

iDFace

GUIA TÉCNICO CONSOLIDADO

Instalação • configuração • cadastros • controle de acesso • operação • diagnóstico

Edição de referência: 20 de outubro de 2026

Este documento é um guia técnico original, baseado em consulta à documentação pública da Control iD. Ele não é uma transcrição integral da documentação oficial e não substitui diagramas elétricos, ilustrações e atualizações publicados pelo fabricante. Os links em cada capítulo permitem consultar os detalhes e imagens originais.

Fonte oficial: [Documentação oficial do iDFace](#)

Fonte oficial: [Guia rápido oficial em PDF](#)

Índice dos capítulos

1. Visão geral e especificações
2. Instalação física e elétrica
3. Primeiro uso e navegação
4. Rede e interface web
5. Usuários, credenciais e cadastros
6. Horários, departamentos e feriados
7. Importação, exportação e backups
8. Modos e regras de controle de acesso
9. Reconhecimento facial e vídeo
10. Interfonia SIP e contatos
11. Relatórios e registros
12. Sistema, diagnóstico e segurança
13. Rotinas de manutenção e checklist
14. Referências oficiais

Observação: a organização temática deste guia facilita a consulta, mas alguns nomes de submenu variam conforme a versão do firmware e os recursos licenciados.

1. Visão geral e especificações

O iDFace é um controlador de acesso com reconhecimento facial, display touchscreen de 3,5 polegadas, comunicação Ethernet e interface de gerenciamento via navegador. Pode funcionar localmente ou integrado a um sistema externo.

- Capacidade indicada pela fabricante: até 200 mil usuários e até 30 mil faces, dependendo do modelo e da licença.
- Reconhecimento facial por identificação 1:N e verificação 1:1; detecção de rosto vivo.
- Conexões e recursos: Ethernet 10/100 Mbps, USB host, Wiegand e módulo de acionamento externo (MAE).
- Alimentação de referência: 12 V / 2 A; grau de proteção IP65, sujeito à instalação correta.

A quantidade de faces e os recursos adicionais dependem da versão do equipamento, licença e firmware. Verifique as especificações do número de série antes de um projeto de grande porte.

Fonte oficial: [Consultar capítulo completo e imagens](#)

2. Instalação física e elétrica

Escolha do local

Evite incidência solar direta sobre a área de reconhecimento e planeje a passagem dos cabos antes da fixação. A recomendação de altura do topo do suporte é aproximadamente 1,35 m para pessoas a pé e 1,20 m para uso dentro de veículos.

Fixação e proteção

Instale o módulo de acionamento externo na área protegida. Observe o posicionamento dos cabos, suporte e vedação traseira. A tampa e a borracha de vedação são essenciais para conservar o grau de proteção do aparelho.

Alimentação, MAE e fechaduras

O MAE liga o terminal aos circuitos de acionamento, botoeira, sensor de porta e interfaces Wiegand. Confira a pinagem diretamente no diagrama da fabricante antes de energizar. Dimensione a fonte para toda a corrente consumida, caso seja compartilhada com outros dispositivos.

ATENÇÃO: ligações elétricas e acionamento de fechaduras dependem do tipo de trava e de suas tensões. Consulte os desenhos originais de eletroímã, solenoide e fechadura eletromecânica; não use este resumo como esquema de ligação.

Fonte oficial: [Consultar capítulo completo e imagens](#)

3. Primeiro uso e navegação

Na primeira inicialização, o aparelho solicita idioma, região, concordância com os termos e alteração das credenciais da interface web.

- A tela inicial mostra data e hora e o resultado das identificações.
- Use [MENU] para abrir as áreas de cadastros, configurações, relatórios, acesso, interfonia e reconhecimento facial.
- Campos de texto e seletores possuem telas próprias de edição. Após mudanças, confirme a gravação.

Para registros e auditoria, corrija a data e a hora antes de colocar o equipamento em produção.

Fonte oficial: [Consultar capítulo completo e imagens](#)

Fonte oficial: [Interação com a tela e o menu](#)

4. Rede e interface web

Configurar IP

Caminho: [MENU] → [CONFIGURAÇÕES] → [REDE] → [PROPRIEDADES DE REDE]. Defina DHCP ou informe IP estático, máscara, gateway e porta web. Configure DNS quando necessário.

Acessar por navegador

Com o terminal e o computador na mesma rede ou em redes com comunicação permitida, digite o endereço IP do equipamento no navegador. Autentique-se com o usuário e a senha definidos na configuração inicial.

Gerenciamento de rede

A documentação também descreve nome do dispositivo, certificados e opções de OpenVPN, inclusive visualização de status e obtenção de logs.

