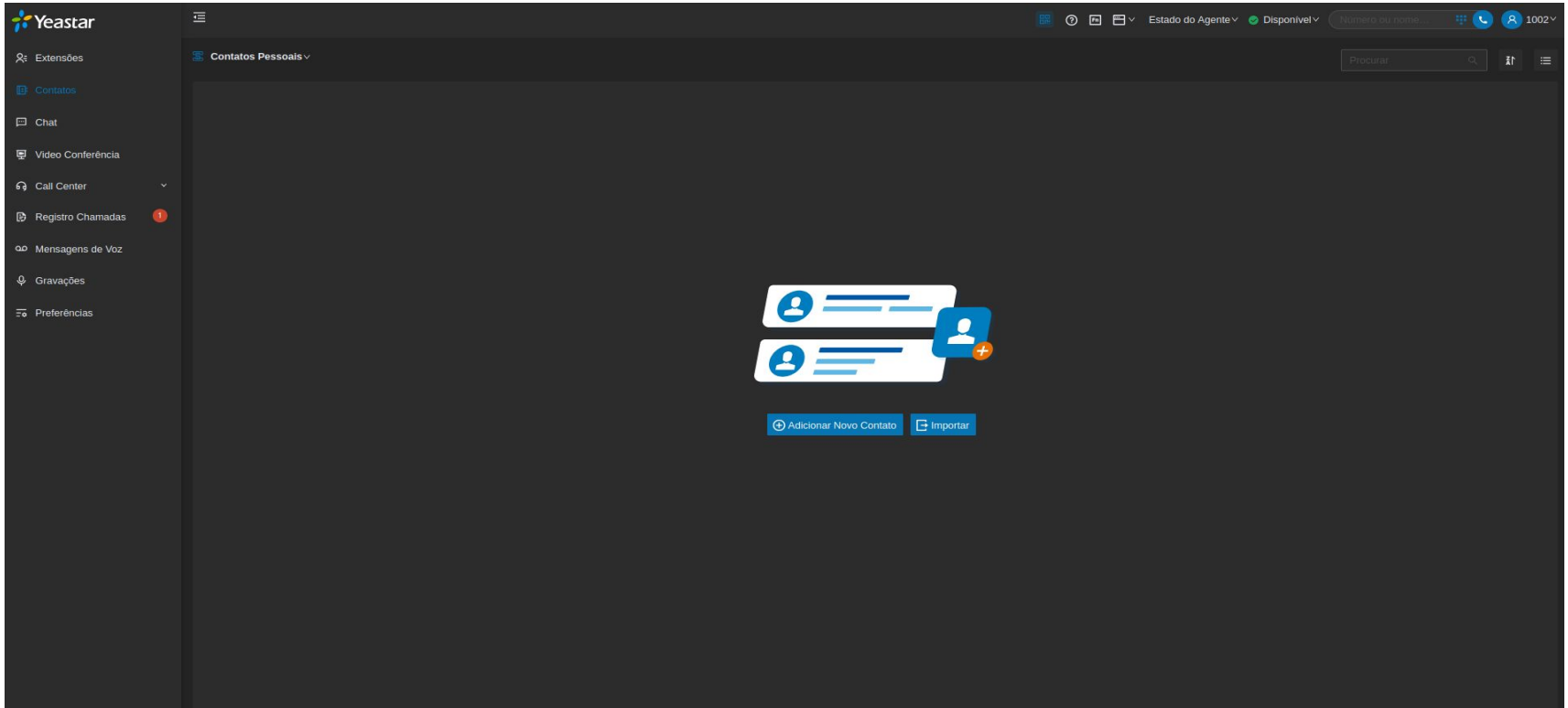


2.7 Avaliação do Ambiente do Supervisor



Tela de Início

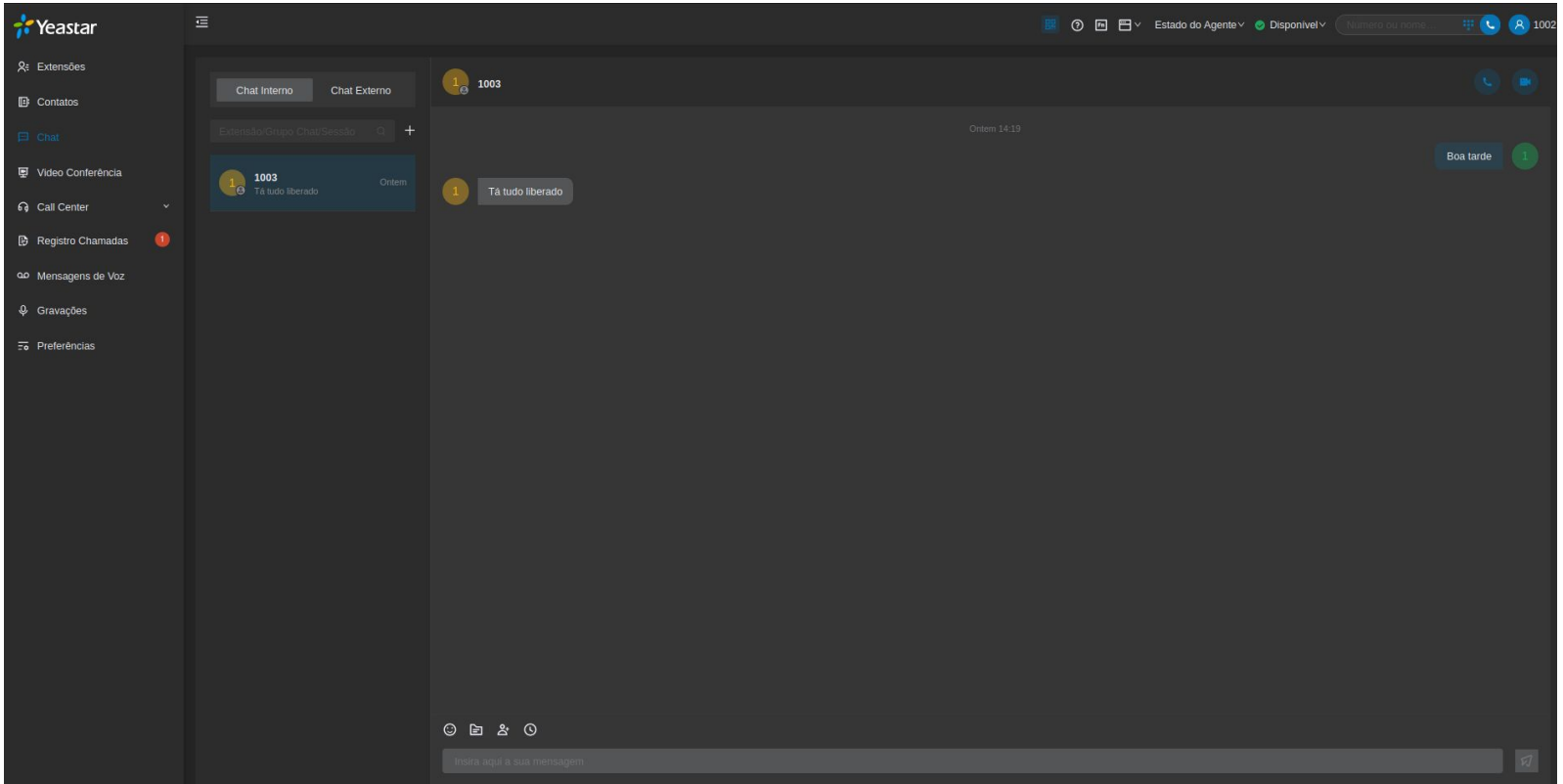
2.7 Avaliação do Ambiente do Supervisor



Contatos

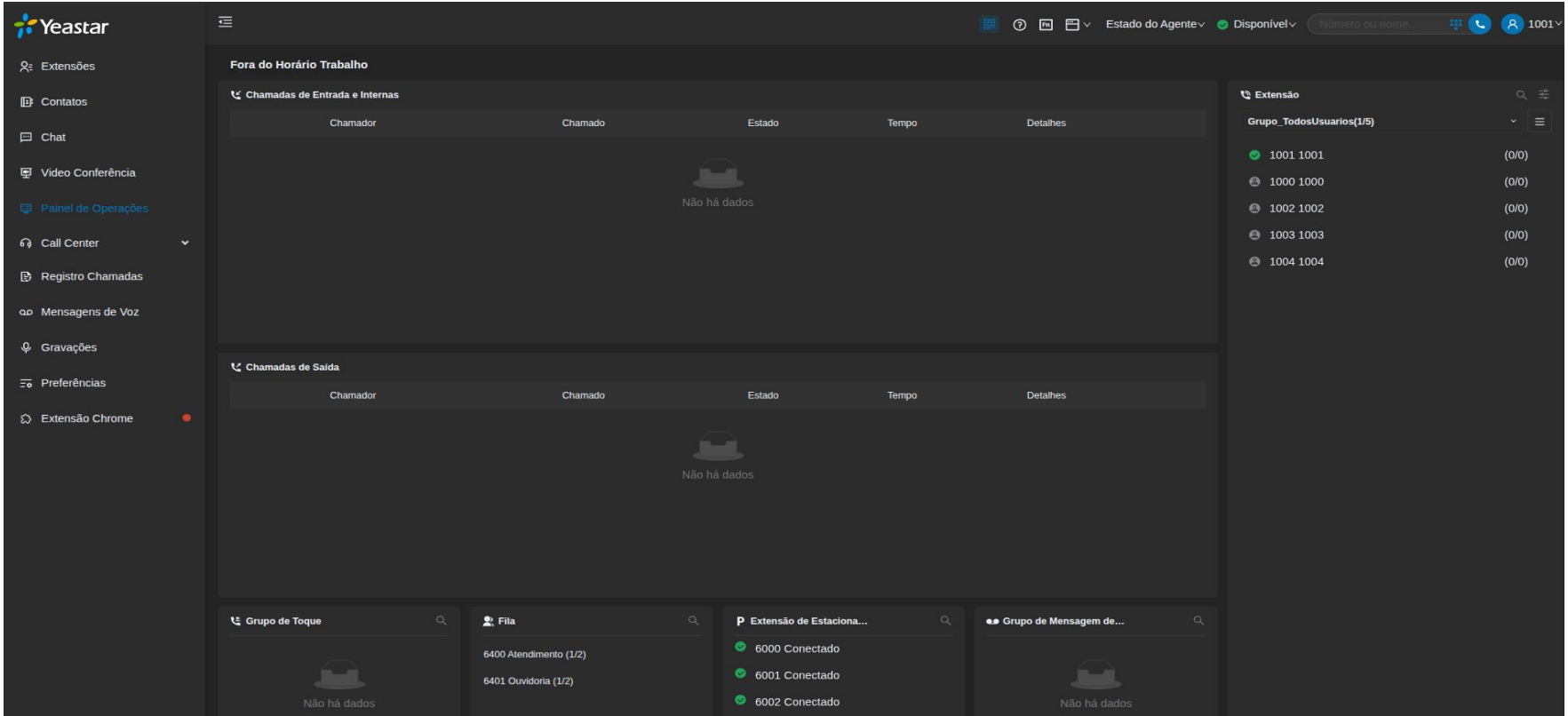
2.7 Avaliação do Ambiente do Supervisor

Chat (Interno e Externo)



2.7 Avaliação do Ambiente do Supervisor

Painel de Operações

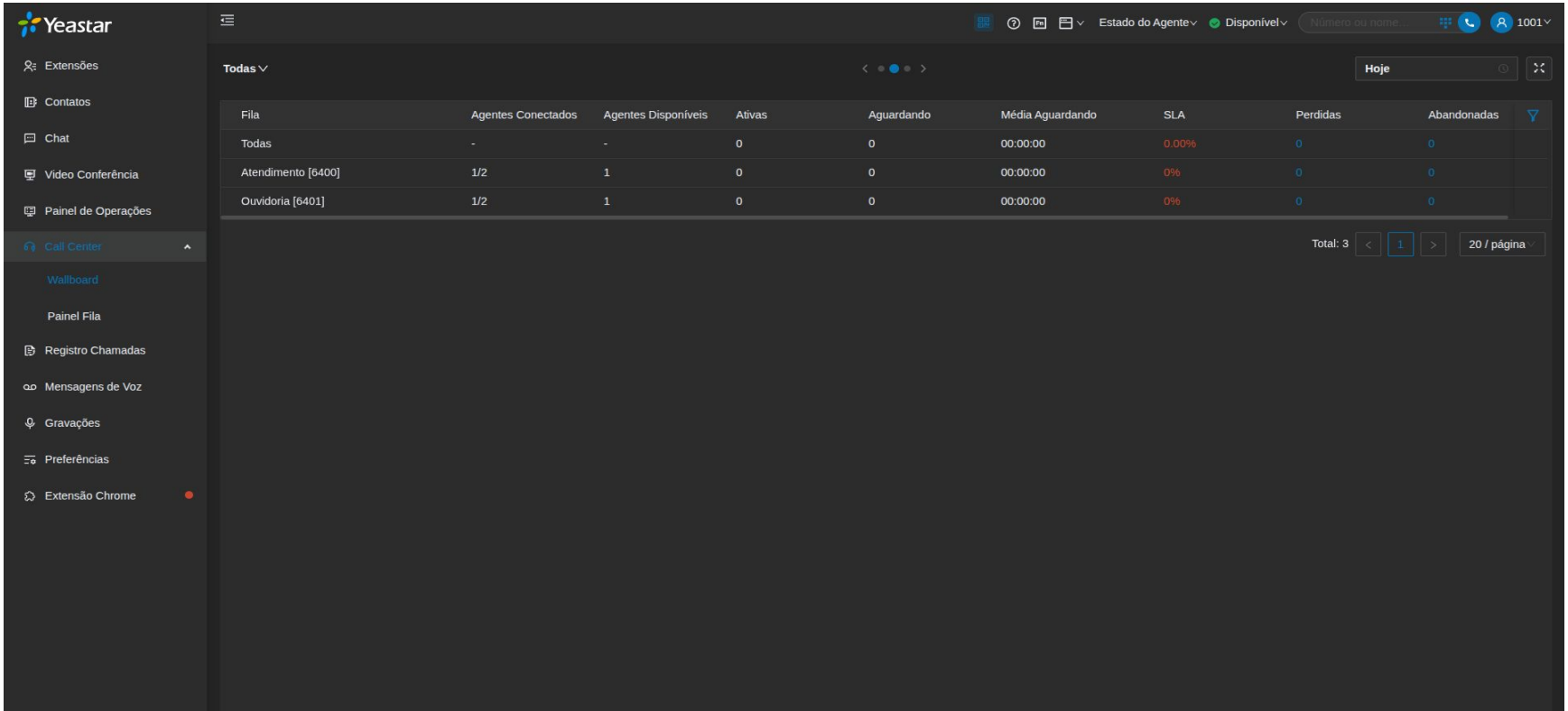


2.7 Avaliação do Ambiente do Supervisor

Dashboard

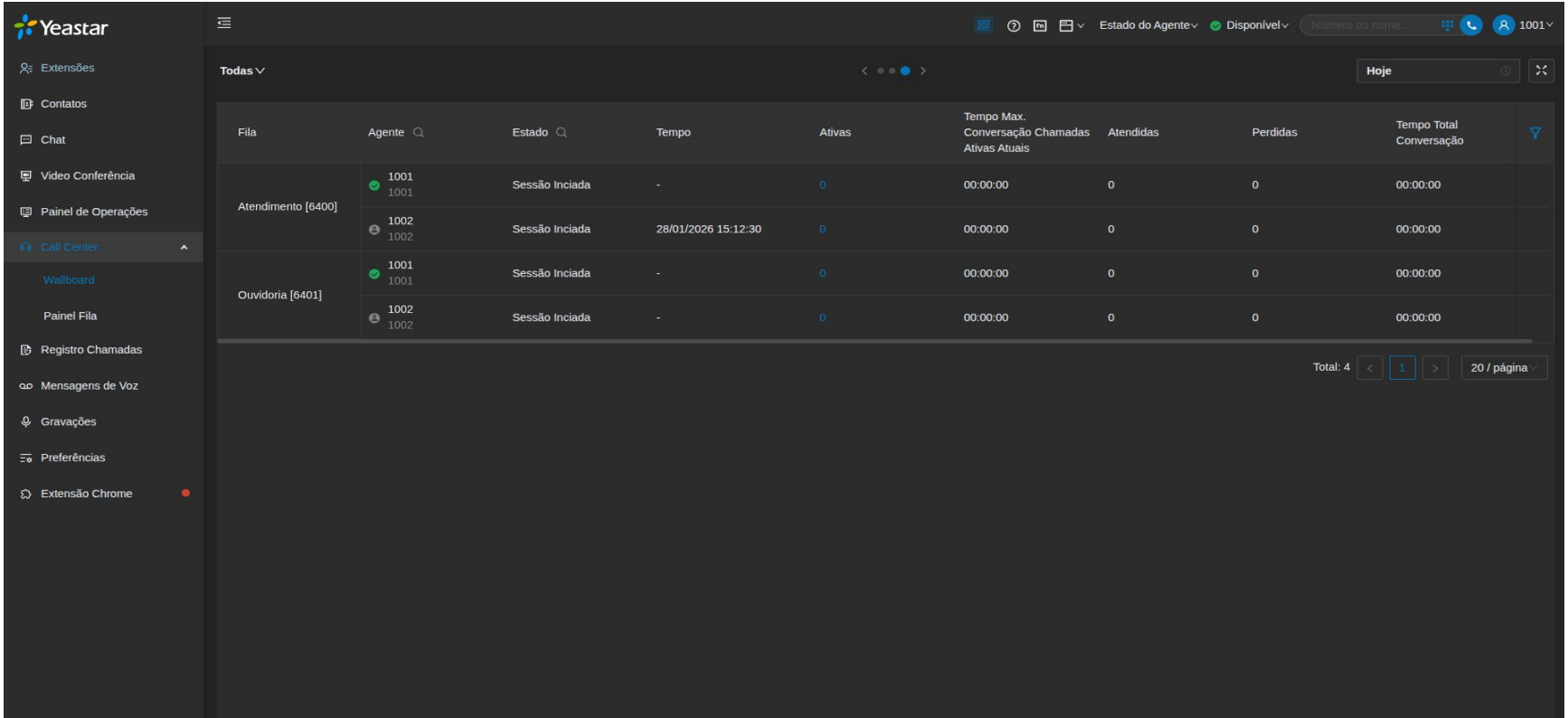
2.7 Avaliação do Ambiente do Supervisor

Dashboard (2)



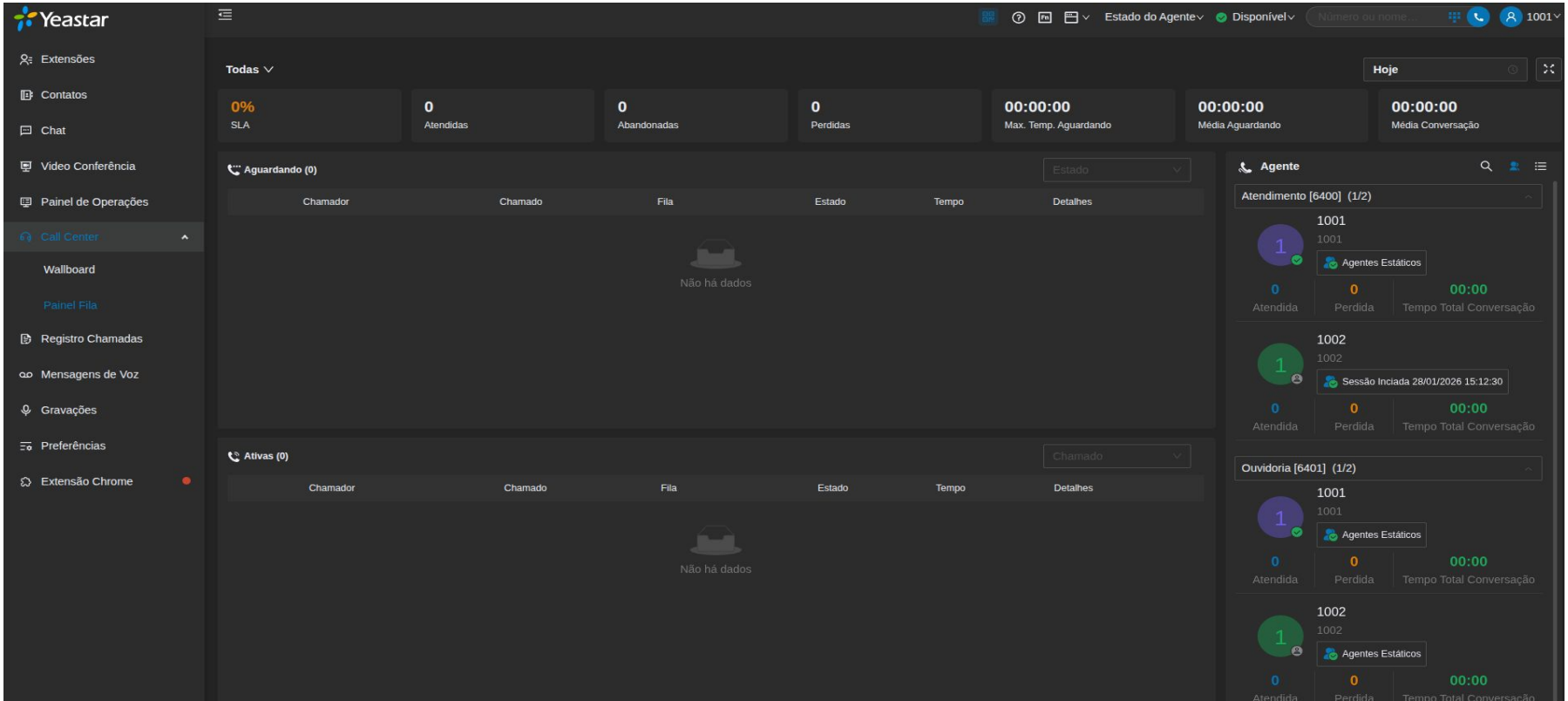
2.7 Avaliação do Ambiente do Supervisor

Dashboard (3)

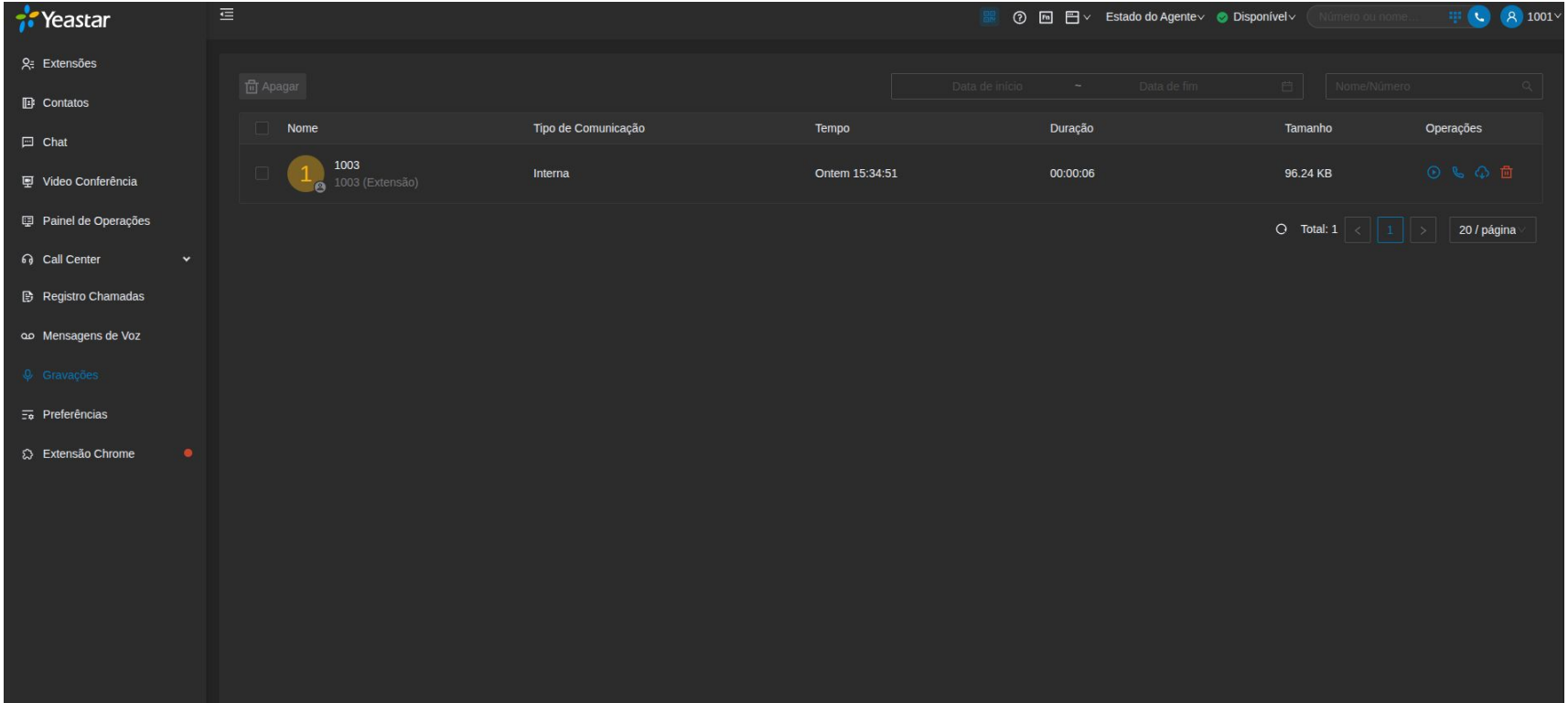


2.7 Avaliação do Ambiente do Supervisor

Operação da Fila



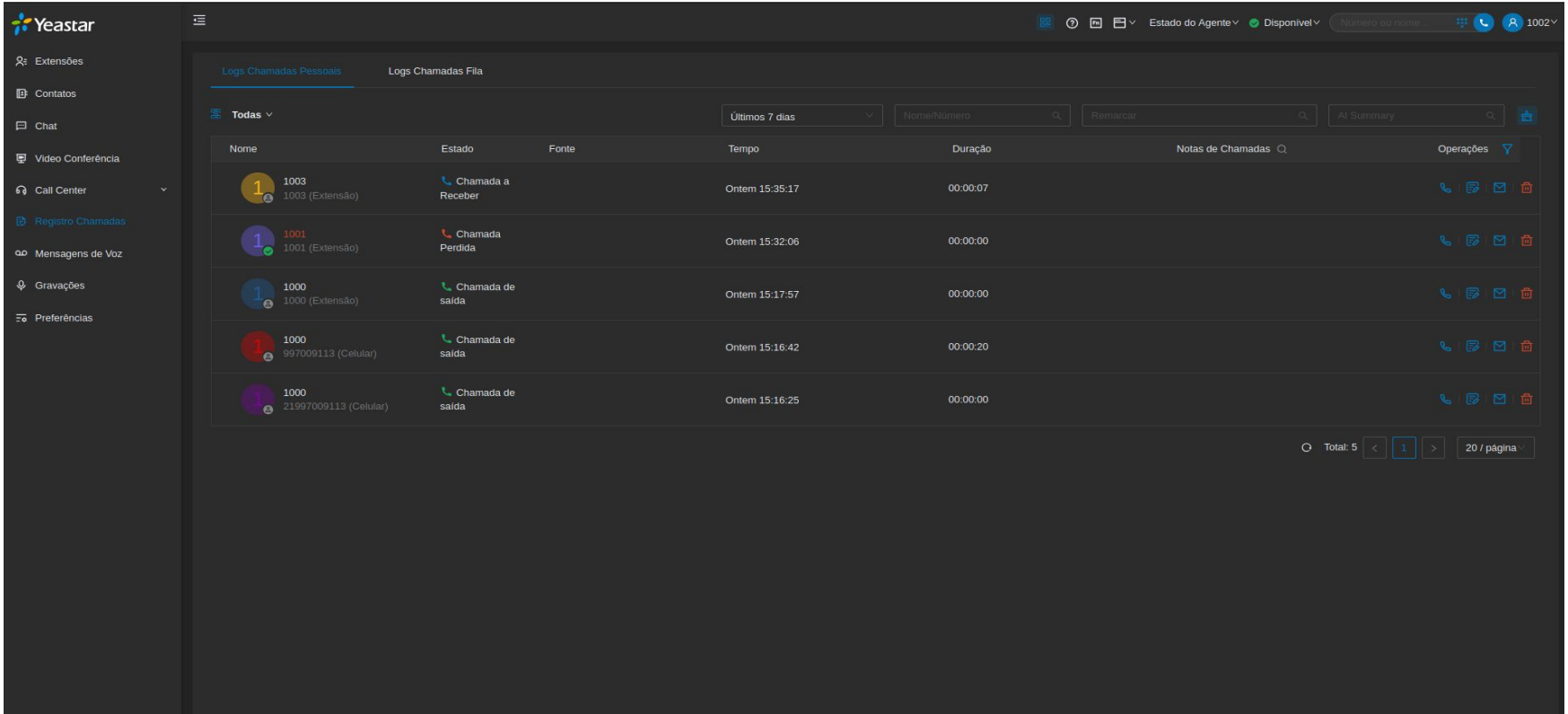
2.7 Avaliação do Ambiente do Supervisor



Gravações

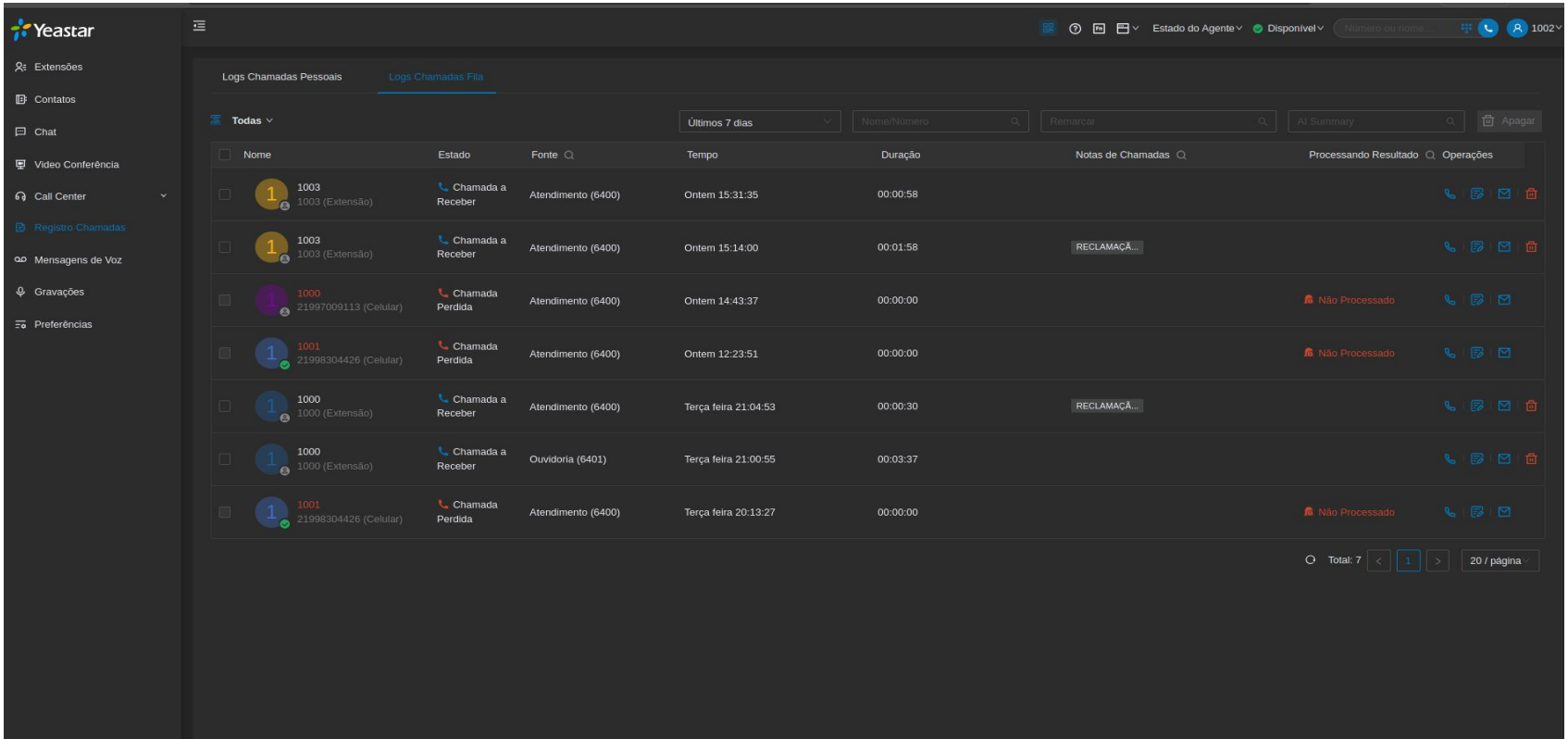
2.7 Avaliação do Ambiente do Supervisor

Registros de Chamadas



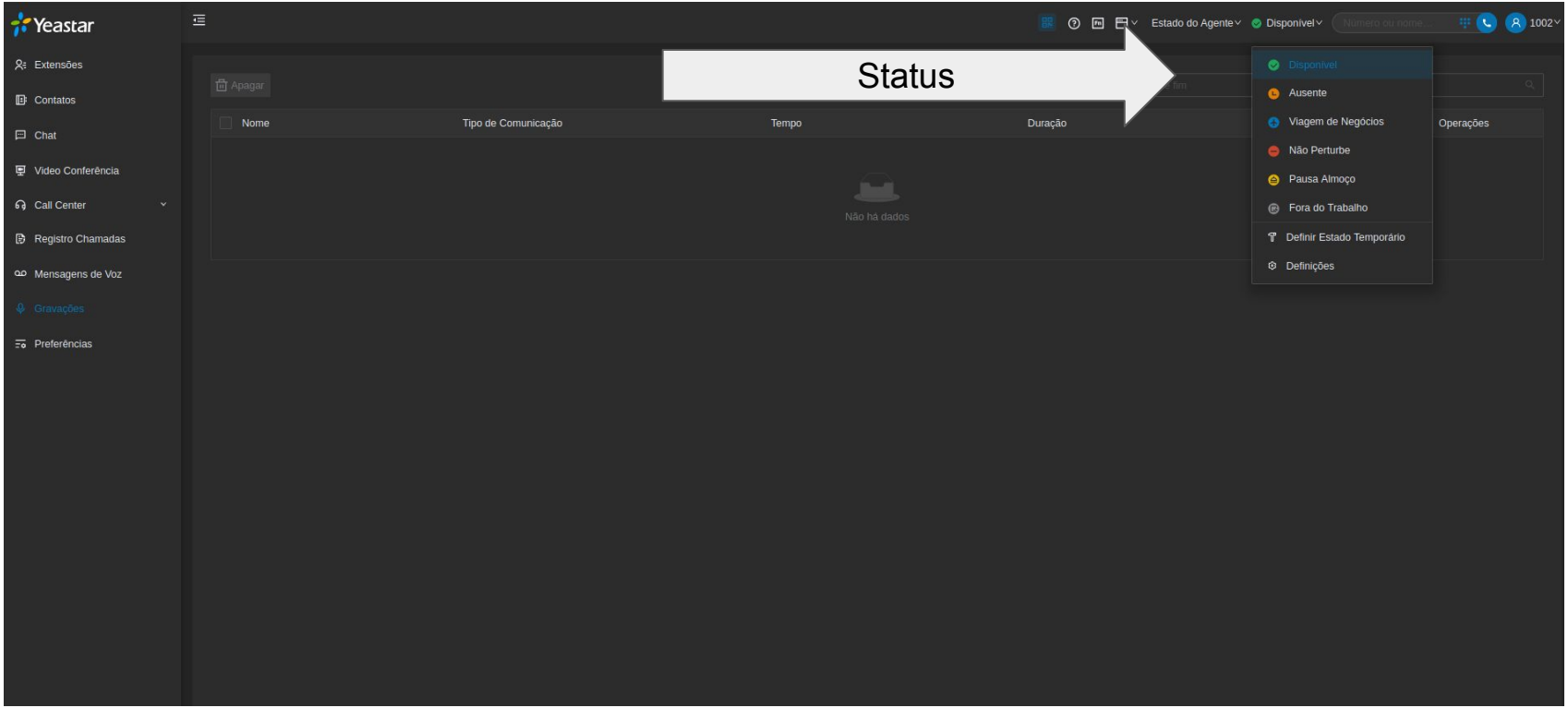
2.7 Avaliação do Ambiente do Supervisor

Registros de Atendimento Fila



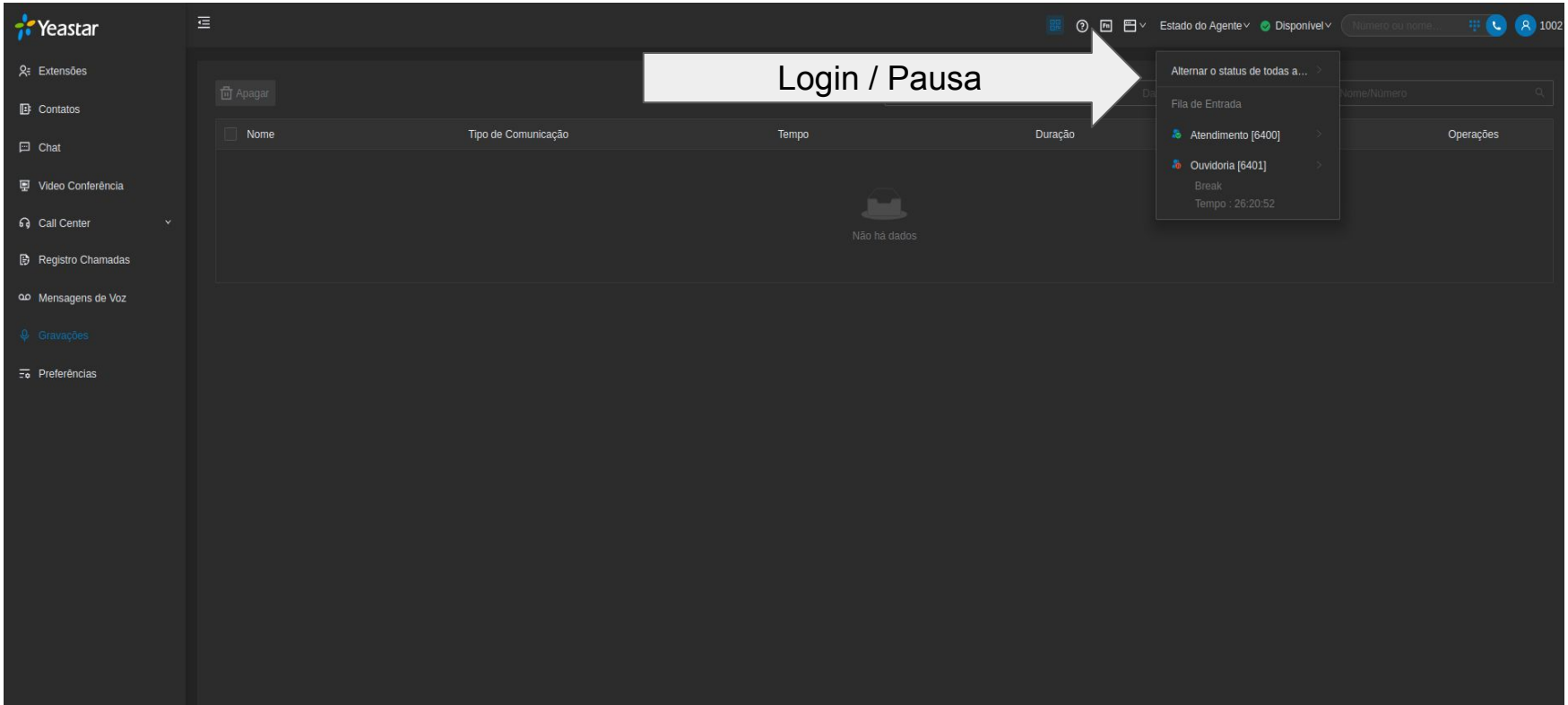
2.7 Avaliação do Ambiente do Supervisor

Administração de Status



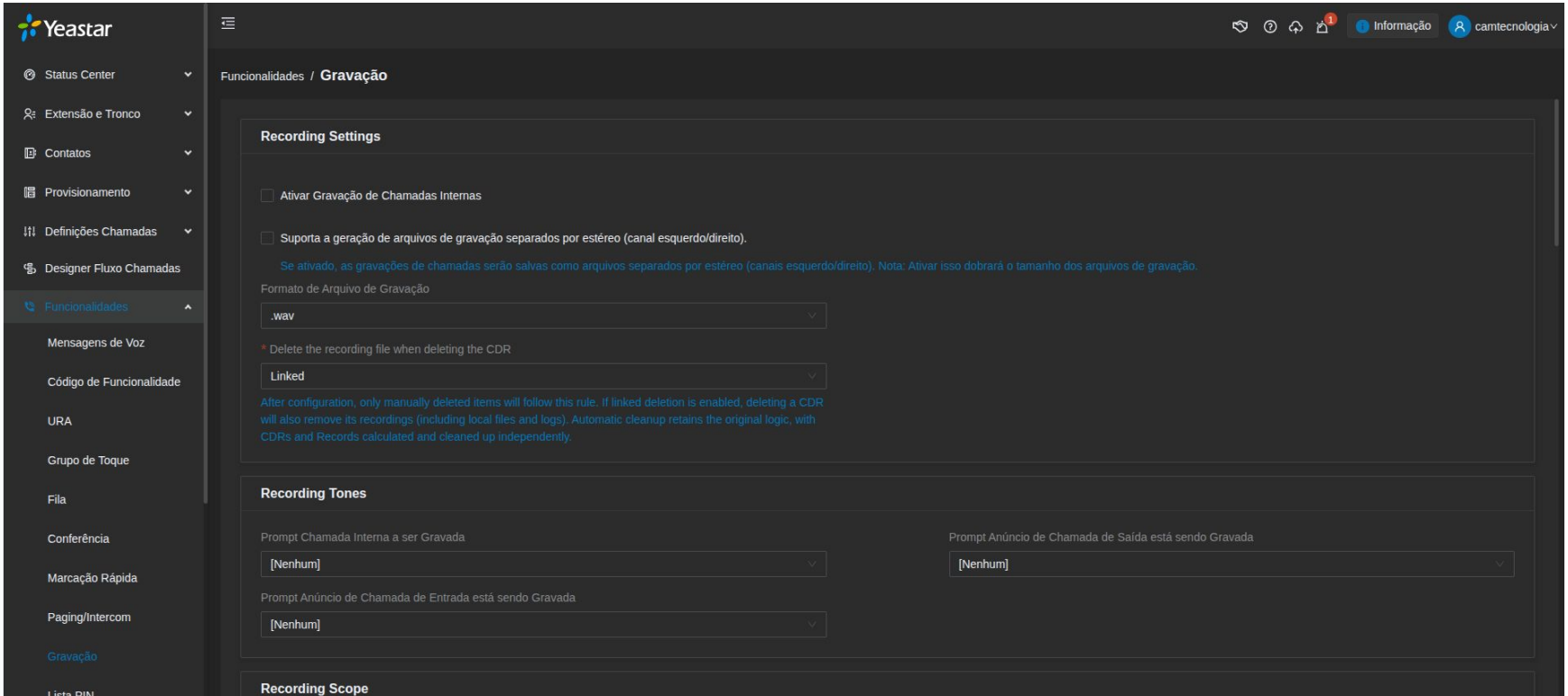
2.7 Avaliação do Ambiente do Supervisor

Gestão de Status em Fila



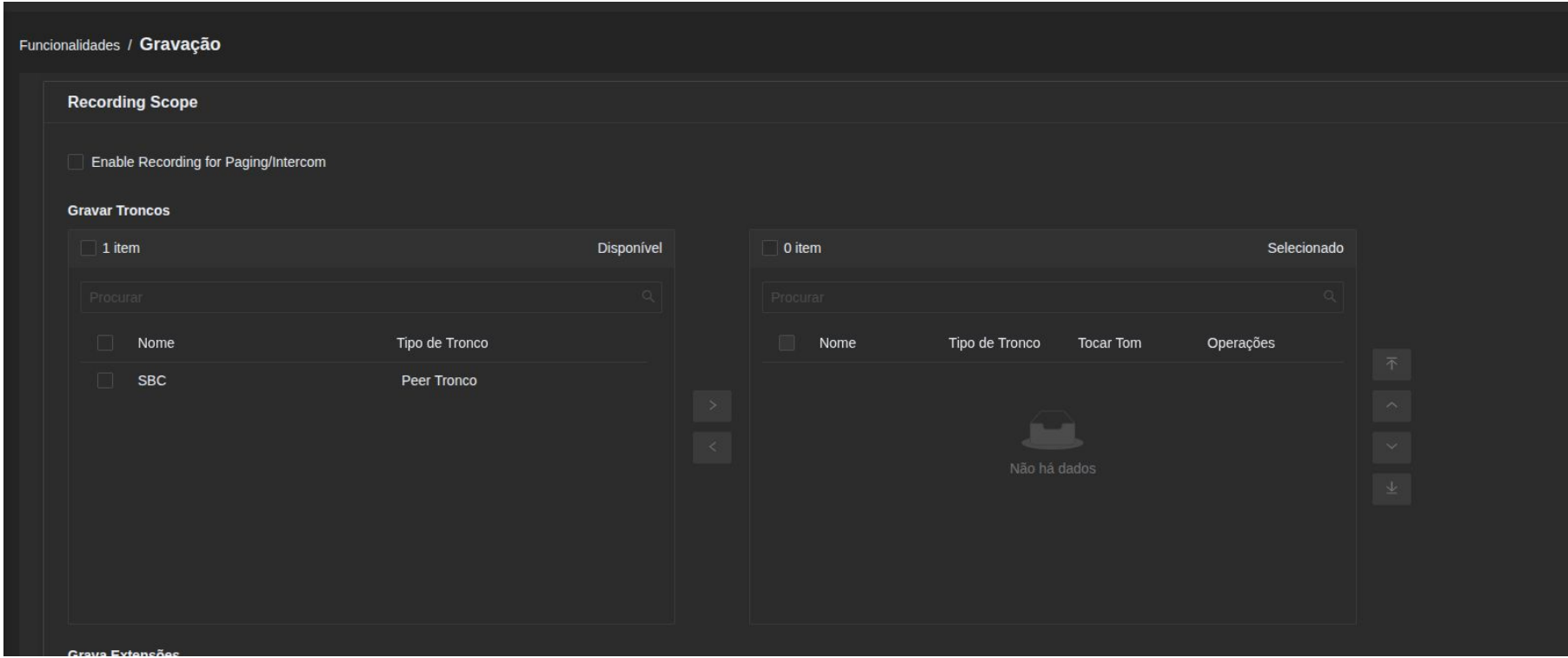
2.8 Avaliação do Ambiente de Gravação

Gestão do Fluxo de Gravaçã



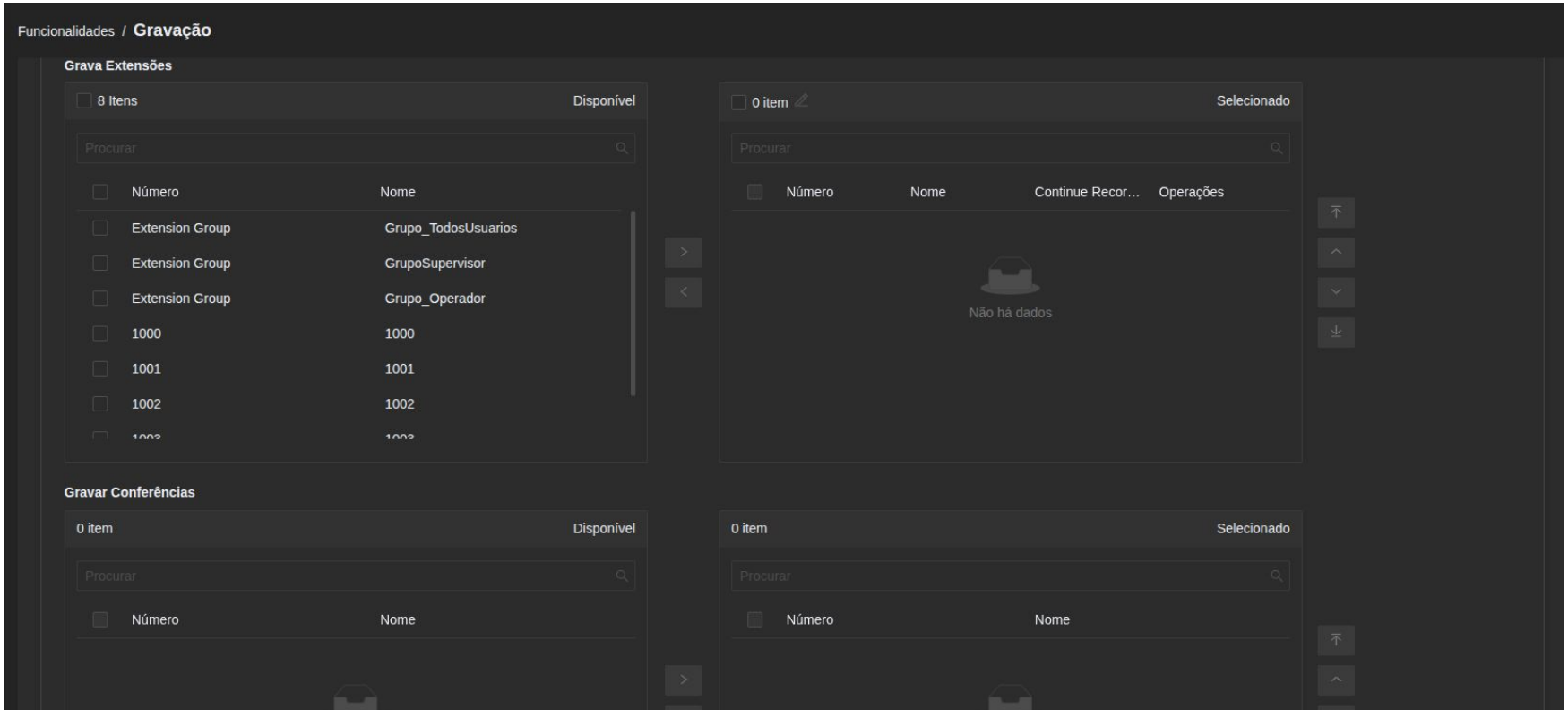
2.8 Avaliação do Ambiente de Gravação

Gestão do Fluxo de Gravaçaõ (2)



