efflux solutions

efflux-solutions.com

Efflux Solutions Limited
Suite 4, 2nd Floor The West Wing Montarik House, 3 Bedlam Ct, GX11 1AA, Gibraltar

Efflux Cloud Capture:
Documento Técnico sobre Segurança.

Documento Técnico
Ver. 1.0
Janeiro, 2026

Contents

1. Visão Geral do Sistema 3

2. Introdução: O cenário em evolução do processamento de documentos 3
2.1 Portal do Provedor Principal 4
2.2 Portal do Fornecedor 4
2.3 Portal do Inquilino e Proprietário 5
2.4 Portal do Usuário 5
2.5 Aplicação Desktop 6
2.6 Cliente MFP 6
2.7 Armazenamento em nuvem 6
2.8 Armazenamento ECC 6

3. Arquitetura multilocatário 7

4. Controle de Acesso Baseado em Funções (RBAC) 8
4.1 Matriz de Acesso de Gerenciamento 8
4.2 Matriz de Acesso Funcional 9

5. Identificação e autenticação de usuários 10

6. Política de Senhas 10

7. Logout automático e gerenciamento de sessão 11
Cliente MFP 11
Portal Web e Cliente Desktop 11

8. Autenticação por PIN 12

9. Integração com o Microsoft Entra ID 13

10. Fluxo de autenticação e gerenciamento de tokens 14

11. Segurança de Rede e Isolamento de Serviços 15

12. Proteção de Dados e Isolamento de Locatários 15

13. Registros de Log e Auditoria 16

1. Visão Geral do Sistema

Efflux Cloud Capture é uma solução de captura de documentos baseada em nuvem que permite às organizações coletar, processar e encaminhar documentos de forma segura a partir de múltiplas fontes de entrada. A plataforma oferece suporte a uma ampla variedade de marcas de impressoras multifuncionais (MFPs), conta com um cliente Windows dedicado e permite uploads via navegador, possibilitando que os usuários capturem documentos independentemente do dispositivo ou da localização. Os administradores podem gerenciar usuários de forma centralizada, registrar dispositivos compatíveis e configurar fluxos de trabalho de captura por meio de uma interface unificada na nuvem.