Evite expor a interface web diretamente à internet. Prefira rede de administração protegida e credenciais exclusivas. Ao trocar o IP, registre o novo endereço para não perder o acesso.

Fonte oficial: [Consultar capítulo completo e imagens](#)

Fonte oficial: [Credenciais e ativação da interface web](#)

5. Usuários, credenciais e cadastros

Criar e localizar usuário

Caminho: [MENU] → [CADASTROS] → [USUÁRIOS]. Use [ADICIONAR], informe o identificador (ID), o nome, quando aplicável, e associe o usuário aos departamentos necessários. A busca aceita nome ou ID.

Métodos de identificação

Associe ao registro individual os métodos disponíveis em seu modelo, como face, cartão ou credencial configurada. Prefira um usuário por pessoa, para manter a rastreabilidade.

Editar ou excluir

Localize o usuário, abra o cadastro e altere seus atributos. A exclusão remove os dados cadastrais e não pode ser simplesmente desfeita; eventos antigos podem permanecer associados apenas ao ID.

Administradores

A atribuição de permissões administrativas protege menus sensíveis. A remoção global de administradores deve ser reservada a procedimentos autorizados, pois pode deixar o menu sem restrição até novo cadastro.

Fonte oficial: [Consultar capítulo completo e imagens](#)

6. Horários, departamentos e feriados

Horários e intervalos

Em [CADASTROS] → [HORÁRIOS], defina regras com períodos de tempo e dias da semana. Os horários delimitam quando uma pessoa ou um departamento pode obter liberação.

Departamentos

Organize usuários por grupo. Quando um usuário pertence a diversos departamentos, as regras associadas aos departamentos precisam ser verificadas em conjunto.

Feriados

Em [CADASTROS] → [FERIADOS], configure nome, data, tipo de feriado e eventual repetição. Em seguida, referencie esses tipos nos intervalos relevantes.

Depois de alterar calendário ou departamentos, teste pelo menos um acesso permitido e um acesso negado. A lógica final depende das associações efetivas do usuário.

7. Importação, exportação e backups

Caminho: [MENU] → [CADASTROS] → [IMPORTAR/EXPORTAR]. Insira um dispositivo USB e selecione a operação desejada.

- Exportação de usuários: transfere registros e credenciais cadastradas, conforme recursos disponíveis.
- Backup: destinado à conservação de dados do mesmo equipamento, incluindo registros de acesso.
- Sincronização: transporta dados entre equipamentos sem os logs de acesso, segundo a documentação.
- Logs de acesso: extrai os eventos para consulta.

Os arquivos exportados podem conter dados pessoais e biométricos sensíveis. Proteja o pendrive, limite o acesso aos arquivos e respeite as regras de retenção e privacidade da organização.

Fonte oficial: [Consultar capítulo completo e imagens](#)

8. Modos e regras de controle de acesso

Standalone

O terminal administra localmente os usuários, credenciais, horários e as regras necessárias para tomar a decisão de acesso.

Pro / online

O terminal identifica a credencial e utiliza uma solução externa para autorizar a tentativa, conforme a arquitetura e as configurações. Existem ainda opções de integração específicas, como modos vinculados a iDBlock.

Parâmetros de operação

No menu [ACESSO], configure o modo, a duração do acionamento, as formas de identificação, as validações aplicáveis e protocolos como Wiegand/OSDP, se suportados. Há também parâmetros de intertravamento.

A aplicação efetiva das regras pode variar entre Standalone, Pro e contingência. Verifique a lógica e os requisitos de comunicação antes da implantação.

Fonte oficial: [Consultar capítulo completo e imagens](#)

9. Reconhecimento facial e vídeo

Identificação facial

O menu [CONFIG. FACIAL] concentra as definições relativas a câmera e critérios de reconhecimento. A documentação aborda detecção de máscara e outras características de captura e validação.

Qualidade do cadastro

Cadastre o rosto com iluminação equilibrada, enquadramento adequado e sem obstruções. Evite contraluz forte e teste a identificação após o cadastro.

Transmissão de vídeo

As funções RTSP e ONVIF, quando habilitadas e suportadas, permitem transmissão de imagem a sistemas compatíveis. O RTSP utiliza por padrão a porta 554; ajuste a segurança de acesso e as credenciais para a infraestrutura.

Defina controles de privacidade e segurança para armazenamento de imagens e identificação biométrica; restrinja também o acesso a fluxos de câmera.

Fonte oficial: [Consultar capítulo completo e imagens](#)

10. Interfonia SIP e contatos

SIP

Caminho: [MENU] → [INTERFONIA] → [CONFIGURAÇÕES SIP]. Ative o recurso e informe endereço do servidor e portas apropriadas. No modo cliente SIP, configure ramal, login e senha de acordo com o servidor de telefonia.