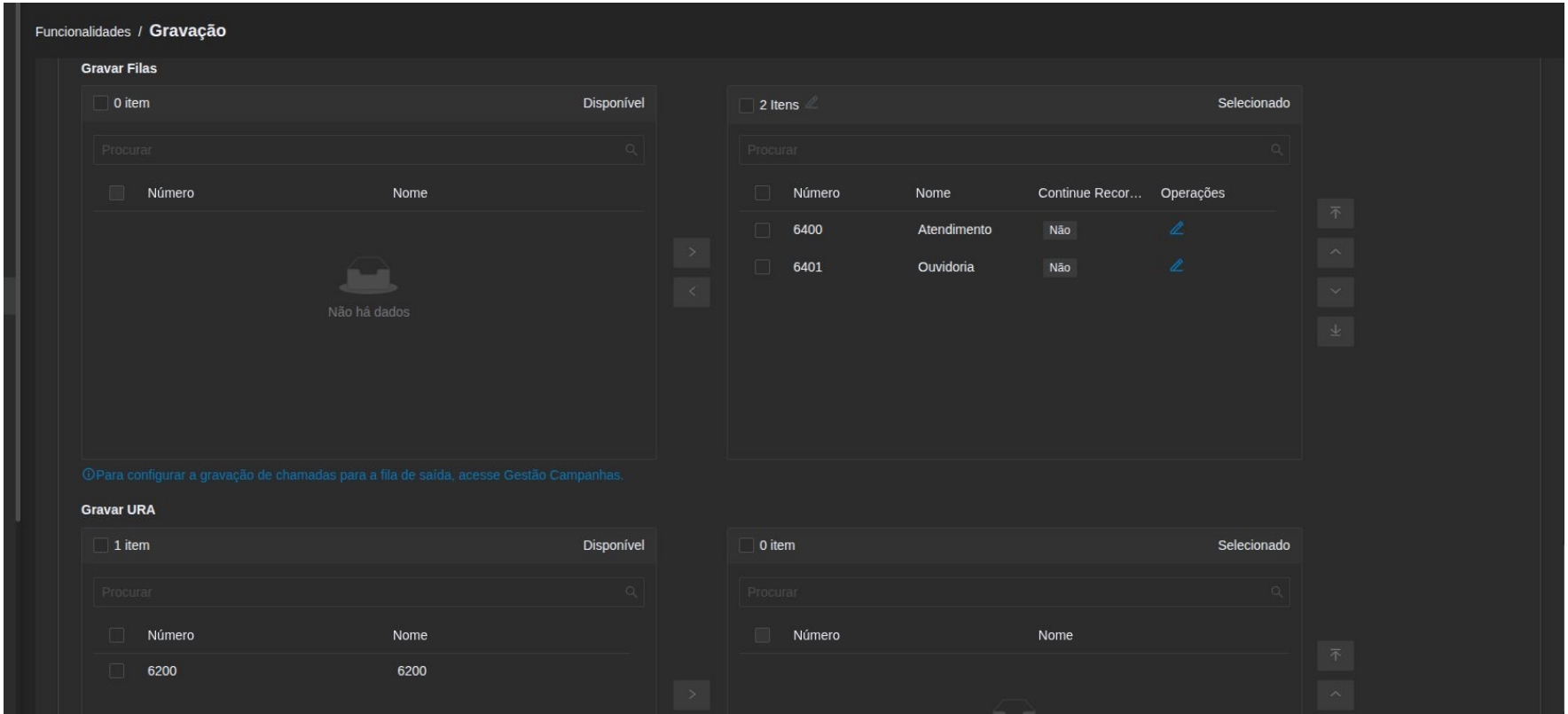
2.8 Avaliação do Ambiente de Gravação

Gestão do Fluxo de Gravação (3)



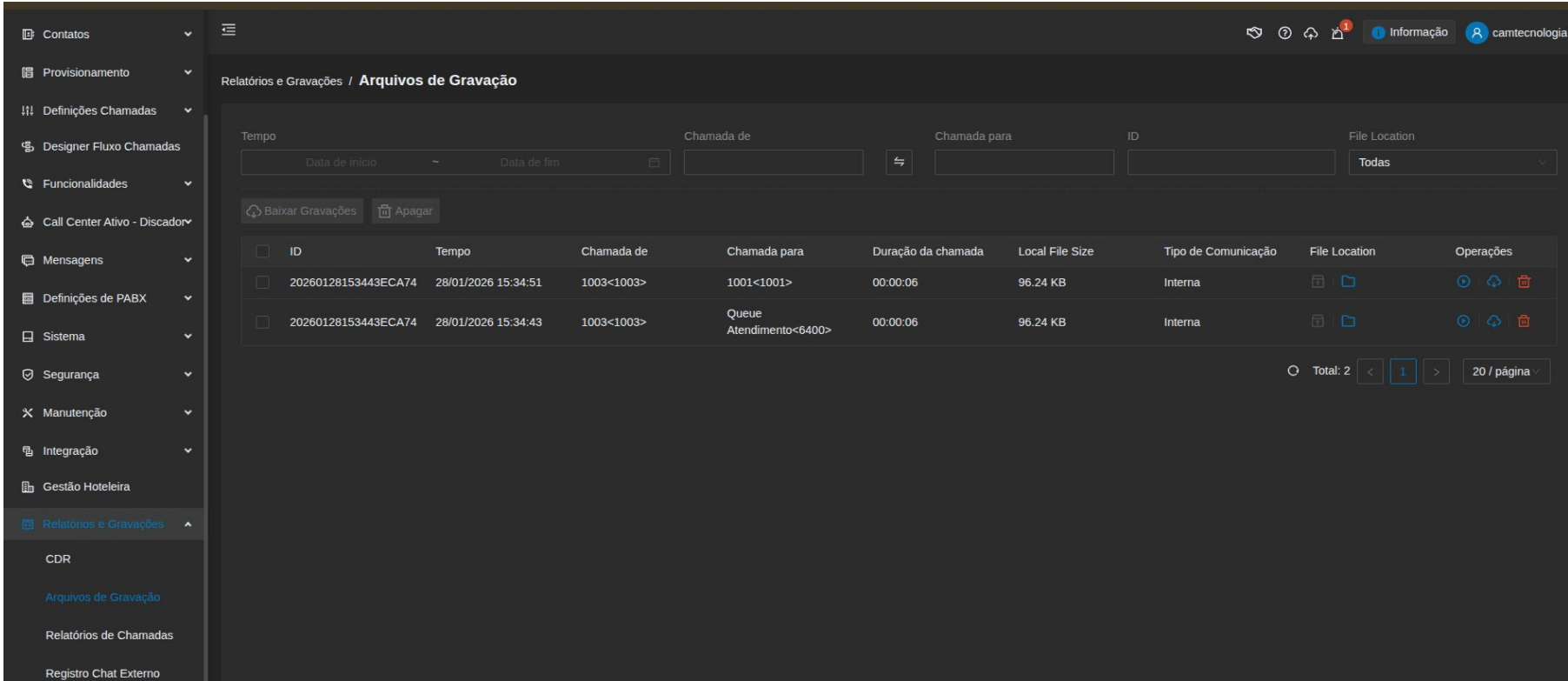
2.8 Avaliação do Ambiente de Gravação

Gestão do Fluxo de Gravaçaõ (4)



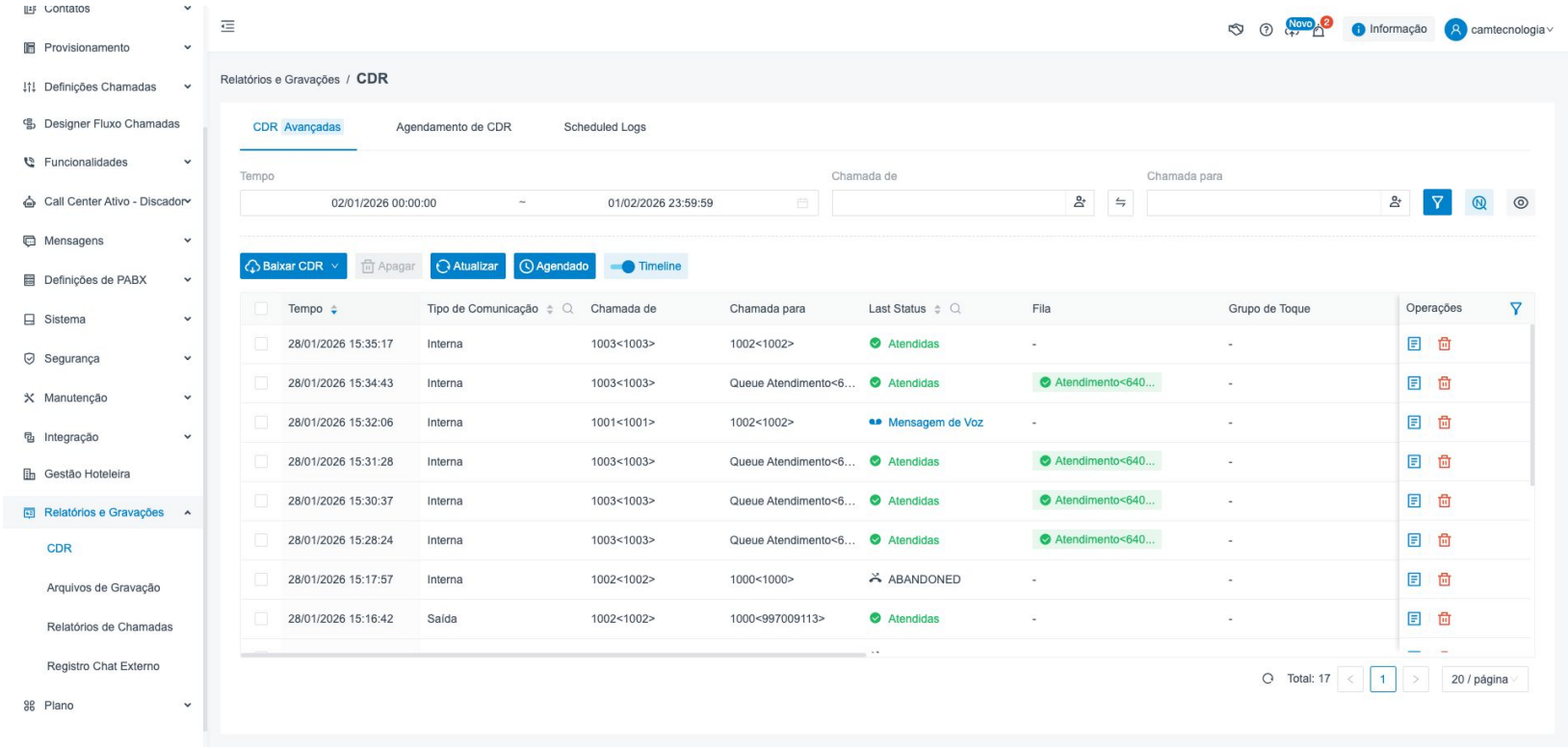
2.8 Avaliação do Ambiente de Gravação

Listar chamadas gravadas



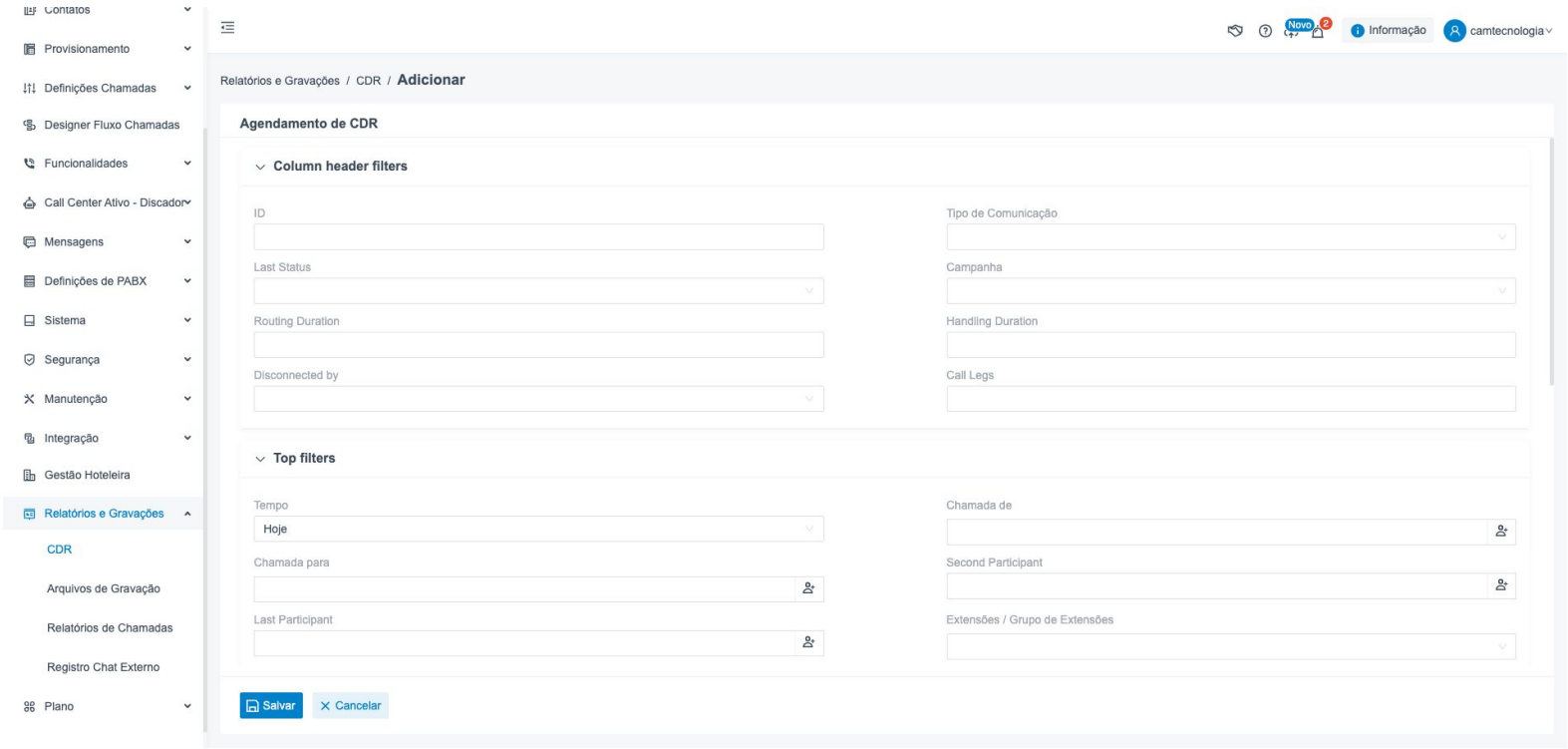
2.9 Avaliação do Sistema de Tarifação e Bilhetagem

Registro de Chamadas

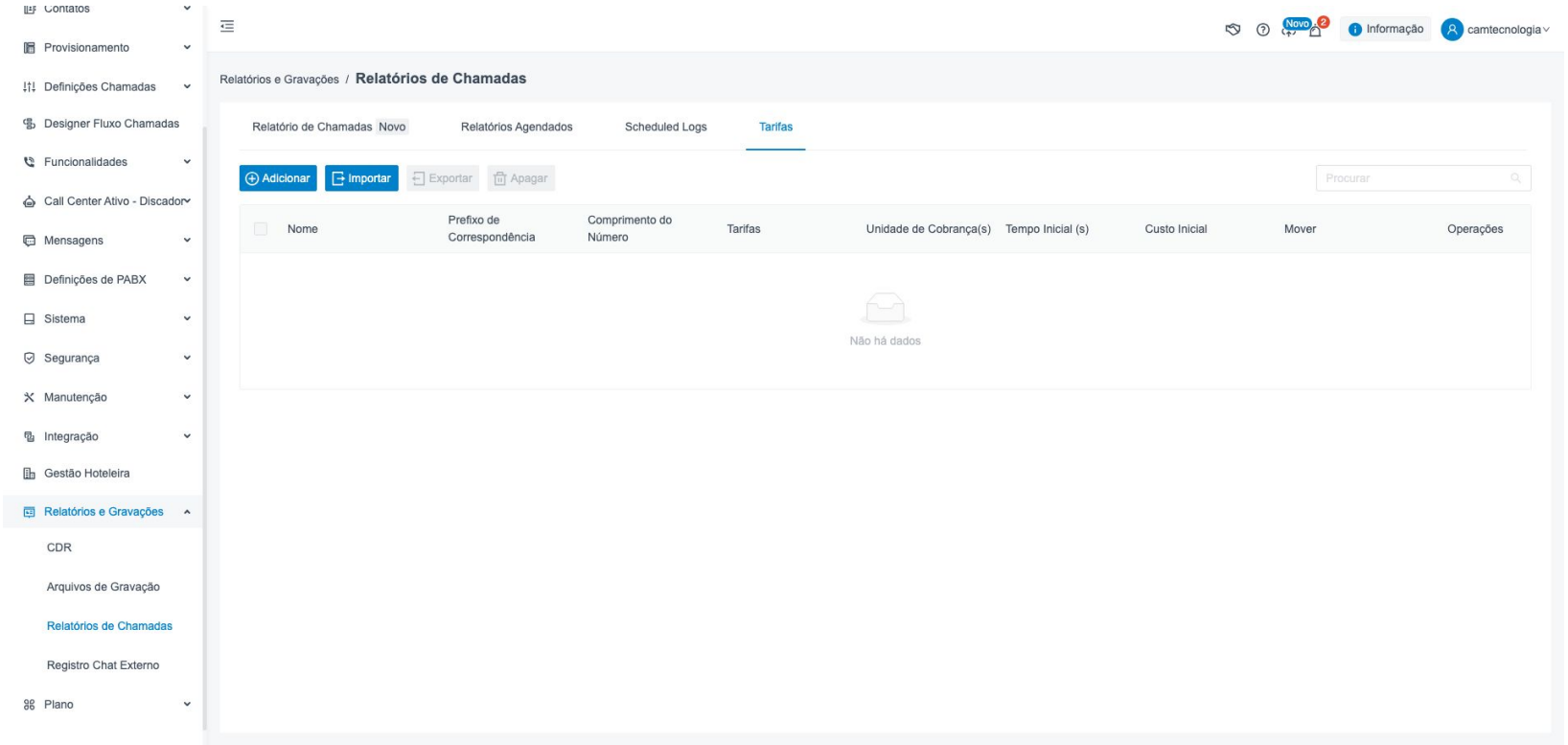


2.9 Avaliação do Sistema de Tarifação e Bllhetagem

Relatórios automáticos



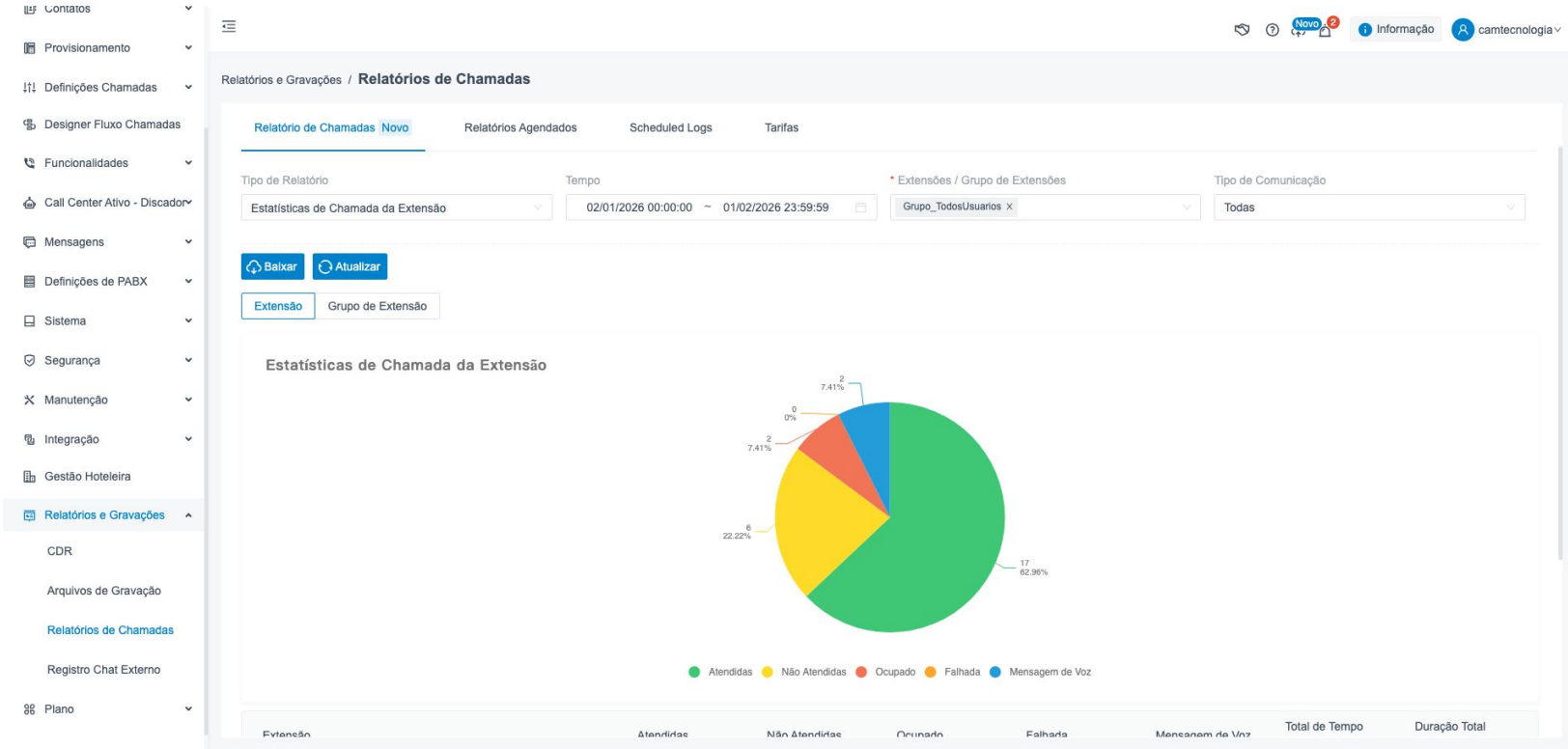
2.9 Avaliação do Sistema de Tarifação e BIlhetagem



Tarifação

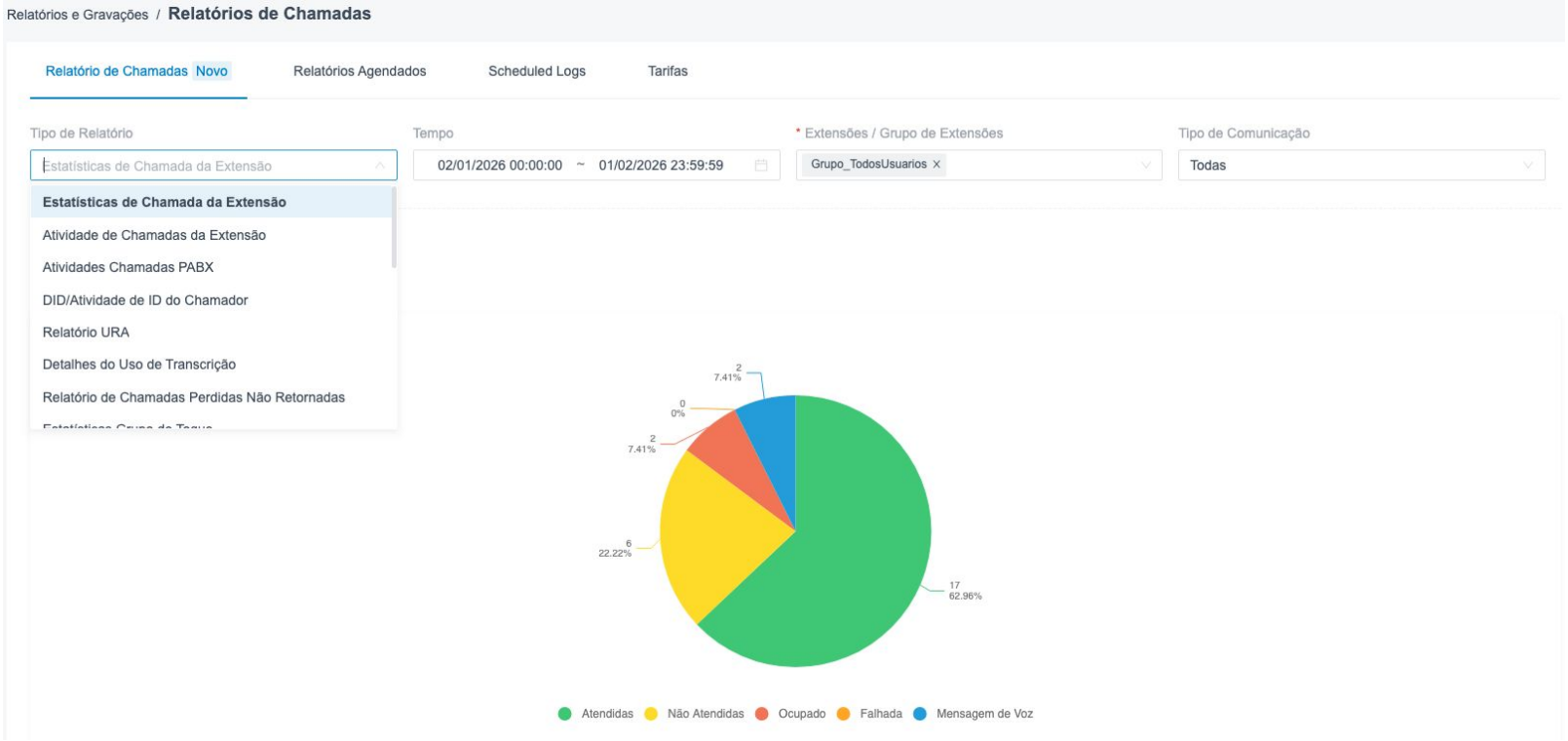
2.10 Avaliação do Sistema de Geração de Relatórios

Relatórios de Chamadas



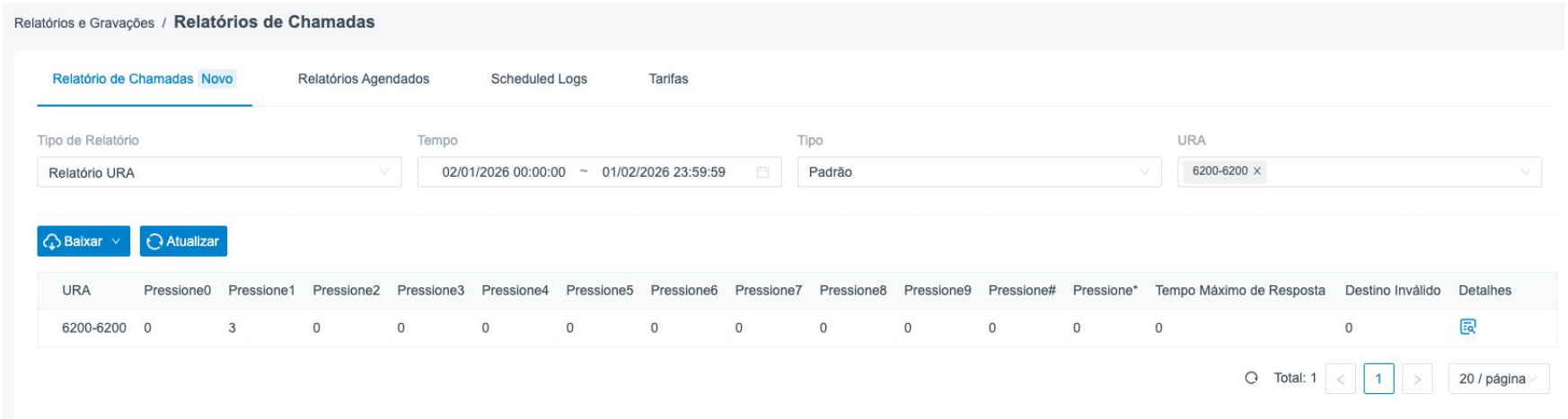
2.10 Avaliação do Sistema de Geração de Relatórios

Relatórios de Chamadas (2)



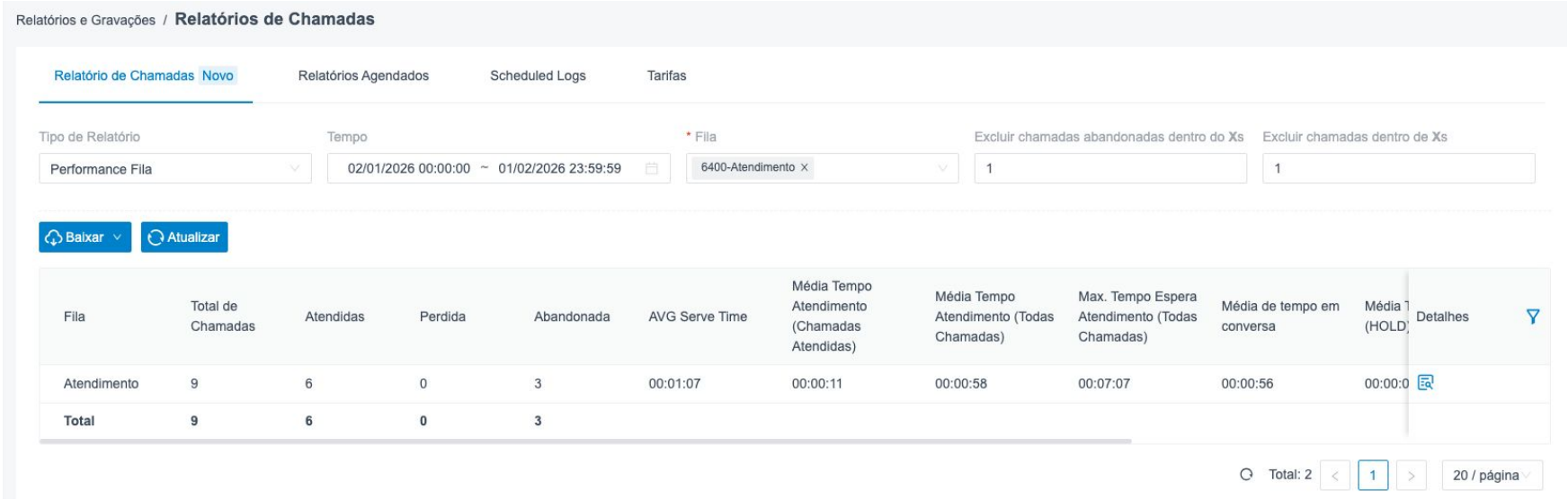
2.10 Avaliação do Sistema de Geração de Relatórios

Relatórios de Chamadas (3)

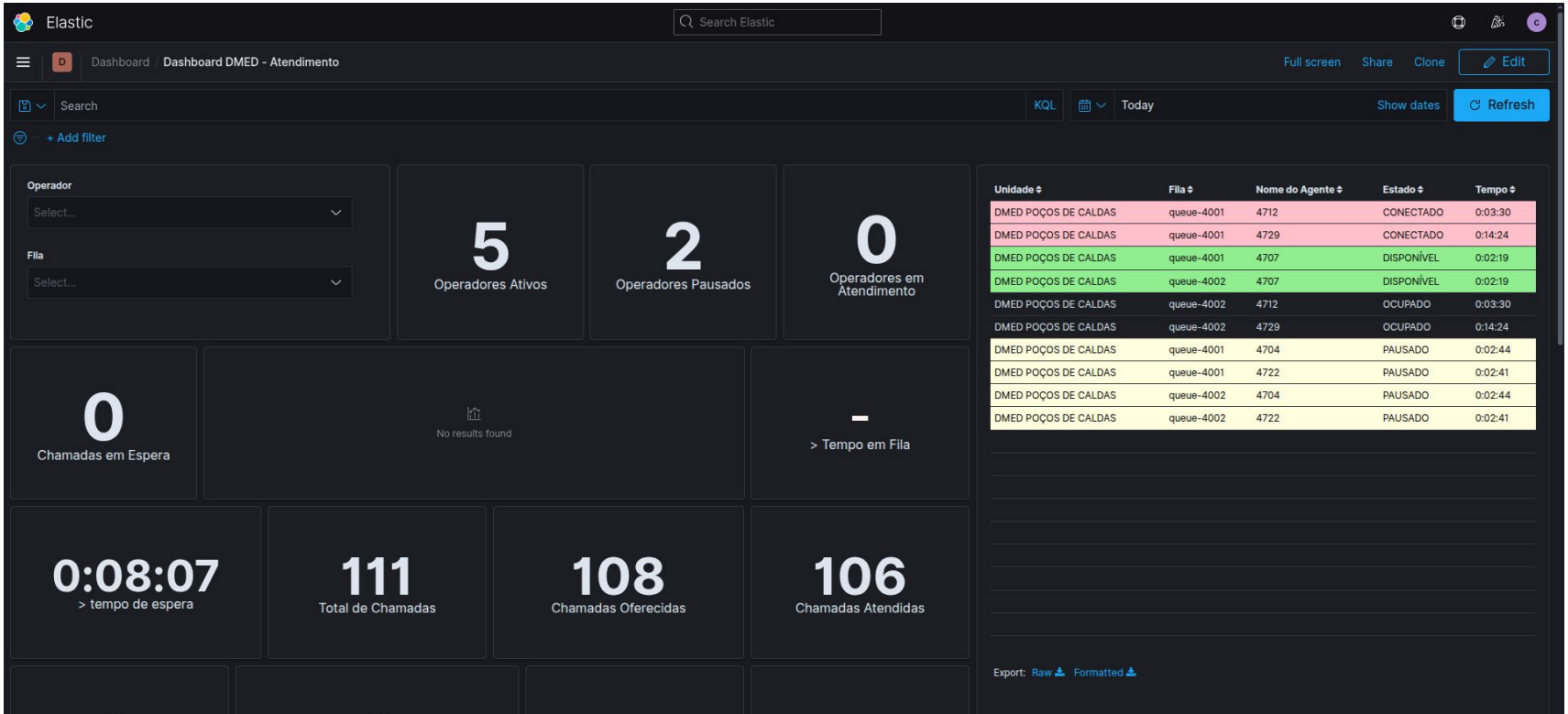


2.10 Avaliação do Sistema de Geração de Relatórios

Relatórios de Chamadas (4)

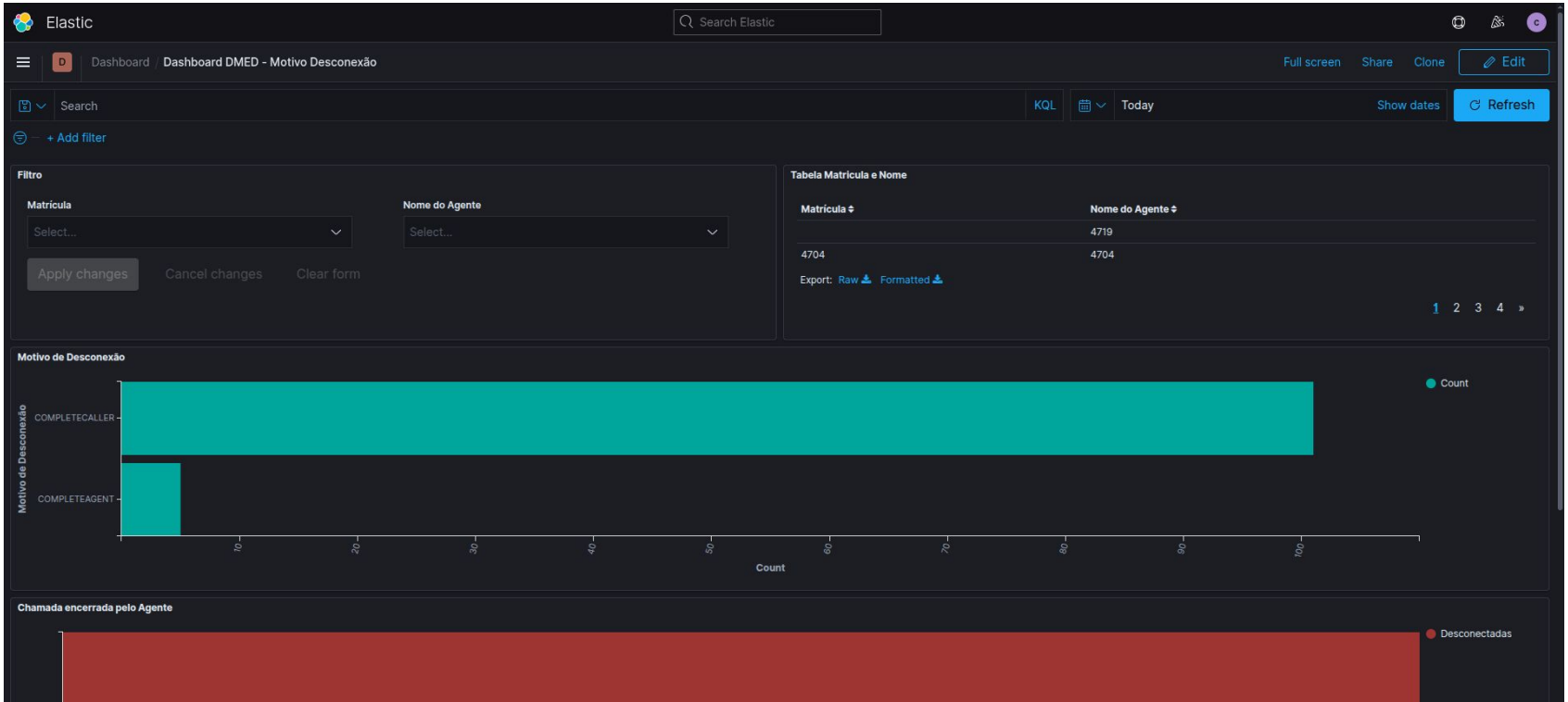


2.10 Avaliação do Sistema de Geração de Relatórios



BI

2.10 Avaliação do Sistema de Geração de Relatórios



BI (2)

PARTE III
DEMONSTRAÇÕES GERAIS

3.1 Avaliação da Ajuda Online

Canais de Atendimento da CAM

NOSSOS CANAIS DE SUPORTE

Ticket
atendimento.camtecnologia.com.br

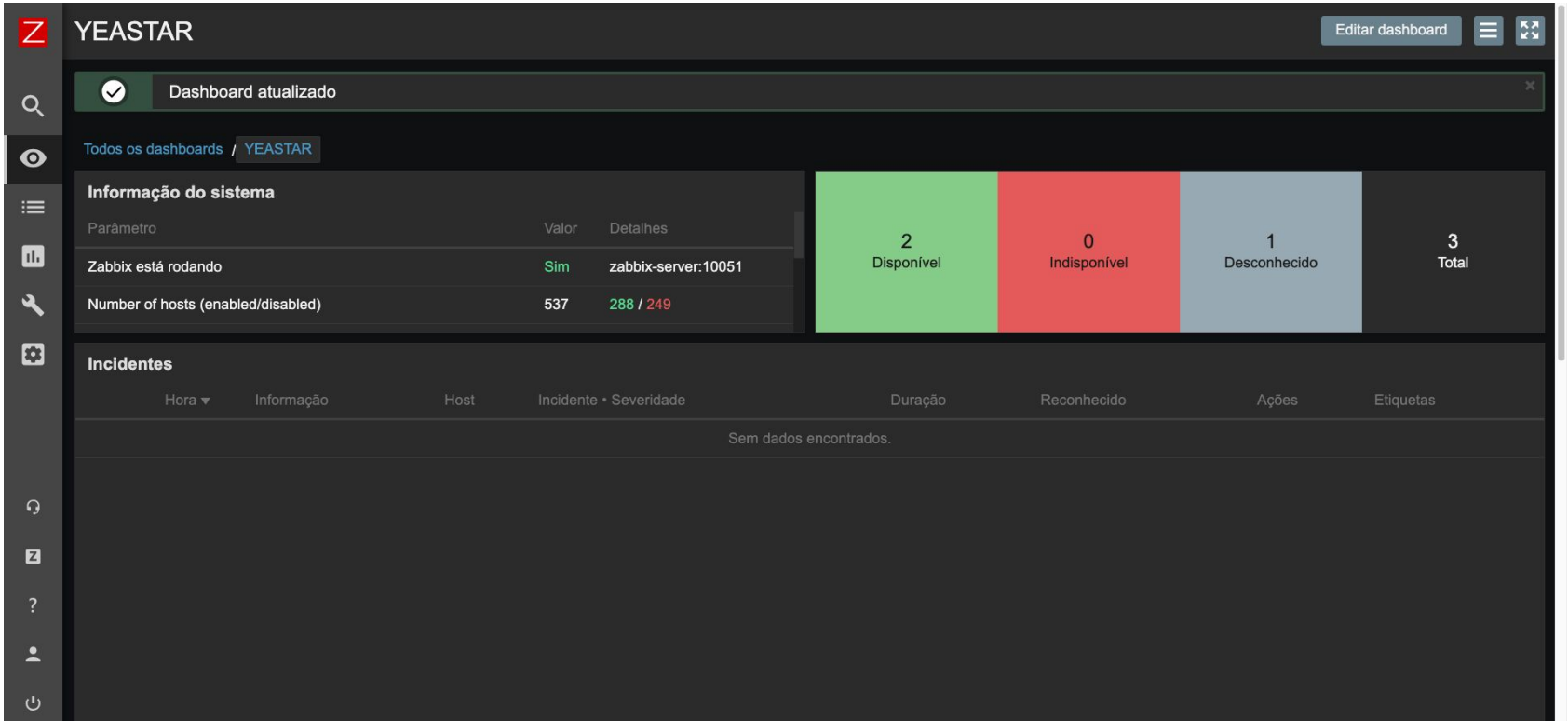
E-mail
suporte@camtecnologia.com.br

Telefone
(21) 3189-1050

0800
0800-494-1050

Chat
chat.camvoip.com.br/livechat

3.2 Avaliação da Central de Serviços



Monitoramento e NOC

Siga-nos

@camtecnologiavoip

cam tecnologia

CAM TECNOLOGIA

OBRIGADO

Thiago Maluf Resende
CEO

(21) 99700-9113
thiago@camtecnologia.com.br

Av. Pastor Martin Luther King Jr, 126 Nova América Offices, Torre 2000,
Sala 408 Del Castilho | Rio de Janeiro | RJ

CAM TECNOLOGIA

VSBC ONE W

KHOMP

Manual do usuário

vSBC One W

KHOMP

ENABLING TECHNOLOGY

07300261

Índice

As informações contidas neste documento são consideradas como precisas e confiáveis no momento da sua publicação. Antes de consultar este documento, verifique as notas de versão correspondente a versão do software que está sendo executado.

Este documento está sujeito a alterações sem aviso prévio.

Data de publicação: 01 de janeiro de 2022

1. Introdução

Este manual tem como objetivo auxiliar o profissional responsável por instalar, configurar e gerir o vSBC One.

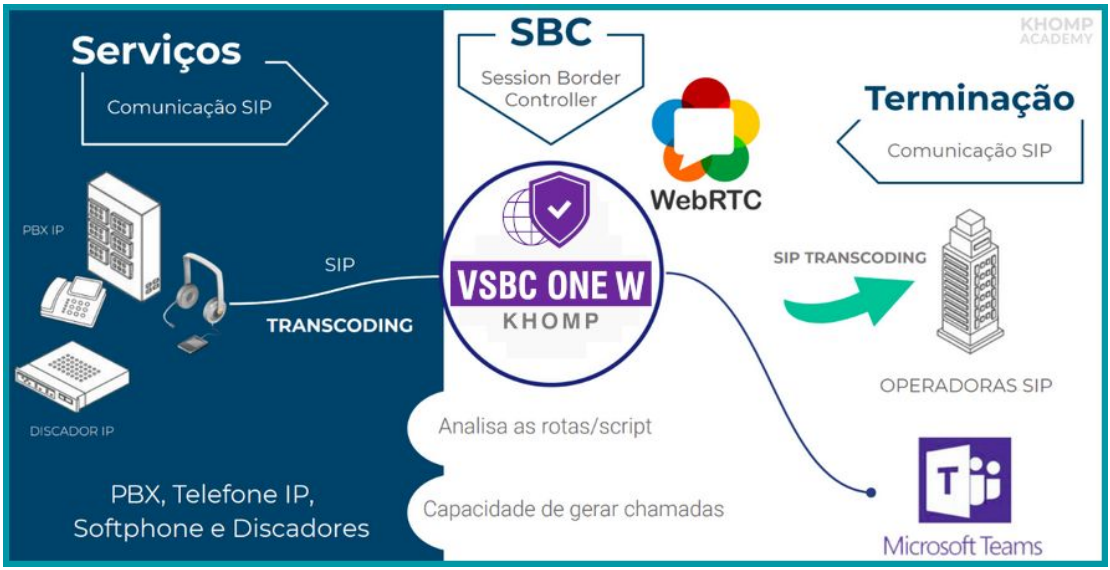
1.1. Apresentação

O vSBC One W é a nova versão do Session Border Controller em software da Khomp que pode ser instalado em variados tipos de infraestruturas, seja em servidor físico (bare metal), virtualizado, ou ainda, na nuvem. É uma poderosa ferramenta desenvolvida especificamente para controlar o tráfego da operação de telefonia.

Um SBC é um equipamento colocado entre redes distintas para proteção e interconexão do tráfego VoIP. O vSBC One W possui mecanismos de segurança para detecção de comportamentos e fontes maliciosas de tráfego, criptografia das chamadas, normalização de pacotes com erro, além de impedir o tráfego de pacotes SIP não autorizados na rede VoIP. Possui recursos para NAT e transcoding, oferecendo, juntamente às features de segurança, interconexão entre diferentes redes VoIP, fazendo a tradução entre protocolos de rede e codecs .

O vSBC One W é um software que pode ser instalado nos mais variados cenários, oferecendo flexibilidade e economia em sua implantação. Pode operar em servidores físicos, ambientes virtualizados, como VMWare®, ou ainda, em ambientes cloud como Azure, AWS, Huawei, Oracle e Google Cloud. Desta forma, é possível ter um SBC robusto, com recursos avançados de roteamento e segurança e acessível de qualquer lugar.

1.2. Cenário proposto



2. Acesso inicial

O vSBC One W é uma solução de software que pode ser instalada de duas maneiras:

- A **primeira opção** é através de um arquivo ".iso".
- A **segunda opção** é a partir de um sistema operacional já instalado (comum em ambientes de cloud, onde a criação de uma nova máquina é feita através de uma imagem de um sistema já instalado). Esta etapa só pode ser realizada pela equipe Khomp de implantação.