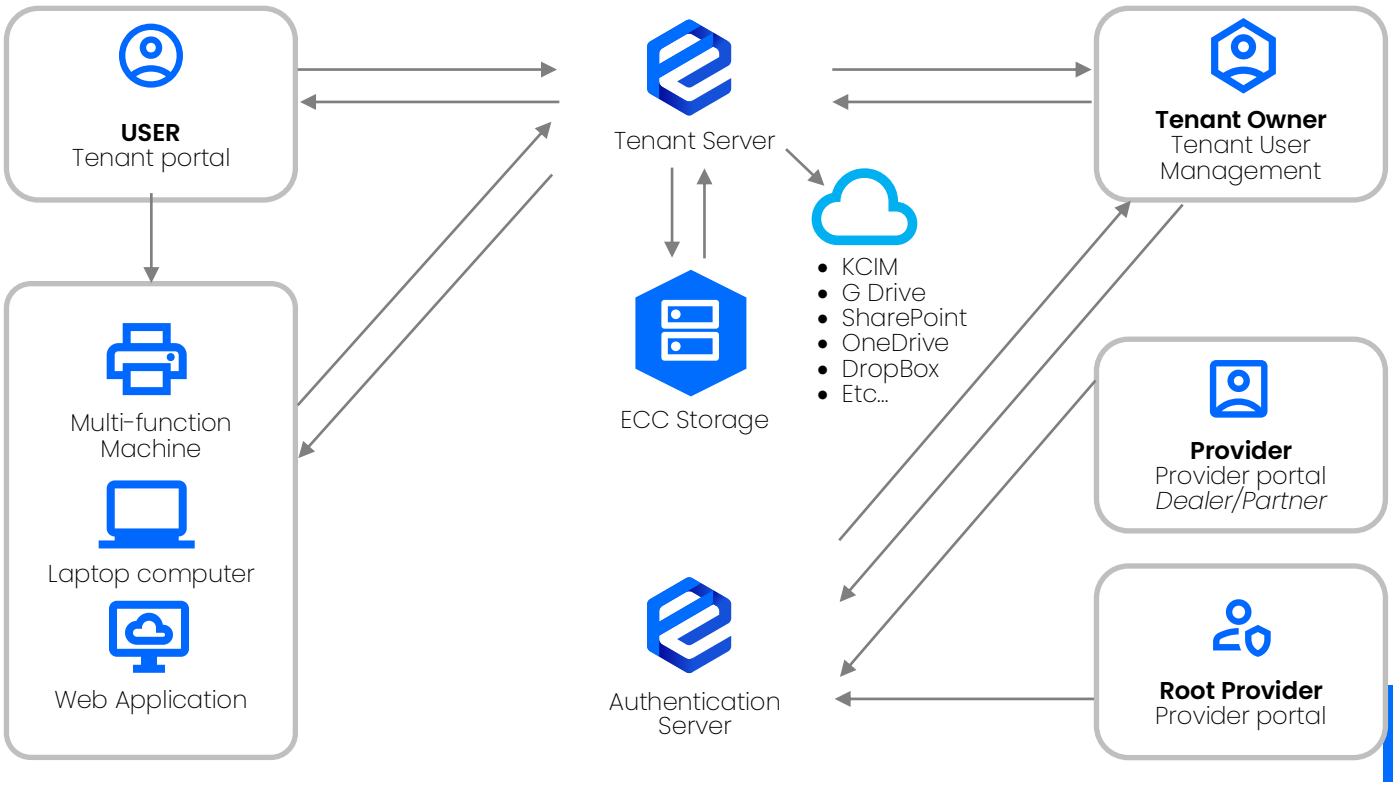
Este documento técnico apresenta a revendedores e usuários uma visão geral das medidas de segurança implementadas no Efflux Cloud Capture. A proteção das informações dos clientes e dos dados dos documentos é um objetivo fundamental do projeto da plataforma. Todos os ativos de informação processados pelo Efflux Cloud Capture são protegidos por uma arquitetura de sistema segura, configuração controlada e mecanismos de segurança em camadas integrados ao serviço.

---

2. Introdução: O cenário em evolução do processamento de documentos

Efflux Cloud Capture consiste no seguinte componente::

- **Painel de Administração do Provedor Principal**
- **Portal do Provedor (Parceiros e Revendedores)**
- **Portal do Proprietário do Tenant**
- **Portal do Usuário**
- **Cliente para Desktop**
- **Cliente para MFP**
- **Integrações de Armazenamento em Nuvem**
- **Armazenamento do Tenant**



2.1 Portal do Provedor Principal

O Painel de Administração do Root Provider é uma interface administrativa segura, baseada na web, acessível apenas a pessoal de suporte autorizado da Efflux Solutions. Ele é utilizado para operar, dar suporte e gerir a plataforma Efflux Cloud Capture, não sendo acessível a revendedores, parceiros ou clientes finais.

Por meio do Painel de Administração, a equipe de suporte da Efflux pode gerenciar operações do ciclo de vida dos *tenants*, incluindo ativações pendentes, verificação de novas organizações e monitoramento de *tenants* ativos. O sistema oferece visibilidade sobre pedidos de instâncias e de licenças, permitindo que as equipes de suporte analisem, aprovem e gerenciem o provisionamento e as renovações de forma controlada.

O Painel Administrativo também oferece suporte ao gerenciamento centralizado de licenças, à administração de parceiros e revendedores e ao gerenciamento de contas administrativas. Recursos de gerenciamento de versões permitem que a equipe de suporte da Efflux controle as versões de software disponíveis e atribua ou modifique versões específicas para cada organização, conforme necessário.

