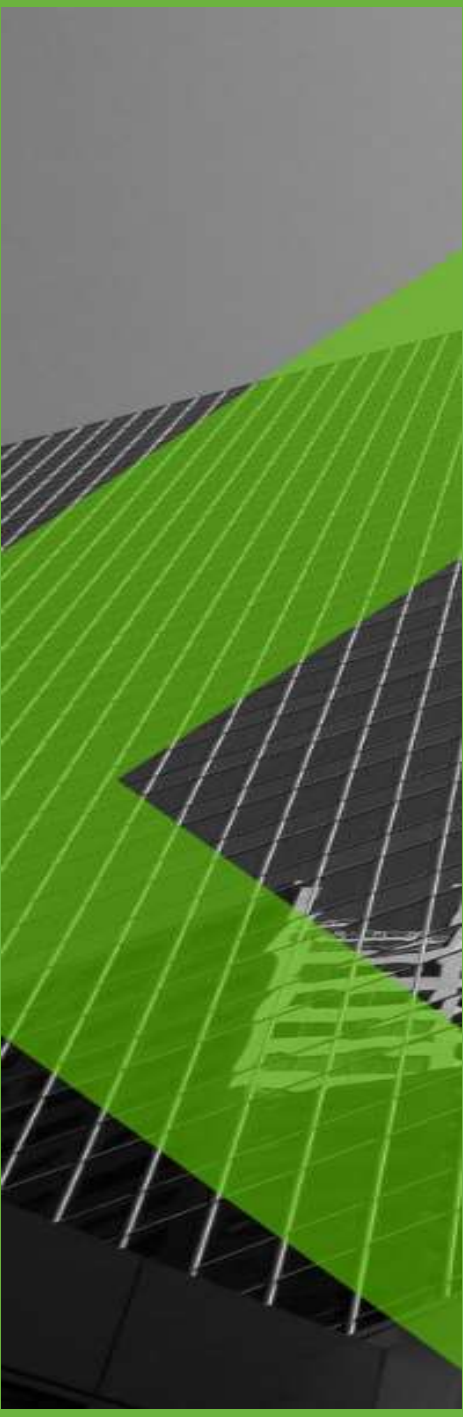

KeyAccess

CHECKLIST DE VERIFICAÇÃO

Autoatendimento de Visitantes com Reconhecimento Facial

Versão	1.0
Público-alvo	Técnico Integrador
Aplicação	Sites com biometria facial já em operação

ÍNDICE

Como usar este documento
Siga as seções na ordem apresentada. Em cada seção, verifique os itens e marque o status no Checklist Resumido (Seção 4). Se algum item não passar, resolva-o antes de continuar. Não ative o recurso sem que todos os itens estejam OK.

1 OBJETIVO

Este documento orienta o técnico integrador na verificação das condições mínimas de sistema e infraestrutura antes de ativar o recurso de autoatendimento de visitantes com reconhecimento facial em sites que já possuem biometria facial em operação para colaboradores fixos.

⚠ Atenção

Este documento foi desenvolvido pelo time KeyAccess com o objetivo de orientar o integrador e o cliente na avaliação das condições de sistema e infraestrutura necessárias para a ativação do recurso de autoatendimento de visitantes com reconhecimento facial.

O checklist é uma ferramenta de apoio à tomada de decisão e deve ser conduzido e analisado pelo próprio integrador em conjunto com o cliente. O resultado não é submetido nem avaliado pelo time KeyAccess.

A identificação e resolução de não conformidades antes da solicitação de ativação do recurso são de responsabilidade do integrador e do cliente. O time KeyAccess estará disponível para suporte técnico durante o processo de ativação, uma vez que as condições mínimas estejam atendidas.

2 O QUE MUDA QUANDO O RECURSO É ATIVADO

Ao realizar o check-in, a foto do visitante é capturada e sincronizada com o servidor KeyAccess e com os dispositivos de reconhecimento facial (PADs), viabilizando o controle de entrada e saída. Caso o sistema identifique falha ou demora no processo de sincronização, um QR Code é gerado automaticamente e passa a funcionar como mídia de identificação alternativa para entrada e saída do visitante.