Para a instalação através do arquivo ".iso", acesse o link a seguir para obter a imagem do disco:

khomp.com/suporte/downloads

Após instalado o sistema operacional em uma máquina (computador), o software apresentará a seguinte interface:

2.1. Acesso à Interface Web

Para ter acesso à interface de gerenciamento KWebPortal (chamada de Interface Web), digite em seu navegador Web o endereço IP mostrado na interface do software (como indica a imagem anterior).

O login e senha padrões para o acesso, são observados a seguir:

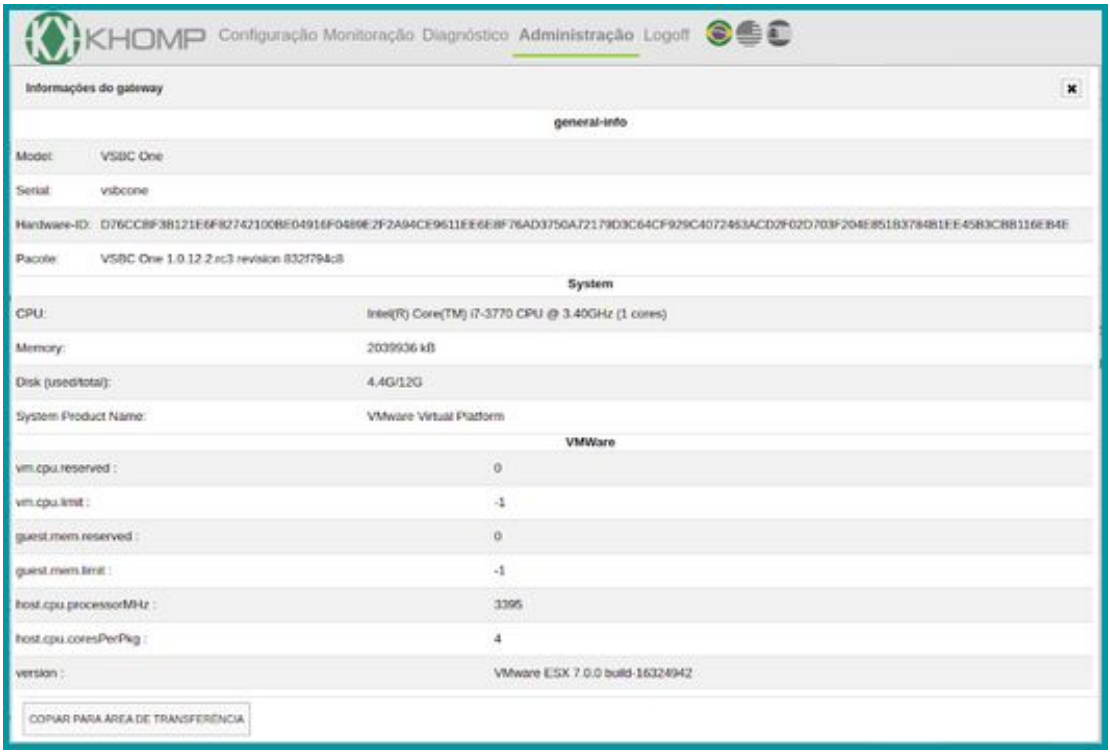
Usuário: **admin**

Senha: **khomp**

Atenção	• Após o primeiro acesso, é recomendado alterar a senha de acesso como medida de segurança. • A nova senha deve ser fornecida somente ao administrador do sistema.

3. Informações do vSBC One W

Para verificar o modelo do equipamento e a versão atual, acesse os menus "**Administração**" → "**Informações do gateway**" na Interface Web.



3.1. Adicionar licença

A licença é o arquivo que ativa o vSBC e lista os diferentes recursos disponíveis para aquele dispositivo, como número de chamadas simultâneas e número de registros simultâneos. As licenças são adquiridas diretamente com a Khomp.

Há quatro tipos de licença possíveis para ativar o vSBC One W, sendo duas locais e as outras de acesso remoto.

O licenciamento local acontece quando todo o processo de autenticação da licença é feito localmente, sem necessidade de acessar nenhum servidor de licença remoto.

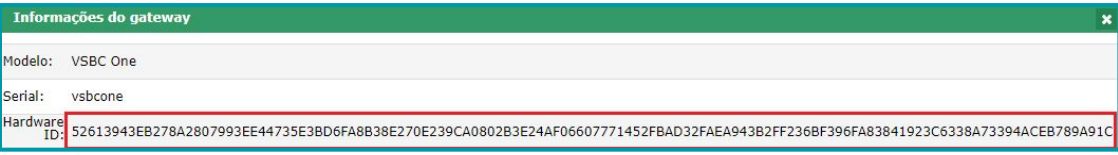
No licenciamento de acesso remoto, é imprescindível que haja um servidor de licenças. A tabela com os tipos existentes de licença e a suas descrições, é observada a seguir

Tipo de licença	Descrição
HardwareID - local	A licença hardware ID é gerada utilizando o hardware id da máquina que será licenciada. Este valor é um identificador único gerado a partir dos componentes de hardware. Isto significa que ela só pode ser utilizada pelo computador específico para o qual ela foi gerada, não podendo ser transferida para outro computador. Também é necessário substituí-la caso exista uma mudança nos componentes de hardware do computador (ao adicionar uma placa de rede extra, por exemplo). **Esta licença não permite a utilização de High Availability (HA)**.
Server Local - local	Este tipo de licenciamento fornece recursos a serem disponibilizados por um servidor de licenças rodando no próprio Gateway. A licença é vinculada ao hardware ID da máquina. Quando uma máquina com uma licença Server local tem o modo HA ativado, ela gera uma licença do tipo remote automaticamente para consumir os recursos da licença server. Em gateways, **esta licença é destinada à utilização em modo HA**.
Server Khomp - remoto	A licença server remote utiliza servidores de licença instalados no local do cliente, assim a quantidade de vSBCs utilizados pode variar dependendo da carga e das necessidades do cliente. **Esta licença permite a utilização de HA**.
Server Cloud - remoto	A licença Cloud é um tipo de licenciamento remoto que utiliza servidores de licença gerenciados pela Khomp. **Esta licença permite a utilização de HA**.

3.2. Instalar licenças

1. Acesse o menu "**Administração**" → "**Informações do gateway**".

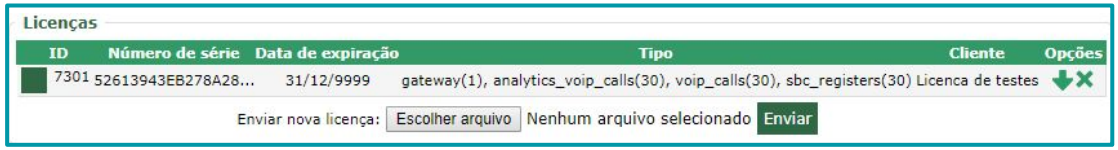
2. Para a licença HardwareID, copie a informação exibida no campo "Hardware ID". Indique esta informação para a Khomp, este valor é necessário na geração da licença HardwareID. Aguarde o recebimento do arquivo da licença. A licença é enviada no formato zip. É necessário descompactar o arquivo para utilizá-lo.

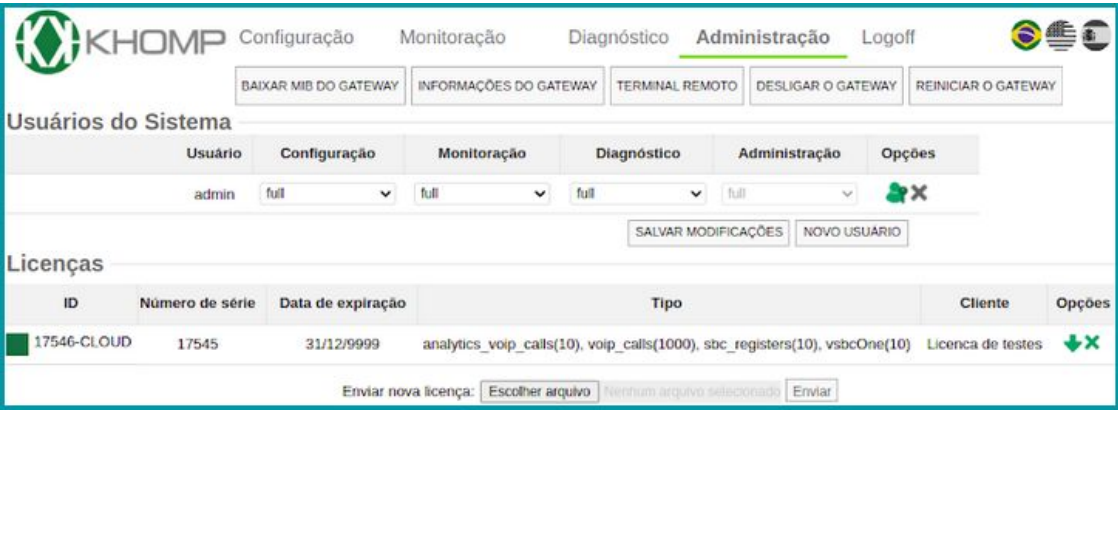


3. No painel "Licença", clique no botão "Escolher arquivo". Selecione o arquivo recebido. Este arquivo deve ter a extensão klf.

4. Clique no botão "Enviar".

5. Ao final, o painel de licença irá exibir as informações da licença.





Para configurar cada tipo de licença é necessário ir em "**Configuração**" → "**Sistema**" → "**Servidores de Licenças**".

São três tipos de servidores possíveis: "Default", "Custom" e "Cloud".

- **Servidor Default**: É utilizado para licenças do tipo HardwareID e Server.
- **Servidor Custom**: Para licenciamento com servidor de licenças próprio, associado à licenças do tipo Remote. Apenas nesse caso, é possível configurar os endereços dos servidores, nos demais, as configurações de endereços são fixas. É possível ajustar também o timeout de conexão com os servidores.
- **Servidor Cloud**: É utilizado para licenciamento na nuvem Khomp.

Nota	• A licença de nuvem (CLOUD) utiliza a porta 14140 para comunicação. Em cenários de comunicação externa esta porta precisa estar liberada no firewall de rede para que a comunicação chegue até o gateway. O firewall do gateway já vem liberado por padrão para aceitar esta comunicação externa. • Para uso do HA é importante que as instâncias master e spare do gateway estejam na mesma versão.

3.3. Atualização de pacotes

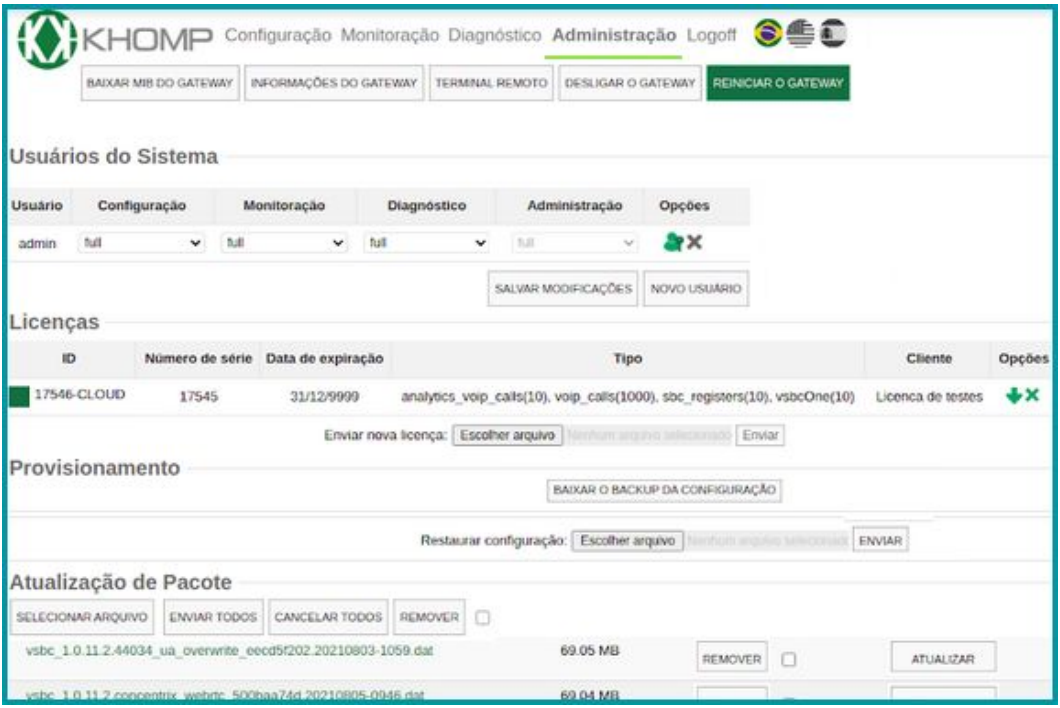
Para a atualização de pacotes acesse o seguinte link para obter o pacote de atualização: khomp.com/suporte/downloads. Baixe o arquivo requerido para a sua máquina.

Para subir o pacote em seu vSBC One W, acesse "**Administração**" → "**Atualização de Pacote**".

Selecione o arquivo baixado em "SELECIONAR ARQUIVO".

Após selecionado, clique em "ENVIAR TODOS".

Ao término do envio, clique em "ATUALIZAR".



4. Certificados para criptografia TLS

É possível registrar conjuntos de chave privada, certificado e *trust store* para serem utilizados pelo equipamento. O gateway pode gerar certificados auto-assinados ou instalar certificados gerados externamente.

4.1. Criar certificado auto-assinado

Para criar ou adicionar um certificado TLS acesse: "**Configuração**" → "**Rede**" → "**Certificado TLS**".
Preencha o formulário que será apresentado.
Ao enviar o formulário, aguarde a Interface Web confirmar a criação do certificado e abrir o formulário de edição.
O formulário de criação de certificado auto-assinado contém:

Campo	Descrição
Nome	Nome da configuração TLS
Tamanho (bits)	Tamanho em bits da chave privada a ser gerada utilizando valores aleatórios, quanto maior a chave, mais segura, porém, requer mais processamento para ser utilizada
Algoritmo de cifragem	Habilita cifragem da chave privada com o algoritmo desejado, requer "Senha de cifragem".
Senha de cifragem	Senha que será utilizada para a cifragem e decifragem da chave privada, deve ser preenchido somente se um "Algoritmo de cifragem" foi selecionado.
Confirmar senha de cifragem	Deve conter a mesma senha digitada no campo "Senha de cifragem", deve ser preenchido somente se um "Algoritmo de cifragem" foi selecionado.
País (C)	País a ser informado no campo C do certificado.
Estado ou província	Estado ou província a ser informado no campo ST do certificado.
Cidade ou localização (L)	Cidade ou localização a ser informada no campo L do certificado.
Organização ou empresa (O)	Nome da organização ou empresa a ser informado no campo O do certificado.
unidade organizacional ou departamento (OU)	Nome da unidade organizacional ou departamento a ser informado no campo OU do certificado.
Nome Comum (CN)	Nome a ser informado no campo CN do certificado.
Endereço de E-Mail (emailAddress)	Endereço de E-Mail do contato ou responsável pelo equipamento a ser informado no campo emailAddress do certificado.
Tempo de expiração (dias)	Tempo de expiração do certificado, contado em dias.

4.2. Adicionar ou editar certificados

Ao solicitar que seja adicionado um certificado existente, o sistema irá gerar e gravar a configuração com valores pré-definidos, abrindo o formulário de edição para alterações e envio dos arquivos que se deseja associar a esta configuração.

O formulário de edição contém:

Campo	Descrição
Nome	Nome da configuração TLS.
Senha de cifragem	Quando configurada é a senha utilizada para decifrar a chave privada e apresentará um link para alterar a senha. Caso ainda não esteja configurada, apresenta o campo para adição de uma senha. **Atenção** A chave privada nunca é alterada por este campo; caso deseje decifrar e recifrar a chave com nova senha, é necessário fazer o download da chave, realizar as alterações e fazer upload da nova chave com a nova senha.
Habilitar Trust Store padrão	Caso habilitado, o trust store padrão do sistema deverá ser carregado e utilizado em conjunto com o trust store fornecido por esta configuração, o trust store padrão contém os certificados públicos de autoridades certificadoras largamente utilizadas e é fornecido como parte do firmware do vSBC One, não pode ser alterado.
Habilitar verificação do certificado	Esta opção depende de do Trust Store e/ou Trust Store padrão habilitados e obrigará a verificação do certificado apresentado pelo ponto remoto no handshake do TLS ter sido emitido por qualquer das autoridades certificadoras reconhecidas. Caso não seja configurado um Trust Store e o Trust Store padrão esteja desabilitado, esta configuração é ignorada e qualquer certificado oferecido pelo ponto remoto será aceito.
Chave privada	Quando não se tem chave privada associada, este campo apresentará a possibilidade de enviar uma chave privada; quando há uma chave privada, apresentará a condição de uso da chave e seu tamanho (caso a condição seja ok) e botões para baixar ou remover).
Certificado	Quando não se tem certificado associado, este campo apresentará a possibilidade de enviar um certificado. Quando existir um certificado, o campo apresentará as condições de uso do certificado e botões para baixar ou remover o mesmo.
Trust Store	Quando não se tem trust store associado, este campo apresentará a possibilidade de enviar um trust store. Quando existir um trust store, o campo apresentará as condições de uso do trust store e botões para baixar ou remover o mesmo.

Atenção

- O certificado deve estar no formato "**.pem**". Após a configuração feita, lembre-se de clicar em "Salvar".
- Quando for utilizado o WebRTC, é necessário que o certificado TLS seja configurado. Além disso, desabilite o checkbox "Habilitar verificação do certificado".
- Após feita a configuração do certificado, acesse "**Configuração**" → "**Rede**" → "**VoIP**", e adicione a porta TLS.

4.3. Certificados emitidos por Autoridades Certificadoras confiáveis

O vSBC não requer que o certificado utilizado tenha sido emitido por Autoridades Certificadoras (CA) confiáveis, porém, é muito comum utilizar clientes WebRTC implementados utilizando navegadores comuns, como Chrome e Firefox.

Os navegadores costumam autorizar conexões TLS somente com dispositivos utilizando certificados emitidos por CAs confiáveis. Ou seja, ao utilizar o vSBC com WebRTC, é comum ter que utilizar estes certificados.

Os certificados podem ser adquiridos somente através das empresas que possuem CAs confiáveis.

Também é possível conseguir os certificados a partir de organizações sem fins lucrativos, como a Let's Encrypt, porém estes certificados costumam expirar mais rapidamente e necessitam de passos extras na sua geração.

5. Configurando o certificado do serviço (opcional)

Para acessar a Interface Web utilizando o certificado, acesse "**Configuração**" → "**Sistema**" → "**Serviços**".

Em "Certificado para utilizar no HTTPS", selecione o certificado desejado.

Atenção

- Clique em salvar e em aplicar, e depois reinicie o equipamento.
- Esta etapa é opcional pois não faz parte da comunicação SIP.

6. Configurar data e hora

O ajuste da data e hora afeta o registro dos Logs, arquivos CDR e funcionamento das rotas que operam por período de funcionamento.

6.1. Configuração manual

Insira as informações no campo data, hora e fuso horário, seguindo o formato exigido na descrição dos campos (**dd/mm/yyyy** para data e **hh:mm:ss** para a hora).

6.2. Integração com servidor NTP/SNTP

1. Habilite a opção NTP/SNTP.

2. Defina o tempo máximo de espera (em segundos) para que o vSBC One tente se comunicar com o servidor.

3. Para adicionar mais servidores NTP/SNTP, clique na opção Adicionar servidor e insira o endereço de acesso.

4. Clique no botão Salvar. Por fim, clique no botão Aplicar para que as alterações entrem em operação.

O vSBC One realiza uma tentativa de comunicação com o servidor NTP/SNTP dentro de tempo máximo de espera definido. Se não houver comunicação com o servidor dentro deste tempo, é realizado uma tentativa de comunicação com o próximo servidor, se configurado.

7. Histórico de configuração

O histórico de configurações do vSBC One W pode ser observado na Interface Web do sistema ao acessar os menus "**Configuração**" → "**Sistema**" → "**Histórico de configuração**". Nesta página, é possível ver alterações que foram feitas nas configurações e restaurar configurações anteriores.

8. Configuração das Interfaces

Esta página permite a configuração das interfaces de rede do vSBC. A quantidade de interfaces exibidas corresponde à quantidade de interfaces físicas no equipamento ou na máquina virtual.

Assim, para cada interface, temos os seguintes campos:

Campo	Descrição
Nome da interface	Nome da interface no sistema operacional. A alteração deste nome requer o reboot do sistema.
Label da interface	Identificador da interface nas configurações do vSBC. Pode ser alterado sem a necessidade de reboot.
Modo de configuração	Seleciona o método de configuração relacionado a rede: • **Estático**: Endereço IP, máscara de sub-rede e gateway de rede, são atribuídas manualmente. • **Dinâmico** (DHCP): Esta interface recebe as definições de rede atribuídas por um servidor DHCP disponível na rede. DHCP para IPv6 não é suportado.
Endereço IP	Em modo estático, selecione o endereço IP do vSBC. Lembre-se, o endereço IP deve ser exclusivo e não pode ser atribuído a nenhum outro dispositivo.
Máscara de sub-rede	Intervalo de endereços IP disponíveis na rede.
Gateway	Endereço do gateway de rede. É necessário setar ao menos um gateway como gateway padrão a partir do botão de seleção ao lado do campo gateway.

8.1. Criar interfaces VLAN e alias

A partir da interface física, é possível criar interfaces VLANs e alias associadas.

8.1.1 Criar interface VLAN

A partir do botão "CRIAR INTERFACE VLAN", é possível iniciar o processo.

O campo "Nome da Interface" define a partir de qual interface física esta interface VLAN será criada.

O campo "VLAN ID" define o ID da VLAN a qual esta interface vai estar conectada (ID entre 2 e 3999).

8.1.2 Criar interface alias

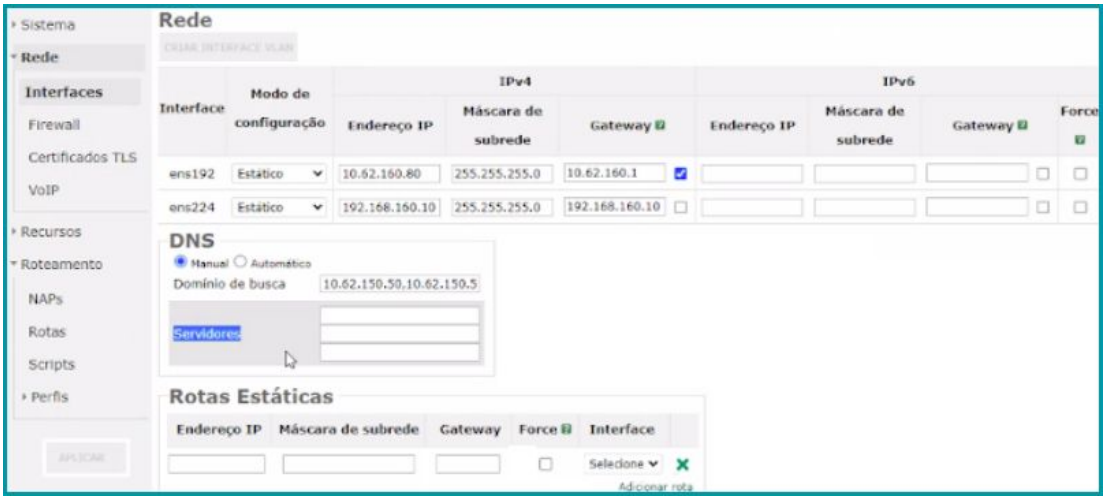
Ao lado de cada interface física, há um botão "+". Este botão possibilita configurar mais de um endereço IP por interface, criando **interfaces alias**.

As interfaces alias possuem "labels". Os labels possuem a interface original, seguido de "**:**" (dois-pontos) e do "número sequencial" (por exemplo, "**ens192:1**")

8.2. Configurar DNS

Configure o domínio de busca (também conhecido como domínio de pesquisa), configure o endereço dos servidores DNS primário, secundário e terciário que serão utilizados na ordem de preferência fornecida para a resolução de nomes na rede.

Você pode definir até 3 servidores DNS, os endereços devem estar separados por vírgulas, como mostra a imagem a seguir.



8.3. Configurar rotas estáticas

Permite definir uma rota estática, especificando endereço IP, máscara de sub-rede, gateway e interface de rede. As rotas estáticas criadas possuem prioridade sobre as demais rotas existentes.

Para inserir outra rota, clique em Adicionar rota, logo abaixo da tabela de rotas estáticas.

Salve as configurações e acesse o KWebPortal (Interface Web) utilizando o novo endereço IP definido.

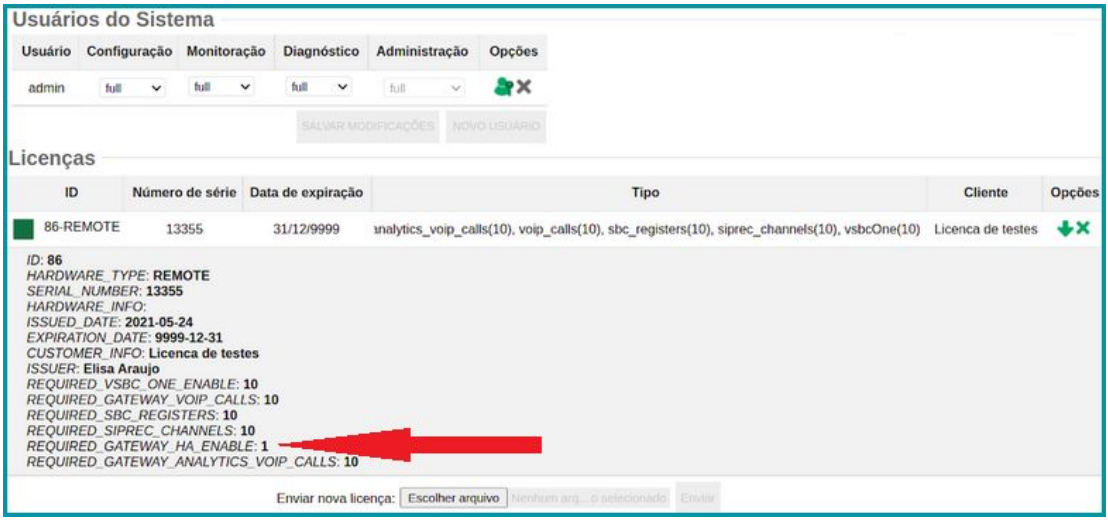
9. Configurar HA - Alta Disponibilidade

HA (High Availability) é um recurso que permite que uma máquina secundária (spare) com o vSBC One W instalado, assuma o tráfego quando ocorrer algum problema com a máquina principal (master).

Para o correto funcionamento do HA, é necessário que ambas as máquinas estejam na mesma rede física. A máquina spare vai espelhar as configurações da máquina master, dando continuidade na operação.

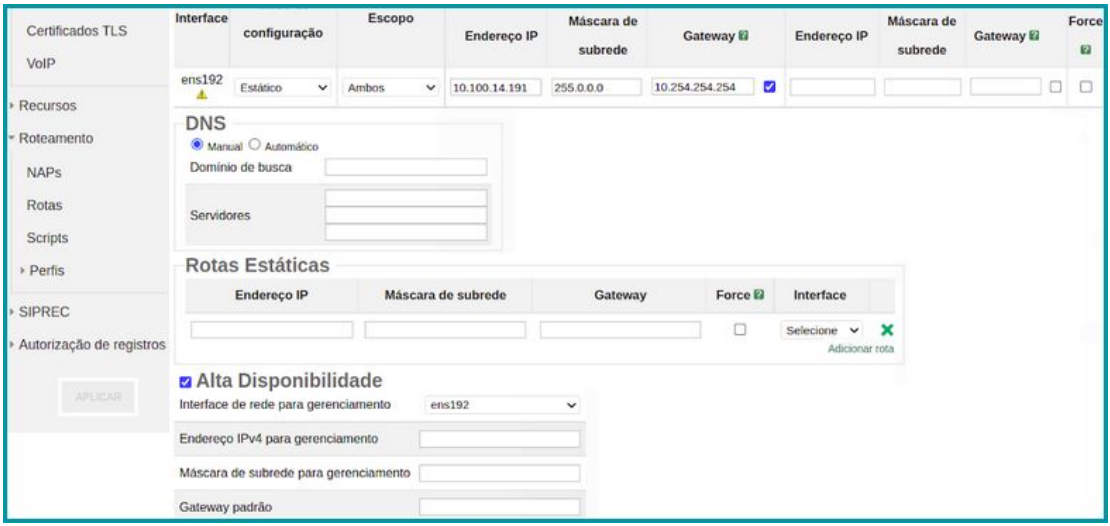
Para configurar o HA nas máquinas, aplique o passo a passo observado a seguir:

1. Confira se sua licença contempla a opção do HA no menu "Administração". No campo "Licenças", clique na licença e verifique se há o campo "HA_ENABLE: 1".

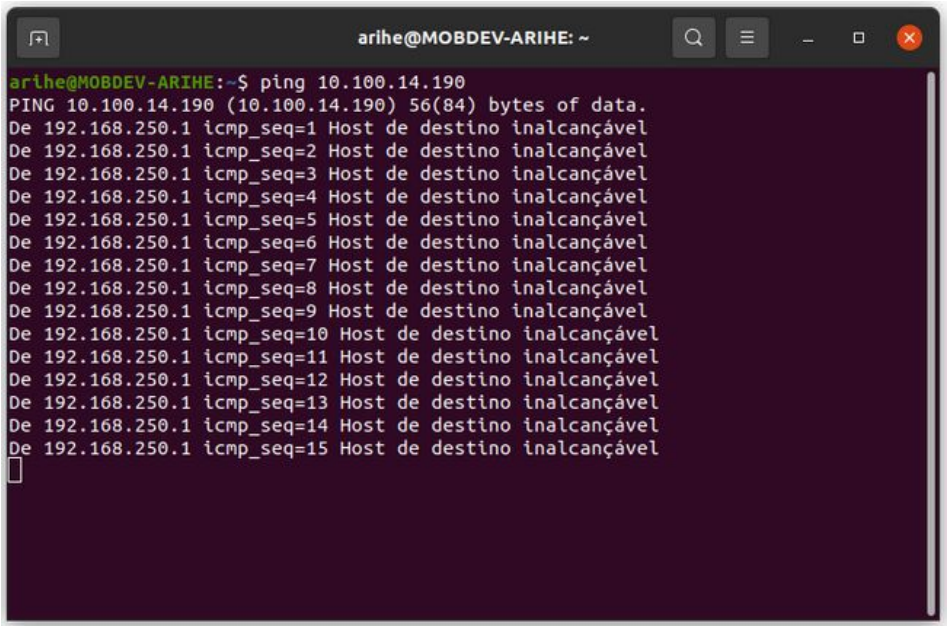


2. Acesse o caminho "**Configuração**" → "**Rede**" → "**Interfaces**" e configure as interfaces de rede como **estáticas**. Não é possível configurar máquinas em HA com interfaces com IP dinâmico (DHCP). Indique os dados de endereço IP, máscara de subrede e gateway.

3. Feita a configuração da interface, vá para o final do menu "Interfaces" e habilite o HA, indicando a interface escolhida. É necessário configurar primeiro a máquina master antes de poder configurar a spare.



4. Selecione o endereço IPv4 para gerenciamento distinto do endereço IP da máquina master. O endereço IP de gerenciamento é um IP que nunca será compartilhado entre as máquinas. O IP de gerenciamento da master somente será atribuído à master e deve ser o IP utilizado para gerenciar e configurar a master após a configuração do HA. É muito importante que nenhum outro equipamento na rede esteja usando o IP que está sendo configurado como IP de gerenciamento. Recomendamos a execução de um ping no endereço almejado, como no exemplo da imagem a seguir:



5. Visto que o endereço IP de destino é inalcançável, indique este endereço no IPv4 para gerenciamento. Agora este endereço será responsável pelo gerenciamento da master.

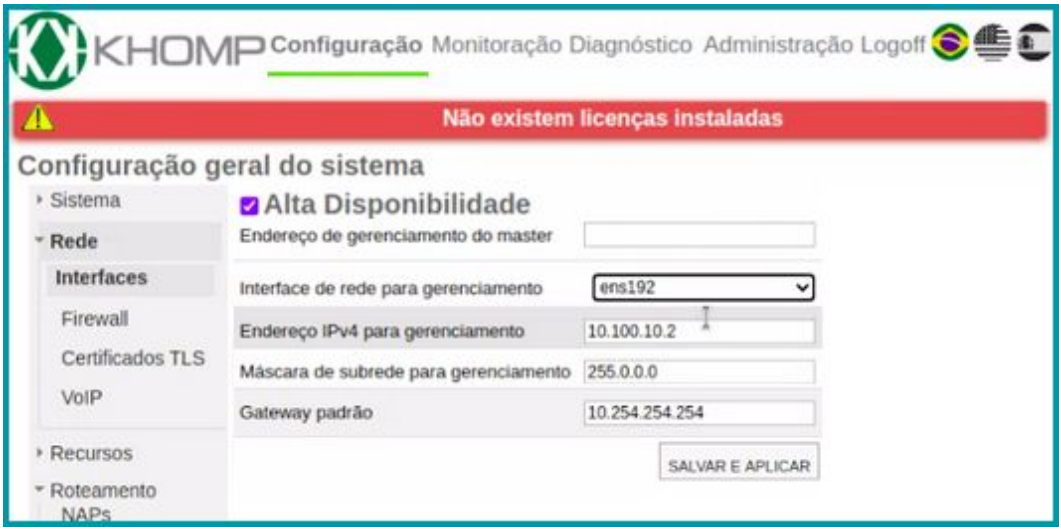
6. Com os mesmos dados da interface, complete os dados da máscara de subrede e o gateway.

7. Na Interface Web da máquina spare, acesse "**Configuração**" → "**Rede**" → "**Interface**". Lembre-se que, na máquina spare é necessário não ter uma licença instalada.

8. Habilite a opção "Alta disponibilidade" (HA).

9. No campo "Endereço de gerenciamento do master", adicione o endereço IP de gerenciamento configurado na master.

10. Preencha os campos de endereço IPv4 para gerenciamento com o IP da máquina, a máscara de subrede e o gateway que deve ser igual ao da máquina master.



11. Acesse os menus "**Monitoração**" → "**Sistema**". Nesta interface podemos ver a configuração da função HA (High Availability ou Alta Disponibilidade). É possível averiguar quais máquinas estão online e realizar transições manuais no sistema. A transição é o processo de trocar qual das máquinas está assumindo o tráfego SIP.

10. Rede firewall

10.1. Endereços liberados

O vSBC permite a configuração de um firewall customizado, incluindo liberação e bloqueio de endereços IPs, habilitação de serviços de rede por interface e detecção de intrusão.

Neste manual, serão alterados os endereços liberados (como exemplo). Acesse "**Configuração**" → "**Rede**" → "**Firewall**" e clique no botão "ADICIONAR" (abaixo de "Endereços liberados"), como demonstra a imagem a seguir.

Os endereços desejados devem ser adicionados um de cada vez.

Nota	• **ANY**: Deixa explícito que qualquer endereço IP poderá acessar o vSBC One W, seja via Interface Web, FTP, SSH e SNMP. • **Endereço IP**: Apenas os endereços IP definidos poderão acessar o vSBC. Exemplo: 192.168.0.5 • **Prefixo de rede**: Apenas os endereços IP pertencentes à faixa especificada poderão acessar o vSBC One W. Exemplo: 192.168.109.0/24

Após verificar as configurações, salve e aplique clicando em "SALVAR E APLICAR" no canto inferior direito da interface.

10.2. Endereços bloqueados

Ao habilitar esta opção, bloqueia qualquer endereço IP que não esteja definido em "Endereços liberados".

Atenção	• Ao habilitar esta opção, certifique-se de que tenha ao menos um endereço IP liberado para acesso ao vSBC One W. • É possível perder o acesso ao equipamento a partir de uma configuração incorreta de firewall.

Após verificar as configurações, salve e aplique clicando em "SALVAR E APLICAR" (no canto inferior direito da interface).

11. Serviços habilitados por interface de rede

Neste subtítulo são definidos os serviços de rede que serão liberados para cada interface de rede. Lembrando que a configuração é cumulativa, ou seja, a lista de endereços liberados e bloqueados tem precedência sobre esta configuração.

A lista de serviços disponíveis é observada na tabela a seguir:

Serviço	Descrição
FTP	Permite a transferência de arquivos.
HTTP	Habilita o acesso à Interface Web.
SSH	Permite administrar de forma remota o vSBC.
SNMP	Habilita o gerenciamento da rede.
ICMP	Permite responder a requisição ICMP (ping).

12. Configurar detecção de intrusão

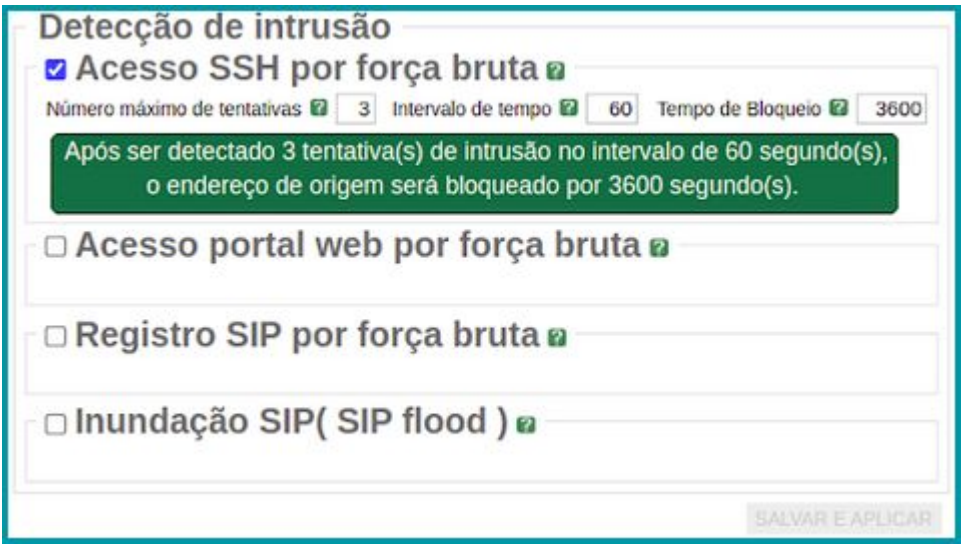
O vSBC One W possui a capacidade de bloquear temporariamente a comunicação com um endereço IP de um dispositivo que tentou acessá-lo e foi mal sucedido múltiplas vezes. O bloqueio é realizado seguindo regras de segurança que se encontram nesta sessão de configuração.

Para configurar a detecção de intrusão através da Interface Web do vSBC One W:

1. Para habilitar este recurso, clique em + Detecção de intrusão.

2. Depois, basta habilitar o tipo de detecção desejado. São quatro tipos de detecção:

- Acesso SSH por força bruta: Bloqueio por excesso de tentativas com falha de acesso SSH.
- Acesso ao portal web por força bruta: Bloqueio por excesso de tentativas com falha de acesso à interface web.
- Registro SIP por força bruta: Bloqueio por excesso de tentativas com falha de registro.
- Inundação SIP (SIP flood): Proteção contra SIP flood.



3. Ao habilitar um tipo de detecção, serão exibidos os campos a seguir. Configure-os de acordo com suas políticas de segurança:

- Número máximo de tentativas: Número máximo de tentativas de acesso ao vSBC One W por um dispositivo. Se este limite for atingido, o endereço IP do dispositivo será bloqueado pelo tempo definido no campo 'Tempo de bloqueio'.
- Intervalo de tempo: Intervalo de tempo, em segundos, que um dispositivo poderá tentar acessar o vSBC One W. Por exemplo: Se houver 3 tentativas mal sucedidas de acesso em 60 segundos, o endereço IP será bloqueado.
- Tempo de bloqueio: Tempo em segundos que um dispositivo, que ultrapasse os limites anteriores, ficará sem poder acessar o vSBC One W. Ao fim do tempo de bloqueio, o dispositivo poderá tentar acessar o vSBC One W novamente.

4. Por fim, clique no botão "Salvar e Aplicar" para que as alterações entrem em operação.

13. Configurações VoIP

Nesta seção são feitas as configurações VoIP do vSBC One W. As configurações aplicadas aqui são globais, e afetam todas as sessões e troncos SIP.

ⓘ	**Nota**	Sempre que houver alterações nas configurações de VoIP, é necessário reiniciar o vSBC One W após clicar no botão "Aplicar".

Acesse "**Configuração**" → "**Rede**" → "**VoIP**", para aplicar as configurações da chamada VoIP.
A tabela a seguir contém a descrição dos campos da configuração do VoIP.

Campo	Descrição
Modo de operação	Os "Modos de operação" são os métodos de processamento de áudio no sistema: **BRIDGE**: Mínima manipulação do áudio, não é possível fazer transcoding. **FULL RTP PROCESSING**: É possível a utilização de qualquer feature, porém requer mais processamento.
Maior porta RTP	Valor máximo da porta RTP que deve ser utilizada para trafegar o áudio das ligações SIP.
Menor porta RTP	Valor mínimo da porta RTP que deve ser utilizada para trafegar o áudio das ligações SIP.
Porta UDP	Porta utilizada para o protocolo SIP sobre UDP.

Campo	Descrição
Porta TCP	Porta utilizada para o protocolo SIP sobre TCP.
Porta TLS	Porta utilizada para o protocolo SIP sobre TLS.
Porta SIP (WebSocket)	Porta utilizada para o protocolo SIP sobre WebSocket.
Porta SIP (Secure WebSocket)	Porta utilizada para o protocolo SIP sobre Secure WebSocket
Ativar substituição automática de caracteres especiais	Alguns caracteres possuem significado especial nos números de A e B (como '#', por exemplo) e necessitam ser codificados como entidades especiais. Alguns equipamentos, entretanto, não aceitam esta codificação. Na maioria dos casos a configuração padrão é a mais indicada.
Ignorar o campo "Contact" dos cabeçalhos, utilizando o campo "To" em seu lugar	Em algumas configurações, as informações desejadas de origem da ligação não estão no campo "Contact" do SIP, mas sim no campo "To". Marcando esta configuração, os dados de origem da chamada serão lidos do campo "To" ao invés do campo "Contact".
Utilizar PRACK (RFC 3262)	Caso habilitado, será enviado o Header Require:100rel nas mensagens 101-199 solicitando o Provisional ACK como resposta.
Habilitar RTCP	Caso habilitado, utiliza RTCP para o controle dos pacotes RTP.
Tipo de payload para o telephone-event	Determina qual tipo de payload DTMF será enviado no SDP.
Tipo de payload para o codec AMR	Determina qual tipo de payload será utilizado para o codec AMR.
Tipo de payload para o codec Opus	Determina qual tipo de payload será utilizado para o codec Opus.
Identificação do usuário do URI	Adiciona a identificação selecionada a URI.
Enviar o parâmetro "transport" do URI	Insere o parâmetro transport, com o tipo de protocolo utilizado a URI.
Tamanho do pacote de áudio	Determina o tamanho do pacote de áudio utilizado em milisegundos.
ToS para pacotes SIP (DSCP)	Marcação dos pacotes de sinalização para ToS.
ToS para pacotes de mídia (DSCP)	Marcação dos pacotes de mídia para ToS
Criptografia TLS	Seleciona a opção de certificado TLS a ser utilizado para os protocolos TLS, WSS e DTLS.

Na seção 'Timers', encontram-se as configurações específicas de temporização SIP.

Campo	Descrição
Timer H	Tempo máximo, em milissegundos, de retransmissão de pacotes SIP. O tempo padrão é 32000 milissegundos.
Espera pelo ACK após 2xx	Tempo máximo, em milissegundos, para a confirmação (ACK) de estabelecimento do diálogo (resposta 200 OK para um INVITE). O tempo padrão é 32000 milissegundos.

Atenção

- Para a utilização do WebRTC é necessário que a Porta SIP (Secure WebSocket) esteja setada, assim como o RTCP deve estar habilitado.
- É necessário ter um certificado para utilizar TLS ou WSS.

14. Configurar NAP

O vSBC One W funciona em um conceito de associações entre NAPs e Rotas.

NAP - Network Access Point é uma representação lógica para agrupar troncos SIP. Estas NAP's serão usadas no roteamento das chamadas, podendo ser pontos de origem, destino ou ambos. Acesse "**Configuração**" → "**Roteamento**" → "**NAPs**" → "**NOVA NAP**".

Nota

- Uma NAP (Network Access Point) é um ponto que pode ser usado como entrada e/ou saída das chamadas.
- A criação da NAP é um procedimento obrigatório. Pois ao criar rotas, é necessário selecionar uma NAP como origem/destino das chamadas.

Antes de vermos o que cada configuração faz é importante sabermos de alguns conceitos importantes para a configuração do WebRTC.

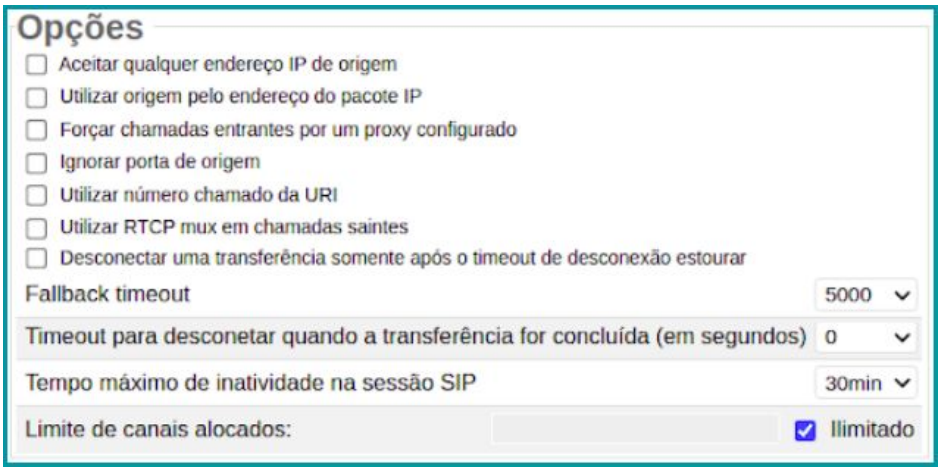
Campo	Descrição
SIP	O Protocolo de Iniciação de Sessão é um protocolo de código aberto de aplicação, que utiliza o modelo “requisição-resposta”, similar ao HTTP, para iniciar sessões de comunicação interativa entre utilizadores.
RTP	RTP é um protocolo utilizado para o transporte de mídias contínuas de tempo real em uma conexão ponto a ponto, como áudio, vídeo ou dados de uma simulação.
UA	End points (ou pontos finais) que usam o SIP para estabelecer e negociar sessões são chamados de user agents (UA). Geralmente, os user agents são chamados de User Agent Server (UAS) e User Agent Client (UAC). No entanto, UAS e UAC são entidades lógicas apenas, sendo que cada UA possui um UAC e UAS. UAC é a parte do UA responsável por enviar requisições e receber respostas. UAS é a parte do UA responsável por receber requisições e enviar respostas.

Campo	Descrição
NAT	NAT significa Tradução de Endereço de Rede. Através de um sistema NAT, endereços privados são traduzidos em um endereço IP público quando são enviadas solicitações de saída dos dispositivos de rede para a Internet. Um processo inverso ocorre quando os dados recebidos, geralmente como uma resposta a solicitações específicas, são enviados para uma rede local. Neste caso, o NAT altera o endereço IP público para o endereço IP privado do dispositivo específico para o qual o pacote de dados é direcionado.
STUN	Um servidor STUN é um servidor público que responde a requisição com o IP e a porta de origem da requisição. Dessa forma é possível para uma máquina com o IP privado em um rede com NAT acrescentar o seu IP público na sinalização SIP. Um exemplo de servidor STUN público e gratuito: stun.l.google.com:19302
ICE	O protocolo ICE pode ser entendido como uma extensão do STUN. Ele é uma forma de enviar múltiplos candidatos de IP (Internos e externos) na sinalização, de forma que durante o diálogo se identifique qual é o endereço apropriado. Senso os possíveis fontes de candidatos: • Endereços locais da máquina. • Respostas de requisições STUN. • Respostas de requisições TURN. • Endereços adicionados manual.
Websocket	Protocolo de comunicação bidirecional sobre uma única comunicação TCP.
Secure Websocket	Websocket com criptografia.
DTLS	Versão do TLS para a transmissão de datagramas.