Todas as funções administrativas estão organizadas em uma interface estruturada para garantir a separação de responsabilidades, a rastreabilidade das ações e a operação segura da plataforma.

2.2 Portal do Fornecedor

O Portal do Fornecedor é uma interface baseada na web, projetada para que parceiros e revendedores gerenciem seus clientes e interações comerciais com o Efflux Cloud Capture. O acesso a este portal é restrito a contas autorizadas de parceiros e revendedores e não oferece controle administrativo em nível de plataforma.

Por meio do Portal do Provedor, parceiros e revendedores podem enviar à Efflux Solutions solicitações de criação de novos *tenants* e pedidos de renovação de licenças. O portal oferece visibilidade do histórico e do status atual dos pedidos, bem como do status operacional dos *tenants* associados, incluindo o estado de ativação e a validade da licença.

Controles de acesso baseados em funções definem o escopo da visibilidade e as capacidades de gerenciamento:

- Parceiros podem gerenciar sua rede de revendedores adicionando revendedores às suas contas. Eles têm visibilidade de todos os *tenants* e pedidos associados tanto à sua própria organização quanto aos seus revendedores registrados.

- Revendedores têm acesso restrito e podem visualizar e gerenciar apenas os *tenants* e pedidos associados às suas próprias contas.

Essa separação de funções garante limites claros de responsabilidade, ao mesmo tempo que permite aos parceiros e revendedores gerenciar com eficiência as atividades de integração de clientes e licenciamento.

2.3 Portal do Inquilino e Proprietário

O Portal do Proprietário do Tenant é uma interface de gerenciamento baseada na web, utilizada por administradores do tenant para configurar e operar seu próprio ambiente Efflux Cloud Capture. O acesso é restrito a usuários autorizados dentro do tenant e não permite visualizar outros tenants nem acessar controles em nível de plataforma.

Por meio deste portal, proprietários e administradores do tenant podem gerenciar usuários e o controle de acesso em suas organizações. Isso inclui criar e gerenciar contas de administradores e usuários padrão, definir grupos de usuários e atribuir permissões a esses grupos. O portal oferece suporte à integração com o Microsoft Azure Entra ID, permitindo que os tenants conectem seus serviços de diretório e importem usuários para a plataforma.

O Portal do Proprietário do Tenant também fornece visibilidade operacional do ambiente do tenant. Os administradores podem monitorar o status dos serviços do tenant, analisar logs do sistema provenientes da infraestrutura do tenant hospedada no Azure e realizar verificações operacionais básicas.

Contas de usuário temporárias podem ser criadas quando necessário para atender a cenários de acesso de curta duração.

Esses recursos permitem que os tenants mantenham o controle sobre o acesso de usuários, a integração de identidades e a supervisão operacional, mantendo-se isolados de outros tenants e da administração da plataforma Efflux subjacente.

2.4 Portal do Usuário

O Portal do Usuário é uma interface baseada na web utilizada pelos usuários finais para realizar atividades cotidianas de captura e processamento de documentos no Efflux Cloud Capture. O acesso aos recursos é regido por funções de usuário e permissões atribuídas.

Por meio do Portal do Usuário, os usuários podem fazer o upload de documentos para processamento e acompanhar o status dos documentos enviados ao longo do fluxo de trabalho de captura. Com base em suas permissões, os usuários podem criar, atualizar e excluir modelos, conexões e listas de seleção utilizados no processamento e no roteamento de documentos.

Os documentos processados são disponibilizados na seção de download do portal, onde os usuários podem acessar e recuperar com segurança os resultados finais. A visibilidade é restrita aos documentos associados ao *tenant* e às permissões do usuário, garantindo o isolamento entre usuários e organizações.

2.5 Aplicação Desktop

O Efflux Desktop Client é um aplicativo para Windows que permite aos usuários capturar e enviar documentos diretamente de suas estações de trabalho. Após o login, o cliente carrega e exibe os modelos acessíveis ao usuário com base nas permissões a ele atribuídas.