⚠ Atenção

O novo recurso necessita do perfeito funcionamento do servidor, rede local e conexão de internet. É obrigatório realizar as verificações abaixo antes de ativar.

3 CONDIÇÕES GERAIS DE INFRAESTRUTURA

As condições abaixo não fazem parte do checklist de verificação, mas são requisitos fundamentais para o funcionamento estável e contínuo do sistema. Sua ausência representa risco operacional e deve ser endereçada pelo cliente antes da ativação do recurso.

Alimentação elétrica Todos os equipamentos de controle de acesso, servidores e ativos de rede devem estar conectados a no-break e gerador. O no-break garante a continuidade imediata da operação em caso de queda de energia, enquanto o gerador assegura o funcionamento do sistema por períodos prolongados. Ambos são requisitos obrigatórios e complementares — a presença de apenas um deles não é suficiente para garantir a disponibilidade e estabilidade do sistema.

Aterramento elétrico Todos os equipamentos devem possuir aterramento elétrico eficiente e dentro das normas técnicas vigentes. A ausência de aterramento adequado pode causar danos aos equipamentos, instabilidade no sistema e riscos à segurança das pessoas.

4 CHECKLIST RESUMIDO

Use esta seção para acompanhar todas as verificações. Marque cada item após concluir a verificação detalhada nas seções seguintes.

Link de Internet

#	Item a verificar	Status
1	**Banda:** ≥ 50MB dedicados ao KeyAccess	☐ OK ☐ NÃO OK
2	**Latência:** ≤ 50ms de média	☐ OK ☐ NÃO OK
3	**Perda de pacotes:** = 0%	☐ OK ☐ NÃO OK
4	**Sistemas concorrentes:** Nenhum sistema estrangulando o link de internet	☐ OK ☐ NÃO OK

Rede Local

#	Item a verificar	Status
5	**Sistemas concorrentes:** Rede local sem sistemas comprometendo a banda	☐ OK ☐ NÃO OK
6	**CFTV e alto consumo:** Sistemas segregados ou com QoS configurado	☐ OK ☐ NÃO OK

Servidor

#	Item a verificar	Status
7	**RAM total:** ≥ 32GB	☐ OK ☐ NÃO OK
8	**CPU:** Média ≤ 70% durante o pico	☐ OK ☐ NÃO OK
9	**RAM livre:** ≥ 20% disponível durante o pico	☐ OK ☐ NÃO OK
10	**Disco — % Disk Time:** ≤ 70%	☐ OK ☐ NÃO OK
11	**Disco — Queue Length:** ≤ 1	☐ OK ☐ NÃO OK
12	**Espaço em disco:** ≥ 1TB Total	☐ OK ☐ NÃO OK
13	**Espaço em disco:** ≥ 40% livre na partição do KeyAccess	☐ OK ☐ NÃO OK
14	**Rede:** ≤ 60% da banda utilizada	☐ OK ☐ NÃO OK
15	**Disponibilidade:** Sem reinícios não programados recentes	☐ OK ☐ NÃO OK
16	**Windows Update:** Sem pendências e atualização automática desabilitada	☐ OK ☐ NÃO OK

KeyAccess

#	Item a verificar	Status
18	**Versões:** Todos os módulos e controladoras na última versão	☐ OK ☐ NÃO OK

18	**Módulos:** Todos online e funcionando	☐ OK ☐ NÃO OK
19	**Módulo cloud:** Operacional	☐ OK ☐ NÃO OK
20	**Módulos faciais:** Operacionais	☐ OK ☐ NÃO OK
21	**PADs no sistema:** Todos online e em funcionamento	☐ OK ☐ NÃO OK

Dispositivos Faciais (PAD)

#	Item a verificar	Status
22	**Comunicação servidor → PAD:** Latência ≤ 5ms e perda de pacotes = 0% em cada dispositivo	☐ OK ☐ NÃO OK
23	**NTP:** Configurado e testado em todos os PADs	☐ OK ☐ NÃO OK
24	**Capacidade do PAD:** Ocupação calculada e aprovada ($O \leq C_{max}$)	☐ OK ☐ NÃO OK