Para cada tipo de NAP, existirão configurações específicas. A tabela a seguir descreve os campos. Na sequência, há um exemplo prático de uma NAP SIP configurada.

Campo	Descrição
Nome	Nome escolhido para a NAP.
Tipo	Selecione a opção "SIP" para configurar uma NAP VoIP.
Perfil	Permite a escolha do perfil de telefonia, em dúvida recomenda-se a opção "Utilizar perfil padrão", que atende a maioria dos cenários.
Script	Permite a seleção de um script criado previamente em Configuração → Roteamento → Script.
Domínio	Endereço IP do host.
Porta do domínio	Porta SIP de escuta do domínio.

Campo	Descrição
Desativado	Sem registro.
Enviar Registro	Registra o vSBC no host da NAP.
Receber e finalizar registro	Endpoint de registro. Permite que agentes se registrem no vSBC.
Receber registro a ser encaminhado	Ponto de entrada de registro. Opção para fazer o roteamento de registro.
Encaminhar Registro	Ponto de saída de registro. Opção para fazer o roteamento de registro.



Campo	Descrição
Aceitar qualquer endereço IP	Ao ativar, possibilita que a NAP aceite pacotes vindo de qualquer endereço IP.
Utilizar origem pelo endereço do pacote IP	Se ativado, utiliza o endereço do pacote IP como "Domínio" para validação em ligações entrantes, ao invés de utilizar o valor contido no campo "From".
Forçar chamadas entrantes por um proxy configurado	Se ativado, serão aceitas apenas as chamadas originadas dos servidores proxy definidas na "Lista de Proxy".
Ignorar porta de origem	Ao ativar, possibilita ignorar a porta de origem do pacote SIP em ligações entrantes.
Utilizar número chamado pela URI	Se ativado, utiliza o número chamado enviado no header "RequestURI" ao invés de utilizar o valor do campo "To" em ligações entrantes.
Utilizar RTCP mux em chamadas saíntes	Quando ativado, permite o uso de RTCP mux em chamadas saintes.
Desconectar uma transferência somente após o timeout de desconexão estourar	• Tempo máximo, em milissegundos, de retransmissão de pacotes SIP. O tempo padrão é 32000 milissegundos. • Tempo máximo, em milissegundos, para a confirmação (ACK) de estabelecimento do diálogo (resposta 200 OK para um INVITE). O tempo padrão é 32000 milissegundos.
Fallback timeout	Tempo limite para realizar a chamada por esta rota. Se houver indisponibilidade deste servidor SIP, outra rota válida é utilizada.
Tempo máximo de inatividade na sessão SIP	Período para o encerramento da chamada caso o servidor SIP fique inativo (RFC 4028 - Session Timer). Esta opção serve para evitar que uma sessão SIP fique ativa por um período indeterminado, uma vez que a sessão é encerrada apenas com o evento BYE. Desta forma, o vSBC One encerra a chamada, caso o servidor SIP não faça uma revalidação. Valor padrão: **30 minutos**.
Limite de canais alocados	Limita a quantidade de canais VoIP que esta NAP pode usar. Este limite se aplica a ligações entrantes e saintes. É necessário desabilitar a opção "Ilimitado" para então, poder definir um valor. Valor padrão: ilimitado.

Keep alive é um recurso para se observar se a NAP está ativa.

Se o recurso estiver ativado, o vSBC irá verificar se o host da NAP está ativo frequentemente. Caso a NAP não retorne uma resposta, o vSBC irá considerar a NAP inativa.

Opções para utilizar o Keep Alive: Desativado, SNMP ou SIP OPTIONS.

Valor padrão: Desativado.

Campo	Descrição
Interface de rede para o protocolo SIP	Define qual a interface de rede que deve ser utilizada para o protocolo SIP.
Interface de rede para o protocolo RTP	Define qual a interface de rede que deve ser utilizada para o protocolo RTP.
Modo de travessia NAT	Habilita ou desabilita o suporte à travessia de NAT. As opções são: Desativado, Servidor STUN, ICE e Endereço IP externo fixo.
STUN	Caso esteja habilitada a travessia de NAT por "Servidor STUN", este campo deve ser preenchido com o endereço IP do servidor STUN. Indica-se o servidor google. Exemplo: stun.l.google.com
Porta do STUN	Caso esteja habilitada a travessia de NAT por "Servidor STUN ou ICE", este campo deve ser preenchido com a porta de rede do servidor STUN. Indica-se o servidor google. Exemplo: **19302**
STUN a ser utilizado com o ICE	Caso esteja habilitada a travessia de NAT por "ICE", este campo deve ser preenchido com o endereço IP do servidor STUN. Indica-se o servidor da google. Exemplo: stun.l.google.com
Endereço IP externo para o protocolo SIP com ICE	Deve ser colocado o endereço IP público do vSBC.
Endereço IP externo para o protocolo SIP	Caso esteja habilitada a travessia de NAT por "Endereço IP externo fixo". Também no campo "Endereço IP externo para o protocolo RTP", este campo deve ser preenchido com o endereço IP externo utilizado para o protocolo SIP.
Endereço IP externo para o protocolo RTP	Caso esteja habilitada a travessia de NAT por "Endereço IP externo fixo", este campo deve ser preenchido com o endereço IP externo utilizado para o protocolo RTP.

Campo	Descrição
Aceitar qualquer tipo de transporte para o SIP em chamadas entrantes	Aceita qualquer protocolo de sinalização SIP entrante para este NAP.
Aceitar qualquer tipo de transporte para o áudio (RTP) em chamadas entrantes	Aceita qualquer protocolo de áudio RTP entrante para este NAP.
Tipo de transporte para o SIP	Define o tipo de transporte a ser utilizado para o protocolo SIP. Onde para o WebRTC temos como principais protocolos o **WS** e **WSS**.
Tipo de transporte para o áudio	Define o tipo de transporte a ser utilizado para o protocolo RTP. Onde para o WebRTC temos como principal protocolo o **DTLS**.
Configurações dos proxys: Host, Porta, Interfaces para sinalização e áudio, e tipo de transporte para sinalização e áudio.	Proxys utilizados para aceitar chamadas, ou para enviar, como opções em caso de fallback.
Sobrescrever Header "From"	Sobrescreve o header "From" dos pacotes SIP, quando a NAP é utilizada como destino. Deve ser utilizado o formato: 127.0.0.1:5060

14.1. Configuração de NAPs com registro

As NAPs que estão utilizando as opções "Receber e finalizar registro" ou "Receber registro a ser encaminhado" necessitam de alguns cuidados a mais na sua configuração.

Os campos "Domínio" e "porta" possuem um comportamento levemente diferente de NAPs sem estas opções de registro.

Domínio

O campo "Domínio" de uma NAP com registro, deve coincidir com o URI no REGISTER enviado pelo agente. Ou seja, este campo deve conter o FQDN ou IP público utilizado pelo agente para realizar a conexão com o vSBC. Por exemplo, vsbc.khomp.com.

porta

O campo "porta do domínio" deve receber o valor da porta configurada para o protocolo de transporte selecionado para o SIP nesta NAP. Por exemplo, caso se deseje que a NAP aceite tráfego SIP utilizando o transporte TLS e este transporte está configurado na porta 5061, é necessário inserir o valor 5061 no campo "porta do domínio".

A seguir, apresentaremos uma imagem representando a configuração da NAP onde o vSBC é acessado pelo FQDN "vsbc.khomp.com" e a qual está configurada para utilizar o protocolo WSS (configurado na porta 5063).

15. Configuração de rotas de registro

Rotas de chamada

Nas rotas de chamada, são configuradas as rotas e NAPS que fazem a conexão das chamadas de um ponto a outro. Acesse "Configuração" → "Roteamento" → "Rotas de registro" → "NOVA ROTA", para a criação de uma rota de registro.

As únicas NAPs disponíveis para seleção de NAPs de origem em rotas de registro são aquelas que foram configuradas como "Receber registro a ser encaminhado".

Somente as NAPs configuradas como "Encaminhar registro" estarão disponíveis para a configuração de NAPs de destino em rotas de registro.

Rotas de registro

As rotas de registro, por outro lado, são utilizadas para configurar o encaminhamento de registro. Cenário útil quando outro equipamento deve lidar com a gerência de registros.

Nota

- Após a criação de uma rota de registro, são criadas duas rotas de chamada implícitas. Uma com as mesmas NAPs de origem e destino e outra com os campos trocados.
- Este comportamento tem o intuito de facilitar a configuração de cenários onde o equipamento responsável pelo registro também possa rotear as chamadas relacionadas a estes registros.
- Caso este comportamento não seja desejado, pode-se utilizar rotas de chamada para alterá-lo. As **rotas de chamada** têm prioridade sobre as **rotas de registro**!

Campo	Descrição
Nome	Nome para identificação da rota.
Prioridade	Prioridade de verificação da rota sobre as demais, caso a rota seja semelhante a outra. Este valor varia entre 0 e 99, onde 0 indica rota com prioridade máxima e 99 indica a rota com prioridade mínima.
NAP origem	Selecione o NAP de entrada do registro.
NAP destino	Selecione o NAP para onde deve ser encaminhada o registro caso todas as regras sejam satisfeitas

Atenção

Após o ajuste das configurações, deve-se clicar no botão "Aplicar" no canto inferior esquerdo.

16. Obter acesso à documentação adicional

Você encontra o manual e outros documentos em nosso site, www.khomp.com. Veja a seguir como se cadastrar e acessar nossa documentação:

Para usuários que não possuem cadastro:

1. No site da Khomp, acesse o menu "Suporte Técnico" → "Área restrita".
2. Clique em "Inscreva-se".
3. Escolha o perfil que melhor o descreve.
4. Cadastre seu endereço de e-mail. É necessário utilizar um e-mail corporativo.
5. Preencha o formulário que será enviado ao seu e-mail. Caso não tenha recebido em sua caixa de entrada, confira sua caixa de spam.
6. Siga os passos descritos a seguir para fazer login na área restrita.

Para usuários que possuem cadastro:

1. Acesse o menu "Suporte Técnico" → "Área restrita".
2. Faça login com seu endereço de e-mail e senha cadastrada.
3. Acesse a opção Documentos. Você será direcionado à Wiki da Khomp.

Você também pode entrar em contato com nosso suporte técnico através do e-mail suporte.comunicacoes@khomp.com , pelo telefone +55 (48) 37222940.

Manual do Usuário

Linha KMG One

KHOMP

ENABLING TECHNOLOGY

07300403

Khomp - Todos os direitos reservados

Índice

1. Introdução

Este manual é destinado aos profissionais responsáveis por administrar os media gateways da linha KMG. Este documento contém as informações necessárias para a instalação, configuração e gerenciamento, assim como as especificações técnicas dos media gateways.

1.1. Como ler este manual

Se este é seu primeiro contato com o KMG, recomenda-se a leitura completa deste manual. Se você está familiarizado com o gateway, os principais procedimentos estão divididos em tópicos para facilitar a busca pela resolução de um problema ou dúvida.

No início de cada seção de configuração, é descrito o caminho para acessar a interface de configuração. Dependendo da versão do seu KMG, o caminho de acesso pode ser diferente. Para verificar a versão do seu KMG, consulte a seção *"Verificar versão do KMG"* neste manual.

Os recursos que estiverem presentes apenas em determinados modelos, serão notificados no início da seção correspondente ao recurso. O mesmo vale para os recursos que são disponibilizados mediante aquisição de licença adicional.

2. Apresentação da linha KMG

KMG é a linha de media gateways da Khomp desenvolvida para oferecer modularidade e segurança à sua rede de telefonia.

Modularidade porque você pode ter todas as interfaces de telefonia em um único media gateway. Desta forma você pode ter interfaces de telefonia digital E1/T1, interfaces analógicas FXS e FXO e interfaces de telefonia móvel GSM 2G e 3G com um único media gateway.

Todos os modelos da linha possuem recursos de segurança proporcionados pelo SBC (Session Border Controller) da Khomp. Desta maneira você possui os recursos necessários para aumentar a segurança da sua rede de telefonia.

Além dos recursos mencionados, com os media gateways da linha KMG você pode obter economia nos custos com tarifação de telefonia. Com a criação de rotas de menor custo, você pode direcionar cada chamada para a operadora que ofereça a menor tarifação. Além de rotas de menor custo, é possível criar ainda fallback de rotas, balanceamento e, ainda, rotas que operam conforme o horário programado.

Legenda: *Imagem modelo KMG 3200 One.*

Toda a configuração e gerenciamento é feito através de uma Interface Web que pode ser acessada por qualquer navegador.

2.1. Visão geral dos modelos

A seguir você encontra uma visão geral dos modelos da linha KMG One.

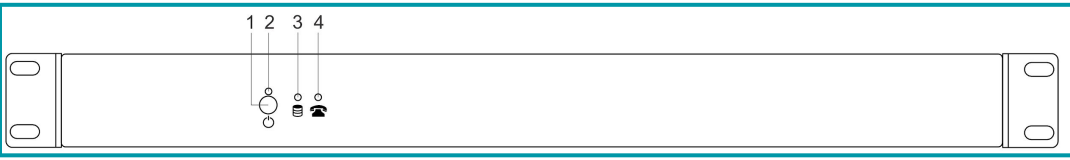
Atenção

- O hardware do produto pode ser substituído sem aviso prévio.
- A substituição acontece quando a matéria prima não é encontrada no mercado ou quando surgem hardwares melhores.
- Quando o hardware é substituído, o produto vai operar com o mesmo potencial da configuração anterior.

2.1.1. KMG 200 One

O KMG 200 é um media gateway de baixa densidade que suporta até 240 chamadas simultâneas com até 2 links E1/T1 internos, além de até 8 módulos externos para as tecnologias E1, GSM, FXS, FXO ou VoIP SBC. Com a possibilidade de até 120 chamadas com transcoding (G.729/G.722 ↔ G.711). Veja a seção *"Capacidade de chamadas simultâneas"* neste manual para mais informações sobre a capacidade do KMG 200. É adquirido com a opção de 0, 1 ou 2 links internos E1/T1.

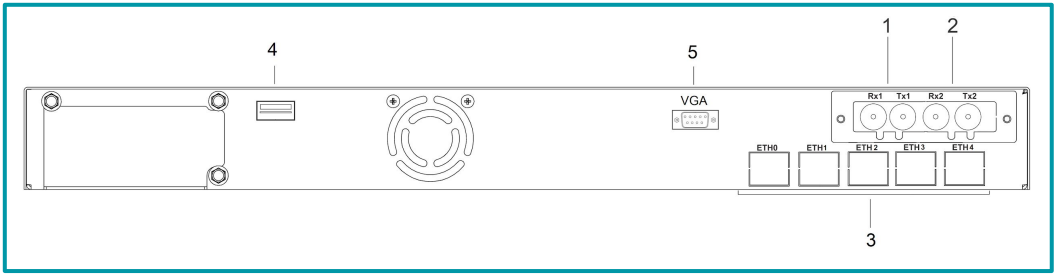
Vista frontal



Legenda:

1	Botão liga / desliga
2	LED de energia
3	Status da atividade do disco
4	Status da atividade dos módulos de telefonia

Vista traseira



Legenda:

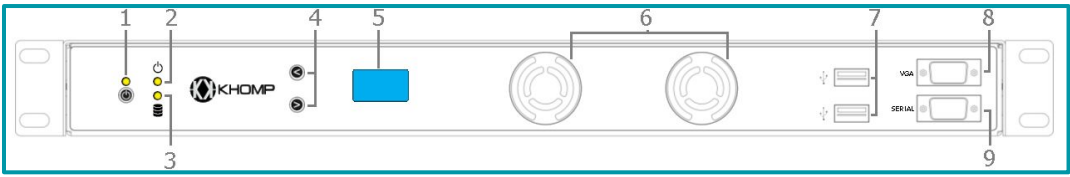
1	Link 1 do E1/T1
2	Link 2 do E1/T1
3	ETH0 a ETH4: porta Ethernet gigabit. Porta de rede padrão.
4	Porta USB 2.0
5	Porta VGA

2.1.2. KMG 3200 One

O KMG 3200 é um dispositivo de alta densidade que pode ter até 64 links E1/T1 ou 2000 chamadas simultâneas para as tecnologias E1, GSM, FXS, FXO ou VoIP SBC. Com a possibilidade de até 1000 chamadas com transcoding (G.729/G.722 ↔ G.711). Veja a seção *"Capacidade de chamadas simultâneas"* neste manual para mais informações sobre a capacidade do KMG 3200.

As interfaces de telefonia são disponibilizadas somente através dos módulos externos de telefonia → Módulo KMG (veja a seção *"Interfaces de telefonia"* neste manual para mais informações).

Vista frontal

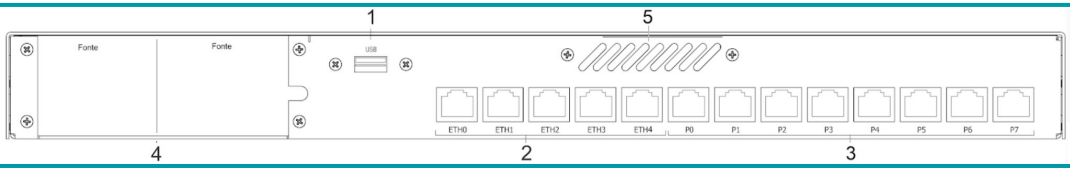


Legenda:

1. Botão Liga/Desliga.
2. LED de energia.
3. LED de atividade no disco.
4. Botões para navegação do display LCD frontal.
5. Display LCD para exibir informações do gateway.
6. Entrada e saída de ar para refrigeração interna.
7. Duas portas USB 2.0.
8. Porta VGA.
9. Interface serial (RS-232 conector DB-9).

- LED Status da fonte redundante apagado: Indica que as duas fontes estão ligadas.
- LED Status da fonte redundante piscando: Indica que uma das fontes está desligada.

Vista traseira



Legenda:

1. Porta USB 2.0.
2. Interfaces de rede para gerenciamento e VoIP.
3. Interfaces de rede para conexão com módulos externo de telefonia ou VoIP.
4. Fonte de energia.
5. Entrada/saída de ar (refrigeração interna).

2.2. Recursos da linha KMG One

Os recursos a seguir estão presentes em todos os modelos da linha KMG One.

- Interface Web HTTP/HTTPS com gerenciamento de usuários e controle de acesso.
- Suporte às interfaces de telefonia: E1/T1, FXS, FXO e GSM 2G e 3G.
- Suporte às sinalizações TDM ISDN e R2 (R2 disponível somente para E1).
- Codecs suportados:
  - G.711 A-law.
  - G.711 μ-law.
  - G.729A.
  - G.722.
  - GSM.
  - DVI4.
- Cancelamento de eco.
- Roteamento baseado em:
  - Origem e destino.
  - Prefixo.
  - Horário.
  - Consulta a base de Portabilidade.
  - Script de roteamento.
- Balanceamento de carga no roteamento.
- CDR personalizável e suporte a RADIUS.
- Suporte SNMP.
- Buffer de Jitter para corrigir automaticamente as latências na rede de forma dinâmica.
- Travessia NAT (IP externo, STUN).
- Provisionamento (exportação e importação de configurações).
- Suporte a TR-069.
- Suporte a SIP-I.
- DTMF: In band, Out band – RTP (RFC 2833) ou Out band – SIP Info.
- Histórico e restauração de alterações de configuração via Web.
- Terminal remoto com advanced CLI (Command Line Interface).

2.2.1. Recursos de segurança

- Ocultação da topologia de rede.
- Detecção de pacotes RTP maliciosos.
- Lista de controle de acesso → ACL.
- Proteção contra pacotes malformados.
- Bloqueio de chamadas por destino e origem.
- Proteção DoS/DDoS.
- Protocolos SIP TLS e SRTP (SDES e DTLS).

2.2.2. Recursos opcionais

Os recursos a seguir são disponibilizados através da aquisição de licença adicional (não incluso no KMG por padrão)

- Sobrevivência → SAS.
- Alta Disponibilidade → HA[1].
- Autorização de Registros.
- Suporte a ISUP (SS7), SIGTRAN.

[1] *O KMG 400 One não suporta a função HA. O módulo EBS interno, se existir, não suporta a função HA.*

2.3. Interfaces de telefonia → Módulo KMG

As interfaces de telefonia podem ser disponibilizadas através do Módulo KMG → módulo externo de telefonia ou integrado no próprio media gateway (KMG 200 e KMG 400).

Os Módulos KMG possuem diferentes modelos que oferecem as interfaces E1/T1, FXS, FXO e GSM, proporcionando um media gateway escalável e com expansão otimizada.

***Legenda**: Imagem do Módulo KMG.*

Os módulos são conectados ao servidor do KMG através da interface Ethernet. Foram projetados para instalação em rack, sendo que cada módulo ocupa 1U e meio rack de 19 polegadas.

Legenda: *Exemplo de montagem de um KMG 3200 One com 8 Módulos KMG.*

Visão traseira dos Módulos KMG

Legenda: *Módulo KMG E1.*

Legenda: *Módulo KMG GSM.*

Legenda: *Módulo KMG FXO.*

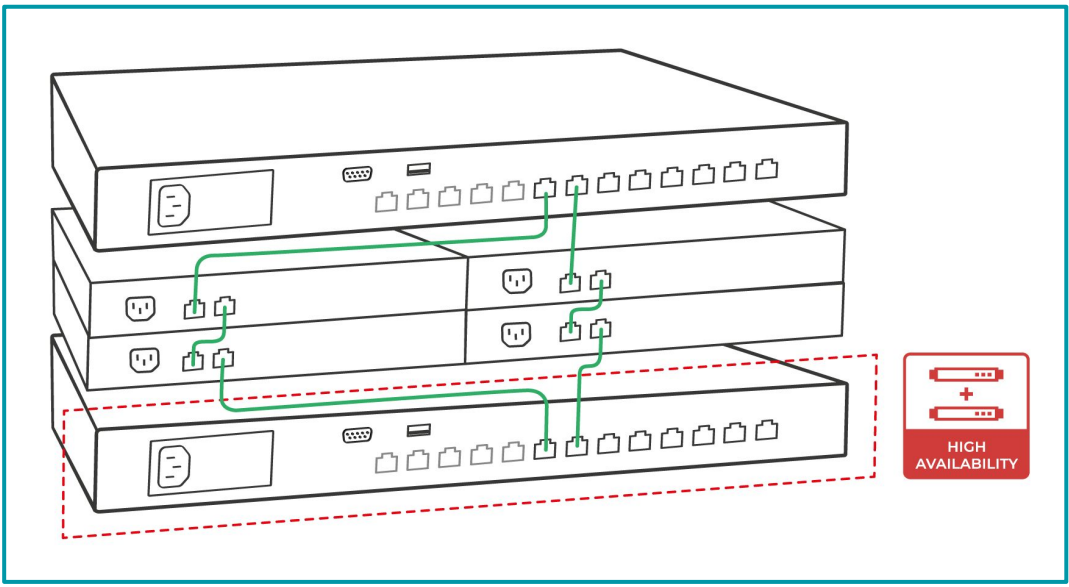
Legenda: *Módulo KMG FXS.*

Legenda: *Módulo KMG Modular (sem interfaces de telefonia).*

ⓘ	**Nota**	O módulo KMG é uma variação comercial do módulo EBS, sendo explicitamente o mesmo hardware, diferenciando apenas pela forma de licenciamento de recursos.

2.3.1. Conexão física dos módulos KMG

Os módulos precisam ser conectados às interfaces que serão usadas para isso. Maiores informações podem ser verificadas na seção *"Configurações de rede"*. A conexão física pode ser realizada conforme a imagem a seguir:



O módulo KMG é conectado à interface de rede configurada, e caso a quantidade de módulos externos seja maior que a quantidade de portas disponíveis no servidor, a segunda interface de rede do módulo pode ser conectada a primeira interface de rede do segundo módulo, permitindo o uso da capacidade máxima do equipamento, realizando a conexão em cascata em até um nível.

Caso exista a solução de HA, o segundo módulo de telefonia pode ser conectado ao servidor KMG spare, estabelecendo a conexão completa de alta disponibilidade do sistema, contemplando todos os módulos externos de telefonia.

2.4. Capacidade de chamadas simultâneas

A quantidade de chamadas simultâneas do KMG é a soma de todos os canais de telefonia (E1/T1, FXS, FXO e GSM) e sessões VoIP. Se o equipamento estiver configurado em modo transcoding o valor é reduzido pela metade para o uso dos codecs g.729 e G.722 devido ao processamento realizado.

KMG 200 → Até 240 chamadas simultâneas TDM ou VoIP (SBC). No caso de transcoding este valor é reduzido pela metade, ou seja 120 chamadas simultâneas em qualquer sinalização.

KMG 3200 → Até 2000 chamadas simultâneas TDM ou VoIP (SBC). No caso de transcoding este valor é reduzido pela metade, ou seja 1000 chamadas simultâneas em qualquer sinalização.

3. Especificações técnicas

A seguir são fornecidas as especificações técnicas do media gateway e dos módulos de telefonia.

3.1. Media gateway

A seguir você encontra as especificações técnicas dos media gateways.

Item	KMG 200 One	KMG 3200 One
Rede	5 x RJ45 10/100/1000 Mbps	13 x RJ45 10/100/1000 Mbps
Dimensões (L x A x C)	430x44x185 mm	437,8x44,45x380 mm
Peso aproximado	3,2 Kg (sem embalagem)	7,5 Kg (sem embalagem)
Temperatura de operação	0–50 °C	
Umidade de operação	10–90% não condensado	
Fonte de energia → Full range	100–240 VAC, 50/60 Hz	
Consumo máximo de energia	150 W	120 W

3.2. Módulo Externo de telefonia

A seguir você encontra as especificações técnicas dos Módulos KMG.

Item	Módulo KMG E1	Módulo KMG GSM	Módulo KMG FXO	Módulo KMG FXS	Módulo KMG Modular
Rede	2 x RJ45 10/100 Mpbs				
Dimensões (L x A x C)	220,5 x 44,5 x 280 mm				
Peso aproximado (sem embalagem)	2,6 a 2,8 Kg	2,6 a 4 Kg	2 a 2,2 Kg	2,7 KG	2,6 KG
Temperatura de operação	0–50 ºC				
Umidade de operação	10–90% não condensado				
Fonte de energia → Full range	100–240 VAC, 50/60 Hz				
Consumo máximo de energia	150 W	150 W	120 W	150 W	120 W

3.3. Interfaces de telefonia

E1/T1

Item	Descrição
Conector disponível	BNC coaxial ou RJ45
Resistência elétrica	• BNC coaxial: 70 Ohms • RJ45: 120 Ohms
Sinalização	ISDN e R2 (R2 somente para E1)
Uso do ISDN	PRI (Primary Multiplex)

GSM

Item	Descrição
Tamanho do SIM card suportado	mini SIM (2FF)
Bandas suportadas	• 2G Quad-band: 850/900/1800/1900 MHz • 3G Penta-band: 850/900/1700/1900/2100 MHz com fallback para 2G Quad-band

FXO

Item	Descrição
Sensor de ring mínimo	13,5 Vrms@ 13–68 Hz
ensor off-hook	5–20 V

FXS

Item	Descrição
Tensão de toque (ring)	50–70 Vpp/25 Hz
Tipo de linha	Balanceada
Resistência de loop (máxima)	1300 Ohms, incluindo aparelho telefônico
Corrente de loop	20 mA
Alimentação dos ramais	27 VDC
Distância suportada[1]	• Até 5 Km com fio de 100 Ohms/Km (Condutor de cobre AWG24) • Até 4 Km com fio de 125 Ohms/Km (Condutor de cobre AWG26)

[1] *Considerando aparelho telefônico com circuito de loop de 300 Ohms.*

4. Instalação do KMG

O KMG foi projetado para ser instalado em racks de 19 polegadas. O media gateway (servidor), ocupa 1U. Os módulos externos de telefonia → Módulo KMG, ocupam 1U adicional e meio rack. Se você adquiriu apenas um Módulo KMG, é enviado uma aba para fixação no rack.

A instalação, tanto do media gateway quanto do Módulo KMG, deve ocorrer em ambientes com temperatura variando entre 0 a 50º celsius e com umidade entre 0 a 90% não condensado.

4.1. Conexão de rede

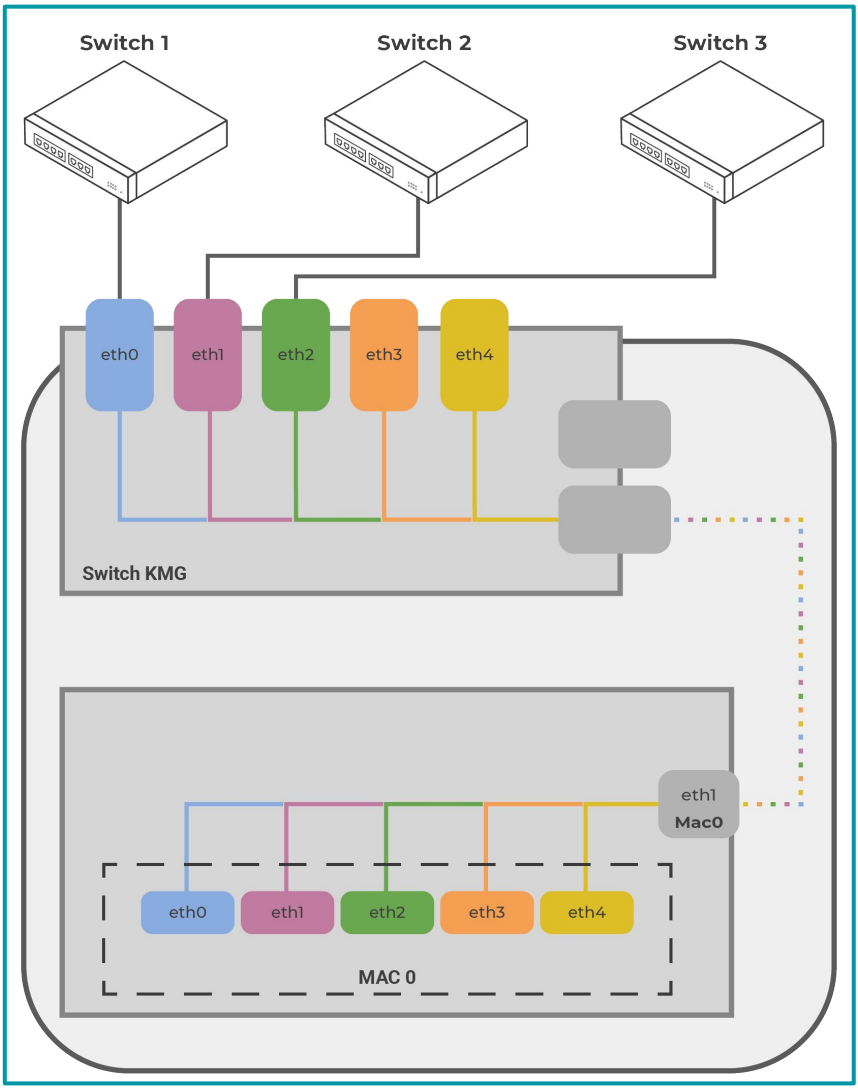
Os media gateways possuem um switch com controladora de rede dedicado. Este switch varia a quantidade de portas de rede externas de acordo com o modelo. A tabela a seguir possui a descrição dos gateways e a respectiva quantidade de portas de rede.

Quantidade de portas	Modelo
5	KMG 200 One
	KMG 400 One
8	KMG 1600 One
13	KMG 3200 One

Legenda: *Vista traseira do KMG 200 One com dois Links E1*

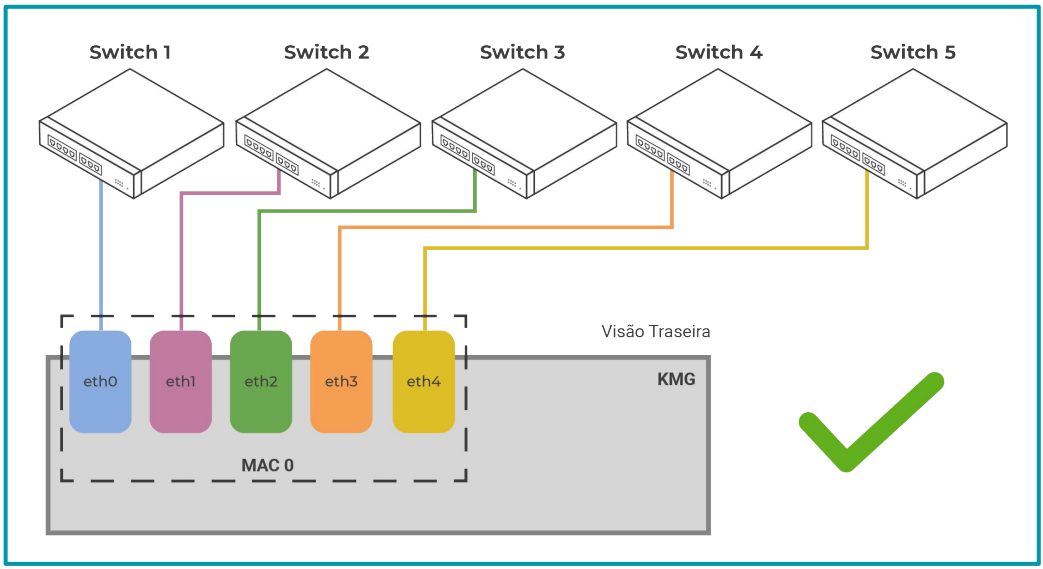
As interfaces de rede dos gateways que possuem 5 portas de rede são nomeadas da seguinte forma: eth0, eth1, eth2, eth3 e eth4. Estas cinco interfaces possuem o mesmo endereço MAC, pois estão ligadas a mesma porta da controladora de rede. Portanto é necessário que cada porta do KMG seja conectada em redes fisicamente separadas. Em cada interface de rede virtual é possível a configuração de VLAN possibilitando sua propagação à rede local.

Na imagem a seguir o KMG foi conectado em 5 redes fisicamente separadas.

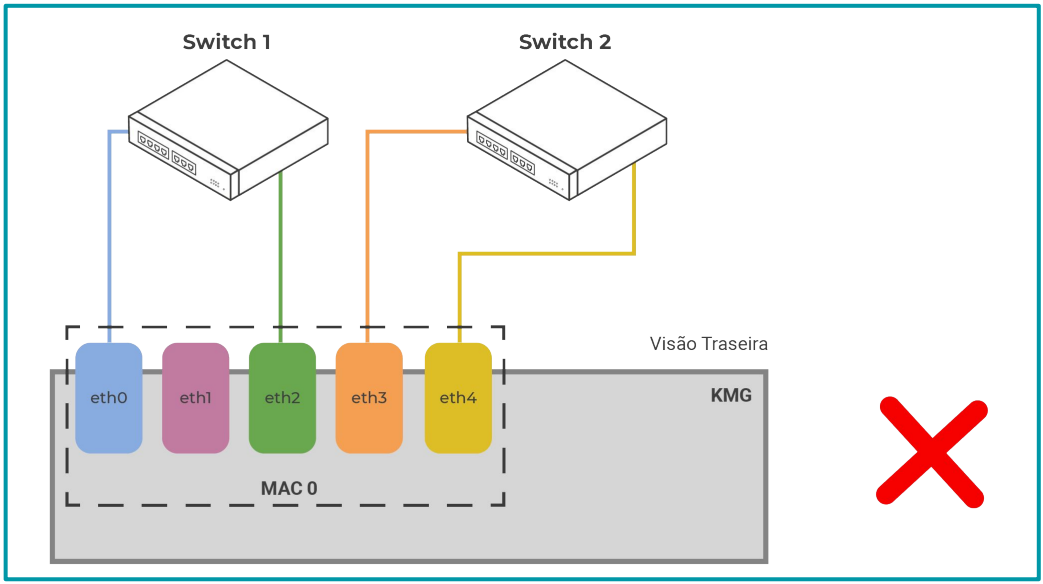


Legenda: *Fluxo interno de rede no KMG com 5 portas de rede*

Conecte as portas do KMG em redes físicas diferentes, uma vez que o endereço MAC é compartilhado entre as portas de rede, conforme demonstrado na figura a seguir.



Legenda: *Exemplo da instalação correta.*



Legenda: *Exemplo de uma instalação incorreta.*

KMG com 8 portas de rede → KMG 1600 One

O KMG 1600 apesar de ter 8 portas de rede externas, segue as mesmas especificações e conexões que o KMG 400.

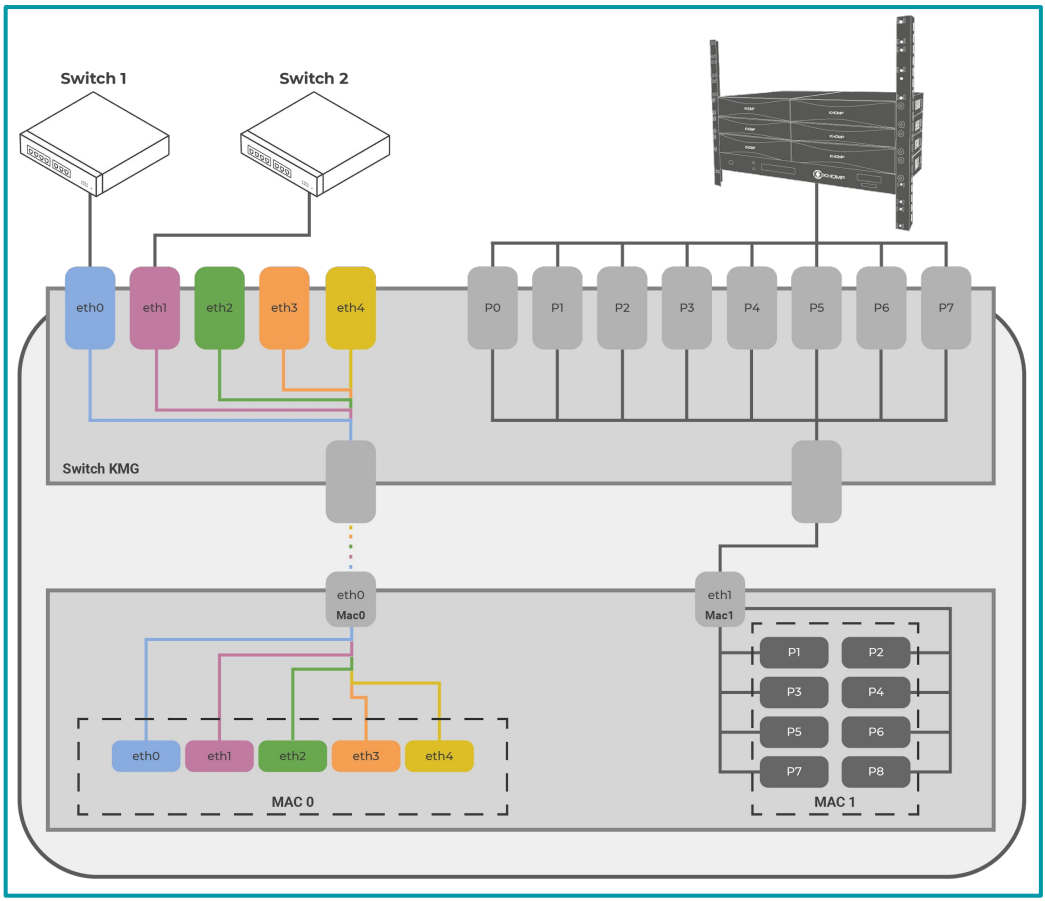
KMG com 13 portas de rede

Legenda: *Visão traseira do KMG 3200 One.*

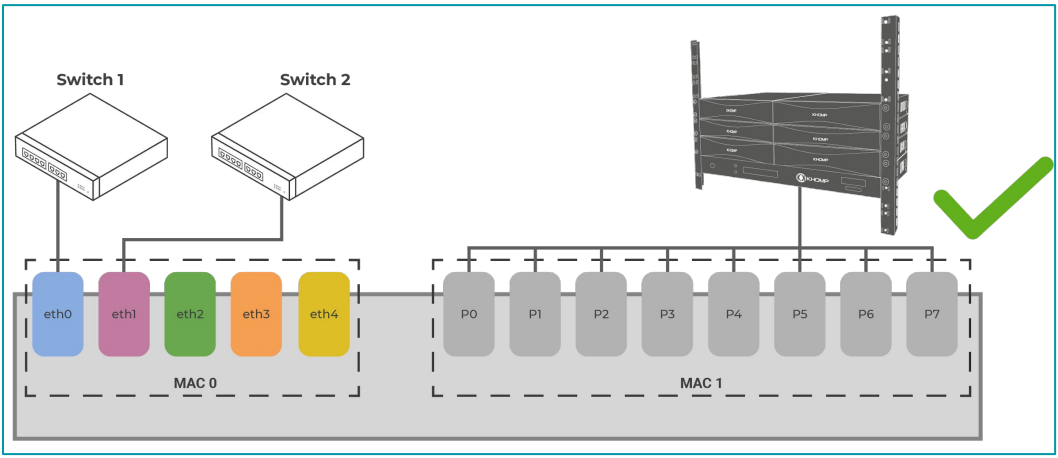
As interfaces de rede do KMG, com 13 portas (10/100/1000 Mbps), estão dispostas da seguinte forma: As portas eth0, eth1, eth2, eth3 e eth4 podem ser utilizadas exclusivamente para rede e possuem o mesmo endereço MAC, pois estão ligadas a mesma porta da controladora de rede. Portanto, é necessário que as portas eth0 à eth4 sejam conectadas em redes fisicamente separadas.

As 8 portas de rede finais, de P0 a P7, são especificadas para conexão com módulos externos de telefonia → Módulo KMG, mas também podem ser usadas para conexão com outras redes VoIP, desde que sejam redes diferentes. Estas interfaces possuem um endereço MAC distinto das portas eth0 à eth4.

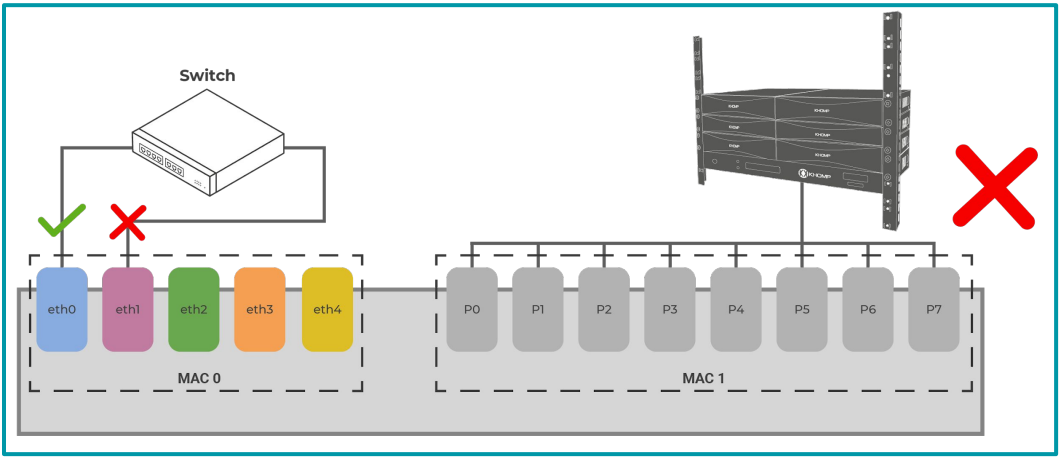
Na imagem a seguir o KMG de 13 portas está conectado em 2 redes fisicamente separadas.



Legenda: *Fluxo interno de rede no KMG com 13 portas de rede*



Legenda: *Exemplo da instalação correta.*

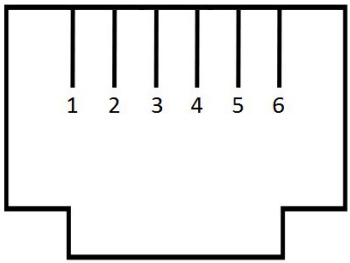


Legenda: *Exemplo de uma instalação incorreta.*

4.2. Conexão analógica → FXO

A interface analógica FXO é disponibilizada através de conector RJ11. A tabela a seguir informa o esquema do cabo para conexão na interface FXO.

Pino RJ11	Função
1	Não conectado
2	Não conectado
3	Ring
4	Tip
5	Não conectado
6	Não conectado

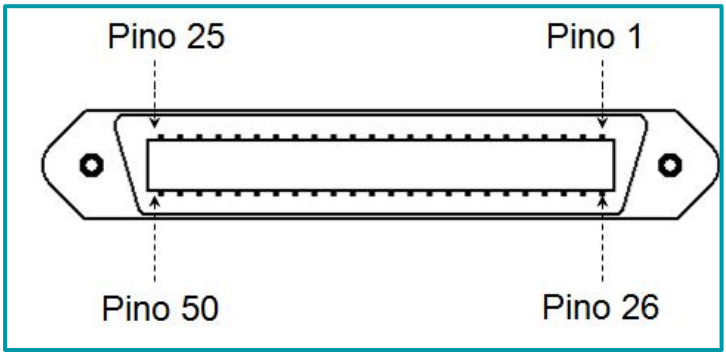


4.3. Conexão analógica → FXS

A interface FXS pode ser disponibilizada de duas formas: Conexão Centronics e RJ45. No módulo KMG FXS, você encontra uma conexão Centronics. No KMG 400 e no Módulo KMG Modular com FXS, esta interface é disponibilizada a través de conectores RJ45.

4.3.1. Conector Centronics

Nesta conexão os ramais são conectados através do conector Centronics de 50 vias. O conector deve ser montado de acordo com as seguintes especificações para o correto funcionamento do módulo:



Legenda: *Disposição dos canais no conector Centronics.*

Pino	Sinal	Pino	Sinal	Canal
1	TIP01	26	RING1	1
2	TIP02	27	RING2	2
3	TIP03	28	RING3	3
4	TIP04	29	RING4	4
5	TIP05	30	RING5	5
6	TIP06	31	RING6	6
7	TIP07	32	RING7	7
8	TIP08	33	RING8	8

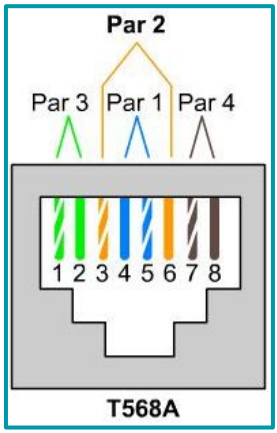
Pino	Sinal	Pino	Sinal	Canal
1	TIP01	26	RING1	1
2	TIP02	27	RING2	2
3	TIP03	28	RING3	3
4	TIP04	29	RING4	4
5	TIP05	30	RING5	5
6	TIP06	31	RING6	6
7	TIP07	32	RING7	7
8	TIP08	33	RING8	8

Pino	Sinal	Pino	Sinal	Canal
1	TIP01	26	RING1	1
2	TIP02	27	RING2	2
3	TIP03	28	RING3	3
4	TIP04	29	RING4	4
5	TIP05	30	RING5	5
6	TIP06	31	RING6	6
7	TIP07	32	RING7	7
8	TIP08	33	RING8	8

4.3.2. Conector RJ45

As interfaces FXS da plataforma KMG são disponibilizadas em módulos de oito canais, divididos em dois conectores RJ45. É possível usar uma caixa conversora RJ45 ↔ RJ11, ou conectar diretamente aos dispositivos analógicos, através do esquema a seguir.

Pino RJ45	Cor Padrão TIA568A	Conector 0-3	Conector 4-7
1	Verde-branco	RING 1	RING 5
2	Verde	TIP 1	TIP 5
3	Laranja-branco	RING 2	RING 6
4	Azul	TIP 3	TIP 7
5	Azul-branco	RING 3	RING 7
6	Laranja	TIP 2	TIP 6
7	Marrom-branco	RING 4	RING 8
8	Marrom	TIP 4	TIP 8



Legenda: *Conector Fêmea.*

5. Conhecendo a Interface Web

Esta seção fornece uma descrição da Interface Web do KMG. A Interface Web possibilita a "Configuração", "Monitoração", "Diagnóstico" e "Administração" dos produtos da linha KMG.

5.1. Requisitos do computador para o acesso

O computador cliente usado para acessar a Interface Web do KMG deve atender aos seguintes requisitos:

- Conexão de rede com o KMG.
- Um dos seguintes navegadores:
  - Google Chrome.
  - Mozilla Firefox.
  - Internet Explorer.
- Resolução de tela recomendada: 1920 x 1080 pixels.

5.2. Acessar a Interface Web

O procedimento a seguir descreve como acessar a Interface Web do KMG.

