

Authentik com Nextcloud

Link: <https://integrations.goauthentik.io/chat-communication-collaboration/nextcloud/>

O que significa o texto abaixo referente ao Nextcloud e o Authentik: aviso Se você precisa de criptografia do lado do servidor, deve usar LDAP. OpenID e SAML causarão perda irrevogável de dados. A criptografia do lado do servidor Nextcloud requer acesso à senha em texto claro do usuário, à qual o Nextcloud só tem acesso quando usa LDAP porque o usuário insere sua senha diretamente no Nextcloud.

Esse aviso é **muito importante** — ele fala de uma limitação séria entre o Nextcloud e provedores de identidade como o Authentik.

Vamos traduzir e explicar de forma clara ☐☐

?? Ideia central

O problema é a **criptografia do lado do servidor (Server-Side Encryption)** do Nextcloud.

☐☐ Esse tipo de criptografia **precisa da senha do usuário em texto claro**.

? O que o aviso quer dizer

?? Com LDAP (funciona)

Quando você usa LDAP:

- O usuário digita a senha **direto no Nextcloud**
- O Nextcloud recebe a senha em texto claro
- Ele usa essa senha para:
 - gerar chaves
 - descriptografar arquivos

☐☐ Exemplo:

- LDAP ou Active Directory
-

? Com OpenID / SAML (problema)

Quando você usa:

- OpenID Connect (OIDC)
- SAML

O que acontece:

- O login é redirecionado para o Authentik
 - O Nextcloud **NUNCA vê a senha**
 - Ele só recebe um **token de autenticação**
-

? Consequência grave

Sem a senha:

- o Nextcloud **não consegue descriptografar os dados**
- arquivos podem ficar inacessíveis

Daí o aviso:

“perda irrevogável de dados”

Ou seja:

- você pode perder acesso aos arquivos criptografados
 - mesmo sendo o administrador
-

? Resumo simples

Método	Nextcloud vê a senha?	Criptografia funciona?
LDAP	<input type="checkbox"/> Sim	<input type="checkbox"/> Sim

Método	Nextcloud vê a senha?	Criptografia funciona?
SAML	<input type="checkbox"/> Não	<input type="checkbox"/> Não
OpenID (Authentik)	<input type="checkbox"/> Não	<input type="checkbox"/> Não

?? Importante (muita gente ignora isso)

Esse problema não é bug:

é **limitação de design** do Nextcloud

? O que você deve fazer

?? Opção 1 — Usar Authentik + Nextcloud (sem criptografia)

- Pode usar OIDC/SAML normalmente
- **NÃO ativar Server-Side Encryption**

recomendado na maioria dos casos

?? Opção 2 — Usar criptografia

- Usar LDAP/AD direto no Nextcloud
 - Não usar SSO via OIDC/SAML
-

?? Opção 3 — Alternativa moderna

- Não usar criptografia do Nextcloud
- Usar:
 - criptografia no disco (LUKS, ZFS, etc.)
 - criptografia no storage

mais seguro e sem esse problema

? Insight importante

A criptografia do Nextcloud:

- é considerada **limitada**
 - não é “zero-knowledge”
 - depende da senha do usuário
-

? Conclusão

O aviso basicamente diz:

Se você usar Authentik com OpenID ou SAML, NÃO ative a criptografia do Nextcloud, ou você pode perder seus dados.

Se quiser, posso te orientar na melhor arquitetura:

- Authentik + Nextcloud seguro
- com SSO funcionando
- sem risco de perda de dados

Só me diz como você pretende usar

Authentik com Nextcloud seguro

Perfeito — dá pra montar uma integração **segura e moderna** entre Authentik e Nextcloud sem cair naquele problema da criptografia.

Vou te passar o **modelo recomendado hoje (produção)**

? Arquitetura segura (recomendada)

? Autenticação

- Authentik → **OpenID Connect (OIDC)**
 - Nextcloud → login via SSO
-

? Criptografia (IMPORTANTE)

NÃO usar:

- criptografia do lado do servidor do Nextcloud

☐ Usar no lugar:

- criptografia de disco:
 - LUKS (Linux)
 - ZFS encryption
 - ou criptografia no storage (cloud, NAS, etc.)
-

? Componentes

- Nextcloud
 - Authentik (IdP)
 - PostgreSQL (recomendado para ambos)
 - Redis (performance)
 - Reverse proxy (Traefik ou Nginx)
-

? Fluxo de login

1. Usuário acessa Nextcloud
2. Redireciona para Authentik
3. Login no Authentik
4. Volta autenticado via token (OIDC)

☐ senha nunca passa pelo Nextcloud (isso é bom)

?? Configuração resumida

1. No Authentik

Criar:

- **Application**
- **Provider → OpenID Connect**

Configurar:

- Redirect URI:

https://cloud.seudominio.com/apps/user_oidc/code

Scopes:

openid profile email

2. No Nextcloud

Instalar app:

- **"OpenID Connect Login"**

Configurar algo assim:

```
'oidc_login_provider_url' => 'https://auth.seudominio.com/application/o/',  
'oidc_login_client_id' => 'nextcloud',  
'oidc_login_client_secret' => 'SECRET',  
'oidc_login_auto_redirect' => true,  
'oidc_login_end_session_redirect' => true,  
'oidc_login_button_text' => 'Login com SSO',  
'oidc_login_attributes' => [  
  'id' => 'sub',  
  'name' => 'name',  
  'mail' => 'email',  
],
```

?? Hardening (segurança de verdade)

? No Authentik

- ativar MFA (2FA)
 - políticas de senha forte
 - limitar tentativas de login
-

? No Nextcloud

- HTTPS obrigatório
 - headers de segurança
 - usar Redis para cache
 - usar PostgreSQL (evitar SQLite)
-

? Infraestrutura

- backup frequente
 - snapshots
 - firewall (ex: só portas 80/443 abertas)
-

?? Coisas que você NÃO deve fazer

☐ Ativar:

- Server-Side Encryption do Nextcloud

☐ Misturar:

- LDAP + OIDC ao mesmo tempo (gera conflito)
-

? Extras (opcional, mas top)

- Provisionamento automático de usuários via Authentik
 - Grupos → roles no Nextcloud
 - Logout único (Single Logout)
-

? Resumo final

- ✓ Authentik + OIDC = melhor UX
 - ✓ Sem criptografia interna do Nextcloud
 - ✓ Segurança via infra (disco + rede)
 - ✓ Escalável e moderno
-

Revision #2

Created 9 April 2026 19:29:19 by Administrador

Updated 9 April 2026 19:37:34 by Administrador