5 VERIFICAÇÃO DE INTERNET

5.1 Banda mínima

- **Como acessar:** Abra o navegador no servidor KeyAccess e acesse fast.com ou speedtest.net
- **Quando medir:** No horário de maior movimento do site
- **Critério:** ≥ 50MB

5.2 Latência

- **Como acessar: Iniciar** → cmd → pressione Enter
- **Comando:** `ping google.com -n 20`
- **O que analisar:** Coluna "Média" exibida ao final do resultado
- **Critério:** Média ≤ 50ms. Acima disso, investigar com o provedor.

5.3 Perda de pacotes

- **Como acessar:** Mesmo prompt de comando do item anterior
- **Comando:** `ping google.com -n 100`
- **O que analisar:** "Perdidos" no resumo final
- **Critério:** 0% de perda. Qualquer valor acima de 1% indica problema de estabilidade.

5.4 Sistemas concorrentes no link de internet

- **O que verificar:** Se outros sistemas do site utilizam o mesmo link e se há controle sobre o consumo de cada um.

- **Exemplos de risco:** CFTV com gravação em nuvem, acesso externo de imagens ou monitoramento remoto, backups externos, compartilhamento com administração, VoIP ou streaming sem limitação de banda.
- **Como verificar:** Se possível, observar o gráfico de utilização no roteador ou firewall durante o pico.
- **Critério:** O KeyAccess deve ter banda garantida. Se houver concorrência, verificar se há QoS configurado ou se é possível configurar.

6 VERIFICAÇÃO DE REDE LOCAL

6.1 Sistemas concorrentes na rede local

- **O que verificar:** Se há sistemas de alto consumo de rede operando na mesma infraestrutura do KeyAccess, especialmente sistemas de CFTV.
- **Por que é relevante:** Sistemas de CFTV são um dos principais causadores de degradação silenciosa da rede local. Câmeras transmitindo em alta resolução para um NVR na mesma rede dos PADs competem diretamente com o tráfego do controle de acesso, causando lentidão e falhas no reconhecimento.
- **Como verificar:** Verificar a topologia da rede. Verificar se CFTV e SCA (controle de acesso) estão em VLANs separadas ou se compartilham o mesmo switch sem segregação.
- **Critério:** O ideal é que o Controle de Acesso opere em rede segregada do CFTV. Se não houver segregação, deve existir ao menos QoS garantindo banda para o sistema. Sem nenhuma das duas condições → registrar como risco e verificar se há degradação aparente da rede ou os sintomas mencionados acima.

7 VERIFICAÇÃO DO SERVIDOR

Premissas obrigatórias antes de coletar qualquer dado

A medição só é válida se: • Realizada no horário de maior movimento do site • O servidor estiver em operação normal — sem instalações, atualizações, backups ou qualquer atividade fora da rotina diária em execução

7.1 CPU, RAM, Disco e Rede

Escolha uma das opções abaixo conforme sua disponibilidade de horário:

Opção A — Gerenciador de Tarefas (use se puder estar presente no horário de pico)

1	Iniciar → digite `Gerenciador de Tarefas` → aba **Desempenho**
2	Observe os gráficos de CPU, Memória, Disco e Rede durante **pelo menos 10 minutos contínuos** no horário de pico
3	Registre os valores médios observados e compare com os critérios abaixo

Opção B — Coletor de Dados do perfmon (use se não puder estar presente no horário de pico)

1	Iniciar → digite `perfmon` → pressione Enter
2	No painel esquerdo: **Conjuntos de Coletores de Dados → Definidos pelo Usuário**
3	Clique com botão direito → **Novo → Conjunto de Coletores de Dados**
4	Escolha **Criar manualmente (Avançado)**
5	Adicione os contadores da tabela abaixo
6	Defina o intervalo de coleta: **1 minuto**
7	Configure a pasta de saída — ex: Área de Trabalho
8	Inicie a coleta **antes** do horário de pico e encerre após o pico
9	Visualize o relatório em: **Relatórios → Definidos pelo Usuário**