1. Abra um navegador Web padrão.

2. Digite o endereço IP atribuído na eth0 do KMG. Se o endereço IP está no padrão de fábrica, digite o endereço IP descrito na tabela a seguir, conforme o modelo do seu KMG.

Modelo KMG	Descrição	Máscara de sub-rede
KMG 200 One	**10.10.10.10**	**255.0.0.0**
KMG 400 One	**10.10.10.20**	
KMG 3200 One	**10.10.10.30**	
KMG 1600 One	**10.10.10.40**	

3. Digite o seu usuário e senha de acesso. Se for o primeiro acesso, utilize o usuário e a senha padrão descritos a seguir.

Usuário	Senha
admin	**khomp**

Nota	No primeiro acesso, é recomendável alterar a senha de acesso do usuário admin como medida de segurança.

5.3. Áreas da interface do usuário

A Interface Web é dividida em quatro seções:

- Configuração: Contém as opções para configuração de rede, criação de troncos SIP, troncos E1, configuração das interfaces analógicas, GSM, codecs e demais configurações do gateway.
- Monitoração: Contém opções para monitoramento das interfaces de telefonia e dos canais VoIP.
- Diagnóstico: Contém opções para exibição das principais mensagens de operação do KMG, além de permitir fazer o download ou visualizar os Logs.
- Administração: Contém opções para gerenciamento do gateway, como atualização do da versão do equipamento, alteração de senha de acesso a Interface Web e provisionamento.

Alguns recursos e opções podem estar disponíveis em determinadas versões do equipamento. Este manual informa a versão que determinado recurso se encontra disponível.

A Interface Web conta com ajuda em quase todos os campos referenciadas com o símbolo "?", o que pode auxiliar a configuração do equipamento.

5.3.1. Verificando a versão do KMG

A versão do KMG é exibida no menu administração no botão informações do gateway. Diversas informações são apresentadas nesta janela onde consta a versão do pacote que está instalado no KMG.

6. Operação do KMG

O KMG é capaz de realizar o controle e roteamento das chamadas telefônicas recebidas de uma rede e encaminhar para outra conforme as regras programadas.

Para configurar o roteamento no gateway, é preciso conhecer os conceitos de "NAP", "Rotas" e como eles se relacionam.

"NAP" (Network Access Points), é um ponto de entrada e/ou saída de ligações. Que representa um ou mais canais E1/T1, GSM, FXS e FXO, um host/usuário SIP, ou um SIP Trunk, definindo assim grupos de canais que poderão ser utilizados por uma ou mais rotas como origem (ligações entrantes) ou destino (ligações saintes).

As "Rotas" são associações entre NAPs de origem e destino. Ou seja, ao criar uma rota, o usuário precisa selecionar o NAP de origem, que é o ponto de entrada das ligações no Gateway, e o NAP de destino, que são as ligações saintes.

O roteamento pode ser baseado no número de origem, número de destino e resultado da consulta por portabilidade, pode-se também restringir as rotas por horários, configurar rotas alternativas que serão utilizadas como fallback e "retry", como também podem ser criados scripts de roteamento de chamadas avançados utilizando a linguagem LUA.

Quando há uma chamada entrante, todas as rotas que possuam como NAP de Origem, o NAP no qual a chamada foi recebida, serão avaliadas na ordem de prioridade definida na configuração. A primeira rota que satisfazer a todos os filtros será utilizada para alocar a chamada sainte, utilizando o NAP de Destino configurado.

O progresso da chamada sainte é monitorado e poderá resultar no comportamento de "retry" caso ela desconecte prematuramente (antes do atendimento), ou ocorra o timeout para completamento e a causa de desconexão esteja mapeada no perfil da chamada entrante como "retry". O fallback é um recurso semelhante ao "retry", disponível apenas para NAP de destino SIP com diversos servidores proxy configurados. Este recurso permite o KMG alterar o proxy da chamada sainte, caso este não responda em tempo hábil, sem disparar o recurso de "retry".

Caso ocorra um "retry", serão retomadas as avaliações das rotas a partir da próxima prioridade estabelecida para as rotas válidas do NAP de Origem.

Para facilitar a configuração e o gerenciamento do produto foi desenvolvida a Interface Web que reune todas as configurações e recursos divididos em 4 grandes categorias: "Configuração", "Monitoração", "Diagnóstico" e "Administração".

Para criar uma rota básica basta concluir os passos a seguir.

- **Passo 1**: Crie um NAP que servirá como NAP de Origem e outra que servirá como NAP de Destino em:

"**Interface Web**" → "**Configuração**" → "**Roteamento**" → "**NAPs**"

- **Passo 2**: Configure uma Rota de um NAP para outra, em:

"**Interface Web**" → "**Configuração**" → "**Roteamento**" → "**Rotas**"

Os detalhes do funcionamento do KMG e a descrição dos campos em cada menu estão descritos ao longo deste manual.

7. Configuração

7.1. Rede

O menu rede contém todas as configurações relacionadas com as configurações de rede do equipamento. Interfaces, Firewall e certificados TLS. Não é necessário reiniciar o equipamento para aplicar estas configurações.

7.1.1. Configurar a rede

O menu rede contém todas as configurações relacionadas com as configurações de rede do equipamento. Interfaces, Firewall e certificados TLS. Não é necessário reiniciar o equipamento para aplicar estas configurações.

"**Configuração**" → "**Rede**" → "**Interfaces**"

Este menu exibe as opções para configuração das interfaces de rede do KMG. Nesta página Web você pode configurar as interfaces de rede para conectar o KMG à rede VoIP, definir a interface de rede para ser usada com um módulo externo de telefonia → Módulo KMG, além de configurações de DNS e rotas estáticas.

No painel 'Rede' é exibido uma tabela para configuração de cada interface de rede. A tabela a seguir descreve o uso de cada opção.

As opções das interfaces de rede serão exibidas conforme o modo de operação definido. As demais opções serão exibidas somente se o modo de configuração for "Estático".

No botão editar é possível realizar as configurações pertinentes a determinada interface de rede. No botão adicionar é possível adicionar uma interface VLAN.

Veja na tabela a seguir, a descrição de cada parâmetro das interfaces:

Campo	Descrição
Interface	Relação das interfaces de rede disponíveis no KMG. A quantidade de interfaces exibidas varia de acordo com o modelo do KMG.
Modo de operação	Seleciona o modo que a interface irá operar: • Desativada: Não ativa esta interface. • Rede: Modo de operação como interface de rede. • Módulo EBS: A interface de rede será usada para conexão com um módulo externo de telefonia → Módulo KMG. A exibição desta opção varia conforme a interface de rede e modelo do KMG.

Rede

Campo	Descrição
Tipo	Protocolo IPv4 ou IPv6 que será utilizado nesta interface de rede.
Método de configuração	Seleciona o método de configuração relacionado a rede: • Estático: Endereço IP, máscara de sub-rede e gateway de rede, são atribuídas manualmente. • Dinâmico (DHCP): Esta interface as definições de rede atribuídas por um servidor DHCP disponível na rede. DHCP para IPv6 não é suportado.
Endereço IP	Endereço IP atribuída à interface de rede.
Máscara de sub-rede	Máscara de sub-rede atribuída à interface de rede.
Gateway	Definição do gateway de rede. Se houver outra interface de rede com outro gateway de rede definido, é necessário especificar o gateway de rede padrão clicando no checkbox ao lado.

Para cada interface de rede é possível criar VLANs configurando o ID requisitado. Ao clicar em adicionar, serão exibidas as opções a seguir:

Campo	Descrição
ID	ID de VLAN a ser utilizado por esta interface de rede.

A linha KMG permite a configuração de até 45 IPs, distribuídos entre EBS, interfaces, *alias* e VLANs.

Configurar DNS

Configure o domínio de busca, também conhecido como domínio de pesquisa, e o endereço dos servidores DNS primário, secundário e terciário que serão utilizados na ordem de preferência fornecida para a resolução de nomes na rede.

Você pode definir até 3 servidores DNS.

Configurar rotas estáticas

Permite definir uma rota estática no KMG, especificando endereço IP, máscara de sub-rede, gateway e interface de rede. As rotas estáticas criadas possuem prioridade sobre os demais roteamentos existentes.

Para inserir outra rota, clique em Adicionar rota, logo abaixo da tabela de rotas estáticas.

7.1.2. Configurar Firewall

São definidas as configurações de controle de acesso ao KMG e definição dos serviços de rede que poderão se comunicar com o gateway.

Os protocolos a seguir são liberados, independente das configurações aplicadas no firewall do KMG:

- UDP nos protocolos SIP, RTP e SNMP.
- TCP nos protocolos FTP 1, HTTP e SSH 1.
- ICMP. Somente para responder echo.

O acesso através dos protocolos SSH e FTP tem proteção ativa contra força bruta. Ambos aceitam no máximo 3 tentativas de conexão consecutivas sem sucesso e entram em um modo de espera de 120 segundos. Para aceitar novas tentativas de acesso é necessário esperar o tempo de 120 segundos, a contagem de tempo é reiniciada se a tentativa for efetuada antes de completar os 120 segundos.

A configuração do firewall é realizada na seguinte ordem:

1. Definir os endereços liberados. Se qualquer endereço IP for liberado, as demais configurações não serão aplicadas mesmo que estejam configuradas.

2. Bloquear os endereços que não estejam na lista de endereços liberados.

Ainda é possível:

- Habilitar/Desabilitar serviços de rede para cada interface disponível no KMG
- Configurar detecção de intrusão

Se o campo 'Endereço liberado' estiver como "ANY", as opções observadas anteriormente não terão efeito mesmo se houver configuração.

Endereços liberados

São especificados os endereços IP que poderão ter acesso ao KMG. Se nenhum valor for inserido, é considerado que qualquer endereço IP poderá acessar o KMG. Porém o acesso se restringe somente à Interface Web e ao registro SIP. Esta configuração é usada em conjunto com a configuração de Endereços Bloqueados. Clique no botão Adicionar e aplique uma das opções a seguir:

- ANY: Deixa explícito que qualquer endereço IP poderá acessar o KMG. Seja através da Interface Web, FTP, SSH e SNMP.
- Endereço IP: Apenas os endereços IP definidos poderão acessar o KMG. Por exemplo: 192.168.0.5 .
- Prefixo de rede: Apenas os endereços IP pertencentes a faixa especificada poderão acessar o KMG. Por exemplo: 192.168.109.0/24 .

Nota	É recomendado liberar apenas os endereços IP que terão acesso ao KMG. Para isso marque a opção Bloquear todos os endereços que não se encontram na lista de endereços liberados.

Endereços bloqueados

Ao habilitar esta opção, bloqueia qualquer endereço IP que não estiver definido em "Endereços liberados".

Atenção	Ao habilitar esta opção, certifique-se de que tenha ao menos um endereço IP liberado para acesso ao KMG.

Serviços habilitados por interface de rede

Neste são definidos os serviços de rede que serão liberados para cada interface de rede. Lembrando que a configuração é cumulativa, ou seja, a lista de endereços liberados e bloqueados tem precedência sobre esta configuração.

7.1.2.1. Configurar detecção de intrusão

O KMG possui a capacidade de bloquear temporariamente a comunicação com um endereço IP de um dispositivo que tentou acessá-lo e foi mal sucedido. O bloqueio é realizado seguindo regras de segurança que se encontram nesta sessão de configuração.

Para configurar a detecção de intrusão através da Interface Web do KMG:

1. Para habilitar este recurso, clique em + Detecção de intrusão, conforme mostra a imagem a seguir:

2. Depois, basta habilitar o tipo de detecção desejado. São quatro tipos de detecção:

- Acesso SSH por força bruta: Bloqueio por excesso de tentativas com falha de acesso SSH.
- Acesso na Interface Web por força bruta: Bloqueio por excesso de tentativas com falha de acesso à Interface Web.
- Registro SIP por força bruta: Bloqueio por excesso de tentativas com falha de registro. Disponível somente se houver licença de "Autorização de Registros".
- Inundação SIP (SIP flood): Proteção para SIP flood. Disponível somente se houver licença de "*Autorização de registros*".

3. Ao habilitar um tipo de detecção, serão exibidos os campos a seguir. Configure-os de acordo com suas políticas de segurança:

- Número máximo de tentativas: Número máximo de tentativas que um dispositivo poderá tentar acessar o KMG. Se este limite for atingido, o endereço IP do dispositivo será bloqueado pelo tempo definido no campo 'Tempo de bloqueio'.
- Intervalo de tempo: Intervalo de tempo, em segundos, que um dispositivo poderá tentar acessar o KMG. Por exemplo: Se houver 3 tentativas mal sucedidas de acesso em 60 segundos, o endereço IP será bloqueado.
- Tempo de bloqueio: Tempo em segundos que um dispositivo, que ultrapasse os limites anteriores, ficará sem poder acessar o KMG. Ao fim do tempo de bloqueio, o dispositivo poderá tentar acessar ao KMG novamente.

4. Clique no botão "Salvar". Por fim, clique no botão "Aplicar" para que as alterações entrem em operação

7.1.3. Gerenciar certificados TLS

"**Configuração**" → "**Rede**" → "**Certificados TLS**"

É possível registrar conjuntos de chave privada, certificado e trust store para serem utilizados pelas interfaces VoIP do equipamento. Uma chave privada pode ser gerada automaticamente pelo equipamento junto com um certificado auto-assinado, utilizando o botão 'Criar certificado auto-assinado', ou arquivos existentes podem ser enviados para uma nova configuração, utilizando o botão 'Adicionar certificado existente', utilizando o botão de edição da configuração que se deseja alterar.

ⓘ	**Nota**	Apenas os módulos de *Sobrevivência* e *Autorização de Registros,* permitem configuração por interface, módulo de roteamento utiliza a primeira configuração disponível em todas as interfaces.

Criar um certificado auto-assinado

Preencha o formulário que será apresentado. Ao enviar o formulário, aguarde a Interface Web confirmar a criação do certificado e abrir o formulário de edição.

O formulário de criação de certificado auto-assinado contém:

Campo	Descrição	Versão
Nome	Nome da configuração TLS	4.0.2
Tamanho (bits)	Tamanho em bits da chave privada a ser gerada utilizando valores aleatórios, quanto maior a chave, mais segura, porém, requer mais processamento para ser utilizada	
Algoritmo de cifragem	Habilita cifragem da chave privada com o algoritmo desejado, requer "Senha de cifragem"	
Senha de cifragem	Senha que será utilizada para a cifragem e decifragem da chave privada, deve ser preenchido somente se um "Algoritmo de cifragem" foi selecionado	
Confirmar senha de cifragem	Deve conter a mesma senha digitada no campo "Senha de cifragem", deve ser preenchido somente se um "Algoritmo de cifragem" foi selecionado	
País (C)	País a ser informado no campo C do certificado	
Estado ou província (ST)	Estado ou província a ser informado no campo ST do certificado	
Cidade ou localização (L)	Cidade ou localização a ser informada no campo L do certificado	
Organização ou empresa (O)	Nome da organização ou empresa a ser informado no campo O do certificado	
Unidade organizacional ou departamento (OU)	Nome da unidade organizacional ou departamento a ser informado no campo OU do certificado	
Nome comum (CN)	Nome a ser informado no campo CN do certificado	
Endereço de E-Mail (emailAddress)	Endereço de E-Mail do contato ou responsável pelo equipamento a ser informado no campo emailAddress do certificado	
Tempo de expiração (dias)	Tempo de expiração em dias do certificado	

Adicionar ou editar certificado existente

Ao solicitar que seja adicionado um certificado existente, o sistema irá gerar e gravar a configuração com valores pré-definidos, abrindo o formulário de edição para alterações e envio dos arquivos que se deseja associar a esta configuração.

O formulário de edição contém:

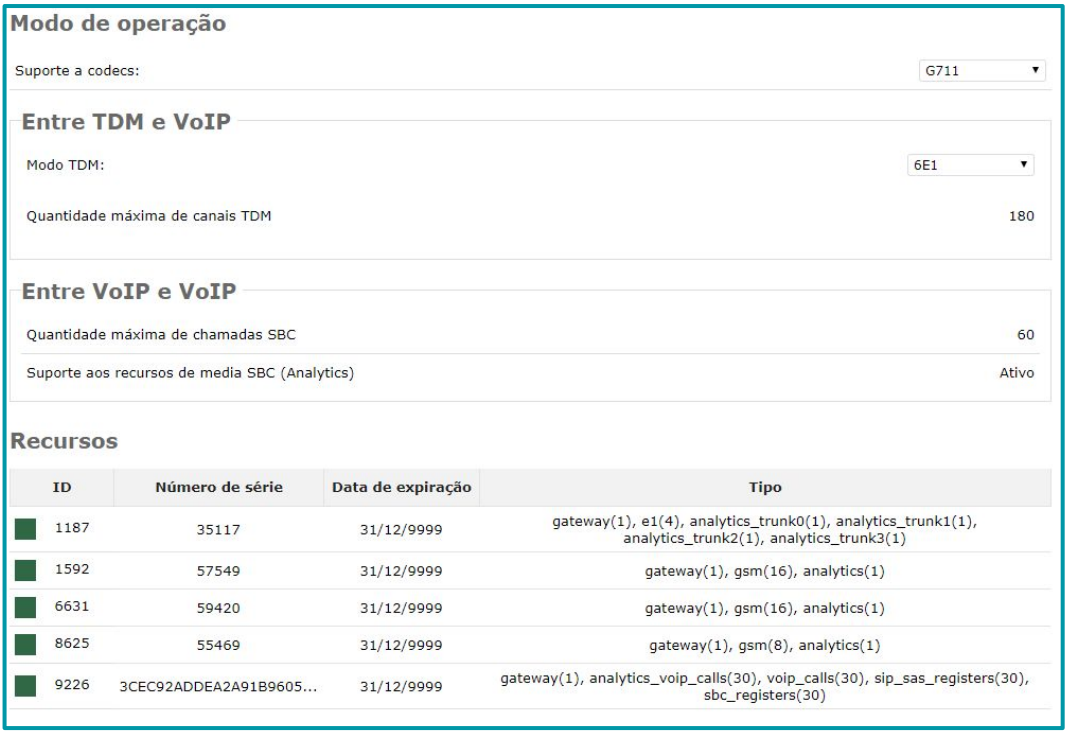
Campo	Descrição	Versão
Nome	Nome da configuração TLS	4.0.2
Senha de cifragem	Quando configurada é a senha utilizada para decifrar a chave privada e apresentará um link para alterar a senha. Caso ainda não esteja configurada, apresenta o campo para adição de uma senha **ATENÇÃO:** A chave privada nunca é alterada por este campo, caso deseje decifrar e recifrar a chave com nova senha, é necessário fazer o download da chave, realizar as alterações e fazer upload da nova chave com a nova senha.	
Habilitar Trust Store padrão	Caso habilitado, o trust store padrão do sistema deverá ser carregado e utilizado em conjunto com o trust store fornecido por esta configuração, o trust store padrão contém os certificados públicos de autoridades certificadoras largamente utilizadas e é fornecido como parte do arquivo de atualização do KMG, não pode ser alterado	
Habilitar verificação do certificado	Esta opção depende de do Trust Store e/ou Trust Store padrão habilitados e obrigará a verificação do certificado apresentado pelo ponto remoto no handshake do TLS ter sido emitido por qualquer das autoridades certificadoras reconhecidas. Caso não seja configurado um Trust Store e o Trust Store padrão esteja desabilitado, esta configuração é ignorada e qualquer certificado oferecido pelo ponto remoto será aceito	
Chave privada	Quando não se tem chave privada associada, este campo apresentará a possibilidade de enviar uma chave privada, quando existe uma chave privada, apresentará a condição de uso da chave e seu tamanho (caso a condição seja ok) e botões para baixar ou remover	
Certificado	Quando não se tem certificado associado, este campo apresentará a possibilidade de enviar um certificado, quando exite um certificado, apresentará as condições de uso do certificado e botões para baixar ou remover	
Trust Store	Quando não se tem trust store associado, este campo apresentará a possibilidade de enviar um trust store, quando existe um trust store, apresentará as condições de uso do trust store e botões para baixar ou remover	

7.2. Sistema

Este menu agrupa todas as configurações de sistema que necessitam reiniciar o equipamento para validação.

7.2.1. Configurar o modo de operação

O modo de operação define o modo de operação e consequentemente o conjunto de codecs suportado pelo KMG. A configuração do modo de operação irá depender das licenças aplicadas no KMG, da capacidade máxima de chamadas simultâneas suportada pelo KMG, e os codecs usados pelos troncos conectados o gateway.



Para configurar o modo de operação:

1. Acesse o menu "Configuração" → "Sistema" → "Modo de operação".

2. Configure o suporte a codecs selecionando uma das opções abaixo:

- Bridge: O KMG não aplica nenhum tratamento sobre as chamadas trafegadas pelo gateway, possibilitando assim o tráfego de qualquer codec de audio e video.
- G711: O KMG aceita chamadas com os seguintes codecs: G.711 A-law, G.711 μ-law, GSM e DVI4.
- Transcode: O KMG aceita o transcoding de chamadas com os seguintes codecs: G.729A e G.722.

3. No painel 'Entre TDM e VoIP' é possível selecionar a quantidade de canais TDM a ser utilizada, ou selecionar a opção para uso exclusivo em modo SBC, conforme abaixo:

- SBC ONLY: O KMG não aceita chamadas entre telefonia TDM e VoIP, apenas o modo SBC está habilitado.
- E1-G711: O KMG aceita chamadas entre TDM e VoIP. Existem diferentes níveis de E1 cadastrados para cada tipo de equipamento.

4. No painel 'Entre VoIP e VoIP', será apresentado o valor restante de chamadas conforme as opções que foram selecionadas anteriormente informando a quantidade máxima de chamadas VoIP disponíveis e o conforme o suporte a codecs configurado.

5. Clique no botão "Salvar".

6. Reinicie o gateway para que estas configurações entrem em operação. Será exibido uma mensagem com um botão para reiniciar o gateway, ou você pode reiniciar posteriormente (veja a seção *"Desligar e reiniciar o KMG"*).

ⓘ	**Nota**	Os campos "Quantidade máxima de canais TDM" e "Quantidade máxima de chamadas SBC" exibem a capacidade de chamadas simultâneas suportada pelo KMG, conforme o modo de operação definido.

7.2.2. Configurações VoIP

O modo de operação define o modo de operação e consequentemente o conjunto de codecs suportado pelo KMG. A configuração do modo de operação irá depender das licenças aplicadas no KMG, da capacidade máxima de chamadas simultâneas suportada pelo KMG, e os codecs usados pelos troncos conectados o gateway.

"Configuração" → "Sistema" → "VoIP"

Nesta você pode alterar as configurações VoIP do KMG. As configurações aplicadas aqui são globais, aplicáveis em todas as seções e troncos SIP.

É possível configurar separadamente as portas utilizadas para cada interface.

A tabela a seguir contém a descrição dos campos da configuração do VoIP do KMG.

Campo	Descrição	Versão
Maior porta RTP	Valor máximo da porta RTP que deve ser utilizada para trafegar o áudio das ligações SIP para cada interface de rede.	-
Menor porta RTP	Valor mínimo da porta RTP que deve ser utilizada para trafegar o áudio das ligações SIP para cada interface de rede.	
Porta UDP	Porta SIP utilizada para o protocolo UDP. Qualquer servidor que precisar se conectar com o KMG deverá usar esta porta para tráfego do protocolo SIP para cada interface de rede.	4.1.1
Porta TCP	Porta SIP utilizada para o protocolo TCP. Qualquer servidor que precisar se conectar com o KMG deverá usar esta porta para tráfego do protocolo SIP para cada interface de rede.	
Porta TLS	Porta SIP utilizada para o protocolo TLS. Qualquer servidor que precisar se conectar com o KMG deverá usar esta porta para tráfego do protocolo SIP para cada interface de rede.	
Ativar substituição automática de caracteres especiais	Alguns caracteres possuem significado especial nos números de A e B (como '#', por exemplo). E necessitam ser codificados como entidades especiais. Porém alguns equipamentos não aceitam esta codificação. Na maioria dos casos a configuração padrão é a mais indicada.	-
Ignorar o campo "Contact" dos cabeçalhos, utilizando o campo "To" em seu lugar	Em algumas configurações, as informações desejadas de origem da ligação não estão no campo "Contact" do SIP, mas sim no campo "To". Marcando esta configuração, os dados de origem da chamada serão lidos do campo "To" ao invés do campo "Contact".	
Utilizar PRACK (RFC 3262)	Caso habilitado, será enviado o Header Require:100rel nas mensagens 101-199 solicitando o Provisional ACK como resposta.	
Habilitar RTCP	Caso habilitado, utiliza RTCP para o controle dos pacotes RTP.	
Tipo de payload para o telephone-event	Determina qual tipo de payload DTMF será enviado no SDP.	

Campo	Descrição	Versão
Identificação do usuário do URI	Adiciona a identificação selecionada a URI.	-
Enviar o parâmetro "transport" do URI	Insere o parâmetro transport, com o tipo de protocolo utilizado a URI.	
Tamanho do pacote de áudio	Determina o tamanho do pacote de audio utilizado em milisegundos.	
ToS para pacotes SIP (DSCP)	Marcação dos pacotes de sinalização para ToS.	
ToS para pacotes de mídia (DSCP)	Marcação dos pacotes de mídia para ToS.	
Criptografia TLS	Seleciona a opção de certificado TLS a ser utilizado pelo sistema.	

Na seção "*Timers*", encontram-se as configurações específicas de temporização SIP.

Campo	Descrição
Timer H	Tempo máximo, em milissegundos, de retransmissão de pacotes SIP. O tempo padrão é 32000 milissegundos.
Espera pelo ACK após 2xx	Tempo máximo, em milissegundos, para a confirmação (ACK) de estabelecimento do diálogo (resposta 200 OK para um INVITE). O tempo padrão é 32000 milissegundos.

ⓘ	**Nota**	Sempre que houver alterações nas configurações de VoIP, é necessário reiniciar o KMG após clicar no botão "*Aplicar*".

7.2.3. Configurar Serviços

"**Configuração**" → "**Sistema**" → "**Serviços**"

São configurados os serviços disponíveis no KMG. Atualmente é possível configurar a porta HTTP e habilitar o serviço HTTPS definindo a porta e certificado a ser utilizado.

7.2.3.1. SNMP V3

As instruções a seguir apresentam o procedimento de configuração do protocolo de gerenciamento de rede "SNMP V3" para gateways da linha KMG One.

É possível configurar o protocolo SNMPv3 na interface de administração do gateway. O SNMPv3 tem recursos de segurança aprimorados, como autenticação e privacidade. O gateway continua a oferecer suporte a SNMP V1 e ao SNMP V2 (versões padrão).

⚠ **Atenção**	O SNMP V3 só pode ser configurado nos gateways KMG One a partir da versão **4.1.57.6A**.

Para configurar, acesse a Interface Web de configuração do gateway nos menus indicados a seguir:

Configuração → Sistema → Serviços → SNMP

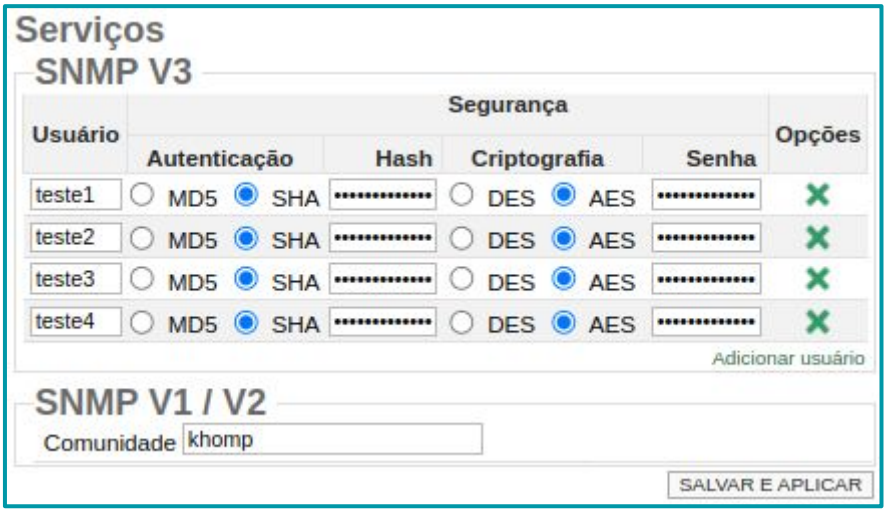
A tabela observada a seguir auxilia o administrador na configuração da interface.

Campo	Descrição
Usuário	Nome de usuário SNMPv3
Autenticação (protocolo de Autenticação)	Algoritmo que você deseja usar para autenticar o SNMPv3: • SHA usa Secure Hash Algorithm (SHA) em seu protocolo de autenticação; • MD5 usa Message Digest 5 (MD5) em seu protocolo de autenticação.
Hash	Senha hash para o protocolo de autenticação
Criptografia	Algoritmo que você deseja utilizar para descriptografar as mensagens SNMP: • DES usa Data Encryption Standard (DES) como algoritmo de decriptografia das mensagens SNMPv3; • AES usa Advanced Encryption Standard (AES) como algoritmo de decriptografia das mensagens SNMPv3.
Senha	Senha utilizada para descriptografar as mensagens SNMPv3

Após configurar a interface, clique no botão "Salvar e aplicar".

SALVAR E APLICAR

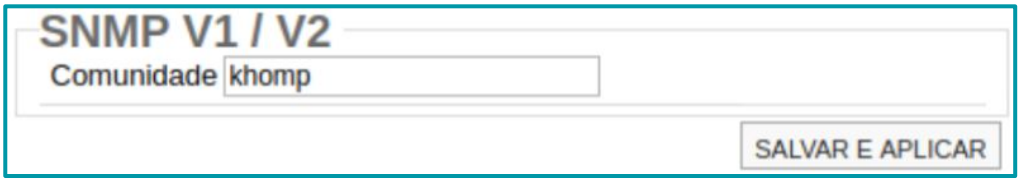
A imagem a seguir é um exemplo da interface configurada.



7.2.3.1. SNMP V2 e SNMP V1

Para configurar, acesse a Interface Web de configuração do gateway nos menus indicados a seguir:

Configuração → Sistema → Serviços → SNMP



A tabela observada a seguir auxilia o administrador na configuração da interface.

Campo	Descrição
Comunidade	Nome da comunidade SNMP

Após configurar a interface, clique no botão "Salvar e aplicar".

7.2.4. Configurar Data e hora

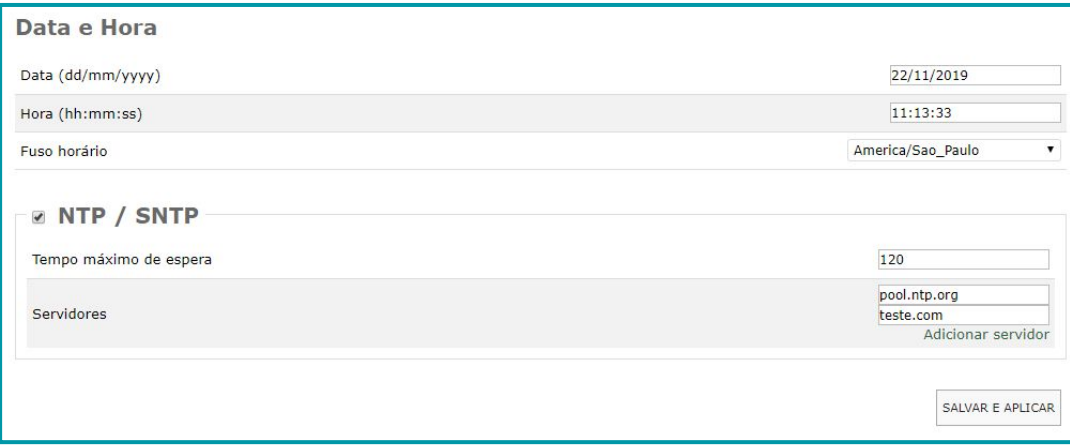
A data e hora no KMG pode ser configurada de forma manual ou pode ser obtida por um servidor SNTP/NTP.

Atenção — É altamente recomendável que a data e hora do KMG estejam corretamente configuradas, pois o registro de Logs, registros das chamadas nos arquivos CDR e rotas com restrição de tempo são afetadas por esta configuração.

7.2.4.1. Alterar data e hora manualmente

Para configurar a data e hora manualmente através da Interface Web do KMG:
Acesse o menu "**Configuração**" → "**Sistema**" → "**Data e Hora**"

1. No campo 'Data' e 'Hora', insira a data e hora de acordo com o local onde o KMG está instalado (exemplo: 05/01/2018).



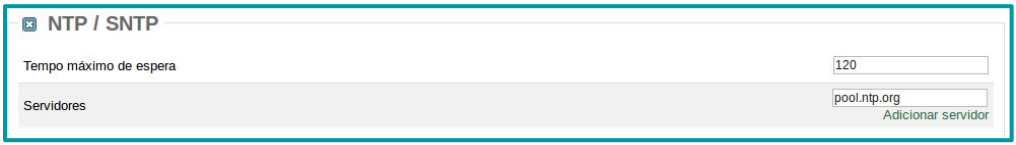
2. No campo 'Fuso horário', selecione o fuso horário de acordo com o local onde o KMG está instalado.

3. Clique no botão Salvar. Se nenhuma outra configuração for realizada, clique no botão Aplicar.

4. Reinicie o gateway para que estas configurações entrem em operação. Será exibido uma mensagem com um botão para reiniciar o gateway, ou você pode reiniciar posteriormente (veja a seção 'Desligar e reiniciar o KMG').

7.2.4.2. Alterar data e hora automáticamente usando NTP/SNTP

Para configurar a data e hora manualmente através da Interface Web do KMG:
Acesse o menu "**Configuração**" → "**Sistema**" → "**Data e Hora**"



1. Habilite a opção NTP/SNTP.

2. No campo 'Tempo máximo de espera', defina o tempo (em segundos) de tentativa de comunicação entre o KMG e o servidor NTP/SNTP.

3. No campo 'Servidores', configure o endereço IP ou FQDN do servidor NTP/SNTP. Para adicionar outro servidor, clique na opção "Adicionar servidor".

4. Clique no botão "Salvar". Se nenhuma outra configuração for realizada, clique no botão "Aplicar".

5. Se a data e hora sofrer alterações, reinicie o gateway para que estas configurações entrem em operação. Será exibido uma mensagem com um botão para reiniciar o gateway, ou você pode reiniciar posteriormente (veja a seção "*Desligar e reiniciar o KMG*").

Nota

- Pode ser necessário configurar o DNS no KMG para o correto funcionamento da configuração automática de data e hora.
- Algumas versões de navegadores apresentam inconsistências ao atualizar, manualmente, a data e hora do sistema.

7.2.5. Configurar Histórico de configurações

"**Configuração**" → "**Sistema**" → "**Histórico de configuração**"

Neste menu consta todo o histórico de alteração de configurações do equipamento. É possível ver o usuário e IP de acesso, horário da alteração. Bem como verificar quais alterações foram realizadas e restaurar as mesmas caso necessário.

Atenção	Ao realizar a restauração de configuração para um determinado ponto, todas as configurações serão restauradas para o ponto selecionado. Demais alterações posteriores serão desfeitas.

7.3. Telefonia

Este menu apresenta todas as configurações relacionadas a telefonia.

Nota	É necessário ter interface E1/T1 conectada ao KMG para que este menu seja exibido.

7.3.1. Sinalização

"**Configuração**" → "**Telefonia**" → "**Sinalização**"

É possível alterar os perfis de sinalização do equipamento que são aplicados aos links E1/T1 e canais de telefonia GSM, FXO e FXS. Todas as configurações padrão existentes se referem às normas dos protocolos. Você pode editar ou copiar um perfil para alterar suas propriedades conforme a necessidade.

Os perfis serão aplicados em todos os links ou canais de telefonias de um módulo de telefonia → Módulo KMG. Não é possível aplicar um perfil de sinalização em apenas parte dos canais de um mesmo módulo.

7.3.1.1. Editar perfil de sinalização

> **Atenção** — Altere essas configurações somente se houver necessidade e se você possuir conhecimento sobre cada sinalização.

1. No perfil que será alterado, clique no ícone 
2. Altere as propriedades necessárias.
3. Clique no botão "Salvar". Se nenhuma outra configuração for realizada, clique no botão "Aplicar" para que as alterações entrem em operação.

7.3.1.2. Copiar perfil de sinalização

Se você tiver dois módulos de telefonia que exijam perfis diferentes, você pode copiar um perfil e alterar suas propriedades. Desta maneira você cria um novo perfil para aplicar em módulos diferentes.

1. No perfil que terá suas propriedades copiadas, clique no ícone 
2. No campo 'Nome' defina uma descrição diferente do perfil original. Altere as propriedades necessárias.
3. Clique no botão "Salvar".
4. Consulte a seção "Aplicar perfil de sinalização no módulo de telefonia" a seguir para aplicar o perfil criado em um módulo de telefonia.

7.3.1.3. Aplicar perfil de sinalização no módulo de telefonia

Após criar um novo perfil, através da cópia de um perfil existente, é necessário aplicar este perfil no módulo de telefonia. Se for editado apenas um perfil existente, esta etapa não será necessária, pois ela será carregada após clicar no botão "Aplicar".

1. Acesse o menu "**Configuração**" → "**Dispositivo**".
2. Será exibido a imagem de um Módulo KMG com suas propriedades. Clique sobre o módulo que contém a interface de telefonia que terá seu perfil alterado. Os módulos internos disponíveis no KMG 200 e KMG 400 também serão exibidos com a imagem do Módulo KMG.

3. Na coluna 'Perfil', selecione o perfil que você criou. Será exibido somente o perfil compatível com a tecnologia da interface de telefonia. Por exemplo: Se a interface for E1/T1, será exibido somente os perfis de sinalização compatíveis com esta interface, como R2, ISDN, entre outras.

4. Clique no botão "Salvar". Se nenhuma outra configuração for realizada, clique no botão "Aplicar" para que as alterações entrem em operação.

7.3.2. Configurando propriedades dos Links E1/T1

"**Configuração**" → "**Telefonia**" → "**Links E1/T1**"

É possível alterar os perfis de sinalização do equipamento que são aplicados aos links E1/T1 e canais de telefonia GSM, FXO e FXS. Todas as configurações padrão existentes se referem às normas dos protocolos. Você pode editar ou copiar um perfil para alterar suas propriedades conforme a necessidade.

Os perfis serão aplicados em todos os links ou canais de telefonias de um módulo de telefonia → Módulo KMG. Não é possível aplicar um perfil de sinalização em apenas parte dos canais de um mesmo módulo.

A tabela a seguir contém a descrição dos campos disponíveis nesta Interface:

Campo	Descrição
Serial	Informa o número de série do módulo E1.
Apelido	Descrição do módulo para auxiliar na sua identificação. Por exemplo: O nome da operadora de telefonia a qual o link está conectado. Este apelido é exibido na criação de tronco E1 (menu Configuração → Roteamento → NAPs).
Sinalização	Selecione a sinalização do link.
Sincronismo (clock)	Define se a interface de telefonia deve receber ou gerar o clock de referência no link. São duas opções: • Receber: Usado quando o KMG é conectado com uma operadora de telefonia fixa (PSTN). • Gerar: Usado quando o KMG é conectado à um PBX digital.
Dígitos de entrada	Número mínimo de dígitos do número do destino a serem pedidos à central remota.
CRC	Se habilitado, o KMG utiliza o recurso CRC. É necessário que o dispositivo conectado ao KMG também tenha suporte a CRC.

As configurações da tabela vista anteriormente costumam ser as únicas definições a serem alteradas. Pois dependem do tipo de conexão, PBX digital ou PSTN.

Para mais configurações do link, clique no botão Configurações avançadas. Serão exibidas mais colunas na tabela mostrada. Estas configurações devem ser alteradas somente se houver necessidade ou se for solicitado pela sua operadora de telefonia fixa.

A tabela a seguir contém a descrição dos campos disponíveis:

Campo	Descrição
Modo de operação	Selecione se o link irá operar como E1 ou T1.

7.3.3. Plano de discagem

"**Configuração**" → "**Telefonia**" → "**Plano de discagem**"

O Plano de discagem estabelece uma sequência esperada de dígitos discados. Se o gateway obteve uma sequência esperada, o número é aceito e enviado para o roteamento. Caso contrário, a chamada é recusada. É possível cadastrar planos contado com as regras de discagem do seu cenário e associar posteriormente este plano ao Link E1, ou NAP FXS.

Para validar os dígitos discados, regras devem ser incluídas na configuração do plano de discagem. Cada regra define um prefixo necessário para validar a sequência.

As Regras são definida utilizando uma sequência de valores de acordo com a sintaxe da tabela a seguir:

Dígitos	0 1 2 3 4 5 6 7 8 9 A B C D * #
Wild card	X
Opção	[2578], [136], [29], ...
Intervalo	[0-9], [3-6], [5-7], [0-2], ...
Opção e intervalo	[57-9], [0246-8], [2-579], ...

O "X" pode assumir qualquer dígito numérico. Por exemplo, a regra "0XX4837222900" deve coincidir com a sequência "0214837222900" e falhar com "0##4837222900".

Dígitos numéricos dentro de "[]" denotam uma lista de opções e/ou um intervalo numérico. Por exemplo, a regra "2[38][6-9]X" deve coincidir com a sequência "2370" e falhar com "2470" ou "2350". O wild card "X" equivale ao intervalo "[0-9]".

Opção e intervalo podem ser utilizados na mesma estrutura "[]". Por exemplo, a regra "2[37-9][2-46]X" deve coincidir com as sequências "2360", "2830" e "2720". A mesma regra deve falhar com "2450", "2100" e "2070".

Nota

- Uma sequência que coincide parcialmente com uma regra pode ser aceita no plano de discagem. Por exemplo, a regra "XXXX" aceita a sequência "123" ou "456" após a sinalização definir que não há mais números a serem enviados.
- A validação da sequência é por prefixo. Por exemplo, a sequência recebida "12345" coincide com a regra "XXXX".

No plano de discagem, as regras são definidas em uma determinada ordem. A primeira regra possui prioridade sobre a segunda, a segunda regra possui prioridade sobre a terceira e assim por diante. Se uma regra falha, esta é removida da lista de verificação. Se a sequência coincidir, será com a regra de maior prioridade na lista de verificação. Se os dígitos discados cumprem pelo menos uma regra, a sequência recebida é aceita. Se todas as regras falham, a chamada é recusada.

7.3.4. SS7/SIGTRAN

"**Configuração**" → "**Telefonia**" → "**SS7/SIGTRAN**""

ⓘ	**Nota**	Esta opção é exibida somente se o KMG possuir licença de SS7/SIGTRAN.

Seção com as configurações relacionadas a utilização dos protocolos de interconexão SS7 e SIGTRAN.

O KMG tem suporte a sinalização SS7 e SIGTRAN em seus módulos E1. Estas sinalizações são utilizadas para entroncamento inter-operadoras, e para interconexão com dispositivos do núcleo de suas redes.

A Khomp suporta os protocolos MTP2, MTP3 M2PA e ISUP. Para mais informações sobre estes protocolos, por favor consulte as recomendações da ITU.

São necessárias licenças especiais para utilização da sinalização SS7 ou SIGTRAN com o KMG. Estas licenças podem ser adquiridas com o departamento comercial da Khomp. As licenças estarão atreladas ao número serial do equipamento.

7.3.4.1. Configuração SS7/SIGTRAN

Inicialmente deve-se configurar todos os links a serem utilizados com a sinalização ISUP. Tanto os links que serão utilizados para sinalização (MTP2/M2PA) quanto os links que serão utilizados para voz (Circuit Groups) ou ambos. Após isto acessar o menu SS7/SIGTRAN da Interface Web do KMG. Para maior facilidade na configuração tenha em mãos o Projeto Técnico de Interconexão → PTI.

7.3.4.2. MTP2/M2PA

Deve-se configurar quais dos links serão utilizados como links para sinalização para os protocolos MTP2 e M2PA. É necessário pelo menos um link com sinalização.

MTP2: Adicione o link definindo o nome , dispositivo e modo de operação do link a ser configurado. Além disto podem ser alterados os timers padrões do protocolo MTP2.

M2PA: Adicione o link M2PA cliente ou servidor e definindo um nome. Cliente: Indique o endereço e porta local do KMG e o endereço e porta remota do servidor. Servidor: Indique o endereço e porta do cliente remoto.

M2PA → Configuração de porta local: Porta local utilizada para receber as informações de conexão caso seja configurado um link M2PA servidor neste equipamento.

7.3.4.3. Point Codes

Configuração relacionada aos "Point Codes". São necessários pelo menos dois Point Codes configurados, o local e o remoto. Ao preencher o formato decimal, o campo do formato 3-8-3 será atualizado.

7.3.4.4. MTP3

Configurações relacionadas ao protocolo MTP3, deve-se configurar os Linksets e as Rotas.

Linksets

Configuração dos linksets para associação dos links configurados. Para adicionar um Linkset, é necessário configurar efetuar os seguintes procedimentos:

1. Selecione a Origem (Point Code de Origem) que será o point code utilizado por este Ponto de Sinalização.
2. Selecione o Adjacente (Point Code Adjacente) que é o point code do Ponto de Sinalização imediatamente ligado neste linkset.
3. Selecione o Indicador da rede.
4. Selecione qual link será utilizado por este linkset, dfinindo o valor do SLC (Signaling Link Code) a ser utilizado por este link (este valor deve ser igual ao valor no ponto de sinalização adjacente).

Routes

Configuração de rotas para MTP3.

Para criar uma rota, selecione o PointCode de destino e associe o linkset que possa ser utilizado para alcançar este point code.

Caso seja possível alcançar este point code utilizando mais de um linkset, clique em "Adicionar Linkset à Rota" e volte ao passo 3 quantas vezes forem necessárias. Note que a ordem de inclusão será a ordem de prioridade do linkset para alcançar o point code configurado.

7.3.4.5. ISUP

Configurações referentes aos grupos de circuitos ISUP:

Circuit Groups

Configuração dos Circuit Groups e definição dos timeslots a serem utilizados.

Para adicionar um Circuit Group:

1. Selecione a Origem (Point Code de Origem) que será o point code utilizado como origem das ligações.
2. Selecione o Destino (Point Code de Destino) que será o point code utilizado como destino das ligações.
3. Selecione o link que será utilizado para o tráfego de voz.
4. Defina o valor do CIC (Circuit Identification Code) inicial deste Circuit Group. Este deve ser exatamente igual ao configurado na outra ponta do link.

⚠ Atenção	O KMG não permite a utilização do timeslot 0 e 16 como circuito a ser utilizado na configuração de Circuit Groups.

Caso haja alguma limitação quanto aos timeslots do link que possam ser utilizados, marque ou desmarque as caixas referentes aos timeslots que devem ser utilizados por este Circuit Group.

7.4. Recursos

Timers

Definição dos timers de sinalização ISUP.

Este menu apresenta todos os recursos gerais do equipamento que podem ser adquiridos separadamente dependendo de cada necessidade e cenário.

7.4.1. Integrações

Este menu apresenta todos os recursos gerais do equipamento que podem ser adquiridos separadamente dependendo de cada necessidade e cenário.

7.4.1.1. Insight!

"**Configuração**" → "**Recursos**" → "**Integrações**" → "**Insight!**"

Configurações para permitir acesso através do Insight! a interface Web do KMG. Para tanto é necessário carregar a configuração de VPN fornecida pelo Insight e é necessário que o portal Web (Interface Web) esteja configurado para HTTPS.

7.4.1.2. Device Management

"**Configuração**" → "**Recursos**" → "**Integrações**" → "**Device Management**"

Configurações de integração com o sistema Device Management da Broadsoft que consiste em através de requisições HTTP/HTTPS permitir a atualização de configuração e versão do KMG de forma remota e centralizada através da plataforma Broadsoft.

7.4.1.3. TR-069

"**Configuração**" → "**Recursos**" → "**Integrações**" → "**TR-069**"

Configurações referentes ao suporte ao protocolo TR-069 permitindo a atualização de configuração ou versão do KMG de forma remota e centralizada através de um servidor ACS.

7.4.1.4. Outros sistemas

"**Configuração**" → "**Recursos**" → "**Integrações**" → "**Outros sistemas**"

Nota	Para usar este recurso é necessário ter interface GSM.

Utilizado para integração com o KSMS System que é a plataforma da Khomp desenvolvida para o envio de mensagens SMS, permitindo alcançar clientes através de campanhas de envio de SMS.

Mais informações sobre esta plataforma estão disponíveis no site da Khomp. Para utilizar este recurso, é necessário que o KMG esteja conectado à internet.