Os usuários podem selecionar um modelo e enviar documentos para processamento por meio do fluxo de trabalho de captura configurado. O cliente desktop também oferece suporte à funcionalidade de pasta monitorada (*hot folder*), permitindo definir pastas locais que são monitoradas continuamente. Documentos colocados em uma pasta monitorada configurada são enviados e processados automaticamente, utilizando modelos e regras de automação predefinidos.

Essa funcionalidade viabiliza cenários de captura de documentos não assistida ou semiautomatizada, mantendo uma lógica de processamento consistente e o cumprimento das permissões definidas.

2.6 Cliente MFP

O Efflux MFP Client é um aplicativo embarcado, instalado em impressoras multifuncionais (MFPs) compatíveis, que permite aos usuários capturar documentos diretamente pelo painel do dispositivo. Após a autenticação, o cliente exibe os modelos acessíveis ao usuário conectado, com base nas permissões atribuídas.

Os usuários podem digitalizar documentos utilizando um modelo selecionado e enviá-los ao Efflux Cloud Capture para processamento. Os documentos capturados seguem o fluxo de trabalho configurado e associado ao modelo, garantindo consistência no processamento e no encaminhamento.

2.7 Armazenamento em nuvem

Como solução de armazenamento em nuvem de terceiros, o ECC oferece suporte a integrações com Google Drive, Dropbox, KCIM OneDrive e SharePoint Online. Ao estabelecer uma conexão com o seu armazenamento em nuvem, o ECC pode fazer o upload automático do documento processado para esse armazenamento.

2.8 Armazenamento ECC

Cada locatário dispõe de um armazenamento isolado de 10 GB, que pode ser utilizado para armazenar e baixar o documento processado.

3. Arquitetura multilocatário

O Efflux Cloud Capture foi projetado com uma **arquitetura de locatário dedicado (*dedicated-tenant*)** para garantir um alto nível de isolamento entre os clientes. Cada novo cliente recebe seu próprio ambiente de locatário, hospedado no Microsoft Azure.

Para cada locatário, é implantada uma **instância de servidor separada**, com **endereço IP** e **URL de serviço exclusivos**. Todo o processamento de documentos, acesso de usuários e execução de fluxos de trabalho ocorrem exclusivamente dentro do ambiente daquele locatário.

Os recursos de processamento **não são compartilhados entre locatários**. Cada locatário opera com serviços de computação, armazenamento e aplicação isolados, assegurando que o desempenho, a disponibilidade e a carga de trabalho de um locatário não afetem os de outro. Nenhum dado de documento, metadado, configuração ou recurso do sistema é acessível entre os limites dos locatários.

Essa arquitetura proporciona uma separação segura e robusta, desempenho previsível e conformidade simplificada, ao eliminar a exposição de dados entre locatários e impor um isolamento rigoroso no nível do locatário, tanto na camada de infraestrutura quanto na de aplicação.

4. Controle de Acesso Baseado em Funções (RBAC)

Efflux Cloud Capture implementa **o controle de acesso baseado em funções (RBAC)** em todos os portais e componentes do sistema. O acesso a funcionalidades e dados é determinado pela função atribuída ao usuário, garantindo que eles possam apenas visualizar ou realizar ações explicitamente permitidas dentro de seu escopo de responsabilidade.

O RBAC é aplicado de forma consistente no gerenciamento de *tenants*, no processamento de documentos e no acesso do cliente, a fim de manter a separação de segurança e a responsabilidade (*accountability*).