Contador a adicionar	O que mede
`Processor → % Processor Time`	Uso da CPU
`Memory → Available MBytes`	RAM disponível
`PhysicalDisk → % Disk Time`	Ocupação do disco
`PhysicalDisk → Avg. Disk Queue Length`	Fila de espera do disco
`Network Interface → Bytes Total/sec`	Tráfego de rede

Critérios de avaliação — válidos para ambas as opções:

Recurso	✓ OK — pode prosseguir	✗ Atenção — não ative
RAM total	≥ 32 GB	< 32 GB
CPU	Média ≤ 70% no pico	Média > 70% sustentado
RAM livre	≥ 20% disponível	< 20% disponível
Disco — % Disk Time	≤ 70%	> 70%
Disco — Queue Length	≤ 1	> 1
Rede	≤ 60% da banda	> 60% — investigar causa

Sobre o critério de CPU

O gráfico sempre mostrará picos pontuais — isso é normal. O que importa é a média sustentada durante o período de pico. Um pico de 90% por 3 segundos não é problema. Uma média de 75% durante 15 minutos é.

⚠ Rede com utilização alta constante

Pode indicar outro processo consumindo banda — backup automático, CFTV sem segregação ou sistema de terceiros. Identificar e resolver antes de prosseguir.

7.2 Espaço livre em disco

- **Como acessar:** Explorador de Arquivos → Este Computador
- **O que analisar:** Barra de uso da partição onde o KeyAccess está instalado
- **Critério:** Disco total ≥ 1TB e mínimo 40% de espaço livre na partição do KeyAccess

7.3 Disponibilidade do servidor

- **Como acessar:** Iniciar → `PowerShell` → pressione Enter
- **Comando:** `Get-WinEvent -FilterHashtable @{LogName='System'; Id=6005} | Select-Object -First 50`
- **O que analisar:** Data e hora das inicializações
- **Critério:** Reinícios frequentes e não programados indicam instabilidade. Se o servidor reiniciou mais de uma vez na última semana sem motivo conhecido, investigar antes de prosseguir.

7.4 Windows Update

- **Como acessar:** Iniciar → Configurações → Windows Update
- **O que verificar:** Se há atualizações pendentes que exijam reinício e se a atualização automática está habilitada
- **Critério:** Nenhuma atualização pendente. Atualização automática **desabilitada** — reinicializações automáticas e desassistidas podem interromper o sistema em horário de operação. Atualizações devem ser agendadas e supervisionadas pelo responsável.

8 VERIFICAÇÃO DO KEYACCESS

Confirmar que o sistema está atualizado e íntegro em todos os seus componentes.

8.1 Versão do KeyAccess, dos módulos e controladoras

- **Como verificar:** Fazer o login no KeyAccess → observar se no canto superior direito da tela há indicadores de atualização pendente.
- **Critério:** O KeyAccess Server e todos os módulos instalados devem estar na versão mínima indicada abaixo ou superior. Versões desatualizadas podem causar incompatibilidades com o novo recurso.

> ⚠ **Atenção**
>
> Atualizar apenas os módulos que estão instalados no site. Não instalar módulos de tecnologias que não são utilizadas na instalação. Verifique quais módulos estão presentes antes de iniciar as atualizações.

Versões mínimas obrigatórias:

Componente	Versão mínima
KeyAccess Server	2.2.29
Cloud	2.0.15
Hikvision	1.0.32
ControlID	1.0.38
Megvii	1.0.50
Barrier HIK	1.0.7
Dahua Facial	1.0.7
HIKCentral	1.0.4
Intelbras	1.0.2

8.2 Status dos módulos

- **Como verificar: Fazer o login no KeyAccess → acionar o sinótico do sistema.**
- **O que verificar:** Todos os módulos devem estar online e operacionais, especialmente:
  1. **Módulo cloud** — responsável pela comunicação com a plataforma KeyAccess em nuvem
  2. **Módulos faciais** — responsáveis pelo gerenciamento dos dispositivos faciais em campo.
- **Critério:** Qualquer módulo offline ou com erro deve ser resolvido.