7.4.2. Sobrevivência

"**Configuração**" → "**Recursos**" → "**Sobrevivência**"

Nota	Esta opção é exibida somente se o KMG possuir licença de "Sobrevivência".

A Sobrevivência provê ao KMG a capacidade de manter funcionalidades básicas de um PBX em caso de indisponibilidade. O PBX é monitorado e caso seja detectada uma falha o próprio KMG pode assumir o papel do PBX e oferecer recursos de forma limitada, como a manutenção dos registros e das chamadas entrantes e saintes, utilizando os registros conhecidos e a tabela de roteamento do equipamento para o encaminhamento de chamadas.

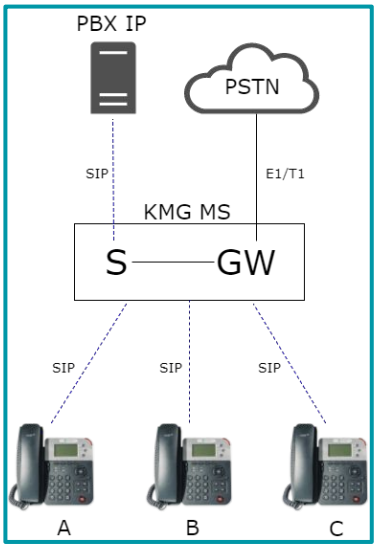
O módulo de Sobrevivência é configurado nos usuários como um proxy para o PBX, portanto todo o fluxo de registros e chamadas passa primeiro pelo módulo de Sobrevivência do KMG antes de chegar ao PBX. O módulo de Sobrevivência verifica a cada intervalo de segundos (configurável), através de SIP OPTIONS, a disponibilidade do PBX. Quando não há resposta ao comando SIP OPTIONS dentro do tempo definido, o KMG assume seu lugar. Neste momento seu modo de operação é alterado de proxy para o modo de Sobrevivência.

No modo Sobrevivência atualmente suportamos as seguintes operações:

- Manutenção dos registros.
- Chamadas locais entre ramais.
- Chamadas entrantes (através de link E1, GSM, FXO do KMG).
- Chamadas saíntes (através de link E1, GSM, FXO do KMG).
- Transferência de chamada (direta e assistida), tanto local quanto externa.

Novos ramais podem se registrar durante o modo de Sobrevivência, mas precisam se registrar novamente quando o PBX voltar a ficar disponível.

Nota	Todos os gateways da linha KMG suportam módulo de Sobrevivência. As licenças devem ser adquiridas separadamente.



Legenda:
S: *Módulo de Sobrevivência.*
GW: *Gateway*.

7.4.2.1. Configuração

Configure no NAP SIP que irá se comunicar com o PBX desejado a opção "Sobrevivência", na lista de proxy, para habilitar o recurso.

7.4.2.1.1. Rede

"**Configuração**" → "**Recursos**" → "**Sobrevivência**" → "**Rede**"

Todas as interfaces de rede do KMG estarão disponíveis para configuração, marque o protocolo desejado (UDP, TCP, TLS), bem como a porta por onde o módulo de Sobrevivência deverá receber os pacotes.

ⓘ	**Nota**	O endereço da interface de rede e a porta configurada na Sobrevivência deverão ser utilizados como configuração de proxy para o PBX no telefone IP ou softphone.

As seguintes opções são apresentadas:

Campo	Descrição	Versão
Interface	Identifica a interface de rede da configuração geral de rede do KMG	4.0.5
IPv4	Configurações para utilizar IP versão 4	
IPv6	Configurações para utilizar IP versão 6	

Opções IPv4 e IPv6

Campo	Descrição	Versão
Nome	Nome da interface de rede na configuração da Sobrevivência	4.0.5
UDP	Habilita utilização de transporte UDP na porta selecionada	
TCP	Habilita utilização de transporte TCP na porta selecionada	
TLS	Habilita utilização de transporte TLS na porta selecionada ⓘ **Nota** — Para habilitar TLS é necessário o carregamento das chaves na configuração TLS global do KMG.	

7.4.2.1.2. Servidores

"**Configuração**" → "**Recursos**" → "**Sobrevivência**" → "**Servidores**"

Nesta área é configurado o servidor SIP (PBX) que a Sobrevivência deverá monitorar e assumir as funcionalidades em caso de falha.

Ao clicar em "Adicionar", um formulário será apresentado para cadastro do servidor contendo os seguintes campos:

Campo	Descrição	Versão
Nome	Identificação do servidor SIP a ser monitorado	4.0.5
Domínio	Identificação do domínio que será utilizado para registro dos usuários	4.1.42.0
Endereço	Constitui a lista de endereços para serem usados no encaminhamento dos registros e chamadas.	
Porta SIP	Porta de rede a ser utilizada para comunicação com o servidor	4.0.5
Transporte	Transporte a ser utilizado para comunicação com o servidor	
Interface	Interface de rede a ser utilizada para se comunicar com o servidor SIP	

Keep Alive

Campo	Descrição	Versão
Intervalo entre testes	Intervalo de tempo (em segundos) que a Sobrevivência deve disparar testes utilizando SIP OPTIONS para detectar falha/indisponibilidade do servidor monitorado	4.0.5
Quantidade máxima de falhas para entrar em Sobrevivência	Quantidade de falhas que devem ocorrer com os testes utilizando SIP OPTIONS para que a Sobrevivência assuma a comunicação no lugar do servidor monitorado	
Expires do registro SIP em modo de Sobrevivência	Tempo (em segundos) que um registro deve ser considerado expirado quando a Sobrevivência está assumindo a comunicação no lugar do servidor monitorado.	

Chamadas

Campo	Descrição	Versão
Ramais para atendimento de chamadas entrantes	Grupo de ramais de atendimento de chamadas entrantes, caso não configurado, todos os ramais registrados serão utilizados como grupo. A Sobrevivência tentará completar as chamadas entrantes tocando cada um dos ramais do grupo por vez, na ordem aqui definida. Ramais de entroncamento não devem constar no grupo de atendimento. **Nota** Quando a Sobrevivência detectar a chamada entrante DDR, o ramal DDR é inserido como primeiro elemento do grupo e, caso conste na lista, poderá tocar mais de uma vez.	4.0.5
Tempo de espera por atendimento	Tempo (em segundos) de espera por atendimento em casa um dos membros do grupo de atendimento. Quando este tempo é atingido, a Sobrevivência cancelará a chamada e fará uma chamada para o próximo ramal do grupo	
Ramais de entroncamento	Ramais (ou registros) que devem ser considerados como entroncamento pela Sobrevivência. Os ramais identificados nesta lista serão utilizados para a realização de chamadas saintes quando se está em modo Sobrevivência, sendo que uma chamada sainte pode tentar utilizar mais de um ramal de entroncamento (na ordem definida por esta configuração). Caso nenhum dos ramais de entroncamento esteja disponível ou esta configuração esteja vazia, a Sobrevivência tentará realizar chamadas saintes sem registro para o módulo de roteamento	

7.4.3. Autorização de Registros

Nota Esta opção é exibida somente se o KMG possuir licença de "Autorização de Registros".

Configurações relacionadas com o módulo de Autorização de registros. Esta aplicação permite que usuários externos externos tenham acesso ao PBX da rede interna, utilizando o KMG para autorizar os registros, mantendo a segurança e ocultação de topologia, garantindo a identidade e confidencialidade dos usuários.

7.4.3.1. Configurações de rede

"**Configuração**" → "**Recursos**" → "**Autorização de registros**" → "**Geral**" → "**Configurações de Rede**"

Todas as interfaces de rede do KMG estarão disponíveis para configuração. Para cada interface habilitada, informe se o transporte de dados será UDP, TCP ou TLS, e indique a porta que será utilizada. No caso de TLS, escolha a configuração TLS no campo correspondente. Para habilitar o TLS, acesse o menu "Configuração" → "Sistema" → "VoIP" → "Criptografia TLS".

Nota O valor padrão da porta do protocolo SIP é **5060**.

7.4.3.2. Opções gerais

- Portas RTP: Informe o intervalo de valores possíveis das portas RTP para envio e recebimento do áudio.
- Modo de funcionamento: Escolha entre os modos "Forward" ou "Back-to-back", que serão explicados com mais detalhes a seguir.

Forward: Nesse modo, as solicitações de registro recebidas pelo KMG são encaminhadas para o primeiro servidor ativo, dentre os servidores configurados na tela "Servidores".

Back-to-back: Nesse modo, os registros são tratados de forma independente para cada servidor configurado. Para utilizar esse modo, os usuários devem ser previamente autenticados via consulta a uma base de dados LDAP. As configurações da base de dados LDAP são as seguintes:

- Servidores LDAP (Primário ou Alternativo): Configuração da base de dados LDAP para realizar a consulta às informações de registro dos usuários.
  - Endereço: Endereço IP do servidor onde se encontra a base de dados LDAP.
  - Porta: Porta que será utilizada pelo KMG para acessar a base de dados LDAP. A porta padrão para o LDAP é 389 e para o LDAPS é a 636.
  - Schema: O tipo de base de dados que será utilizada, podendo ser LDAP ou LDAPS.

É obrigatório configurar o Servidor LDAP Primário. A configuração do Servidor LDAP Alternativo é opcional. Caso configurado, ele será utilizado se a consulta ao servidor primário apresentar falhas.

- Realizar BIND: Caso a base de dados LDAP solicite credenciais de acesso, o usuário e a senha podem ser informados ao selecionar o checkbox Realizar BIND.
- Pesquisa: Parâmetros de busca e avaliação dos usuários no servidor LDAP, através de uma regra que deve ser inserida e deverá ser atendida pelos usuários que tentarem se registrar, dependendo do resultado encontrado com a regra, uma ação pode ser tomada.
  - Base DN: A regra de verificação que deve ser atendida para validação do usuário, a partir de id e valores que serão extraídos da base de dados LDAP.
  - Filtro: Filtro de comparação entre o valor extraído da mensagem REGISTER, e o valor extraído da base de dados LDAP, a partir da regra Base DN. Se os valores forem idênticos, então o usuário terá o acesso liberado.
  - Scope: Nível da base de dados onde o valor extraído do para a Autorização de Registros será pesquisado no LDAP.
  - Nome do atributo Senha: Identificador utilizado para o atributo utilizado como senha na base de dados.
  - Expiração de registro: No modo back-to-back, os tempos de expiração de registro são independentes nos UAS e nos UAC. Indique o tempo de expiração no UAS no campo "Tempo de expiração no UAS" e os valores máximo, mínimo e padrão do tempo de expiração no UAC nos campos da seção "Tempo de expiração no UAC".

7.4.3.3. Opções avançadas

- Manter chave de criptografia no Re-Invite: Ao utilizar TLS, selecione essa opção para utilizar a mesma chave de criptografia na ocorrência de um Re-Invite.
- Validação de registro rigorosa (strict address-of-record): Aceita mensagens subsequentes ao REGISTER (INVITES, etc.) apenas se forem identificadas pelo mesmo address-of-record informado no REGISTER.
- Usar o mesmo transporte do UAC: Utiliza o mesmo transporte do UAC para a troca de mensagens com o UAS.
- UAC Keep Alive (OPTIONS): Envia Keep Alive, por meio de pacotes OPTIONS, para os UAC. Para cada tipo de transporte (UDP, TCP ou TLS), escolha o intervalo em segundos para o envio dos pacotes, ou utilize a opção "Desativado" para não enviar Keep Alive.

ⓘ	**Nota**	Clique em Salvar para guardar as configurações, e em Aplicar para enviá-las ao KMG

7.4.3.4. Perfis de mídia para Autorização de Registros

Os perfis de mídia guardam os codecs que poderão ser utilizados pelos usuários do serviço de Autorização de Registros ao realizar chamadas por meio do KMG. Podem ser configurados em:

"Configuração" → "Recursos" → "Autorização de registros" → "Perfis de mídia"

Para adicionar um novo perfil, clique no botão Adicionar. Na tela que será apresentada, dê um nome ao perfil, selecione os codecs permitidos, e os transportes de mídia (UDP-RTP, UDP-SRTP ou TCP-RTP) relacionados a cada transporte da sinalização (SIP UDP, SIP TCP ou SIP TLS).

Nota	Clique em Salvar para guardar as configurações, e em Aplicar para enviá-las ao KMG

7.4.3.5. Servidores para Autorização de Registros

O KMG realiza a autorização ou não de novos registros, e quando autorizado, envia o registro para os servidores configurados, de acordo com o modo de operação selecionado (Forward ou Back-to-back). Para configurar os servidores, acesse:

"Configuração" → "Recursos" → "Autorização de registros" → "Servidores"

Para adicionar um novo servidor, clique no botão Adicionar e configure os seguintes parâmetros:

- Nome: Nome de identificação do servidor.
- Domínio: Domínio associado ao servidor.

No painel Endereços, configure os seguintes campos relacionados ao servidor:

- Endereço: Endereço de rede IP do servidor.
- Porta: Porta de rede que será utilizada para acessar o servidor.
- Transporte: Transporte de dados entre o KMG e o servidor, podendo ser UDP, TCP ou TLS.
- Keep Alive (OPTIONS): Intervalo de tempo para envio do Keep Alive, mensagem que verifica que a estrutura de rede está conectada e funcionando.
- Interface de rede: Interface de rede do KMG que será utilizada para se comunicar com o servidor VoIP;

Cada servidor pode ter mais de um endereço. Para adicionar um novo endereço, clique no link Adicionar endpoint.

- Modo de operação:
  - BRIDGE: Não há tratamento da mídia da chamada pelo KMG, não ocorrendo transcoding. Selecione um perfil de mídia para o UAC e um para o UAS. O KMG aceitará chamadas com quaisquer codecs, mesmo se diferentes dos configurados no perfil de mídia.
  - TRANSCODE: Possibilita a conversão entre diferentes codecs. Selecione um perfil de mídia para o UAC e um para o UAS.
  - FILTERED-BRIDGE: Encaminhamento das chamadas APENAS quando o dispositivo telefônico ou o servidor apresentar suporte aos mesmos codecs disponibilizados para uso no KMG. Nesse caso não há transcoding, e se o dispositivo telefônico ou o servidor não apresentar um codec compatível, a chamada será ignorada. Os codecs aceitos serão os configurados pelo perfil de mídia escolhido.

Nota	Clique em Salvar para guardar as configurações, e em Aplicar para enviá-las ao KMG

Os servidores configurados serão mostrados numa lista. Para tornar um servidor como o principal para envio das mensagens, pressione o ícone indicado pela estrela (*configurar UAS como principal*).

7.4.3.6. Políticas para Autorização de Registros

Utilizando as políticas de Autorização de Registros, é possível permitir ou não o registro de usuários e a realização de chamadas através do KMG. A verificação é feita por meio da análise dos métodos do protocolo SIP, como o REGISTER, INVITE, etc. Para configurar as políticas para Autorização de Registros, acesse:

"Configuração" → "Recursos" → "Autorização de registros" → "Políticas"

As políticas podem ser utilizadas juntas, e um registro só será efetuado se atender a todas as regras contidas nelas.

7.4.3.6.1. Todos os métodos: validação User-Agent

Por meio de expressões regulares, libera, bloqueia ou repassa a verificação para os demais métodos, com base no cabeçalho User-Agent recebido. Caso a mensagem não contenha o campo esperado, ele será considerado vazio (expressão regular ^$).

- Expressões regulares para validação do User-Agent: Expressões regulares que devem ser verificadas para que as ações possam ser tomadas.
- Ação caso avaliado positivamente: Se o valor extraído do cabeçalho User-Agent atender a regra estabelecida, a ação configurada será tomada.
- Ação caso avaliado negativamente: Se o valor extraído do cabeçalho User-Agent não atender a regra estabelecida, a ação configurada será tomada.

As ações possíveis são:

- ACCEPT → Aceita a requisição.
- DROP → Ignora a requisição.
- NEXT → Repassa a requisição ao próximo nível de políticas.

7.4.3.6.2. Método REGISTER: pré autorização

É uma verificação feita quando um aparelho telefônico tenta se registrar no PBX IP por meio do KMG.

A seguir, é apresentado um exemplo de mensagem do tipo REGISTER:

```
REGISTER sip:10.3.0.34;transport=TCP SIP/2.0
From: "Khomp 00"<sip:3321000@10.3.0.34>;tag=a92908-0-13c4-58ac54c5-60440b51-58ac54c5
To: "Khomp 00"<sip:3321000@10.3.0.34>
Call-ID: aa44d0-0-13c4-58ac523f-1df7d2a3-58ac523f
CSeq: 3 REGISTER
Via: SIP/2.0/TCP 10.100.10.246:5060;branch=z9hG4bK-58ac54c5-612b2463-2af4becf
Expires: 3650
Allow: INVITE,CANCEL,BYE,REFER,NOTIFY,SUBSCRIBE,INFO,ACK,MESSAGE
user-Agent: IPS 200 V4.0.2.6 9726
Max-Forwards: 70
Supported: replaces,100rel,eventlist
Contact: <sip:3321000@10.100.10.246:5060;transport=TCP>
Authorization: Digest
username="3321000",realm="asterisk",nonce="1487699055/ebd4bf6fd11830a630fe61e
9587def33",uri="sip:10.3.0.34;transport=TCP",response="d9f680586ffb746cae9dfbfa0ff046ab",
algorithm=MD5,cnonce="61
2464",opaque="28a16df8265154d3",qop=auth,nc=00000002
Content-Length: 0
```

- Utilizar valores do cabeçalho SIP → Os seguintes campos da mensagem SIP podem ser utilizados para a verificação:
  - AUTHORIZATION → Dados de autenticação do usuário.
  - FROM → Identificação da origem da mensagem.
  - TO → Identificação de destino da mensagem.

- Configuração LDAP → Configuração da base de dados LDAP para realizar a verificação da informação extraída em Utilizar valores do cabeçalho SIP:
  - Endereço: Endereço IP do servidor onde se encontra a base de dados LDAP.
  - Porta: Porta que será utilizada pelo KMG para acessar a base de dados LDAP. A porta padrão para o LDAP é 389 e para o LDAPS é a 636.
  - Schema: O tipo de base de dados que será utilizada, podendo ser LDAP ou LDAPS.

- Realizar BIND → Caso a base de dados LDAP solicite credenciais de acesso, o usuário e a senha podem ser informados ao selecionar o checkbox Realizar BIND.
- Pesquisa → Parâmetros de busca e avaliação dos usuários no servidor LDAP, por meio de uma regra que deverá ser atendida pelos usuários que tentarem se registrar. Dependendo do resultado encontrado com a regra, uma ação pode ser tomada.
  - Base DN: A regra de verificação que deve ser atendida para validação do usuário, a partir de id e valores que serão extraídos da base de dados LDAP.
  - Filtro: Filtro de comparação entre o valor extraído da mensagem REGISTER, e o valor extraído da base de dados LDAP, a partir da regra Base DN. Se os valores forem idênticos, então o usuário terá o acesso liberado.
  - Scope: Nível da base de dados onde o valor extraído será pesquisado na base de dados LDAP.

- Validação de atributos → Ação que deve ser tomada de acordo com o resultado encontrado na avaliação da tentativa de registro.
  - Ação caso avaliado positivamente → Se o valor extraído da mensagem atender a regra estabelecida, uma das ações pode ser tomada:
    - ACCEPT → Aceita o registro.
    - DROP → Ignora o registro.
  - Ação caso avaliado negativamente → Se o valor extraído da mensagem atender a regra estabelecida, uma das ações pode ser tomada:
    - ACCEPT → Aceita o registro.
    - DROP → Ignora o registro.
  - Ação caso não seja possível avaliar → Se o valor extraído da mensagem atender a regra estabelecida, uma das ações pode ser tomada:
    - ACCEPT → Aceita o registro.
    - DROP → Ignora o registro.

7.4.3.6.3. Método INVITE: Verificar estado de registro

Verificação do estado do registro de um usuário, feita quando ele tenta realizar uma chamada (INVITE) através do KMG. Exemplo de mensagem do tipo INVITE:

```
INVITE sip:3321002@10.3.0.34;transport=TCP SIP/2.0
From: "Khomp 00"<sip:3321000@10.3.0.34>;tag=a86188-0-13c4-58ac5814-13bba396-58ac5814
To: "3321002"<sip:3321002@10.3.0.34>
Call-ID: a96a38-0-13c4-58ac5814-71161939-58ac5814@10.3.0.34
CSeq: 1 INVITE
Via: SIP/2.0/TCP 10.100.10.246:5060;branch=z9hG4bK-58ac5814-61380f03-7086c167
user-Agent: IPS 200 V4.0.2.6 9726
Max-Forwards: 70
Supported: replaces,100rel,eventlist
Allow: INVITE,CANCEL,BYE,REFER,NOTIFY,SUBSCRIBE,INFO,ACK,UPDATE,MESSAGE
Contact: <sip:3321000@10.100.10.246:5060;transport=TCP>
Content-Type: application/sdp
Content-Length: 251

v=0
o=IpPhone 2890844526 8000 IN IP4 10.100.10.246
s=IpPhone CALL
c=IN IP4 10.100.10.246
t=0 0
m=audio 10006 RTP/AVP 0 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

- Utilizar valores do cabeçalho SIP: Os seguintes campos da mensagem SIP podem ser utilizados para a verificação:
  - AUTHORIZATION → Dados de autenticação do usuário.
  - FROM → Identificação de origem da mensagem.
  - TO → Identificação de destino da mensagem.

- Positivo se estado está entre: A avaliação é considerada positiva se o estado do registro for:
  - INVALID → O estado não pode ser verificado.
  - REGISTERED → O usuário está registrado.
  - EXPIRED → A sessão de registro está expirada.

- Ação caso avaliado positivamente:
  - ACCEPT → Aceitar a mensagem.
  - DROP → Ignorar a mensagem.

- Ação caso avaliado negativamente:
  - ACCEPT → Aceitar a mensagem.
  - DROP → Ignorar a mensagem.

- Ação caso não seja possível avaliar:
  - ACCEPT → Aceitar a mensagem.
  - DROP → Ignorar a mensagem.

ⓘ	**Nota**	Clique em Salvar para guardar as configurações, e em Aplicar para enviá-las ao KMG.

7.5. Roteamento

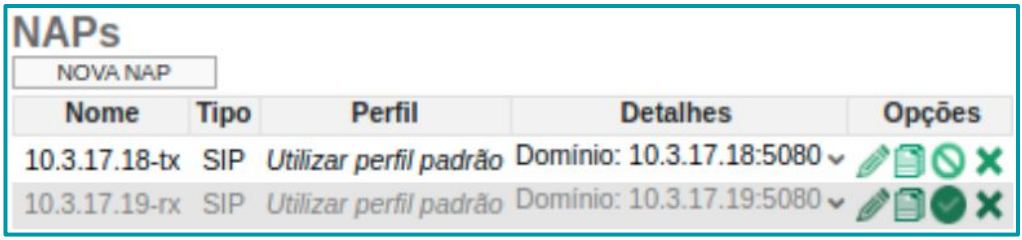
O menu roteamento agrega todas as configurações relacionadas ao roteamento de chamadas que são as configurações mais usuais do equipamento.

No roteamento são configuradas as rotas e NAPS que fazem a conexão das chamadas de um ponto a outro. Além disso, são definidos os perfis, CDR, Portabilidade, Scripts de roteamento entre outras funcionalidades.

7.5.1. NAP

"Configuração" → "Roteamento" → "NAPs"

Como mencionado anteriormente, o KMG funciona em um conceito de associações entre NAPs e Rotas. NAP (Network Access Points) é uma representação lógica para agrupar links E1/T1, canais GSM, canais analógicos FXS/FXO e troncos SIP. Estas NAP's serão usadas no roteamento das chamadas podendo ser pontos de origem, destino ou ambos. Portanto, antes de configurar uma rota, é necessário definir suas NAPs.



As ações possíveis a serem feitas com as NAPs são:

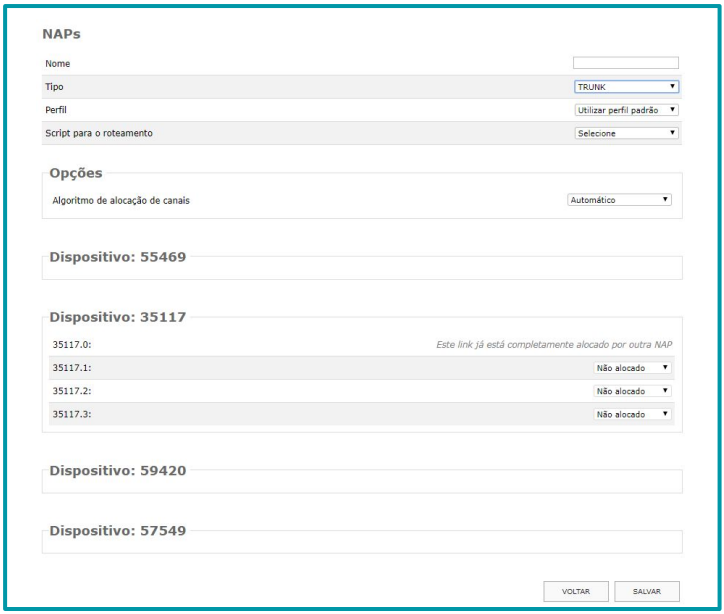
- Nova NAP → NOVA NAP
- Editar configurações da NAP →
- Copiar NAP →
- Ativar ou desativar NAP (caso uma NAP participante de uma rota ativa seja desativada, essa rota se tornará inoperante) → (ativada (desativad
- Excluir NAP →

Ao criar um novo NAP, será possível selecionar um tipo de NAP. Os campos serão exibidos para configuração. Alguns campos são exclusivos e correspondentes ao tipo selecionado. Ao longo desta seção, são descritos mais detalhes sobre cada tipo de NAP.

7.5.1.1. Criar tronco E1/T1

"Configuração" → "Roteamento" → "NAPs"

1. Clique no botão "Nova NAP".
2. No campo "Tipo", selecione a opção "Trunk". Serão exibidas as opções para configuração de um tronco E1/T1.



3. Selecione um perfil de telefonia, ou deixe a opção "Utilizar perfil padrão", que atende a maioria dos cenários. Veja a seção "Configurar propriedades das chamadas" para mais informações sobre perfis.
4. No campo 'Script para o roteamento', selecione um script que foi criado previamente. Veja a seção "Scripts" neste manual para mais informações.
5. No campo 'Algoritmo de alocação de canais', selecione um algoritmo para definir a forma como os canais do link serão utilizados. Veja a seção "Algoritmo de alocação de canais" neste manual para mais informações.
6. No painel 'Dispositivos' serão exibidos todos os módulos conectados ao KMG que possuem interface E1/T1, representado pelo seu número de série.

- Não alocado: O link não será utilizado por esta NAP.
- Todo o link: Todos os canais deste link devem ser utilizados por esta NAP. Se esta opção não estiver sendo exibida, o link está sendo usado de forma fracionada por outra NAP.
- Fracionar o Link: Apenas os canais selecionados serão utilizados por esta NAP. Se algum canal estiver desabilitado, ele está sendo usado por outra NAP.
- Se ao criar um tronco E1 e você visualizar somente a mensagem "Este link já está completamente alocado por outra NAP", significa que todos os links E1/T1 disponíveis estão sendo usados por outra NAP.

7. Clique no botão "Salvar". Se nenhuma outra configuração for realizada, clique no botão "Aplicar" para que as alterações entrem em operação.

Os dispositivos que possuem links E1/T1 que estão completamente alocados, apresentarão uma mensagem informando esta situação. Durante o roteamento, este NAP é válido como origem se o canal alocado para a entrada da chamada está associado a ela.

7.5.1.2. Criar tronco SIP

Uma NAP SIP é o ponto de entrada/saída para ligações VoIP. Ao selecionar este tipo de NAP, são exibidos os campos a seguir.

Campo	Descrição	Versão
Domínio	Endereço IP do host.	–
Porta do Domínio	Porta SIP de escuta do domínio, de onde virão os pacotes e para onde devem ser enviados.	
Vendor	• Esta opção preencherá automaticamente os campos do NAP necessários para trabalhar com o fornecedor selecionado. • Atualmente o KMG ONE oferece compatibilidade com o "Vendor Microsoft Teams".	–

Registro

Campo	Descrição	Versão
Registro	Marque esta caixa caso o domínio requisite registro e autenticação para enviar/receber chamadas.	–
Usuário	Nome do usuário registrado do domínio.	
Usuário de autorização	Nome de usuário que deve ser utilizado para autenticação.	
Senha	Senha para autenticação com o domínio.	
Expiração	Intervalo de tempo em segundos requisitado para a expiração do registro SIP. (Tempo padrão 3600 seg.)	
Aceitar este NAP como origem	Valor padrão: Sempre. Nesse caso não será realizado nenhuma análise e aceitará a NAP como válida. Os outros comportamentos se referem aos campos recebidos no Invite, verificando se o usuário registrado está presente nos campos From, To, ou ambos aceitando ou não a chamada entrante dependendo desta análise realizada.	3.3.0

Opções

Campo	Descrição	Versão
Utilizar origem pelo endereço do pacote IP	Em ligações entrantes, utiliza o endereço do pacote IP como "Domínio" para validação, ao invés de utilizar o valor contido no campo "From".	–
Utilizar o header P-Asserted-Identity como número de origem	Identidade comprovada do originador de uma solicitação em uma rede confiável	
Utilizar RTCP mux em chamadas saintes	Multiplexa os fluxos de RTP e RTCP para as chamadas saintes	
Incluir proxy no cabeçalho Route	Inclui endereço de proxy no header Route	
Repassar os parâmetros do header Refer-to na URI do Invite	Repassa os parâmetros do header Refer-to na URI do Invite	
Timeout para desconectar quando a transferência for estiver concluída (em segundos)	Timeout para desconectar quando a transferência estiver concluída	
Forçar chamadas entrantes por um proxy configurado	Serão aceitas apenas as chamadas originadas dos servidores proxy definidas na "Lista de Proxy"	
Ignorar porta de origem	Em ligações entrantes, ignorar a porta de origem do pacote SIP.	
Utilizar número chamado na URI	Em ligações entrantes, utiliza o número chamado enviado no header "RequestURI" ao invés de utilizar o valor do campo "To".	
Proxy fallback timeout	Tempo limite em segundos para que o proxy configurado nesta NAP seja considerado como destino. Caso nenhuma resposta seja recebida neste tempo, o próximo proxy da lista será utilizado. Caso todos os destinos estejam indisponíveis esta NAP não será utilizada e um retry poderá ser realizado para uma outra rota conforme configuração.	
Tempo máximo de inatividade na sessão SIP	Intervalo de tempo limite para o encerramento da chamada SIP caso apresente inatividade.	
Limite de canais alocados	Limita a quantidade de canais VoIP que podem ser utilizados por esta NAP. Este limite se aplica a ligações entrantes e saintes.	3.0.0

Keep Alive

A indicação dos campos para o "Modo de operação do Keep Alive", são observados a seguir.

Campo	Descrição
Desativado	Neste modo de operação a verificação de estado do NAP não será realizada e será admitido que o NAP estará sempre ativo.
SIP OPTIONS	Neste modo de operação mensagens de verificação SIP OPTIONS serão enviadas a cada intervalo de tempo configurado no campo 'Intervalo entre verificações' para verificar o estado do link.
SNMP	Neste modo de operação o NAP fará uso do protocolo SNMP para verificar o estado link.
Predefinição	A predefinição SNMP oferece compatibilidade com o KMG e Kmedia. Caso o gerenciador SNMP seja um dispositivo diferente destes, também é possível utilizar a opção CUSTOM, tornando a configuração personalizável"
KMG e Kmedia	Caso a predefinição seja para o KMG ou Kmedia.
Índice do link	Índice da tabela SNMP.
Servidor	IP ou domínio do servidor SNMP.
KMG	Caso a predefinição seja para o KMG.
Serial do dispositivo	Número de série KMG na outra extremidade do NAP.
CUSTOM	Caso o dispositivo na outra ponta do NAP seja diferente do KMG ou Kmedia.
Comunidade	String de comunidade (community string) SNMP.
OID	Identificação do objeto SNMP.
Tipo de resposta	Tipo da resposta esperada, pode ser: STRING, HEX-STRING, INTEGER, GAUGE ou OPAQUE.
Resultados esperados	Resultados esperados da mensagem de acordo com o tipo de resposta. Aqui é possível inserir mais de um resultado.
Intervalo entre verificações (em segundos)	Intervalo de tempo em segundos em que a verificação será realizada para os modos de operação SIP OPTIONS e SNMP.

Atenção

- As definições de keep alive dependem de escolher SIP OPTION ou SNMP.
- Com SIP OPTIONS só é permitido escolher o intervalo de verificação.

Rede

Campo	Descrição	Versão
Interface de rede para o protocolo SIP	Define qual a interface de rede que deve ser utilizada para o protocolo SIP	3.2.0
Interface de rede para o protocolo RTP	Define qual a interface de rede que deve ser utilizada para o protocolo RTP	
Modo de travessia a NAT	Habilita ou desabilita o suporte a travessia de NAT	

Modo de travessia NAT

Campo	Descrição	Versão
STUN	Caso esteja habilitada a travessia de NAT por "Servidor STUN", este campo deve ser preenchido com o endereço IP do servidor STUN	2.1.0
Porta do STUN	Caso esteja habilitada a travessia de NAT por "Servidor STUN", este campo deve ser preenchido com a porta de rede do servidor STUN	
Endereço IP externo para o protocolo SIP	Caso esteja habilitada a travessia de NAT por "Endereço externo IP fixo", este campo deve ser preenchido com o endereço IP externo utilizado para o protocolo SIP	3.2.0
Endereço IP externo para o protocolo RTP	Caso esteja habilitada a travessia de NAT por "Endereço externo IP fixo", este campo deve ser preenchido com o endereço IP externo utilizado para o protocolo RTP	
Ignorar o erro nomination timeout no estabelecimento da sessão ICE	Ignorar o erro nomination timeout no estabelecimento da sessão ICE	3.2.0
Servidor STUN a ser utilizado com ICE	Servidor STUN a ser utilizado com ICE	3.2.0
Endereço IP externo para o protocolo SIP com ICE	Endereço IP externo para o protocolo SIP com ICE	3.2.0

Nota

- Os campos STUN e Porta de STUN são apresentados ao escolher "Servidor STUN".
- Os campos SIP e RTP aparecem ao escolher Endereço IP Externo Fixo.

Lista de proxy

Permite adicionar servidores de proxy SIP. Para adicionar um novo servidor, clique em "Adicionar proxy" no canto inferior direito da lista de proxy. Nas opções Interface SIP, Transporte SIP, Interface do áudio e transporte do áudio, é possível utilizar as definições aplicadas no NAP SIP, ou especificar valores diferentes.

Transporte

Campo	Descrição	Versão
Aceitar qualquer tipo de transporte para o SIP em chamadas entrantes	Aceita qualquer protocolo de sinalização SIP entrante para este NAP	4.0.0
Aceitar qualquer tipo de transporte para o áudio (RTP) em chamadas entrantes	Aceita qualquer protocolo de áudio RTP entrante para este NAP	
Tipo de transporte SIP	Define o tipo de transporte a ser utilizado para o protocolo SIP	3.1.0
Tipo de transporte para o áudio	Define o tipo de transporte a ser utilizado para o protocolo RTP	

SIP-I

Campo	Descrição
Ativar suporte	• Checkbox para ativar o suporte da utilização do protocolo ISUP como corpo de mensagem SIP, conforme as RFC 3398 e ITU-T 1912.5 (Profile C). • A versão base do ISUP utilizada é ITU-T92+ e é mandatório o suporte no lado remoto.
Aceitar outras versões como compatíveis	Especificação das versões ISUP que serão aceitas como compatíveis.
Versão	• Identificação de versão do protocolo ISUP a ser utilizada no parâmetro "version" do tipo MIME segundo RFC 3204 cláusula 3: "O uso do parâmetro "version" permite os administradores identificarem versões específicas do ISUP que serão trocadas de forma bilateral". • Para que o conteúdo do ISUP remoto seja aceito, é necessário que a versão coincida com o valor atribuído neste campo ou que a versão base seja ITUT-T92+. • O valor padrão é "itu-t".

7.5.2.3. Configurar canais GSM

NAP GSM cria um ponto para entrada e saída de chamadas através desta interface.

7.5.2.3.1. Opções

O campo "Algoritmo de alocação de canais" define qual algoritmo deve ser utilizado para a alocação dos canais associados a este NAP. Veja "Algoritmo de alocação de canais" para mais detalhes.

O campo "Algoritmo de alocação de canais SMS" permite configurar a utilização dos SIM cards para envio de SMS, no qual é definido o algoritmo de utilização e a ordenação.

- Algoritmo:
  - Primeiro livre: Aloca o primeiro canal que estiver disponível.
  - Round robin: Aloca os canais de forma equilibrada de forma que todos enviem a mesma quantidade de SMS.
  - Ordenação dos canais:
    - Crescente: Aloca do menor canal até o maior.
    - Decrescente: Aloca do maior canal até o menor.

SIM cards

Fornece opções para utilização dos SIM cards em cada modem do dispositivo GSM. Sendo que cada modem possui um SIM card ativo e outro stand-by, podendo ser alterado.

- Minutos de uso para trocar o SIM card: Ao habilitar esta opção, é necessário especificar a quantidade de minutos, conforme contrato com a operadora. Ao atingir a quantidade de minutos definida, o KMG envia a chamada para o SIM card stand-by.
- SMSs enviados para trocar SIM card: Ao habilitar esta opção, é necessário especificar a quantidade de SMS enviado pelo SIM card, conforme contrato com a operadora. Ao atingir a quantidade de SMS definida, o KMG envia para o SIM card stand-by.

Ao clicar no botão "Adicionar manualmente", é possível inserir os SIM cards. Para isso é necessário preencher o ICCID do SIM card.

Controle de consumo

Se esta opção estiver habilitada, fornece opção para controlar a utilização dos SIM cards de forma individual, independente do modelo no qual o SIM card está inserido.

- Período para renovação: Define o período que o SIM card poderá ser usado novamente, caso o limite de minutos ou quantidade de SMS tenha sido atingido. É possível selecionar os seguintes valores: Diário, Semanal ou Mensal. Dependendo do período selecionado, é necessário especificar o momento da renovação no campo a seguir. Por exemplo, se o período selecionado for diário, é necessário especificar a hora da renovação. Caso seja selecionado semanalmente, é necessário especificar o dia da semana e o dia do mês para o período mensal.
- Minutos por período: Quantidade de minutos que um SIM card poderá realizar durante o período definido. Ao atingir essa cota, outro SIM card será usado.
- SMSs por período: Quantidade de SMS que um um SIM card poderá enviar durante o período definido. Ao atingir essa cota, outro SIM card será usado.
- Limites compartilhados: Se esta opção estiver habilitada, tanto a quantidade de minutos quanto o de SMS serão compartilhados entre todos os SIM cards existentes no NAP.
- Intervalo para controle de consumo: Define o intervalo usado para controlar o consumo do plano do SIM card. O primeiro valor indica o tempo da tarifação inicial, independente do tempo da chamada. O segundo valor indica o tempo para a cobrança de minutos adicionais. Portanto, se for definido 60/6, a chamada terá a cobrança referente a 60 minutos, mesmo que a duração seja menor que este tempo. Se esta mesma chamada tiver duração superior a este tempo, o controle de tarifação será de 6 em 6 minutos.
- Trocar cartão SIM: Define o momento em que deverá ocorrer a troca do SIM card.

7.5.1.4. Configurar canais FXS

As rotas FXS são as associações entre o KMG e um NAP FXS como destino, que será utilizado para alocar o canal FXS para o envio. Também é possível definir filtros para sua utilização, como número de destino e consulta a portabilidade.

Crie um novo NAP e selecione o tipo como FXS e note que um menu adicional será apresentado com as opções:

- Marcador de fim de discagem → Dígito que quando discado irá marcar o fim do processo de discagem.
- Tempo limite para discagem → Período para realizar a discagem da chamada, após o fim do tempo limite, a chamada será cancelada.

Ainda no menu adicional, selecione um ou mais canais para compor o NAP e realize as seguintes configurações em:

7.5.1.4.1. Registrar extensões

Campo	Descrição
Domínio	Endereço IP do host.
Porta do Domínio	Porta de escuta do domínio, de onde virão os pacotes e para onde devem ser enviados.
Expiração	Prazo para a validade do registro ser expirado.

Opções

Campo	Descrição
Utilizar origem pelo endereço do pacote IP	Em ligações entrantes, utiliza o endereço do pacote IP como "Domínio" para validação, ao invés de utilizar o valor contido no campo "From".
Forçar chamadas entrantes por um proxy configurado	Tempo máximo de espera de uma resposta via determinado proxy ativo. Ao passar do tempo limite, o próximo proxy ativo será utilizado (fallback). Quando não houver proxies ativos para realizar o fallback, a chamada é encerrada ou ocorrerá o retry para a próxima rota.
Ignorar porta de origem	Em ligações entrantes, ignorar a porta de origem do pacote SIP.
Utilizar número chamado da URI	Em ligações entrantes, utiliza o número chamado enviado no header "RequestURI" ao invés de utilizar o valor do campo "To".
Fallback timeout	Tempo máximo de espera de uma resposta via determinado proxy ativo. Ao passar do tempo limite, o próximo proxy ativo será utilizado (fallback). Quando não houver proxies ativos para realizar o fallback, a chamada é encerrada ou ocorrerá o retry para a próxima rota.
Intervalo entre verificações do Keep Alive (SIP OPTION)	Habilita ou desabilita a verificação de Keep Alive do servidor SIP remoto. Caso habilitada, esta opção desativará o NAP caso a verificação de Keep Alive falhe. Tempo definido em milissegundos.
Tempo máximo de inatividade na sessão SIP	Intervalo de tempo limite para o encerramento da chamada SIP caso apresente inatividade.
Perfil de CODECs da rota	Habilita ou desabilita o uso de determinados codecs de acordo com os Perfis de CODECs criados.

Rede

Campo	Descrição
Interface de rede para o protocolo SIP	Define qual a interface de rede que deve ser utilizada para o protocolo SIP.
Interface de rede para o protocolo RTP	Define qual a interface de rede que deve ser utilizada para o protocolo RTP.

Modo de travessia a NAT	Define qual será o método a ser utilizado de travessia NAT. Os métodos STUN e ICE são suportados.
	• Servidor de STUN: Modo de travessia Session Traversal Utilities for NAT (STUN):
	  • STUN: Este campo deve ser preenchido com o endereço IP do servidor STUN.
	  • Porta do STUN: Este campo deve ser preenchido com o número de porta do servidor STUN.
	• ICE: Modo de travessia Interactive Connectivity Establishment (ICE):
	  • Ignorar o erro nomination timeout no estabelecimento da sessão ICE: Checkox para ignorar ou não o erro nomination timeout na sessão ICE.
	  • Servidor STUN a ser utilizado com ICE: Este campo deve ser preenchido com o endereço IP do servidor STUN.
	  • Porta do STUN: Este campo deve ser preenchido com o número de porta do servidor STUN.
	  • Endereço IP externo para o protocolo SIP com ICE: Este campo deve ser preenchido com o IP externo para o SIP com ICE.
	• Endereço IP externo fixo:
	  • Endereço IP externo para o protocolo SIP: Caso esteja habilitada a travessia de NAT por "Endereço externo IP fixo", este campo deve ser preenchido com o endereço IP externo utilizado para o protocolo SIP.
	  • Endereço IP externo para o protocolo RTP: Caso esteja habilitada a travessia de NAT por "Endereço externo IP fixo", este campo deve ser preenchido com o endereço IP externo utilizado para o protocolo RTP.

Opções avançadas

Campo	Descrição
Sobrescrever header "From"	Esta configuração irá sobrescrever o componente hostport da URI do header FROM nesta NAP (quando ela for usada como NAP Destino). Deve estar no formato HOST:PORTA Ex: 127.0.0.1:5060. Caso a NAP tenha registro configurado, a alteração deste campo pode apresentar problemas.
Enviar a porta no header "TO" do invite	Esta configuração irá definir se deve enviar o campo porta na URI do header TO nesta NAP (quando ela for usada como NAP Destino). Se marcado (padrão) irá enviar HOST:PORTA Exemplo: **127.0.0.1:5060** Caso contrario, enviará apenas HOST Exemplo: **127.0.0.1**

7.5.1.4.2. Lista de proxy

Caso o servidor IP PBX possua proxies, eles devem ser inseridos e configurados na Lista de Proxy. Indicando o endereço de rede, e a porta por onde será possível ter acesso ao servidor e trafegar os dados do KMG.

7.5.1.4.3. Extensões

Tabela onde são cadastrados os ramais dos dispositivos FXS. Estas informações deverão estar de acordo com o servidor SIP.

No cabeçalho da tabela de dispositivos FXS, é exibido o serial. Ao lado há uma opção para preencher o número da extensão e usuário para registro de forma automática. Para isso é necessário apenas cadastrar o menor ramal do intervalo.

Exemplo: Ao cadastrar o ramal 2000, através desta opção, o KMG automaticamente cadastra os demais ramais (2001, 2002, etc.) em todos os canais do dispositivo.

Por fim, há um botão para limpar as extensões cadastradas no dispositivo, caso seja necessário limpar todos.

Segue a descrição de cada coluna desta tabela.

- Canais: Relação dos canais FXS que podem ser incluídos ao NAP (canais que estiverem com a seleção bloqueadas já pertencem a um NAP FXS).
- Número da Extensão: Número de discagem que servirá para identificar o canal;
- Usuário para registro: Usuário para registro da extensão;
- Senha para registro: Senha para registro da extensão.

7.5.1.4.4. Padrão de Ring

Define o padrão do toque para os dispositivos definidos no NAP, em milissegundos. É necessário cadastrar ao menos um tempo de toque e um de silêncio.

Por padrão, o KMG possui 1000 milissegundos de toque e 4 milissegundos de silêncio.

7.5.1.4.5. Cadências

Define o tempo para o tom de discagem e de desconexão que serão transmitidos aos dispositivos cadastrados no NAP. É necessário cadastrar ao menos um tempo de tom e um de silêncio.

7.5.1.5. Configurar canais FXO

As rotas FXO são as associações entre o KMG e um NAP FXO de destino, que será utilizado para alocar o canal FXO para o recebimento de chamadas.

Campo	Descrição
Canais	Relação dos canais FXO que podem ser incluídos ao NAP (canais que estiverem com a seleção bloqueadas já pertencem a um NAP FXO)
Número desta linha	Número que servirá para identificar o canal

7.5.1.6. Configurar grupos de NAP → NAP GROUP

NAPs GROUP representam um agrupamento de outros tipos de NAP, cada um associados a um peso. Quando um NAP deste tipo é associado em uma rota como NAP sainte, as chamadas saintes serão balanceadas entre os membros do grupo utilizando o algoritmo de distribuição selecionado. Quando associado em uma rota como NAP entrante, todos os membros do grupo são candidatos válidos a NAP de entrada para a referida rota.

Grupos nunca têm perfil associado, às chamadas encaminhadas deverão utilizar o perfil da rota, do NAP membro ou padrão.

A chave "dest_nap" no CDR irá conter o nome do NAP membro utilizado para encaminhar a chamada e a chave "nap_group" deve ser utilizada para registrar o nome do grupo.

Campo	Descrição
Forçar distribuição proporcional dos pesos	Ao habilitar esta opção, o gateway irá desconsiderar membros do grupos que tenham excedido seu peso proporcional (ver "Peso") de encaminhamento de chamadas, mesmo quando está ocorrendo um "retry" dentro do grupo. Caso não seja possível encaminhar a chamada a qualquer um dos membros (por ter excedido valor proporcional ou por não ter canal disponível), então o sistema deverá considerar a próxima rota
Algoritmo de distribuição de carga	Seleciona o algoritmo a ser utilizado para realizar a distribuição de carga entre os NAPs membros do grupo
NAP	Seleciona o nome do NAP membro do grupo
Peso	O peso atribuído a cada NAP será normalizado utilizando a fórmula: 100 * PESO / SOMA(PESO), fornecendo um número no intervalo [0..100], denominado peso proporcional, o qual será utilizado para a distribuição de alocação de canais no grupo. Utilize o valor zero no peso para que o NAP seja considerado para alocação somente durante um retry dentro do grupo

7.5.1.6.1. Algoritmos de distribuição de carga

Dois algoritmos estão disponíveis: "Chamadas encaminhadas" e "Chamadas ativas".

- Chamadas encaminhadas: Será considerada a quantidade de chamadas que foram proporcionalmente encaminhadas para cada NAP membro do grupo. Este algoritmo objetiva encaminhar chamadas de maneira proporcional em relação aos pesos atribuídos.
- Chamadas ativas: Será considerada a quantidade de chamadas ativas no momento do encaminhamento em cada NAP membro em relação ao total de chamadas ativas em todos os membros. Este algoritmo objetiva manter chamadas ativas de maneira proporcional em relação aos pesos atribuídos.

Terá maior prioridade de ser utilizado o NAP que o índice calculado está mais distante do seu peso proporcional. Membros que estão com seu estado inativo ou com todos os canais ocupados, serão desconsiderados.

Em caso de "retry" dentro do grupo ou fallback, a proporcionalidade dos pesos pode ser ignorada, permitindo que chamadas sejam encaminhadas para membros que tem como índice resultante um valor maior que o peso proporcional, quando a opção "Forçar distribuição proporcional dos pesos" não está ativa.

Integrantes do grupo com peso de valor zero serão considerados somente na situação de "retry" dentro do grupo ou fallback, sendo que estes não são considerados na geração dos índices e nunca têm prioridade sobre os membros que têm pesos atribuídos.

ⓘ	**Nota**	Ao alterar e recarregar a configuração de um grupo, os contadores de encaminhamento de chamadas serão reiniciados.

Retry dentro do grupo e fallback

Caso uma chamada seja encaminhada para um membro do grupo e este membro não esteja em condições de completar a chamada, então é possível que ocorra um retry dentro do grupo, onde, nesta situação, o próximo membro será utilizado para realizar novo encaminhamento. Este novo encaminhamento é considerado para a utilização do algoritmo Chamadas encaminhadas. A ocorrência do retry dentro do grupo segue as mesmas regras de "retry" das rotas do sistema, logo, se a causa de desconexão não for satisfatória para "retry", este também não ocorrerá no grupo.

Caso uma chamada seja encaminhada para um membro do grupo que suporte fallback e este ocorra, então o mesmo membro do grupo será utilizado para encaminhar novamente a chamada em modo fallback. Este novo encaminhamento é considerado para a utilização do algoritmo Chamadas encaminhadas.

Em ambos os casos, se a opção Forçar distribuição proporcional dos pesos está habilitada, poderá ocorrer com que seja considerada a próxima rota do gateway no lugar de efetuar um retry dentro do grupo ou fallback.

7.5.1.7. Algoritmo de alocação de canais

Em cada NAP é possível definir as configurações de alocação de canais. São duas configurações, sendo a primeira o algoritmo a ser utilizado e a segunda a configuração do algoritmo, quando disponível.

São disponibilizados dois algoritmos de alocação: Primeiro Livre e Round-robin. Eles podem ser configurados para diferentes formas de alocação, conforme o tipo do NAP.

Também é disponibilizada a possibilidade de tornar a configuração de alocação automática, que é o valor padrão para todos os tipos de NAP.

7.5.1.7.1. Alocação de canais no modo automático

Permite que o KMG selecione automaticamente o algoritmo a ser utilizado. Ao aplicar esta configuração é possível que o comportamento varie entre versões.

Atualmente o comportamento automático utiliza o algoritmo "Primeiro Livre", configurado utilizando "Ordenação de Canais" em modo "Crescente'.

7.5.1.7.2. Alocação de canais por primeiro livre

Este algoritmo sempre irá testar os canais do primeiro disponível para ele até o último, em busca de um disponível. Entende-se por primeiro, o primeiro canal resultante da configuração de ordenação.

É possível ordenar os canais pelo seu índice, utilizando "Ordenação de Canais" ou, caso o NAP seja do tipo "Trunk", pode-se utilizar "Ordenação por Links", onde serão considerados o índice do canal e o Link a qual ele pertence.

Recomenda-se a utilização deste algoritmo sempre que a alocação de chamadas entrantes pela operadora segue algoritmo semelhante, com o objetivo de evitar concorrência na alocação dos canais entre o KMG e a operadora.

Exemplo: A operadora ou o PBX sempre aloca do menor para o maior canal disponível, assim, o KMG pode ser configurado para sempre alocar de maneira inversa, ou seja, do maior para o menor canal disponível.

7.5.1.7.3. Round-robin (alocação circular)

Este algoritmo sempre irá testar os canais a partir do próximo em relação ao último canal alocado, em busca de um disponível. Entende-se por próximo em relação ao último, o próximo canal resultante da configuração de ordenação.

É possível ordenar os canais pelo seu índice, utilizando ordenação de canais ou, caso o NAP seja do tipo Trunk (E1/T1), pode-se utilizar "Ordenação por Links", onde serão considerados o índice do canal e o link a qual ele pertence.

Recomenda-se a utilização deste algoritmo para NAP GSM e sempre que o maior fluxo de chamadas for sainte para NAP Trunk.

7.5.1.7.4. Opções de ordenação

A ordenação de canais irá ordenar os canais considerando seu índice e o módulo de telefonia. Serão ordenados segundo a opção selecionada que pode ser "Crescente" ou "Decrescente".

Para equipamentos com múltiplos módulos de telefonia, os canais de mesmo índice em módulos diferentes serão agrupados e ordenados utilizando o número de série do dispositivo como referência.

A ordenação por Links irá ordenar os canais considerando seu índice relativo ao link e o módulo de telefonia. Os canais serão ordenados segundo a opção selecionada que pode ser "Canais menores primeiro" ou "Canais maiores primeiro".

Exemplo: Para um NAP do tipo Trunk configurado com dois links de um mesmo módulo de telefonia, digamos o link 1 e o link 3, optando pelo algoritmo Round-robin e configuração de ordenação por Links, utilizando a opção "Canais menores primeiro", o comportamento para quatro chamadas saintes consecutivas será:

1. Chamada 1 irá utilizar o canal (timeslot) 0 do link 1.
2. Chamada 2 irá utilizar o canal 0 do link 3.
3. Chamada 3 irá utilizar o canal 1 do link 1.
4. Chamada 4 irá utilizar o canal 1 do link 3.

7.5.2. Rotas

"Configuração" → "Roteamento" → "Rotas"

Será exibido uma tabela com as rotas configuradas. Para criar uma nova rota, clique no botão "Nova Rota".

A coluna "Opções" exibe os ícones para:

- Editar configuração de rota → 
- Copiar rota → 
- Ativar rota → 
- Desativar rota → 
- Excluir rota → 

Uma rota pode ter três estados: Ativa, Inativa ou Desativada.

- **Ativa**: a rota possui status de ativa e nenhum de seus NAPs está desativado.
- **Inativa**: a rota possui status de ativa e ao menos um de seus NAPs está desativado, ou seja, a rota está inoperante.
- **Desativada**: a rota sofreu a ação de desativar por parte do usuário.

A tabela observada a seguir indica o significado da maioria os campos observados nesta interface.

Campo	Descrição
Nome	Nome para identificação da rota
Prioridade	Prioridade de verificação da rota sobre as demais, caso a rota seja semelhante a outra. Este valor varia entre 0 e 99, onde 0 indica rota com prioridade máxima e 99 prioridade mínima
NAP origem	Selecione o NAP de entrada da chamada
Número de B	Número de destino da ligação. Os dados da ligação devem corresponder ao deste campo para que esta regra seja aplicada. Aceita expressão regulares (POSIX.1-2001)
Número de A	Número de origem da ligação. Os dados da ligação devem corresponder ao deste campo para que esta regra seja aplicada. Aceita expressão regulares (POSIX.1-2001)
Verificar portabilidade	Esta opção é exibida somente se a portabilidade estiver habilitada. Veja a seção portabilidade neste manual para mais informações. Se habilitada, é verificado se o número a ser discado pertence às operadoras especificadas no campo "Provedores de serviço válidos"
Provedores de serviço válidos	Esta opção é exibida somente se o campo "Verificar portabilidade" estiver habilitada. Seleciona os provedores de serviço que são válidos para essa rota
Alterar número para consulta de portabilidade	É utilizado para formatar o número a ser consultado de acordo com o formato esperado pelo fornecedor do serviço de consulta. Aceita expressão regulares (POSIX.1-2001)
NAP destino	Selecione o NAP para onde deve ser encaminhada a ligação caso todas as regras sejam satisfeitas
Alterar número de B	Modifica o número de B (destino) na ligação sainte, utilizando expressões regulares (POSIX.1-2001)
Alterar número de A	Modifica o número de A (origem) na ligação sainte, utilizando expressões regulares (POSIX.1-2001)
Perfil para o Destino	Seleciona o Perfil a ser utilizado pelo destino. Os perfis são definido no menu Perfis
Restrição de Tempo	Selecione a restrição pré-definida em "Restrição de tempo". Esta regra somente será aplicada nas datas e horários especificados na restrição
Filtro de chamada a cobrar	Esta opção é exibida somente se o NAP de origem for SIP ou E1, com sinalização R2 ou ISDN. Realiza o filtro no canal de origem conforme a opção selecionada. Para NAPs SIP é necessário indicar o cabeçalho de chamada a cobrar no seu Perfil. • Aceitar todas as chamadas: Todas as chamadas serão aceitas. • Aceitar apenas chamadas a cobrar: Apenas chamadas sinalizadas como a cobrar serão aceitas. • Rejeitar chamadas a cobrar: Chamadas sinalizadas como a cobrar não serão aceitas
Indicação de chamada a cobrar	Esta opção é exibida somente se o NAP de destino for VoIP ou E1, com sinalização R2 ou ISDN. Sinaliza a chamada sainte conforme a opção selecionada. Para NAPs SIP é necessário indicar o cabeçalho de chamada a cobrar no seu Perfil. • Chamadas pagas: Chamadas serão sinalizadas como pagas. • Chamadas a cobrar: Chamadas serão sinalizadas como a cobrar. • Encaminhar sinalização: Chamadas serão sinalizadas conforme a chamada entrante

7.5.2.1. Expressões regulares

As expressões regulares seguem o padrão POSIX estendido. Sua definição oficial está disponível no capítulo 9, na seção 4 da especificação POSIX. Para maiores informações, utilize a referência completa, (em inglês).

Exemplos de expressões regulares