4.1 Matriz de Acesso de Gerenciamento

	Status da Licença	Status do Locatário	Usuários	Grupos de usuários	Azure Entra
Provedor Raiz (Suporte a Efluxo)	✓	✓	✓	✗	✗
Fornecedor (Parceiro / Revendedor)	✓	✓	✗	✗	✗
Locatário-Proprietário	✓	✓	✓	✓	✓

Notas:

- O acesso do provedor (nível Root) é limitado apenas a funções operacionais e de suporte.
- Os provedores podem visualizar o status do tenant e da licença, mas não podem gerenciar usuários do tenant nem a configuração de identidade.
- Os proprietários do tenant têm controle total sobre seu próprio tenant, incluindo a integração de identidade e o gerenciamento da estrutura de usuários.

4.2 Matriz de Acesso Funcional

Esta tabela define o acesso a recursos de captura, processamento e configuração de documentos com base nas funções do tenant.

Função	Upload	Status	Estatísticas	Uso de Recursos de Criação	Uso de Recursos	Cliente	Documentos Armazenados
Proprietário	Todos os modelos	Todos os usuários	Todos os usuários	✓	Todos	Todos	Todos
Administrador	Todos os modelos	Todos os usuários	Todos os usuários	✓	Todos	Todos	Todos
Usuário	Modelos atribuídos	Somente uploads próprios	Apenas estatísticas próprias	Se a permissão for concedida	Atribuído ou criado	Atribuído ou criado	Somente documento próprio

Notas:

- Proprietários de Tenant e Administradores de Tenant possuem visibilidade operacional equivalente, mas diferem quanto à autoridade administrativa, conforme definido pela política do tenant.
- Usuários Padrão de Tenant têm acesso restrito aos seus próprios documentos e aos recursos explicitamente atribuídos a eles.
- O acesso a modelos, conexões, cliente para desktop e cliente para MFP baseia-se em permissões e pode ser controlado por meio da atribuição a grupos de usuários.

5. Identificação e autenticação de usuários

Para acessar o Efflux Cloud Capture, os usuários devem fazer login utilizando uma conta verificada e ativa. Durante o cadastro, um e-mail de verificação é enviado para o endereço de e-mail registrado pelo usuário. A conta só se torna utilizável após a confirmação bem-sucedida do link de verificação contido no e-mail.

Apenas contas verificadas e ativas têm permissão para acessar o sistema. Contas não verificadas ou desativadas têm a autenticação negada e não conseguem acessar nenhum portal ou serviço.

Os Proprietários do Tenant podem desativar contas de usuário a qualquer momento. Assim que uma conta é desativada, o acesso ao Efflux Cloud Capture é imediatamente revogado, independentemente do status de autenticação anterior.

6. Política de Senhas

O Efflux Cloud Capture aplica uma política de senha para garantir um nível mínimo de segurança da conta. As senhas dos usuários devem atender aos seguintes requisitos:

- Comprimento mínimo de **8 caracteres**
- Pelo menos **uma letra maiúscula (A–Z)**
- Pelo menos **uma letra minúscula (a–z)**
- Pelo menos **um dígito numérico (0–9)**

Senhas que não atendem a esses requisitos são rejeitadas durante a criação ou a alteração da senha. Essa política ajuda a reduzir o risco de acesso não autorizado decorrente de credenciais fracas ou facilmente adivinháveis.

7. Logout automático e gerenciamento de sessão

O Efflux Cloud Capture implementa controles de logout automático e gerenciamento de sessões para reduzir o risco de acesso não autorizado decorrente de sessões deixadas sem supervisão ou persistentes.

Cada usuário pode visualizar suas sessões de login ativas por meio do portal web. A partir desse painel, os usuários podem encerrar sessões ativas remotamente, permitindo o logout imediato de outros navegadores, dispositivos ou clientes, caso necessário.

O comportamento de tempo limite da sessão varia de acordo com o tipo de cliente:

Cliente MFP
Os usuários são desconectados automaticamente após um período definido de inatividade no dispositivo. Isso evita o acesso não autorizado em ambientes de impressão compartilhados ou públicos.

Portal Web e Cliente Desktop
Quando a opção "**Manter-me conectado**" está ativada, a sessão permanece ativa por até **30 dias**, a menos que o usuário realize o logout manual ou a sessão seja revogada.