8.3 Status dos PADs no sistema

- **Como verificar: Fazer o login no KeyAccess → acionar o sinótico do sistema.**
- **O que verificar:** Todos os PADs cadastrados devem estar online e em funcionamento perfeito
- **Critério:** PAD offline ou com falha = Resolver antes de prosseguir.

9 VERIFICAÇÃO DOS DISPOSITIVOS FACIAIS (PAD)

9.1 Comunicação entre o servidor e os PADs

> **Atenção**
> A verificação deve ser feita individualmente para cada PAD cadastrado. Um dispositivo com problema pode passar despercebido se a verificação for feita apenas de forma genérica no servidor.

- **Como executar:** No servidor, abrir o `cmd` e executar o comando abaixo substituindo o IP pelo endereço de cada PAD:
- **Comando:** `ping [IP do PAD] -n 100`
- **O que analisar:** Tempo de resposta médio e quantidade de pacotes perdidos exibidos ao final

1. **Latência ≤ 5ms** — valores maiores indicam problema de infraestrutura de rede local
2. Perda de pacotes = 0%

- **Se houver perda ou latência alta:** Verificar cabeamento, switch e configuração de IP do PAD, duplicidade de endereços na mesma rede, etc. Resolver antes de prosseguir.

9.2 Sincronização de horário — NTP

O funcionamento adequado do reconhecimento facial depende diretamente da precisão de data, hora e fuso horário configurados no dispositivo. Se esses parâmetros estiverem incorretos, as leituras realizadas fora do padrão temporal produzirão comportamentos erráticos no momento das liberações de acesso.

Por isso, todos os PADs devem ter o horário atualizado automaticamente por um servidor NTP — Network Time Protocol.

Opções de configuração:

Opção	Descrição
a) Servidor KeyAccess como NTP (Recomendado)	O servidor Windows que hospeda o KeyAccess é configurado como servidor NTP local. Ele se sincroniza com a internet e os PADs se sincronizam com ele. Consulte o procedimento SERVIÇO NTP NO SERVIDOR KEYACCESS (Anexo A).
b) Servidor NTP interno da rede	Caso o cliente possua outro servidor NTP na rede, este pode ser utilizado para sincronizar os PADs. Garantir que esse servidor esteja sincronizado com servidores oficiais de forma programada.
c) Servidor NTP externo (internet)	Os PADs sincronizam diretamente com servidores NTP públicos. Em alguns casos será necessário auxílio do time de TI para liberações no firewall.

Como configurar nos PADs:

O caminho de configuração varia conforme o fabricante e modelo do dispositivo. Consulte o manual do fabricante para localizar as configurações de fuso horário e NTP. Em geral, os campos a configurar são: time zone, endereço do servidor NTP, porta NTP e intervalo de sincronização.

Como testar após configurar:

1	Edite manualmente o horário do PAD para um valor incorreto
2	Ative a opção NTP e defina o intervalo para **2 minutos**
3	Aguarde 2 minutos
4	O horário deve ser corrigido automaticamente
5	Se não ocorrer — revisar as configurações e repetir o teste

- **Critério:** NTP configurado, testado e funcionando em todos os PADs. Correção automática confirmada.

9.3 Capacidade de armazenamento do PAD

O PAD possui capacidade máxima de armazenamento de faces (C_{max}) definida pela licença ou modelo adquirido do equipamento. Para ativar o reconhecimento facial para visitantes é necessário confirmar que há margem suficiente para absorver os visitantes sem ultrapassar esse limite.

Variável	Descrição	Como obter
C_{max}	Capacidade máxima de faces do dispositivo	Consulte a licença adquirida ou a especificação técnica do modelo do equipamento junto ao fabricante.
F	Funcionários fixos cadastrados	1. Acesse o **servidor KeyAccess** 2. Navegue até o **relatório de Pessoas** 3. Aplique os seguintes filtros: • **Tipo de cadastro:** Fixo • **Possui identificador:** Ambos • **Pessoas ativas:** Sim 4. Exporte os dados para Excel 5. Realize a contagem do total de registros exportados
ΔF	Crescimento previsto de funcionários	Estimativa fornecida pelo cliente com base na vacância atual do empreendimento ou em mudanças previstas no perfil de ocupação ou alterações no uso dos espaços.
V	Visitantes por dia	1. Acesse o **Sitemaster** 2. No dashboard, localize o gráfico **Público Diário** 3. Selecione o período de **90 dias** 4. Exporte os dados para Excel 5. Na planilha exportada, identifique o maior valor registrado na coluna **Visitantes** **Dica:** O maior valor encontrado representa o pico diário de visitantes e deve ser utilizado como referência para os cálculos de capacidade.