```
^[0-9]{10}$                  → Filtro, aceita exatamente 10 dígitos quaisquer.
^10385555[0-9]{8}$           → Filtro, aceita o prefixo 10385555 + 8 dígitos quaisquer
/(.{10})/021$1/              → Substituição, encaminha 021 + 10 primeiros dígitos
/^10385555([0-9]{8})$/$1/ → Substituição, envia apenas os últimos 8 dígitos (remove o prefixo)
```

Exemplo de rota configurada

Nome	NUMERO_LOCAL	
PRIORIDADE	1	
NAP ORIGEM	DISCADOR_SIP	
NÚMERO DE B	^48[0-9]{8}$	Aceita apenas números com prefixo 48 + 8 dígitos
NÚMERO DE A		Em Branco (não faz distinção pelo número de A)
NAP DESTINO	OPERADORA_01	
ALTERAR NÚMERO DE B	/^48([0-9]{8})$/$1/	Remove o prefixo para discar apenas os últimos 8 dígitos
ALTERAR NÚMERO DE A		Em Branco (não altera o número de A)

7.5.2.2. Retry

Por padrão, quando a rota definida para o encaminhamento da chamada define como NAP de Destino um NAP que não esteja disponível (falha física ou lógica), a rota será ignorada e será utilizada a próxima rota válida.

Se após o encaminhamento da chamada houver falha na ligação, rede congestionada por exemplo, a ligação poderá ser encaminhada utilizando a próxima rota válida, desde que no perfil de configuração da ligação de origem, a causa da falha esteja marcada para Retry.

Como rota válida, considera-se as rotas cujos filtros aceitem a ligação de origem. Caso não haja uma nova rota válida, a ligação será rejeitada.

Nota	Recarregar a configuração do gateway invalidará a funcionalidade de retry para todas as chamadas em curso.

7.5.3. Configurar perfil de chamadas

"Configuração" → "Roteamento" → "Perfis" → "Geral"

Os perfis definem padrões de comportamentos para os canais durante as chamadas. Durante uma chamada sempre são utilizados dois perfis, um para o canal associado como origem e outro para o canal associado como destino, sendo que estes podem ser diferentes. Algumas propriedades do perfil são válidas para ambas associações, outras tem validade somente para origem e outras somente para destino. Como exemplo, uma configuração de geração de cadência, tem validade somente quando o canal está associado a uma chamada como origem.

Nesta opção são exibidas os perfis cadastrados no KMG para utilização nos NAPs e rotas. Na coluna opção, é exibido um botão para tornar o perfil como o padrão do sistema, representado por uma estrela. É possível também copiar um perfil existe ao clicar no botão representado por uma folha dupla.

Para adicionar um novo perfil, clique no botão "Adicionar".

Campo	Descrição	NAP disponível para associação	Versão incluído
Nome	Nome a ser atribuído a este perfil	–	–

Áudio

Campo	Descrição	NAP disponível para associação	Versão incluído
Cancelador de eco	Habilita ou desabilita o cancelamento de eco	Qualquer	–
Supressão de DTMF	Habilita ou desabilita a supressão de DTMF		
Controle de volume	Desabilita, altera com ganho fixo ou habilita controle automático de volume. Ao definir o controle manual, a faixa de ajuste é entre -10 e 10, no qual cada unidade representa 3d		2.1.0

Fax

Campo	Descrição	NAP disponível para associação	Versão incluído
Suporte a Fax	Define qual comportamento deve ser adotado quando é detectado um sinal de FAX. O comportamento adotado difere por sinalização	Qualquer	–

Geral

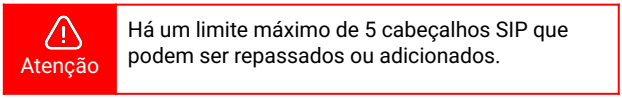
Campo	Descrição	NAP disponível para associação	Versão incluído
Suportar "retry"	Habilita a opção de retry e possibilita configurar o tempo máximo de espera para alocação do canal sainte bem como o conjunto de causas que será utilizado nos registros das chamadas	Qualquer	–
Tempo máximo de espera pela alocação do canal sainte para realizar "retry"	Tempo máximo esperado pelo KMG antes de utilizar outra rota válida		
Causa de desconexão preferencial para mapeamento	Seleciona qual causa de desconexão preferência será usada para mapear a causa de desconexão para o outro canal participante da chamada em caso do sistema ter mais de uma causa de desconexão disponível para mapear e a chamada não tenha sido completada. Exemplo: Caso o gateway tenha realizado mais de um "retry" e não tenha sido possível completar a chamada, é possível utilizar a causa de que não há rota disponível, ou seja, causa do gateway. Utilizar a causa reportada pelo Primeiro canal desconectado, a que originou o primeiro "retry", ou a causa do Último canal desconectado, o que foi tentado pela última vez completar a ligação		
Repassar Display Name	Habilita ou desabilita o encaminhamento do nome de exibição em chamadas de destino VoIP ou ISDN. Para ISDN o valor é limitado em 80 caracteres ASCII	Destino	4.0.0
Cadências	Permite habilitar cadências personalizadas e configurá-las	Qualquer	–

R2

Campo	Descrição	NAP disponível para associação	Versão incluído
Tempo de espera para reconexão	Tempo máximo de espera para a reconexão durante um duplo atendimento	Destino	-
Tempo para esperar condição do lado chamando	Tempo máximo de espera para aguardar o recebimento da causa do lado chamando, antes de enviar a condição padrão		
Condição padrão do lado chamado	Condição padrão a ser enviada caso o tempo para esperar a condição do lado chamando seja atingido		
Desconexão forçada	Habilita o envio da desconexão forçada no R2		

SIP

Campo	Descrição	NAP disponível para associação	Versão incluído
Tipo de envio de DTMF	Opção onde é possível configurar o tipo de padrão de DTMF que pode ser utilizado para envio. As opções disponíveis são In Band, Out Band RTP (RFC 2833) e três tipos de Out Band Sip Info	Qualquer	4.0.0
Enviar cabeçalho personalizado	Opção onde é possível habilitar o uso de um cabeçalho SIP personalizado	Qualquer	2.1.0
Cabeçalho de identificação de chamada a cobrar na origem	Opção onde é possível configurar o cabeçalho de identificação chamada a cobrar na origem e valor que será utilizado para enviar ou receber chamadas a cobrar no SIP	Origem	4.1.43.0
Cabeçalho de identificação de chamada a cobrar no destino	Opção onde é possível configurar o cabeçalho de identificação chamada a cobrar no destino e valor que será utilizado para enviar ou receber chamadas a cobrar no SIP	Origem	4.1.43.0
Repassar os cabeçalhos de extensão (X-Headers)	Habilita ou desabilita o encaminhamento de cabeçalhos de extensão, para chamadas VoIP-VoIP	Qualquer	-
Repassar User-to_User information	O gateway deve repassar o cabeçalho ou elemento de informação User-to-User information da ligação entrante para a ligação sainte	Qualquer	-
Ativar comportamento early media	Habilita ou desabilita a abertura imediata de áudio. Caso habilitado, será possível gerar a cadência "Conectando" em canais de origem SIP. Caso desabilitado, a abertura de áudio se dará quando houver a confirmação de alocação do canal de destino será gerada a cadência "Chamando" ou será comuta o áudio do canal de destino, se houver	Origem	3.3.0
SIP: Ativar envio do cabeçalho Contact no 180 Ringing	Habilita o envio do cabeçalho Contact na mensagem SIP 180 Ringing. Caso esta opção esteja desativada, o cabeçalho será adicionado quando a opção Modo de travessia NAT do NAP estiver configurado	Origem	4.0.0
Utilizar o campo reason do cabeçalho como causa de desconexão	A configuração para que a causa SIP (status-code) seja desconsiderada sempre que o campo Reason estiver disponível para o mapeamento de causa	Origem	4.0.0
Ativar detecção de tons	Habilita a detecção de tons de FAX e DTMF nos canais VoIP. Ao ativar esta opção haverá um maior consumo de processamento do equipamento e a quantidade máxima de chamadas simultâneas será afetada	Origem	4.1.42.0



CODEC

A configuração dos codecs que podem ser utilizados são disponibilizadas no perfil de chamadas. Selecione os codecs que serão usados. Você pode arrastá-los para definir a prioridade, caso houver mais de um codec selecionado.

Mapa de causas

Define as traduções de causa de desconexão entre diferentes sinalizações. Quando uma desconexão é recebida por uma das pernas da chamada, o mapa de causas da outra perna é utilizada para traduzir esta causa para a sua sinalização. Quando a desconexão está partindo de um canal associado como destino, então, o mapa de causas também servirá para determinar se deve ocorrer um retry devido a esta desconexão, logo, a configuração retry é válida somente para a origem.

Exemplo: Para um chamada entre uma origem E1 e um destino SIP, havendo uma desconexão partindo do destino (SIP) (digamos uma rejeição de um INVITE), a causa fornecida pela sinalização SIP será utilizada para determinar se a origem (E1) deve fazer um retry e, caso não deva, qual a causa de desconexão a ser enviada para desconectar a origem (E1).

Campo	Descrição	NAP disponível para associação	Versão incluído
Causa de desconexão	Número e nome da causa de desconexão. Todas as causas têm índices únicos	Qualquer	–
ISDN	Define o valor a ser utilizado para desconectar um canal de sinalização ISDN		
R2	Define o valor a ser utilizado para desconectar um canal de sinalização R2		
SIP	Define o valor a ser utilizado para desconectar um canal de sinalização SIP		
Retry	Habilita ou desabilita o retry, quando esta causa é reportada pelo canal associado como destino	Origem	2.1.0

7.5.4. Configurar período de funcionamento para o roteamento

"Configuração" → "Perfis" → "Período de Funcionamento"

Exibe as restrições de tempo que podem ser aplicadas às rotas. Este recurso permite definir que uma determinada rota opere somente em horário comercial, por exemplo. Ou ainda que uma rota opere somente aos finais de semana. Desta forma é possível configurar o transbordo à outra rota válida, caso a rota principal esteja fora do horário definido.

O KMG já possui algumas restrições padrão, que podem ser removidas ou editadas, clicando nos botões de ação na coluna "Opções".

Para criar uma nova restrição, clique no botão "Nova Restrição de Tempo". É possível definir uma restrição por hora, dia da semana, dia do mês, meses, ou ainda por um conjunto destas restrições. É possível, por exemplo, criar uma restrição no qual uma rota irá operar às segundas e quarta-feira das 08:00 às 18:00. Por fim, clique no botão "Salvar" e depois em "Aplicar" para que as alterações entrem em vigor.

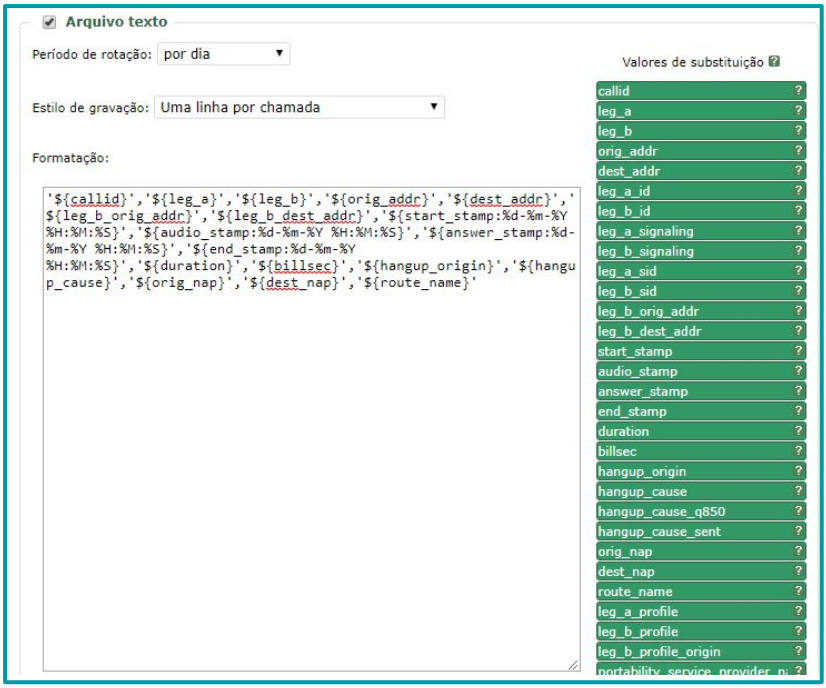
Atenção

Para que a restrição de tempo funcione corretamente, é necessário que o KMG esteja com a data e hora ajustada corretamente.

7.5.5. CDR → Call Detail Record

O CDR é o registro que contém os detalhes das chamadas trafegadas pelo KMG. A lista a seguir contém alguns exemplos de informações que o CDR fornece:

- O número de telefone do assinante que origina a chamada (chamando partido, A-party).
- O número de telefone que recebe a chamada (chamada partido, B-party).
- Dígitos adicionais sobre o número chamado.
- A hora de início da chamada (data e hora).
- O período de duração da chamada.
- A identificação do dispositivo KMG.
- Os resultados da chamada, indicando, por exemplo, se houve ou não conexão da chamada.
- O tipo de tecnologia utilizada na chamada (VoIP, SMS, etc.).
- Alguma condição de falha na chamada.



Os registros podem ser visualizados na Interface Web do KMG, através do menu "Diagnóstico" → "CDR", enviados para um servidor RADIUS, ou para um servidor FTP.

7.5.5.1. Personalizar e ativar CDR

1. Acesse o menu "Configuração" → "CDR" → "Arquivo texto"'.
2. Habilite a opção "Arquivo texto".
3. No campo 'Período de rotação', selecione uma das seguintes opções:

- Por minuto: Será gerado um arquivo por minuto com todas as ligações finalizadas até o final deste minuto.
- Por hora: Será gerado um arquivo por hora com todas as ligações finalizadas até o final desta hora.
- Por dia: Será gerado um arquivo por dia com todas as ligações finalizadas até o final deste dia.

A gravação do registro da chamada é realizada somente no término da ligação. Desta forma os dados completo da chamada sempre ficarão em um único arquivo. Se foi definido a geração de arquivo CDR por minuto, por exemplo, e uma ligação está em curso ao final do minuto da geração do arquivo CDR, o registro desta chamada ficará no próximo arquivo a ser gerado, caso ela seja finalizado no minuto seguinte.

4. No campo 'Estilo de gravação', selecione o estilo que o arquivo CDR será gravado no servidor:

- Uma linha por tentativa de roteamento: Será gerada uma linha de gravação no arquivo a cada tentativa de roteamento realizada, incluíndo "retry".
- Uma linha por chamada: Será gerada uma linha de gravação no arquivo arquivo a cada chamada que for realizada.

5. Na área de texto 'Formatação', personalize o registro CDR. Você pode inserir qualquer texto desejado, todos os campos especiais (${nome_do_campo}) serão substituídos pelos dados da ligação registrada. Os campos disponíveis estão listados à direita da caixa de texto e podem ser adicionados arrastando-o para a caixa de texto ou com um duplo clique sobre o campo desejado. Antes de arrastar o campo para a área de texto, é necessário posicionar o cursor do mouse no local onde é desejado inserir o campo.

6. É recomendável utilizar algum operador entre os campos para facilitar a leitura do arquivo, tal como vírgula (','), ponto e vírgula (';'), ou o que for de melhor visualização. Note que os campos de data e hora possuem várias opções de formatação. Há alguns exemplos disponíveis na ajuda da interface, localizado no canto inferior esquerdo.
Os campos disponíveis possuem um botão de ajudar representado por uma "?" que contém sua descrição. Para visualizar, posicione o cursor do mouse sobre o ícone de ajuda.

7. Clique no botão "Salvar". Se nenhuma outra configuração for realizada, clique no botão "Aplicar" para que as alterações entrem em operação.

7.5.5.2. Enviar CDR para servidor RADIUS

"Configuração" → "Sistema" → "CDR" → "RADIUS"

Servidores RADIUS podem ser configurados para coletar as informações das chamadas do gateway para registro e análise de bilhetagem. Esta Interface Web de configuração permite enviar dados de CDR do KMG para até 3 servidores RADIUS.

Para ativar este recurso, habilite a opção RADIUS e cadastre um servidor. É possível cadastrar até 3 servidores RADIUS.

A descrição de cada campo é verificada a seguir.

Lista de Servidores

Campo	Descrição
Endereço	São aceitos IPv4 como endereços válidos
Porta	Porta do servidor RADIUS. Para definir a porta padrão (1813), utilize o valor 0
Segredo compartilhado	Valor que deve ser compartilhado entre o servidor e cliente (veja mais detalhes na RFC 2865)

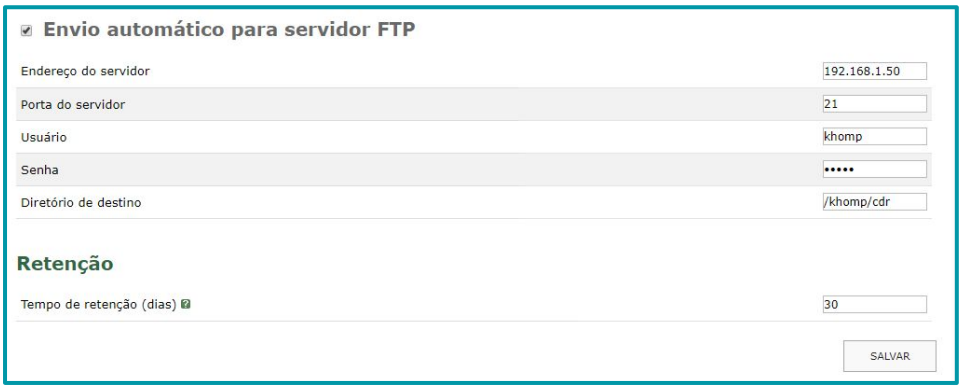
Opções avançadas

Campo	Descrição
Tempo máximo de espera da requisição	Tempo máximo que o KMG deve aguardar por uma resposta válida do servidor RADIUS. Este parâmetro funciona em conjunto com a "Quantidade máxima de retransmissões"
Quantidade máxima de retransmissões	Quantidade máxima de vezes que o KMG deve retransmitir uma pacote para o servidor RADIUS. Este parâmetro funciona em conjunto com o "Tempo máximo de espera da requisição". Caso não haja resposta do servidor após o tempo máximo de espera da última retransmissão, então o próximo servidor deverá ser utilizado ou o pacote será descartado, caso não tenha mais servidores configurados ou todos já estejam inativos, o servidor poderá ser marcado como inativo, caso o tempo de desativação esteja configurado
Tempo de desativação de servidor por falha	Define por quanto tempo um servidor deverá ficar marcado como desativado devido às falhas de transmissão. Durante este período, não serão realizadas novas tentativas. Caso todos os servidores sejam desativados, os pacotes serão descartados. Utilize o valor 0 (zero) para nunca desativar os servidores
Formatação de datas	Formato de data e hora esperado pelo servidor RADIUS
Requisições paralelas	Número de requisições paralelas que devem ser feitas para o servidor RADIUS
Tamanho da fila de envio para descarte de pacotes Acct-Status-Type: Start (1)	Quando a fila de envio for maior que o valor especificado neste campo, novos pacotes do tipo Acct-Status-Type com valor Start (1) serão descartados, permitindo que ainda seja possível enfileirar pacotes Acct-Status-Type com valor Stop (2) até que a fila de envio chegue no valor de "Tamanho máximo da fila". A configuração "Tamanho máximo da fila" tem precedência sobre esta configuração, logo, configure os dois com o mesmo valor ou um valor menor neste campo, caso deseje que a fila tenha apenas o limite máximo
Tamanho máximo da fila	Quando a fila de envio for maior que o valor especificado neste campo, novos pacotes serão descartados

7.5.5.3. Enviar CDR para servidor FTP

"Configuração" → "Sistema" → "CDR" → "Manutenção"

Esta Interface Web contém as opções para que você possa enviar os registros CDR para um servidor FTP a sua escolha.



1. Habilite a opção "Envio automático para servidor FTP".
2. Cadastre as informações do seu servidor FTP nos campos *"Endereço do servidor"*, *"Porta do servidor"*, *"Usuário"*, *"Senha"*, *"Diretório de destino"*.
3. Clique no botão Salvar. O KMG irá testar a conexão com o servidor FTP. Esta operação poderá levar alguns segundos.
4. Por fim, clique no botão Aplicar para que as alterações entrem em operação.

ⓘ	**Nota**	Após clicar no botão "Salvar", o KMG realiza um teste de conexão com o servidor FTP. Durante o teste, não é exibida nenhuma resposta na Interface. Após a conclusão do teste, será exibido o resultado do teste.

7.5.5.4. Configurar tempo de retenção do CDR no KMG

"Configuração" → "Sistema" → "CDR" → "Manutenção"

Os registros CDR ficam armazenados no KMG por um período de 30 dias por padrão. Depois deste período, os registros mais antigos serão removidos. Esta configuração não tem relação com o

Nesta Interface Web você pode alterar o período de retenção. O armazenamento do CDR também é limitado pela capacidade do disco no KMG. No KMG 200, KMG 400 e KMG 1600 é disponibilizado 2,5 GB. No KMG 3200 é disponibilizado 8 GB.

7.5.6. Configurar portabilidade

"Configuração" → "Telefonia" → "Portabilidade"

O recurso de portabilidade, quando ativo, é utilizado no roteamento das chamadas para identificar a operadora do número destino e, com isso, usar a rota de menor custo.

Ao ativar essa opção no sistema, a opção *"Verificar portabilidade"* ficará disponível na configuração de rotas (***"Configuração"*** → ***"Roteamento"*** → ***"Rotas"***). Ao selecioná-la mais duas opções serão disponibilizadas: *"Provedores de serviço válidos"* e *"Alterar número para consulta de portabilidade"*.

Com a consulta à portabilidade ativada, para cada ligação, será consultado à qual operadora o número de destino pertence, e o resultado será armazenado. Caso a operadora do número destino esteja listada no campo *"Provedores de serviço válidos"*, esta rota será utilizada, caso contrário, o roteamento irá testar as próximas rotas.

No campo *"Provedores de serviço válidos"* deve-se selecionar quais operadoras podem ser utilizadas com esta rota.

O campo *"Alterar número para consulta de portabilidade"* é utilizado para formatar o número a ser consultado de acordo com o formato esperado pelo fornecedor do serviço de consulta. Por exemplo, caso o número discado seja 0994899998888 e o fornecedor espere o formato DDD + número, será necessário utilizar uma expressão regular de substituição como esta: /0..([0-9]*)$/$1/, desta forma os 3 primeiros dígitos serão removidos e a consulta será feita utilizando 4899998888.

7.5.6.1. Portabilidade via Webservice

Para habilitar a verificação de portabilidade via Webservice, deve-se entrar com os dados da prestadora de serviço de consulta à portabilidade e importar o conjunto de operadoras que podem ser retornadas pelo serviço de portabilidade (RN1). Este conjunto deve ser fornecido pela prestadora do serviço.

Veja o tópico "Importar dados" para detalhes de como realizar a importação dos códigos RN1.

Campo	Descrição
URL	URL do serviço de portabilidade. Utilize o valor coringa ${number} para indicar onde o número a ser verificado deve ser inserido
Método	Configura o método HTTP a ser utilizado para a requisição
Padrão da resposta	Deve-se configurar uma expressão regular do tipo POSIX, a qual será utilizada para extrair o código da operadora da resposta fornecida pela prestadora do serviço. Manter este campo em branco, significa que a resposta fornecida é composta somente pelo código da operadora
Timeout	Configura o tempo máximo de espera pela resposta
Parâmetros adicionais	Parâmetros a serem submetidos utilizando o método POST. Utilize o valor coring ${number} para indicar a chave que deve conter o número a ser verificado
Usuário	Caso configurado, deve conter o usuário de autenticação do tipo HTTP-BASIC. Também depende do campo Senha estar configurado
Senha	Caso configurado, deve conter a senha de autenticação do tipo HTTP-BASIC. Também depende do campo Usuário estar configurado
Tratamento de erros	Habilita ou desabilita tratamento especial de erros
Quantidade aceitável de erros	Configura a quantidade de erros que o sistema de portabilidade deve aceitar sem tomar ação, ao atingir a quantidade definida, o sistema de portabilidade deve ser desabilitado pelo Tempo de espera em caso de erros definido
Tempo de espera em caso de erros	Define o tempo (em segundos) que o sistema de portabilidade deve ser temporariamente desabilitado, caso a Quantidade aceitável de erros seja atingida. Após este tempo, o serviço é habilitado novament

7.5.6.2. Portabilidade via base de dados local

Habilita a consulta utilizando uma base de dados interna do KMG. Para que este serviço funcione adequadamente, deve-se importar o conjunto de operadoras válidas, o conjunto de números e/ou o conjunto de prefixos.

Quando este serviço está habilitado, a consulta será realizada na seguinte ordem:

1. Verifica-se se o número está definido no conjunto de Números portados.
2. Verifica-se se os n primeiros dígitos do número está definido no conjunto de Prefixos, onde n é o tamanho do prefixo.

7.5.6.3. Importar dados

Para importar os dados, deve-se abrir o assistente de importação pelo botão "Importar dados" e em seguida preencher o formulário. O formulário de importação se aplica tanto para utilização da portabilidade com Webservice quanto para banco de dados local.

O arquivo submetido deve ser um arquivo texto ou texto comprimido em formato "gzip". Caso o arquivo tenha caracteres especiais (acentos, por exemplo), deve-se utilizar codificação UTF-8. O arquivo deve estar em formato de campos separados por caractere bem definido, sendo obrigatório um registro por linha. É recomendado o formato CSV como arquivo texto a ser fornecido. Linhas vazias serão ignoradas.

	Nota	Durante a importação, o serviço de portabilidade ficará indisponível.

O formulário de importação apresenta os seguintes campos:

Campo	Descrição
Arquivo	Arquivo a ser importado
Tipo de dados do arquivo	Selecione o tipo de dados que contém o arquivo. Para portabilidade via Webservice, apenas o tipo de dados Operadoras está disponível
Formato dos campos do arquivo	Selecione o tipo de dado em cada campo de acordo com a ordem com que são apresentados no arquivo sendo importado
Caractere delimitador de campo	Caractere que deve ser reconhecido separador de campo
Caractere de encapsulamento de campo	Caractere que deve ser reconhecido como encapsulador de campo. Quando este caractere é encontrado, é obrigatória a existência de outro caractere igual para o reconhecimento do valor
Remover todo os registros antes de importar	Caso habilitado, apaga todos os registros do "Tipo de dados do arquivo" selecionado antes de iniciar a importação. "Cuidado", pois registros dependentes deste também serão apagados (Números e Prefixos dependem de Operadoras)
Ignorar primeira linha	Caso habilitado, ignora a primeira linha do arquivo. Esta opção existe para compatibilidade com a indicação do nome das colunas na primeira linha
Importação incremental	Caso habilitado, o campo "Operação", preenchido em "Formato dos campos do arquivo" será utilizado como referência de o que fazer com o registro
Ignorar linhas inválidas	Caso habilitado, linhas inválidas (que não foram possíveis de ser importadas) serão descartadas e logadas. Caso desabilitado, a importação finalizará com um erro na primeira linha inválida encontrada

Recomenda-se realizar a primeira importação da base de portabilidade utilizando a seguinte ordem:

1. Operadoras.
2. Números portados (apenas Base de dados local).
3. Prefixos (apenas Base de dados local).

7.5.7. Scripts

"Configuração" → "Roteamento" → "Scripts"

Os produtos da linha KMG possuem suporte para Scripts no formato LUA. Lua é uma linguagem de programação projetada para estender aplicações. Ela permite programação procedural, programação orientada a objetos, programação funcional, programação orientada a dados e descrição de dados. Mais informações sobre LUA podem ser encontradas no site www.lua.org.

A utilização de um script basicamente possibilita realizar alterações no cabeçalho SIP, alterar número de origem e número de destino. É possível manipular as mesmas informações que são registradas no arquivo CDR.

O script é associado à um NAP. Quando a rota possui um NAP com script, então é executado suas instruções. O script pode ser executado tanto em um NAP de origem quanto NAP destino.

7.5.7.1. Adicionar script

1. Clique no botão "Novo Script".
2. Insira o nome do script.
3. Escreva o script na área de texto exibida.
4. Clique no botão "Salvar" e depois em "Aplicar".

A área de texto possui as instruções para manipular os dados das chamadas no KMG. O script obrigatoriamente deve conter as funções observadas a seguir para que seja executado corretamente.