Quando essa opção não está ativada, os usuários são desconectados automaticamente após **3 horas de inatividade**.

As sessões também são encerradas imediatamente se a conta do usuário for desativada por um administrador do tenant ou se o usuário realizar uma ação de logout remoto.

Esses controles garantem uma segurança de sessão consistente em todos os pontos de acesso, equilibrando usabilidade e proteção para diferentes cenários de uso.

8. Autenticação por PIN

Efflux Cloud Capture oferece suporte à autenticação via PIN para login em MFPs, como alternativa à inserção padrão de credenciais no painel do dispositivo. A autenticação por PIN é utilizada exclusivamente para acesso à MFP e não pode ser usada para fazer login no portal da web ou no cliente para desktop.

A autenticação por PIN deve ser habilitada inicialmente pelo Proprietário do Tenant. Uma vez habilitada, os usuários podem gerar e gerenciar seus próprios PINs.

As seguintes regras se aplicam à autenticação por PIN:

- Os PINs podem conter de **6 a 10 dígitos numéricos**
- Os PINs são válidos por **três (3) meses** e devem ser regenerados após a expiração
- Os usuários podem excluir seu PIN a qualquer momento, desativando imediatamente o login baseado em PIN
- Os proprietários do tenant podem desativar a autenticação por PIN globalmente ou revogar o uso de PIN a qualquer momento
- As sessões de login baseadas em PIN são configuradas com uma duração mais curta para reduzir o risco de exposição em dispositivos multifuncionais (MFP) compartilhados

A autenticação por PIN foi projetada para proporcionar acesso rápido e conveniente em dispositivos multifuncionais, mantendo controles de segurança adequados para ambientes de dispositivos compartilhados.

9. Integração com o Microsoft Entra ID

O Efflux Cloud Capture oferece suporte à integração com o **Microsoft Entra ID** para permitir o gerenciamento centralizado de identidades e o logon único (SSO) para os usuários do tenant.

Para habilitar essa integração, o Proprietário do **Tenant deve primeiro conceder permissão** para que o Efflux Cloud Capture acesse o ambiente do Microsoft Entra ID de sua organização. Essa permissão permite que o Efflux Cloud Capture interaja com o Entra ID exclusivamente para fins de federação de identidades.

Após a concessão da permissão, o Proprietário do Tenant **pode importar usuários selecionados** do Microsoft Entra ID para o Efflux Cloud Capture. Quando um usuário importado pertence a um ou mais grupos de usuários no Entra ID, esses mesmos grupos são criados automaticamente no Efflux Cloud Capture e o usuário é associado a eles de acordo.

Uma vez adicionados, os usuários recebem uma notificação por e-mail e podem fazer login no Efflux Cloud Capture utilizando a opção de logon único "**Entrar com o Azure**" (Sign in with Azure).

O Efflux Cloud Capture **não acessa, armazena nem gerencia credenciais do Microsoft Entra ID**. A autenticação é realizada por meio de tokens de identidade seguros emitidos pelo Microsoft Entra ID. Em nenhum momento senhas de usuário ou credenciais de diretório são armazenadas na plataforma Efflux Cloud Capture.

O proprietário do locatário (Tenant Owner) pode **revogar o consentimento do Entra ID a qualquer momento**. Uma vez revogado o consentimento, os usuários não poderão mais se autenticar utilizando o logon único (SSO) do Azure.

10. Fluxo de autenticação e gerenciamento de tokens

O Efflux Cloud Capture utiliza uma **arquitetura de autenticação baseada em tokens** para gerenciar sessões de usuário de forma segura.

Quando os usuários se autenticam usando credenciais locais, o Efflux Cloud Capture emite um **JSON Web Token (JWT)** após a autenticação bem-sucedida. Esse token contém declarações (*claims*) de identidade e autorização do usuário e é necessário para solicitações subsequentes.