Fórmula de ocupação do PAD

$$O = 1{,}1 \times (F + \Delta F + (V \times 2))$$

Resultado	Decisão
$O \leq C_{max}$	✅ PAD aprovado — capacidade suficiente
$O > C_{max}$	❌ Ampliar capacidade

Exemplos práticos:

Exemplo 1 — Situação confortável	
C_{max} = 5.000 | F = 4.000 | ΔF = 200 | V = 100	
O = 1,1 × (4.000 + 200 + (100 × 2)) = 4.840	
✅ **Aprovado**	

Exemplo 2 — Situação no limite	
C_{max} = 5.000 | F = 4.200 | ΔF = 300 | V = 150	
O = 1,1 × (4.200 + 300 + (150 × 2) ≈ 5.280	
⚠ **ampliar capacidade**	

10 CONFIRMAÇÃO FINAL

✅ Pronto para ativar

Todos os itens do Checklist Resumido (Seção 4) com status OK → recurso liberado para ativação.
Informe o resultado positivo da verificação ao SAC KeyAccess e solicite agendamento para ativação do novo recurso
Monitore o funcionamento geral do sistema nas primeiras horas de operação.

❌ Algum item não passou?

Resolva o problema identificado antes de prosseguir. Ativar o recurso com infraestrutura inadequada pode causar lentidão, falhas de reconhecimento ou indisponibilidade do sistema.

A ANEXO A — SERVIÇO NTP NO SERVIDOR KEYACCESS

Este procedimento configura o servidor Windows que hospeda o KeyAccess para funcionar como servidor NTP da rede local, permitindo que os PADs sincronizem o horário automaticamente com ele.

> 📌 **Pré-requisito**
> Todos os comandos abaixo devem ser executados no Prompt de Comando (cmd) aberto como Administrador. Iniciar → digite cmd → clique com botão direito → Executar como administrador

Parte 1 — Configurar o Windows como servidor NTP

Passo 1 — Ativar o servidor NTP:

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer /v
Enabled /t REG_DWORD /d 1 /f
```

Passo 2 — Definir o tipo de sincronização como NTP:

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters /v Type /t REG_SZ
/d NTP /f
```

Parte 2 — Garantir que o servidor está sincronizado com a internet

Passo 3 — Configurar servidores NTP públicos brasileiros (NTP.br — recomendado):

```
w32tm /config /manualpeerlist:"a.ntp.br,0x8 b.ntp.br,0x8" /syncfromflags:manual
/reliable:YES /update
```

Passo 4 — Reiniciar o serviço W32Time:

```
net stop w32time && net start w32time
```

Passo 5 — Forçar sincronização imediata com a internet:

```
w32tm /resync /force
```

Parte 3 — Liberar a porta NTP no firewall do Windows

Passo 6 — O NTP utiliza a porta **UDP 123**. Se o firewall do Windows estiver ativo no servidor, execute o comando abaixo para que os PADs consigam se comunicar:

```
netsh advfirewall firewall add rule name="NTP Server" protocol=UDP dir=in
localport=123 action=allow
```

Parte 4 — Verificação final — confirmar que o servidor NTP está respondendo

Passo 7 — Execute o comando abaixo de qualquer máquina da rede, substituindo o IP pelo endereço do servidor KeyAccess:

```
w32tm /stripchart /computer:[IP do servidor] /samples:5
```

✅ **Critério de aprovação**
Se o comando retornar os offsets de tempo sem erro, o servidor NTP está configurado e respondendo corretamente na rede.