```
function prerouting()
   return true
end

function postrouting()
   return true
end
```

Aplicando script no NAP

Para associar um script em um NAP:

1. Acesse o menu "Configuração" → "Roteamento" → "NAPs".
2. Crie ou edite um NAP.
3. No campo 'Script para o roteamento', selecione o script desejado, que foi adicionado previamente.
4. Clique no botão "Salvar" e depois em "Aplicar".

7.5.8. Gerenciamento dos SIM cards

"Configuração" → "Roteamento" → "Cartões SIM"

	Nota	Esta opção é exibida somente se o KMG possuir interface GSM.

Esta Interface Web exibe os SIM cards, e suas propriedades, inseridos nas interfaces GSM, seja através de módulos internos (KMG 400), ou através dos módulos externos de telefonia → Módulo KMG. Ao inserir um novo SIM card que for devidamente registrado, este será exibido nesta Interface para que seja associado a uma NAP GSM existente.

O ícone "estrela" indica que um novo SIM card foi descoberto.

Ao clicar no ícone "lápis", você pode associar o novo SIM card a um grupo de canais GSM previamente cadastrado e também incluir ou editar o número do SIM card. Este número será usado como número de destino no roteamento.

7.5.8.1. Associar um novo SIM card a um grupo de canais GSM existente → NAP GSM

Ao inserir um novo SIM card, você pode associá-lo a um grupo de canais GSM previamente criado. Veja a seção Configurar canais GSM para mais informações sobre criação de grupo de canais GSM.

Para associar um novo SIM card à uma NAP GSM:

1. Clique no ícone "lápis" do SIM card que será associado a um grupo GSM. 
2. Na coluna 'NAP', selecione o grupo de canais GSM criado (NAP GSM). Repita esta ação se houver mais SIM cards que irão ser associados a uma NAP GSM.
3. Clique no botão "Salvar". Se nenhuma outra configuração for realizada, clique no botão "Aplicar" para que as alterações entrem em operação.

7.5.8.2. Adicionar um SIM card manualmente

Você pode adicionar os SIM cards antes de instalar os SIM cards nas interfaces GSM conectadas ao KMG. Desta forma, quando o SIM card for inserido, ele poderá ser associado a NAP GSM definido automaticamente.

Para adicionar SIM card manualmente:

1. Clique no botão "Adicionar manualmente".
2. Cadastre o ICCID do SIM card. Esta informação deverá ser disponibilizada pela sua operadora de telefonia GSM.
3. Cadastre o número do SIM card. Esta ação é opcional.
4. Na coluna 'NAP', selecione a "NAP GSM" cadastrada previamente.
5. Clique no botão "Salvar". Se nenhuma outra configuração for realizada, clique no botão "Aplicar" para que as alterações entrem em operação.

7.5.9. Criar rotas SMS

As rotas SMS são as associações entre o KMG e um NAP GSM como destino, que será utilizado para alocar o canal GSM para o envio. Também é possível definir filtros para sua utilização, como número de destino e consulta a portabilidade.

Para cada envio de SMS, as rotas serão avaliadas na ordem de prioridade definida na configuração. A primeira rota que satisfazer a todos os filtros será utilizada.

Para enviar e receber SMS utilizando o KMG, está disponível uma API SMS.

Campo	Descrição
Nome	Nome da rota SMS. O nome de ser único entre todas as rotas
Prioridade	A prioridade com qual esta rota será avaliada. Rotas com prioridade menor serão avaliadas antes de rotas com prioridade maior. Não há ordem definida para rotas com a mesma prioridade
Número Destino	Filtro por expressão regular POSIX.1-2001 para o número de destino do SMS
Verificar Portabilidade	Caso habilitado, indicará a utilização da verificação de portabilidade para esta rota
Provedores de serviço válidos	Quando ativado a opção Verificar Portabilidade, seleciona os provedores de serviço que são válidos para essa rota
Alterar número para consulta de portabilidade	Número a ser utilizado para a verificação de portabilidade. Aceita expressão regulares (POSIX.1-2001)
NAP Destino	O NAP que deve ser utilizado para a alocação do canal de sainte SMS, apenas NAPs GSM são apresentadas

7.5.9.1. Teste de envio de SMS

Através do KMG é possível efetuar testes de envio de SMS para garantir que o roteamento SMS configurado está funcionando adequadamente. Para isto deve-se utilizar o formulário de envio informando os campos obrigatórios "Número de Destino" e "Texto da mensagem". É possível ainda solicitar a confirmação de envio.

Ao realizar o envio, os valores do código sms_reference gerado, o ICCID do Sim Card que foi utilizado para enviar o SMS, a rota utilizada e a operadora resultante da consulta a portabilidade, caso alguma das rotas avaliadas utilizem consulta a portabilidade, são apresentados. A confirmação de sucesso do envio (pela operadora) e do recebimento, caso seja solicitado, somente poderá ser efetuada através dos Logs ou do sistema de notificação.

7.5.10. Configurar recebimento de notificações de SMS

"Configuração" → "Roteamento" → "Notificações"

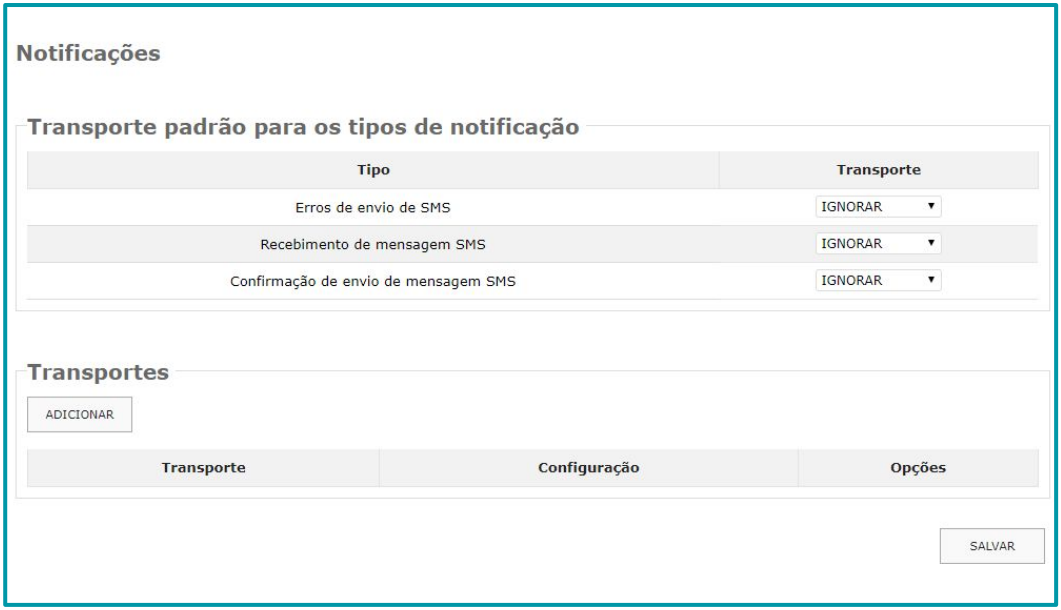
Nota	A opção 'Notificações' é exibida somente se o KMG possuir interface de telefonia GSM.

O KMG, com interface de telefonia GSM, pode enviar o conteúdo de mensagens SMS recebidas para servidores HTTP capazes de receber requisições do tipo GET e POST ou até mesmo API's REST.

Este recurso permite integrar o KMG com sistemas que tratam mensagens SMS recebidas, como um sistema que solicita a resposta de um cliente através de SMS, por exemplo.

São enviados os seguintes tipos de mensagens:

- **Erros de envio de SMS:** Erros emitidos pela operadora de telefonia quando uma mensagem não é entregue.
- **Recebimento de mensagem SMS:** Mensagens enviadas por uma pessoa, por exemplo.
- **Confirmação de envio de mensagem SMS:** Confirmação de entrega da mensagem. Esta opção deverá estar ativada no SIM card.



Para utilizar este recurso, primeiro é necessário cadastrar um servidor HTTP. É possível cadastrar mais de um servidor para receber um tipo de mensagem separadamente, ou enviar todos os tipos para o mesmo servidor.

1. No painel 'Transportes', clique no botão "Adicionar".

2. Será exibido um formulário para cadastrar o servidor que irá receber as mensagens. Segue a descrição dos campos:

Campo	Descrição
Nome	Usado para descrever o servidor. Será exibido para seleção no painel 'Transporte padrão para os tipos de notificação
Usuário para autenticação	Usuário de autenticação do serviço HTTP, ou API REST. Este campo não é obrigatório caso o servidor não exija autenticação
Senha para autenticação	Senha de autenticação do serviço HTTP, ou API REST. Este campo não é obrigatório caso o servidor não exija autenticação
Host ou IP remoto	Endereço do servidor HTTP
Porta remota	Porta do servidor HTTP habilitada para o recebimento deste protocolo
Caminho remoto	Diretório do servidor HTTP onde as mensagens serão armazenadas
Método	Método usado para o envio das mensagens: GET ou POST. Se o método escolhido for POST, serão exibidos as colunas 'Nome' e 'Valor' para cadastro destas informações

3. Clique no botão "OK".

4. Se for necessário cadastrar outro servidor, repita os passos anteriores.

5. Com um servidor cadastrado, você pode escolher qual servidor irá receber cada tipo de mensagem. No painel 'Transporte padrão para os tipos de notificação', selecione servidor cadastrado na coluna 'Transporte'.

6. Clique no botão "Salvar". Se nenhuma outra configuração for realizada, clique no botão "Aplicar" para que as alterações entrem em operação.

7.5.11. Alta Disponibilidade → HA

Nota	• O KMG 400 One não suporta a função HA. • O módulo EBS interno, se existir, não suporta a função HA.

Em caso de falha no hardware principal, um outro KMG do mesmo modelo, assume as funções do gateway preservando as configurações de rede, incluindo os endereços IP. A Alta Disponibilidade foi desenvolvida para operar com ou sem os módulos externos de telefonia.

Um KMG instalado com Alta Disponibilidade oferece "segurança ao sistema" e garante a "continuidade ininterrupta da operação".

Observação: *Para acessar esta imagem em sua melhor definição, acesso o link a seguir:* https://drive.google.com/file/d/1ydFDmaZdAQQ1Mco-tMli9UYEvu4WdSa_/view?usp=sharing

7.5.11.1. Conexão da rede para HA → Alta Disponibilidade

O KMG com HA pode utilizar qualquer porta de rede para este recurso, utilizada para conectar os dois equipamentos, desde que esteja configurada.

Configure um endereço IP para a interface de gerenciamento diferente do endereço IP do KMG para as demais interfaces. Este IP será utilizado para gerência e acesso individual ao equipamento, portanto devem ser distintos entre o Master e Spare. Os IPs das demais portas serão compartilhados entre os equipamentos, sendo que apenas o equipamento ativo responderá por eles.

Ao compartilhar o mesmo endereço IP, é possível conectar o KMG em uma estrutura de rede redundante, e assim garantir o seu funcionamento mesmo quando uma das estruturas de rede estiver inoperante.

7.5.11.2. Alta Disponibilidade com módulos externos de telefonia

Os módulos externos de telefonia da Khomp possuem duas interfaces de rede. Ao usar este módulo em um cenário com HA, tanto o KMG principal quanto o KMG redundante deverão estar conectados no mesmo módulo e na mesma interface de rede do gateway. Por exemplo: Se o KMG principal está conectado à um módulo de telefonia E1, através da interface P0, o KMG redundante também deve estar ligado à este mesmo módulo através da interface P0 também, como mostra a figura anterior. A mesma regra deve ser aplicada às demais interfaces de rede e módulos, se houver.

7.5.11.3. Configuração da Alta Disponibilidade

⚠ Atenção	A ativação/desativação do recurso Alta Disponibilidade é realizada exclusivamente pela equipe de suporte da Khomp.

"Configuração" → "Rede" → "Interfaces"

Com as licenças de alta disponibilidade carregadas no equipamento, as opções de configuração vão estar disponíveis. Inicialmente é necessário configurar o equipamento Master selecionando a interface de rede que será utilizada para gerência, bem como o seu IP e máscara de rede. O mesmo processo é repetido depois no equipamento Spare. A partir deste momento os dois equipamentos estão operando em alta disponibilidade.

Campo	Descrição
Interface de rede	Define a interface de rede para gerenciamento do gateway no qual será aplicada estas configurações
IP de gerenciamento	Endereço IP que será usado para acesso ao KMG. Após a ativação da Alta Disponibilidade, este será o endereço IP real do gateway
Máscara de subrede	Máscara de subrede que será usada para acesso ao KMG. Após a ativação da Alta Disponibilidade, esta será a máscara de subrede real do gateway

7.5.11.4. Funcionamento da Alta Disponibilidade

Quando este recurso está ativado, o endereço IP definido na opção de Alta Disponibilidade passa a ser o endereço IP real do KMG. O acesso à Interface Web será realizado através dele. Toda a configuração de rede aplicada no menu Rede do gateway passa a ser virtual e é replicada para o gateway redundante, assim como as demais configurações. Qualquer alteração nas configurações do KMG será replicado para o gateway redundante.

7.5.11.5. Verificação do gateway principal e reserva

O KMG spare não terá acesso aos menus de configuração, apenas a configuração estará visível, e somente as opções de alta disponibilidade poderão ser alteradas.

O menu **"Monitoração"** → **"Sistema"** também exibe o KMG que é master (principal) e spare (redundante) através do número de série de cada gateway. Além disso, informações sobre o heart-beat são exibidas.

7.6. Configuração básica do TLS

Este subtítulo apresenta os procedimentos para configurar o protocolo de segurança TLS no KMG One, remotamente (via SSH), através de um computador com sistema operacional Windows. Aplique as indicações observadas a seguir para configurar o TLS no sistema.

7.6.1. Configurar o TLS via Interface Web

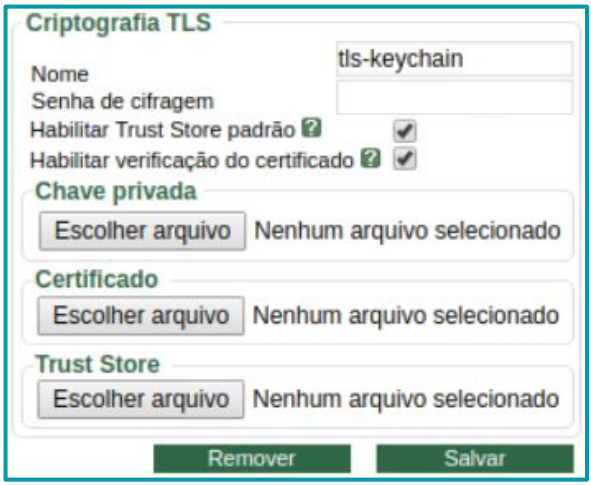
Acesso ao terminal remoto:

1. Acesse a Interface Web (Portal Web) do KMG One.

2. Acesse os menus "Configuração" → "Rede" → "Criptografia TLS".

3. Clique em "Adicionar Certificado Existente".

4. Altere o campo "Nome" para algo facilite na configuração. No exemplo, foi utilizado o nome "tls-keychain".

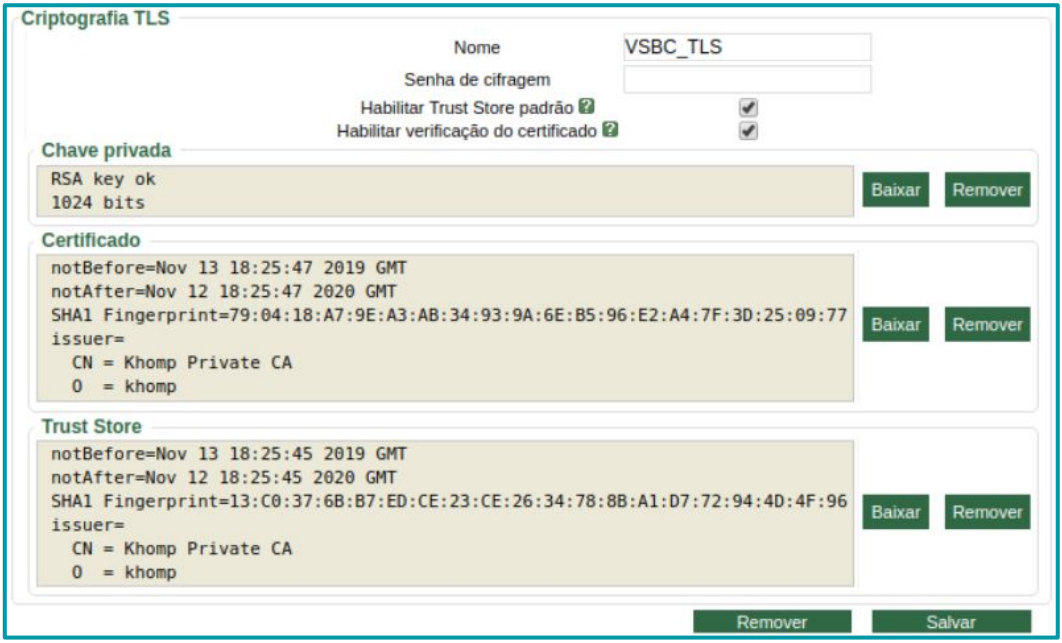


5. Adicione o arquivo da chave privada, geralmente em extensão "**.key**" (um arquivo único para o servidor e outro para o cliente):

6. Adicione o arquivo do certificado, geralmente com extensão .crt ou "**.pem**" (um arquivo único para o servidor e outro para o cliente):

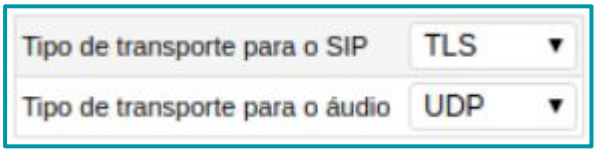
7. Adicione o arquivo da "Trust Store (CA)", geralmente com extensão "**.crt**" ou "**.pem**" que assina o certificado (o arquivo pode ser compartilhado entre o servidor e cliente, se tiver gerado ambos os certificados):

8. Após finalizar a configuração, clique em "Salvar".



9. Acesse os menus "Configuração" → "Sistema" → "VoIP" → "Criptografia TLS", selecione o certificado que deverá ser usado para fazer a criptografia das chamadas:

10. Edite a NAP e altere o tipo de transporte para o SIP (TLS) e/ou o tipo de transporte para o áudio (SRTP):



11. Altere a porta do NAP destino para a porta na qual estará ouvindo TLS no destino (5061 é a porta padrão mais utilizada para TLS):

12. Realize o reboot do equipamento para finalizar a configuração.

Nota	• Ao utilizar TLS, a porta de origem é sempre uma porta aleatória acima de 1024, conforme funcionamento do protocolo TCP. • Por este motivo, é necessário garantir a respectiva liberação de firewall no destino.

8. Monitoramento

"Monitoração"

A interface de Monitoração deve ser utilizada para acompanhar o funcionamento do KMG. Nesta seção é possível verificar as NAPs criadas e acompanhar o status, analisar os dispositivos e módulos de telefonia do KMG e seus respectivos canais.

No campo "Taxa de atualização" é possível definir um período para que a interface atualize as informações automaticamente, conforme o tempo definido. Ou atualizar de forma manual.

8.1. NAP

"Monitoração"→ "NAP"

Relação das informações para monitoração de um ou mais NAPs. As colunas oferecem os seguintes dados.

Campo	Descrição	
NAP	Informa o nome do NAP	–
Tipo	Apresenta o tipo da NAP, podendo esta ser SIP, Trunk ou GSM. Dependendo do modelo de KMG	–
Estado	Informa o estado da NAP para sua utilização	• Ativo • Inativo
Canais	Informa o estado dos canais associados a NAP	• Livre: O canal está livre para fazer ou receber chamadas • Falha: O canal está em falha, impedido de receber ou fazer chamadas • Ocupado: O canal está em uma chamada entrante ou sainte
Detalhes	Apresenta detalhes sobre o NAP. Para cada tipo de NAP, informações distintas podem ser apresentadas	• SIP: São apresentadas informações de registro e Keep Alive da conta SIP, caso configurados • Trunk: Nenhuma informação é apresentada • GSM: Apresentadas informações e permite edição do controle de consumo mensais de minutos e SMS, caso a NAP possua esta configuração habilitada na forma compartilhada

8.2. SIM cards

"Monitoração"→ "Cartões SIM"

Nota	Este recurso está disponível apenas nos equipamentos com interface GSM.

São exibidas as informações de estado dos SIM cards configurados no sistema. Também é possível alterar o controle de minutos e SMS dos SIM cards que possuem esta configuração habilitada.

As colunas oferecem as seguintes informações:

Campo	Descrição	
Cartão SIM	Apresenta as informações de ICCID do SIM card, além das informações de IMSI e operadora caso o mesmo esteja registrado	–
NAP	Informa a NAP em que o SIM card está associado	–
Estado	Informa o estado do SIM card para utilização	• Ativo: SIM card disponível para utilização • Inativo: Indisponível por falta de registro, configuração, controle de consumo ou outros fatores
Estado SMS	Informa o estado dos canais para SMS	• Livre: SIM card disponível para receber ou enviar SMS. • Enviando SMS: SIM card enviando SMS • Recebendo SMS: SIM card recebendo SMS • Limite Atingido: Limite de consumo de SMS foi atingido, neste estado o SIM card fica indisponível para enviar SMS, permitindo somente o recebimento de SMS
Minutos restantes	Apresenta os Minutos restantes para geração de chamada caso o controle de consumo esteja habilitado. É possível a edição deste valor caso o controle de consumo compartilhado não esteja habilitado	--
Minutos configurados	Informa os Minutos mensais configurados para este SIM card	--
SMSs restantes	Apresenta a quantidade de SMSs restantes para o envio de SMS caso o controle de consumo esteja habilitado. É possível a edição deste valor caso o controle de consumo compartilhado não esteja habilitado	--
SMSs configurados	Informa a quantidade de SMSs mensais configurados para este SIM card	--
Detalhes	Apresenta detalhes sobre o SIM card, informando o Dispositivo e o índice em que SIM card se encontra e a última atualização de status	--

8.3. Dispositivos

"Monitoração"→ "Dispositivos"

São exibidas as informações de monitoração dos dispositivos físicos, placas, módulos externos de telefonia (EBS) e dispositivos lógicos (VoIP). Para cada dispositivo são exibidos:

Campo	Descrição	Valores
ID	É a identificação do dispositivo dentro do sistema, sendo um número de 0 a (N) onde N é a quantidade de dispositivos configurados no sistema	–
Serial	Esta é outra forma de identificar um dispositivo, através do número de série o qual é atribuído a um único dispositivo. A Khomp não distribui dois dispositivos com o mesmo número de série	–
Modelo	É o nome do produto	–
Estado	Indica se um dispositivo está ativo ou inativo	• Up → Dispositivo conectado, configurado e funcional • Down → O dispositivo está configurado, porém não está conectado e portanto não está funcional • N/A → Informação não disponível. Esta situação ocorre quando não foi possível recuperar a informação, provavelmente por que um ou mais Serviços essenciais ao funcionamento do sistema não estão ativos
Canais	Panorama da atividade dos canais do dispositivo em um determinado momento. Inclui a quantidade de canais livre, em falha, ou em ligação no momento em que a tela foi atualizada	--
Links	Exibe o status dos dispositivos com link E1/T1. Demais interfaces de telefonia, não vão apresentar dados nesta coluna	--
Opções	Exibe um gráfico mostrando estatísticas das chamadas trafegadas no módulo de telefonia no momento. Estas informações são alteradas conforme a atualização da tela. Veja ao lado o significado das cores exibidas neste gráfico. É possível clicar sobre este gráfico para obter mais detalhes. Veja o item *"gráfico das chamadas"* para mais informações	• Azul → Chamadas completadas • Vermelho → Chamadas com falha • Laranja → Chamadas não atendidas • Cinza → Sem dados para exibir. Não houve tráfego de chamadas

8.3.1. Estado

Em uma situação de funcionamento normal, todos os dispositivos devem estar no estado "Up", assim como todos os links E1 dos mesmos.

Algumas possíveis causas para um dispositivo aparecer como "Down" ou "N/A" são:

- Não estar conectado a rede.
- Não estar alimentado corretamente.
- Estar com algum defeito.
- Não estar configurado corretamente.
- Estar configurado em outro servidor.

8.4. Links

"Monitoração" → "Links"

ⓘ	**Nota**	Este recurso está disponível apenas nos equipamentos com interface de telefonia E1.

Esta seção é específica para monitoração de links digitais. Todos os links configurados no sistema são listados, assim como informações sobre sua situação no momento. As seguintes informações são disponibilizadas:

- Link: Os links são identificados na coluna "Link" por um código formado pelo Número de série do dispositivo e o número do link no dispositivo, e ou nome atribuído (opcional), separados pelo caractere ".".
- Estado: Situação de funcionamento dos links. Indica se um link está ou não ativo de acordo com os seguintes valores:
  - Up → link alinhado, configurado e funcional.
  - Down → o link não está operacional. A coluna "Alarmes" têm informações a respeito da causa.
  - N/A → informação não disponível. Esta situação ocorre quando não foi possível recuperar a informação, provavelmente por que um ou mais Serviços essenciais ao funcionamento do sistema não estão ativos, ou por que o dispositivo do qual este link faz parte não está conectado.
- Alarmes: Informações sobre erros nos links. Quando o link está operacional (Estado="Up"), apenas o caractere "-" é exibido.

  Os possíveis alarmes são:

Alarme	Significado	Possíveis causas
Perda de Sinal	Circuito de Rx interrompido	Cabo desconectado
Alarme de Rede	Recepção de sinal com padrão tudo-1	Cabo conectado, equipamento remoto ligado e não-configurado
FrameSyncLost	Perda do alinhamento de quadro	Cabo conectado, mas equipamento remoto desligado
MultiframeSyncLost	Perda do alinhamento de multiquadro	Equipamento remoto configurado com tipo de sinalização incorreto
Alarme Remoto	Equipamento remoto com algum alarme	• Circuito Tx interrompido • CRC4 não configurado • Falha interna no equipamento remoto
HighErrorRate	Reservado	–
Alarme Desconhecido	Reservado	--
E1Error	Erro no controlador E1	Framer do link (componente de hardware) com problemas
NotInitialized	E1 não inicializado	Dispositivo não configurado
Device Unreacheable	Dispositivo em estado "Down"	Ver item: *"Estado"*

- Variações:Indica se há variações nos contadores de erros dos links. Por exemplo, se em um dado momento um cabo apresentar um mal contato e depois disso o erro desaparecer, os contadores vão indicar que houve algum problema.

Se não houver variações (todos os contadores estiverem zerados), clicando no link "Visualizar" mostrará a tabela de variações sem incrementos de erro. Caso contrário, havendo algum contador com valor maior que zero, o link aparecerá em negrito.

Além disso existe a opção de zerar os contadores, através do link "Limpar".

São monitorados os seguintes contadores:

Alarme	Significado	Possíveis causas
Bloqueado	Contagem de quedas no link	Presença de algum alarme crítico (SignalLost, NetworkAlarm, FrameSyncAlarm ou MultiframeSyncAlarm). Ver item Alarme.
Perda de sinal	Transições do alarme de perda de sinal	Ver Alarme SignalLost
Notificação de alarme	Transições do alarme de rede (tudo-1)	Ver Alarme NetworkAlarm
Alarme de quadro	Transições do alarme de quadro	Ver Alarme FrameSyncLost
Alarme de multiquadro	Transições do alarme de multiquadro	Ver Alarme MultiframeSyncLost
Alarme remoto	Transições do alarme remoto	Ver Alarme RemoteAlarm
Alarme de escorregamento	Quantidade de quadros descartados	Links operando com clocks diferentes
PRBS	Reservado	–
E-Bits incorreto	Quantidade de E-Bits recebidos incorretos	Configuração incorreta de CRC4
Variação Jitter	Reservado	–
Tempo de quadro sem sincronismo	Reservado	–
Quadros sem sincronismo	Reservado	–
Erros de quadro	Quantidade de quadros (timeslot zero) recebidos incorretos	• Presença de alarmes de quadro • Links operando com clocks diferentes • Aterramento precário do equipamento
Violação bipolar	Quantidade de violações bipolares (HDB3) recebidas	• Jumpers de aterramento não conectados • Aterramento precário do equipamento • Circuito físico com problemas
Erro CRC-4	Quantidade de quadros de CRC4 recebidos incorretos	• Configuração de CRC4 incorreta • Aterramento precário do equipamento • Circuito físico com problemas.
N/A	Informação não disponível	• O dispositivo não está conectado • Algum serviço necessário para o funcionamento do sistema não está ativo

- Sinalizações: Exibe o protocolo de sinalização telefônica utilizado no link definido em "configuração" Links E1.

8.4.1. Reiniciar

Desliga e liga o framer do Link, causando um reinício físico do sistema. Todas as chamadas serão derrubadas e o Link será novamente configurado.

8.4.2. Bloquear

Desliga e liga o framer do Link, causando um reinício físico do sistema. Todas as chamadas serão derrubadas e o Link será novamente configurado.

8.5. Canais

"Monitoração" → "Canais"

Esta seção reúne as informações de monitoração dos canais dos dispositivos. Para visualizar a lista de canais, selecione o dispositivo, e então a faixa de canais. Em dispositivos com links digitais, os canais estão agrupados em links.

A lista de canais oferece as seguintes informações:

- Canal: Índice do canal dentro do dispositivo, um número de 0 a N-1 sendo N a quantidade de canais disponíveis no dispositivo.
- Sinalizações: Protocolo de sinalização telefônica associadas aos canais.
- Estado: Informa o estado de um determinado canal. Caso o canal esteja com algum problema, as causas são descritas na coluna "Detalhes". Os valores possíveis são:

Valor	Significado
Idle	O canal está livre para fazer ou receber chamadas
Fail	O canal está em falha, impedido de receber ou fazer chamadas
On Call	O canal está em uma chamada entrante ou sainte

- Detalhes: Informa o estado do canal de forma mais detalhada para cada tipo de interface. Conforme a tabela a seguir:

Interface	AddInfo
E1	• Free • Incomming • Outgoing • Fail • Locked for Outgoing • Locked for Incomming • Remote Lock

Interface	AddInfo
GSM	• Idle • Call in Progress • SMS in Progress • Modem Error • SIM Card Error • Network Error • Not Ready

Interface	AddInfo
VoIP	• Free • Outgoing Lock • Incomming Lock

- Número Discado: Nesse campo, é informado o número de destino da chamada corrente.
- Duração: Duração da chamada corrente.
- Tempo médio: Neste campo é informado o tempo médio das chamadas realizadas.
- Estatísticas: Informa as estatísticas de chamadas computadas pela API K3L.
- Entrantes: Total de chamadas recebidas.
- Saintes:
  - Amount: Total number of outgoing calls.
  - Failures: Unsuccessful outgoing calls.
  - Completed: Successful outgoing calls.

8.5.1. Monitoração de canais GSM

"Monitoração" → "Canais"

Nota	Este recurso está disponível apenas se o KMG possuir interface de telefonia GSM.

- SIM Card: Neste campo é possível selecionar o índice do canal a ser utilizado pelo modem GSM, podendo alternar entre os dois slots existentes 0 e 1.

Atenção	• A solicitação de alteração do SIM Card tem precedência sobre a rotação automática por consumo pode ser configurada no NAP. • Caso haja uma ligação em andamento utilizando o SIM Card, esta será finalizada.

- Operadora: Informa o nome da operadora, cadastrado na célula ERB, em que o modem está registrado no Nível do sinal RX, em porcentagem, recebido na antena GSM. A potência do sinal pode variar de -113dbm (1%) até -51dbm (100%).

8.6. Gráfico estatístico das chamadas

A monitoração dos dispositivos, links (E1/T1) e canais possuem gráficos que mostram as estatísticas das chamadas trafegadas no módulo de telefonia. Para acessar, basta clicar no gráfico em barra presente na coluna "Opções".

As informações exibidas no gráfico são do momento em que foi aberto. Para atualizar os dados, basta clicar no botão "Atualizar gráficos".

Serão exibidos 4 gráficos em pizza:

8.6.1. Estatística do dispositivo

Exibe as informações do dispositivo desde a última inicialização do KMG.

- Completamento de discagem: Porcentagem das chamadas completadas, não atendidas e com falhas, ou seja, que por algum motivo não puderam ser completadas.
- Causa das falhas: Se houver chamadas com falha no gráfico anterior, serão exibidas a porcentagem destas causas.

8.6.2. Estado do canal

Exibe as informações dos canais do dispositivo do momento em que o gráfico foi aberto, ou seja, dados dos canais no momento presente.

- Ocupação: Porcentagem dos canais livre, ocupado, ou em falha.
- Entrantes x Saintes: Se houver canais ocupados no gráfico "Ocupação", são exibidas a porcentagem de chamadas entrantes e chamadas saintes.

8.6.3. Links

Se o dispositivo de telefonia tiver link E1/T1, é possível visualizar o completamento de discagem de todos os links disponíveis no dispositivo, o que poderá ajudar na identificação de possíveis falhas nestes links.

9. Diagnóstico

A área de diagnóstico permite a leitura e download dos Logs dos sistema, e também a alteração dos níveis de Log. Na Interface Web inicial (Resumo), são apresentadas as mensagens mais importantes ou urgentes do sistema. O conteúdo apresentado é o mesmo do arquivo de Log messages.log.

9.1. Download de Logs

Além disto nesta tela é possível realizar o download dos últimos logs do sistema. O download dos últimos Logs serve como facilitador para fornecer um pacote com todos os Logs do sistema para a equipe técnica ou diagnóstico utilizando ferramentas da estação de trabalho sendo utilizada para acessar a Interface Web.

9.2. Entendendo a composição das mensagens de Log

Todas as mensagens contém alguns elementos padrões que auxiliam na sua identificação e origem. Entre estes elementos se destacam:

- O primeiro caractere indica o nível de prioridade da mensagem, e pode ser (por ordem do mais prioritário para o menos prioritário):
  - E → Error: Mensagens de erro, geralmente indicam a incapacidade de um dos serviços de operar adequadamente.
  - W → Warning: Mensagens de aviso de problema grave, geralmente indicam algum comportamento que não incapacita a operação do serviço, porém, pode prejudicar o resultado esperado.
  - I → Information: Mensagens informativas, geralmente indicam início e fim de execução de serviços, bem como início e fim de operação de dispositivos. Este nível de log é apresentado na tela de resumo de logs.
  - N → Notify: Mensagens de notificação, são informações relevantes, porém, normalmente, não são prejudiciais a operação do sistema.
  - T → Trace: Mensagens de depuração, que devem sempre estar desativadas durante operação normal, informam dados de depuração dos serviços, normalmente úteis quando está se diagnosticando algum problema de operação.
- Entre a primeira e a segunda barra "|" sempre estarão a data e hora em que a mensagem ocorreu;
- Da segunda barra "|" até os parênteses no final da linha, a formatação varia de acordo com o serviço;
- No final da linha, entre parênteses, estará o nome do serviço que emitiu a mensagem.

Mensagens em prioridade de erro, aviso e informativa são gravadas no Log do serviço e no Log messages.log.

Algumas convenções comuns, utilizadas pelos serviços:

- Informar o dispositivo utilizando a letra D seguida do número de série do dispositivo.
- Informar o canal utilizando a letra C seguida do número do canal.
- Informar o link utilizando a letra L seguida do número do link.

9.3. Alteração dos níveis de registro e modo de diagnóstico

"Diagnóstico" → "Opções'"

Nesta área é possível ativar o modo diagnóstico e alterar os níveis de Log.

9.3.1. Modo de diagnóstico

⚠ Atenção	Não é recomendado que o modo de diagnóstico fique ativo durante operação normal do equipamento. Sempre que não se fizerem necessárias as mensagens de depuração, este modo deve ser desativado.

9.3.2. Opções avançadas

Permite habilitar ou desabilitar o trace (debug) dos Logs exibidos nesta opção. As demais informações, como informação, avisos e erros, continuarão a ser registrados nos Logs.

O primeiro registro, "Logs", possui o componente "FullLog" que sobrepõe o registro do trace nos demais Logs, não sendo necessário habilitar cada Log individualmente.

Ao expandir os tipos de Logs, é exibido na primeira linha o "Value". A definição feita nesta configuração afeta todos os demais componentes do Log. Portanto, ao habilitar true no Value do Log K3L, o sistema entende que todos os demais componentes deste Log, também serão true, somente se um determinado Log estiver marcado como Never. A seguir são verificados mais detalhes sobre os níveis de depuração de Log.

- False: A depuração do Log (trace) não é registrada no Log. No entanto, se no campo Value ou no FullLog estiver definido true, este valor é sobreposto.
- True: A depuração do Log (trace) é registrada no Log, mesmo que o campo Value ou o FullLog estiver false, este campo continua como true.
- Never: A depuração deste Log nunca será registrada, mesmo que o campo Value ou o FullLog estiver como true.

9.4. Logs

"Diagnóstico" → "Logs"

Fornece acesso aos arquivos de Log dos serviços, onde destacam-se os seguintes Logs:

- messages.log → Todos os Logs de maior importância ou urgência são gravados neste arquivo também.
- k3l_intf.log → Log de depuração dos comandos recebidos e eventos enviados da/pela API para os outros serviços.
- kgateway.log → Log do serviço de roteamento.
- kmp.log → Log do serviço VoIP.
- isdn.log → Log de depuração do ISDN. Possui a opção de análise que mostra de forma amigável os log.
- r2.log → Log de depuração do R2. Possui a opção de análise que mostra de forma amigável os log.
- voip_msg.log → Log de depuração do SIP.
- gsm.log → Logs de depuração do GSM.

9.4.1. Config

Esta opção exibe os arquivos de configuração do KMG com a data da última reinicialização do equipamento.

9.4.2. Licences

Esta opção exibe as licenças aplicadas no KMG. É possível também visualizar e fazer o download do arquivo da licença para backup.

9.4.3. OLD

Logs antigos são automaticamente movidos para o subdiretório /old, onde são arquivados com a data e hora em que foram movidos, posteriormente comprimidos e eventualmente removidos, dependendo da utilização do disco.

O sistema é configurado para reter até 5GB (1 GB no modelo KMG 200) de Logs, somando todos os Logs ativos, antigos e antigos comprimidos. Quando este valor é atingido, os Logs são removidos automaticamente, do mais antigo para o mais recente.

9.5. CDR

"Diagnóstico" → "CDR"

O arquivo CDR é a relação de registros de chamadas realizadas pelo KMG. Para cada chamada realizada, um bilhete de registro é criado para armazenar os dados da chamada.

No ambiente de diagnóstico CDR é possível baixar o arquivo CDR ou visualizá-lo diretamente na Interface Web.

9.6. Captura de pacotes

"Diagnóstico" → "Captura de pacotes"

Permite habilitar a captura de pacotes de rede no gateway. Este arquivo de captura utiliza o formato pcap comprimido, empregando algoritmo gzip. É recomendada a utilização do software livre Wireshark para a visualização dos arquivos de captura.

Os arquivos de capturas serão gravados no diretório /capture, no FTP e também estarão acessíveis pela Interface Web, nesta página.

Uma vez iniciada a captura, ela pode ser finalizada por qualquer uma das três condições:

- Foi solicitado que a captura fosse abortada, pela Interface Web.
- O tempo configurado foi atingido.
- O tamanho máximo permitido foi atingido[1].

[1] *O tamanho máximo é definido por modelo do KMG e é apresentado na ajuda para o campo "Duração".*

São apresentadas as seguintes configurações:

Campo	Descrição
Duração	Tempo máximo de duração da captura (em minutos)
Módulos EBS	Caso habilitado, realiza captura dos pacotes do módulo de telefonia
Filtro por hosts	Se não for definido, captura pacotes originados ou destinados a todos os hosts. Caso seja definido, captura pacotes originados ou destinados somente aos hosts definidos. Pode-se utilizar endereços do próprio gateway para filtrar tráfego por interface de rede, nos modelos com múltiplas interfaces.

10. Administração

Neste menu são apresentadas as opções para gerenciamento do gateway. No menu superior existem alguns botões com algumas funções específicas.

10.1. Monitoração do KMG através de SNMP

O KMG possui um agente SNMP que oferece consultas sobre o estado do equipamento, que inclui: Serviços do gateway, módulos de telefonia (dispositivos), sinalizações e estado dos canais de telefonia, além do envio de alguns comandos. O Download da MIB do KMG é realizado pela própria Interface Web. MIB é o arquivo que contém a base de informações dos objetos do KMG que podem ser consultados.

1. Acesse o menu "Administração".

2. Clique no botão "Baixar MIB do gateway".

Nota	A partir da versão 4.1.42.0 será feito o download de dois arquivo: KHOMP-MIB e KHOMP-KMG-MIB.

Mais informações podem ser obtidas no *"manual do KQueryServer"*.

A MIB desenvolvida para os produtos KHOMP, no formato SMI RFC1065 RFC-1065, pode ser baixada na opção "Baixar MIB do gateway" no menu Administração da Interface Web.

10.2. Informações do gateway

Neste botão são informadas as informações básicas do equipamento, modelo, número serial do equipamento, Hardware ID que é o identificador único do equipamento além da versão do pacote instalado no equipamento.

10.3. Terminal Remoto → CLI

"Administração" → "Terminal Remoto"

É disponibilizada uma nova interface de linha de comando via SSH. Novas opções podem ser consultadas através do comando help do terminal. Para acessá-la clique no botão "Terminal remoto", leia as instruções mostradas na Interface e baixe a chave privada.

10.3.1. Sistemas Linux

1. No terminal, navegue até o diretório onde foi baixada a chave de criptografia.
2. Digite o comando: chmod 400 kmgXXXXX.khomp.com.br.key , onde XXXXX é o serial do seu dispositivo.
3. Digite o comando: ssh -i kmgXXXXX.khomp.com.br.key shell@ip_do_dispositivo.
4. Digite o usuário.
5. Digite a senha.

Observação: *As credenciais para login são as mesmas usadas para o acessar a Interface Web do KMG.*

10.3.2. Sistemas Windows

Acesse o tutorial no link a seguir, para acessar o KMG One remotamente via Windows.

http://docs.khomp.com/wikidocs/images/3/3c/Tutorial_KMG_One_passphrase_-_PT_v1.pdf

10.4. Desligar o gateway

- Desligar → Desliga o gateway.

Após este processo será necessário pressionar fisicamente o botão de liga/desliga no equipamento.

10.5. Reiniciar o gateway

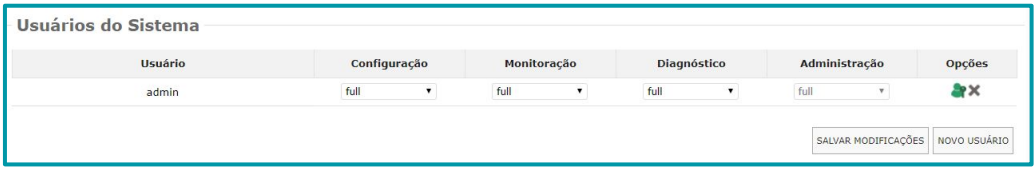
- Reiniciar → Reinicia o gateway.

Desliga todas as ligações e aplica quaisquer configurações que tenham sido salvas e não tenham ainda sido aplicadas.

10.6. Gerenciar usuários do sistema

Adminstração → Usuários do sistema

Podem ser configurados novos usuários com diferentes privilégios de acesso à Interface Web. Os privilégios permitem acessar os quatro menus do gateway: Configuração, Monitoração, Diagnóstico e Administração. Para o menu monitoração, é possível especificar se o usuário poderá ter acesso total ou somente leitura. Estes usuários podem acessar o KMG tanto pela Interface Web quanto por FTP.



10.6.1. Alterar senha de usuário

1. No menu 'Administração', clique no ícone "lápis" do usuário que terá a senha alterada.
2. Digite a nova senha nos campos 'Nova Senha' e 'Repita a senha'.
3. Clique no botão "Salvar".

No próximo acesso ao KMG, será solicitado a nova senha.

10.6.2. Criar nova conta de usuário

1. No menu 'Administração', clique no botão "Novo Usuário".
2. No campo 'Usuário' digite o login de acesso. Por fim informe a senha do usuário.
3. Defina as permissões de acesso deste usuário. É possível atribuir o acesso aos menus: Configuração, Monitoração, Diagnóstico e Administração. Você pode atribuir as seguintes permissões:

- Full: Permissão total. O usuário poderá visualizar e configurar as opções do menu.
- Read: O usuário poderá somente visualizar as informações do menu. Esta permissão só é exibida para o menu Monitoração.
- None: O usuário não terá acesso à seção. O menu não será exibido para este usuário.

10.6.3. Editar e remover contas de usuário

A edição do usuário consiste apenas na alteração de sua senha e das permissões de acesso ao KMG. A edição é realizada no próprio painel 'Usuários do Sistema'.

Para remover um usuário, clique no X, ao lado do ícone de alterar senha.

10.7. Acessar o KMG via FTP

O KMG também pode ser acessado através do protocolo FTP usando o mesmo endereço IP definido para acesso à Interface Web. O acesso ao KMG via FTP é limitado a um acesso simultâneo.

A seguir são descritas as ações e arquivos que podem ser acessados através do FTP:

- Arquivos CDR: Todos os registros CDR ficam disponíveis para download no diretório /cdr. Estes arquivos devem ser removidos manualmente para liberação de espaço.
- Arquivos de Logs do KMG: Todos os arquivos de Logs atuais ficam disponíveis no diretório /log. Arquivos de Logs mais antigos são armazenados no subdiretório /log/old.

Estes arquivos são gerenciados pelo KMG. Os arquivos mais antigos são removidos automaticamente para liberar espaço em disco.

- Arquivos de atualização: Na pasta firmware ficam os arquivos de atualização do KMG. O upload e a gerência destes arquivos pode ser feita tanto via FTP quanto via Interface Web.
- Gravações de auditoria da classificação: No diretório áudio/audit estarão disponíveis as gravações oriundas da auditoria da classificação. Os arquivos desta pasta não são removidos automaticamente e sua manutenção é de responsabilidade do usuário.
- Arquivos para reprodução na classificação: No diretório áudio devem ser colocados os arquivos que se deseja reproduzir com o recurso de Tocar áudio e desligar do classificador de chamadas.
- Arquivos de captura de pacotes de rede: No diretório capture serão gerados os arquivos de captura de pacotes de rede.

Nota	• Todos os usuários têm acesso ao FTP. • Todos os usuários têm acesso ao KMG através do protocolo FTP.

10.8. Licenças

São apresentadas as licenças instaladas para este equipamento.

Para instalar novas licenças, faça o upload da nova licença selecionando o arquivo na caixa Enviar nova licença e clique no botão Enviar a nova licença será instalada.

Nota	Será necessário reiniciar o equipamento para a ativação de novos Links E1.

10.9. Provisionamento

O provisionamento permite que as configurações aplicadas no KMG sejam salvas em arquivo. Desta forma é possível manter um backup das configurações e restaurar quando necessário. Este arquivo também pode ser aplicado em outro gateway KMG.

10.9.1. Download das configurações

1. No menu "Administração" → "Provisionamento", clique no botão "Baixar o backup da configuração".
2. Na janela que será exibida, selecione o local onde o arquivo será salvo.

Será gerado um arquivo único empacotado, compactado e exportado no formato "tar.gz". É necessário utilizar este formato para a restauração das configurações.

O nome do arquivo contém o número de série do KMG e data que foi criado.

Atenção	O arquivo de configuração não deve ser alterado. A alteração indevida poderá inutilizar o arquivo.

10.9.2. Restaurar configurações com arquivo de Provisionamento

1. No menu "Administração" → "Provisionamento", clique no botão "Escolher arquivo", na opção Restaurar configuração.
2. Clique no botão "Enviar". Após este passo é necessário reiniciar o KMG
3. Reinicie o gateway através do menu "Administração" → "Reiniciar o gateway".

Nota	O endereço IP das interfaces de rede do KMG não serão alterados. Desta forma é possível manter o acesso IP após a restauração das configurações.

10.9.3. Aplicação do arquivo de provisionamento em outro KMG

É possível usar o arquivo de provisionamento em outro KMG que seja compatível, ou seja, contenha os mesmos módulos de telefonia. No entanto, é necessário observar alguns critérios. Quando é utilizado somente VoIP (SBC), o procedimento é mais simples. Quando o KMG possui interfaces de telefonia (TDM), alguns requisitos devem ser observados.

Requisitos

- O modelo do KMG no qual será aplicado o arquivo de configuração, deve suportar a mesma quantidade de chamadas simultâneas ou mais. Sendo assim, não é possível restaurar as configurações de um KMG 3200 que suporta até 2000 chamadas em um KMG 2000, que suporta até 240 chamadas. Mas é possível fazer o contrário.
- Se houver módulos externos de telefonia, é necessário que estejam dispostos na mesma ordem e na mesma quantidade do gateway em operação. Caso contrário a estrutura dos dispositivos será incompatível e o backup não será suportado.

Procedimentos

1. Certifique-se de que os gateways atendem os requisitos descritos anteriormente.
2. Verifique se o KMG que terá o arquivo de provisionamento, já possui as licenças aplicadas. Confira no menu "Administração" → "Licenças".
3. Carregue o arquivo de configuração conforme descrito na seção "Restauração das configurações".
4. Reinicie o equipamento para validar as configurações.

10.10. Atualização

Esta seção permite a gerência dos arquivos de atualização da versão do KMG.

São apresentados todos os pacotes disponíveis. Para cada arquivo são apresentadas as opções "Remover" e "Atualizar". Clicando no botão Remover, o arquivo de atualização será removido do sistema. Clicando no botão Atualizar, o arquivo será instalado no sistema e o sistema será automaticamente reiniciado após o fim da instalação.

Para fazer upload de um novo arquivo de atualização, clique no botão "Selecionar Arquivo", escolha o arquivo a ser enviado, mostrado no final da lista de arquivos. Clique em "Enviar" e aguarde o final do upload.

10.11. Porta serial

A porta serial é disponível somente no modelo KMG 3200 e configurada para a velocidade 115200 e tipo de terminal vt100 e deve ser utilizado um cabo de modem nulo para conexão -- http://en.wikipedia.org/wiki/Null_modem -- e um emulador de terminal qualquer (minicom, PuTTY, screen, Hyper Terminal, etcetera).

Exemplo de acesso utilizando o minicom: **$ minicom -b 115200 -D /dev/ttyS0**

10.12. Resolução de problemas

Meus links E1 não alinham

- Problemas físicos comuns:
  - Verifique a qualidade dos cabos através de testadores.
  - Verifique se estão conectados o TX/RX conforme a seção "Instalação" neste guia.
  - "Falta de aterramento". Todos equipamentos que envolvam o sistema de telefonia precisam estar aterrados e necessariamente no mesmo terra (KMG, PBX, modem, nobreak, cabo E1, entre outros). Verifique os itens:
  - Conector do cabo oxidado ou com problema de encaixe.
  - Cabo coaxial partido e com mau contato.
  - Verifique se os conectores da placa E1 estão em bom funcionamento fazendo um loopback entre links E1 do KMG cruzando TX com RX. Se os parâmetros estiverem corretos na "Configuração de Links E1" o LED deve piscar verde.
  - Interferência externa. O cabo é revestido por uma malha de metal, e por isso está sujeito a interferência eletromagnética. Não deve passar dentro de zonas com alta interferência magnética (linhas de alta tensão, ar-condicionado, refrigeradores, etc).
  - Verificar se o modem, PBX ou o que estiver conectado com cabo coaxial no E1 do KMG com impedância de 75 ohms. O modem conectado à este E1 deve estar com a mesma impedância, caso contrário podem ocorrer problemas de sincronismo. Alguns modens possuem conectores RJ 45, sendo a impedância dos cabos de par trançado igual a 120 ohms. Se não houver uma chave para seleção da impedância, utilize conversor de impedância (Balun).

Problemas comuns de configuração

- Certifique-se se o equipamento ao qual O KMG está conectado, tem a mesma configuração de protocolo. Lembre-se que ao utilizar ISDN, uma ponta deve ser configurada como 'ISDN Rede' e a outra ponta como 'ISDN Usuário'.
- O KMG pode gerar ou receber sincronismo pelo E1. Caso o link E1 esteja ligado a uma central pública, esta opção deve estar habilitada para "receber" o sincronismo. Se estiver conectado a um PBX, normalmente esta opção deve estar "gerar" sincronismo.
- O verificador CRC4 está habilitado na configuração do KMG. Se o equipamento que está conectado ao E1 estiver como CRC4 habilitado, também deverá estar habilitado na configuração do KMG, caso contrário não será habilitado.

Link E1 está alinhado porém os canais ISDN estão down

- Verificar Network e User side de cada um dos nós

Estou sem acesso ao equipamento pois a interface rede não responde

- Verificar cabo de rede.
- Verificar se há conflito de IP's na rede.

O áudio das chamadas está mudo

- Verifique se o TX/RX de um E1 não está conectado no TX/RX de outro E1.
- Verifique se o KMG está configurado com os mesmos Codecs do SIP Server "trunkado".
- Verifique se as portas RTPs são as mesmas do SIP Server "trunkado".

As chamadas não estão sendo roteadas

- Verificar a necessidade de utilizar o IP do pacote como endereço para resposta.
- Verificar a necessidade de utilizar o user-part da URI como número de B.
- Verificar se o KMG e o SIP Server estão utilizando a mesma porta para sinalização SIP.
- Verificar inconsistências nas regex de número de A e número de B.

Esqueci o endereço IP configurado no KMG

- O KMG envia em um pacote de rede em broadcast Ethernet todos os endereços de rede configurados em todas as interfaces de rede.
- O pacote utiliza o Ethernet Type 0xF00D, o qual pode ser utilizado para filtrar uma captura de tráfego. É recomendado o software livre Wireshark para realizar a captura do pacote.
- Há também uma verificação se ao menos uma interface de rede está configurada. Caso não haja alguma configurada por mais de cinco minutos desde a inicialização do KMG, então a primeira será configurada com o endereço 10.10.10.10 e máscara de rede 255.0.0.0.
- Dependendo do modelo, a primeira pode ser eth0 ou eth1.

11. Obter acesso à documentação adicional

Você encontra o manual e outros documentos em nosso site, www.khomp.com. Veja como fazer o cadastro e login em nossa área restrita.

Para usuários que não possuem cadastro:

1. No site da Khomp, acesse o menu "Institucional" → "Suporte" → "Área restrita".
2. Clique em "Inscreva-se".
3. Escolha o perfil que melhor o descreve.
4. Cadastre seu endereço de e-mail. É necessário utilizar um e-mail corporativo.
5. Preencha o formulário que será enviado ao seu e-mail. Caso não tenha recebido em sua caixa de entrada, confira sua caixa de spam.
6. Aplique os passos descritos a seguir para fazer login na área restrita.

Para usuários que possuem cadastro:

1. No site da Khomp, acesse o menu "Institucional" → "Suporte" → "Área restrita".
2. Faça login com seu endereço de e-mail e senha cadastrada.
3. Acesse a opção "Documentos". Você será direcionado à wiki da Khomp.

Você também pode entrar em contato com nosso suporte técnico através do e-mail suporte.comunicacoes@khomp.com ou pelo telefone +55 (48) 3722-2940.

À Defensoria Pública do Estado do Rio de Janeiro
Ref.: Pregão Eletrônico nº 90009/2025 – Processo nº E-20/001.005197/2025
Empresa: CAM TECNOLOGIA LTDA – CNPJ: 14.438.757/0001-76

RELATÓRIO DE DEMONSTRAÇÃO DE USO
PROVA DE CONCEITO

Eu, Thiago Maluf Resende, CPF nº 103068457-09, representante legal da empresa CAM Tecnologia Ltda, com sede na Av. Pastor Martin Luther King Jr, nº 126 Nova América Offices, Torre 2000, Sala 408, Bairro Del Castilho, CEP: 20.765-000, Cidade do Rio de Janeiro, RJ, inscrita no CNPJ sob o nº 14.438.757/0001-76, APRESENTA o relatório de demonstração de uso associado a prova de conceito apresentada pela mesma para Defensoria Pública do Estado do Rio de Janeiro no dia 28 de Janeiro de 2026.

1. SUMÁRIO EXECUTIVO

Este relatório consolida os resultados da Demonstração de Uso na Prova de Conceito (POC) realizada para validação da solução ofertada, conforme roteiro do ANEXO VII do Termo de Referência.

2. OBJETIVO DA DEMONSTRAÇÃO

Demonstrar que o software e o hardware ofertados atendem às necessidades do órgão, avaliando aderência técnica, impacto operacional e requisitos funcionais previstos no edital/TR, conforme roteiro de Demonstração de Uso (ANEXO VII).

3. ESCOPO, CONDIÇÕES E REGRAS DA POC

- Prazo e execução: Demonstração realizada em 28/01/2026, conforme agendamento do órgão, observadas as regras do edital/TR.
- Roteiro: Execução baseada no ANEXO VII – Demonstração de Uso.
- Apresentação da Empresa e da Topologia está descrita **na apresentação de Anexo I** a prova de conceito.

4. AMBIENTE DE DEMONSTRAÇÃO

4.1 Dados do ambiente

- Modelo: Nuvem
- URL de acesso: https://pbx-dperj.cambox.cloud [159.138.214.192]
- Acesso apresentado: SIP/UDP, SIP/TCP, SIP/TLS, Web, Aplicativo Desktop e Aplicativo Móvel
- Navegadores utilizados: Chrome, Edge, Firefox
- Perfis demonstrados: Administrador, Supervisor, Operador

- Integrações:
    - Autenticação via AD, Google, Office 365, LDAP
    - API: via Web, via AMI
    - CRM
    - Webhook
    - Banco de Dados

4.2 Telefonia e mídia

- Troncos/rotas: SIP Trunk com número de teste via SBC
- Áudio: Yealink Headset UH34
- Rede: Foi solicitado a liberação do firewall à DPERJ para o endereço IP do servidor em nuvem

5. METODOLOGIA E CRITÉRIOS DE AVALIAÇÃO

A avaliação foi realizada por item do roteiro do ANEXO VII, com registro de evidências de cada etapa. As evidências estão registradas na apresentação de **ANEXO II de Evidências** a esta apresentação.

A empresa CAM TECNOLOGIA LTDA reafirma o cumprimento integral dos requisitos do edital e permanece à disposição para prestar quaisquer esclarecimentos adicionais que se façam necessários.

Rio de Janeiro, 30 de Janeiro de 2026.

Permanecemos à disposição para quaisquer informações adicionais que se façam necessárias.

Atenciosamente,

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2026.02.01 11:05:48 -03'00'

THIAGO MALUF RESENDE
CEO – CAM TECNOLOGIA LTDA
licitacoes@camtecnologia.com.br | (21) 3189-1050