Chamadas

Em [CONFIGURAÇÕES DE CHAMADA] selecione o modo de discagem, incluindo discagem automática ou seleção na lista de contatos. Também há parâmetros de atendimento automático, tempo de registro e keep-alive.

Contatos

Acesse [CONFIGURAÇÕES DE CHAMADA] → [EDITAR CONTATOS], adicione nome e destino. O destino pode ser ramal ou endereço IP, conforme o modo de telefonia utilizado.

Verifique se o servidor SIP, rede e firewall permitem a sinalização e o tráfego de áudio. Teste as chamadas recebidas e realizadas.

Fonte oficial: [Consultar capítulo completo e imagens](#)

Fonte oficial: [Adicionar, editar e excluir contatos](#)

11. Relatórios e registros

Caminho: [MENU] → [RELATÓRIOS]. Os eventos são apresentados em ordem do mais recente para o mais antigo.

Acessos

Filtre por período, usuário ou departamento; opcionalmente selecione apenas eventos autorizados. A visualização distingue autorizações e negativas.

Alarmes

Selecione as causas do alarme e o intervalo de datas. É possível separar eventos disparados dos desativados.

Chamadas

Filtre chamadas efetuadas ou recebidas e, quando necessário, as chamadas acompanhadas de abertura.

Exportação

Quando disponível, conecte pendrive USB e utilize [EXPORTAR]. Guarde os arquivos para conferência ou auditoria.

Fonte oficial: [Consultar capítulo completo e imagens](#)

12. Sistema, diagnóstico e segurança

Hora e sincronização

Em [CONFIGURAÇÕES] → [DATA E HORA], configure relógio, formato e NTP. O sincronismo é importante para evitar divergências de logs.

Interface e acesso remoto

Em [CONFIGURAÇÕES] → [CONFIG. GERAIS] → [INTERFACE WEB], altere as credenciais e, se adequado, desative a interface. Outras opções técnicas incluem SSH, SNMP e URL de reinício.

Diagnóstico

Em [CONFIG. GERAIS] → [SISTEMA] → [DIAGNÓSTICO], consulte funções técnicas. Ative portas e protocolos remotos apenas quando necessários, pelo menor tempo possível.

Restauração

O comando [RESTAURAR CONFIG.] pode apagar os dados e reiniciar o equipamento; existem opções para preservar a rede ou outras configurações. Faça backup validado antes de restaurar.

A opção de reiniciar sem sessão autenticada pode criar um risco operacional de indisponibilidade. Não a mantenha ativada sem motivo específico.

Fonte oficial: [Consultar capítulo completo e imagens](#)

Fonte oficial: [Sincronização de data e hora](#)

Fonte oficial: [Restauração de configurações](#)

Fonte oficial: [Reforço da segurança web](#)

13. Rotinas de manutenção e checklist

Antes da entrega

- Conferir alimentação, tampa de vedação, rede e comunicação com o MAE.
- Validar IP, DNS e sincronização de data/hora.
- Alterar credenciais administrativas e restringir acesso à interface web.
- Criar usuário de teste; testar reconhecimento facial em condições reais.
- Testar liberação, negativa, botoeira, sensor e comportamento da fechadura.
- Validar relatórios e exportar backup inicial.

Manutenção periódica

- Rever usuários e permissões administrativas desnecessárias.

- Verificar sincronização do horário e ocorrências de rede.
- Exportar logs e backups segundo a política interna de retenção.
- Verificar atualizações de firmware com a fabricante antes de alterar o ambiente.

Em problemas de identificação, considere iluminação, posicionamento, obstruções e condição do cadastro antes de alterar parâmetros sensíveis.

14. Referências oficiais

Fonte oficial: [Documentação principal](#)

Fonte oficial: [Instalação](#)

Fonte oficial: [Primeiro uso](#)

Fonte oficial: [Navegação](#)

Fonte oficial: [Cadastros](#)

Fonte oficial: [Importar e exportar](#)

Fonte oficial: [Rede](#)

Fonte oficial: [Interface web](#)

Fonte oficial: [Regras de acesso](#)

Fonte oficial: [Biometria facial](#)

Fonte oficial: [Interfonia SIP](#)

Fonte oficial: [Contatos SIP](#)

Fonte oficial: [Relatórios](#)

Fonte oficial: [Data e hora](#)

Fonte oficial: [Diagnóstico](#)

Fonte oficial: [Restauração](#)

Fonte oficial: [Guia rápido PDF](#)

Material independente de apoio. Control iD e iDFace são nomes usados apenas para identificar a documentação e o produto. Consulte sempre a documentação original antes de executar procedimentos elétricos ou destrutivos.