Documentação da API SCAC v2.1.63 - empresaXX

**Documentação da API SCAC v2.1.63 — empresaXX (Completa e Detalhada)**

**1. Visão Geral**

A API **SCAC** (Sistema de Controle de Acesso Corporativo) é um conjunto de endpoints RESTful que possibilita a comunicação entre controladoras físicas (dispositivos de segurança, como leitores de biometria e teclados) e o servidor da **empresaXX**. Esta comunicação visa garantir o controle automatizado de acesso a ambientes físicos, com alta rastreabilidade e segurança.

* **Versão da API:** 2.1.63
* **Protocolo:** HTTP/HTTPS (recomenda-se o uso exclusivo de HTTPS em produção)
* **Formato de Dados:** JSON
* **Documentação Base:** Swagger (OpenAPI 3.1.1)

A API cobre as seguintes funcionalidades principais:

* Abertura e fechamento de unidades
* Autenticação com biometria e PIN
* Testes de hardware das controladoras
* Sincronização de usuários e vigilantes
* Verificação de status das controladoras

**2. Autenticação**

A autenticação da API SCAC se dá por meio de dois métodos principais:

**2.1 API Key**

Cada controladora deve enviar uma chave única no cabeçalho HTTP da requisição:

**2.2 Intranet Authentication**

Para chamadas feitas internamente via rede da empresaXX, o sistema reconhece domínios de origem autorizados sem exigir autenticação adicional, desde que a chamada ocorra de IPs autorizados.

**3. Recursos da API**

Esta seção apresenta os principais endpoints organizados por finalidade. Cada item é descrito com método HTTP, caminho, parâmetros esperados e exemplo de payload.

**3.1 Abertura/Fechamento de Agência**

**POST /abertura**

**Descrição:** Solicita a abertura da unidade.

**Payload:**

Forma

O conteúdo gerado por IA pode estar incorreto.**POST /fechamento**

**Descrição:** Solicita o fechamento da unidade.

**POST /solicitacoes**

**Descrição:** Lista solicitações pendentes de abertura ou fechamento.

**POST /abertura/teclado-externo**

**Descrição:** Abertura acionada por teclado físico externo.

**POST /controladora/central/request**

**Descrição:** Envia solicitação para análise centralizada (autorização remota).

**POST /controladora/central/response**

**Descrição:** Recebe resposta (autorização ou negação) da central.

**3.2 Testes de Hardware**

**POST /controladora/testes**

Envia os resultados dos testes executados na controladora.

**POST /controladora/request/test**

Solicita a execução de um teste específico na controladora.

**POST /api/test**

Permite realizar testes diretos por nome do periférico (ex: "teclado", "biometria").

**3.3 Sincronização de Dados**

**POST /controladora/sync**

Sincroniza registros de acesso locais com o servidor central.

**GET /controladora/is-legacy/{mac}**

Verifica se a controladora está em modo legado (incompatível com nova versão da API).

**PUT /controladora/custodia**

Alterna entre custódia simples e dupla.

**POST /controladora/sync-user**

Envia dados de um único usuário para sincronização com a controladora.

**POST /controladora/vigilante**

Cadastra ou sincroniza dados do vigilante.

**POST /api/sync/user**

Cadastra dados completos (PIN, biometria e permissões) de um usuário.

**POST /api/controladora**

Atualiza dados da controladora (como IP e MAC address).

**3.4 PIN**

**POST /pin**

Cadastra um novo PIN no sistema.

**DELETE /pin/{id}**

Remove um PIN por ID.

**PATCH /pin/{id}**

Atualiza dados do PIN existente.

**GET /pin/id/{id}**

Retorna detalhes de um PIN específico.

**GET /pin/filter**

Busca múltiplos PINs com base em filtros (ex: tipo, vigência).

**POST /request-pin**

Solicita que a controladora colete um novo PIN fisicamente.

**3.5 Biometria**

**POST /biometria**

Envia o hash de biometria para cadastro.

**POST /request-fp**

Solicita coleta de biometria via leitor físico.

**POST /api/fp**

Salva diretamente uma biometria na controladora.

**DELETE /api/fp**

Remove uma biometria cadastrada na controladora.

**3.6 PIN na Controladora**

**POST /api/pin**

Grava um PIN diretamente na controladora.

**DELETE /api/pin**

Remove um PIN da controladora local.

**3.7 Custódia**

**PUT /api/custodia**

Altera o modo de custódia (simples ou dupla).

**GET /api/historicocustodia**

Consulta o histórico de mudanças de custódia na unidade.

**3.8 Notificações**

**POST /notificacao/pin**

Registra eventos relacionados ao uso do PIN (ex: uso fora do horário).

**3.9 Healthcheck**

**GET /api/healthcheck**

Verifica o estado atual da controladora (tempo online, versão, conectividade).

**3.10 Abertura/Fechamento Remoto**

**POST /api/open**

Abertura remota via API.

**POST /api/close**

Fechamento remoto via API.

**3.11 Vigilantes**

**POST /api/vigilante**

Envia dados de vigilantes autorizados a operar a controladora.

**4. Esquemas de Dados**

Esta seção descreve os principais *schemas* definidos na documentação Swagger, utilizados nos endpoints para envio e retorno de informações.

**4.1 AberturaFechamentoAgenciaType**

Uma imagem contendo Forma

O conteúdo gerado por IA pode estar incorreto.

**4.2 SucessoType**

Forma

O conteúdo gerado por IA pode estar incorreto.

**4.3 ErroType**

Forma

O conteúdo gerado por IA pode estar incorreto.

**4.4 BiometriaType**

Texto

O conteúdo gerado por IA pode estar incorreto.

**4.5 PinType**

Texto

O conteúdo gerado por IA pode estar incorreto.

**4.6 SyncUserType**

Combina biometria, PIN, identidade e dados contratuais de vigilantes.

**5. Formatos de Resposta**

**5.1 Sucesso**

* Código HTTP: 200 OK
* Estrutura: conforme SucessoType

**5.2 Erro de Validação**

* Código HTTP: 400 Bad Request
* Estrutura: conforme ErroType

**5.3 Recurso Não Encontrado**

* Código HTTP: 404 Not Found

**6. Exemplo de Fluxo de Uso**

Texto

O conteúdo gerado por IA pode estar incorreto.