Quando a autenticação via Microsoft Entra ID é utilizada:

- O usuário é redirecionado para uma página de login controlada pela Microsoft.
- A autenticação é realizada inteiramente pelo Microsoft Entra ID.
- O Microsoft Entra ID retorna um token de identidade para o Efflux Cloud Capture.
- O Efflux Cloud Capture valida o token recebido.

Um token de acesso do ECC (JWT) de curta duração é gerado e emitido para o usuário.

O Efflux Cloud Capture não armazena credenciais do Microsoft Entra ID. Toda a autenticação é realizada utilizando tokens de identidade seguros.

Os tokens de acesso são emitidos com um **período de validade limitado**. Quando um token de acesso expira, um **mecanismo de renovação** é utilizado para obter um novo token sem exigir que o usuário insira novamente as credenciais, a menos que a sessão tenha sido revogada ou tenha expirado.

Todos os tokens são validados a cada solicitação. Tokens expirados ou inválidos são rejeitados, impedindo o acesso não autorizado.

Esse modelo baseado em tokens reduz o risco de exposição, limita o uso indevido da sessão e garante uma autenticação segura em todos os componentes do sistema.

11. Segurança de Rede e Isolamento de Serviços

O Efflux Cloud Capture é implantado no Microsoft Azure utilizando uma arquitetura baseada em contêineres.

Cada tenant é provisionado com um ambiente Kubernetes dedicado, isolado dos demais tenants nos níveis de rede e de aplicação.

Dentro de um ambiente de tenant:

- O serviço de **interface web (Web UI)** é disponibilizado por meio de um endpoint público seguro para acesso do usuário.
- O **serviço de mecanismo de processamento (Processing Engine)** não é acessível publicamente e só pode ser acessado internamente pela interface web.
- Bancos de dados e armazenamento de documentos são implantados na rede privada do *tenant* e não estão expostos a redes externas.
- Toda a comunicação entre serviços ocorre por meio de **redes internas privadas** e não é acessível a partir da internet pública.

Este projeto garante que componentes sensíveis, como serviços de processamento de documentos e sistemas de armazenamento, permaneçam protegidos contra acesso externo.

12. Proteção de Dados e Isolamento de Locatários

Todos os dados de clientes processados pelo Efflux Cloud Capture são armazenados no ambiente Azure dedicado do tenant.

Documentos, metadados e logs do sistema são mantidos em **armazenamento isolado por tenant** e não são compartilhados entre tenants.

O acesso a bancos de dados e ao armazenamento de documentos é restrito a serviços internos do ambiente do tenant. Nenhum sistema ou usuário externo pode acessar diretamente os dados armazenados.

Toda a comunicação entre serviços é protegida por meio de canais criptografados. O acesso aos dados é controlado via autorização em nível de aplicação e controle de acesso baseado em funções.

Essa arquitetura garante a confidencialidade, a integridade e o isolamento das informações dos clientes.

13. Registros de Log e Auditoria

Efflux Cloud Capture oferece recursos de registro de logs para dar suporte a auditoria, solução de problemas e monitoramento operacional.

Os seguintes logs estão disponíveis:

- **Logs de tarefas** que registram atividades de processamento de documentos são mantidos por **30 dias**.
- **Logs do mecanismo de processamento** podem ser habilitados pelo Administrador do Tenant. O nível de registro pode ser configurado de acordo com os requisitos operacionais.
- Logs de processamento são mantidos por até **um (1) ano** e armazenados de forma segura no armazenamento isolado do tenant.

Apenas administradores autorizados do tenant podem acessar e baixar os logs. Os logs não são compartilhados entre tenants e não podem ser acessados por outras organizações.

Esses logs proporcionam rastreabilidade da atividade do sistema, mantendo, ao mesmo tempo, o rigoroso isolamento entre tenants.

efflux solutions

bps@efflux-solutions.com
efflux-solutions.com

Europe
South Africa
Asia