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:
Security White Paper.

Whitepaper
Ver. 1.0
January, 2026

Contents

1. System Overview 3

2. Introduction: The Evolving Landscape of Document Processing 3
2.1 Root Provider Portal 4
2.2 Provider Portal 4
2.3 Tenant Owner Portal 5
2.4 User Portal 5
2.5 Desktop Client 6
2.6 MFP Client 6
2.7 Cloud Storage 6
2.8 ECC Storage 6

3. Multitenancy Architecture 7

4. Role-Based Access Control (RBAC) 8
4.1 Management Access Matrix 8
4.2 Functional Access Matrix 9

5. User Identification and Authentication 10

6. Password Policy 10

7. Automatic Logout and Session Management 11
MFP Client 11
Web Portal and Desktop Client 11

8. PIN Authentication 12

9. Microsoft Entra ID Integration 13

10. Authentication Flow and Token Management 14

11. Network Security and Service Isolation 15

12. Data Protection and Tenant Isolation 15

13. Logging and Audit Records 16

1. System Overview

Efflux Cloud Capture is a cloud-based document capture solution that enables organizations to securely collect, process, and route documents from multiple input sources. The platform supports a wide range of multi-functional printer (MFP) brands, a dedicated Windows client, and browser-based web uploads, allowing users to capture documents regardless of device or location. Administrators can centrally manage users, register supported devices, and configure capture workflows through a unified cloud interface.

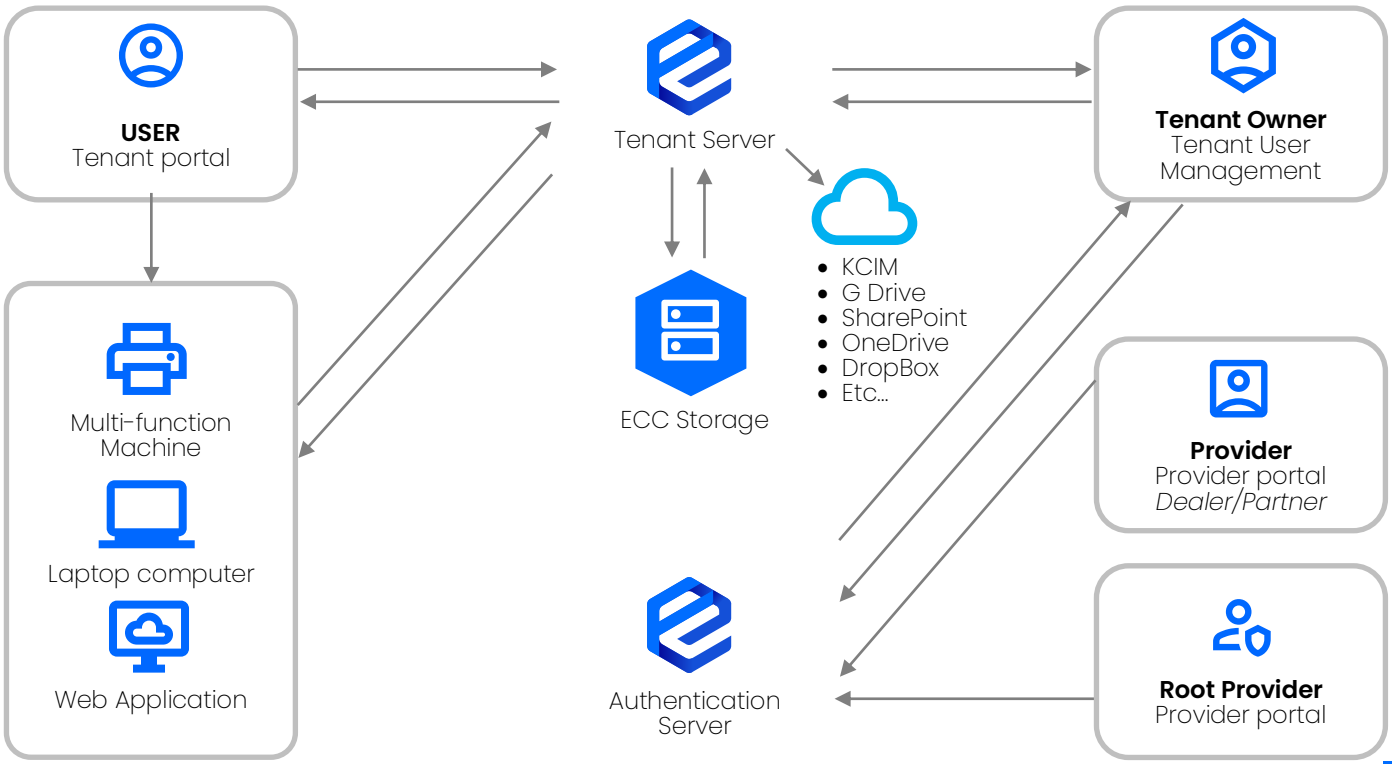
This white paper provides dealers and users with an overview of the security measures implemented in Efflux Cloud Capture. Protecting customer information and document data is a core design objective of the platform. All information assets handled by Efflux Cloud Capture are protected through secure system architecture, controlled configuration, and layered security mechanisms built into the service.

---

2. Introduction: The Evolving Landscape of Document Processing

Efflux Cloud Capture consists of the following component:

- **Root Provider Admin Panel**
- **Provider Portal (Partners and Dealers)**
- **Tenant Owner Portal**
- **User Portal**
- **Desktop Client**
- **MFP Client**
- **Cloud Storage Integrations**
- **Tenant Storage**



2.1 Root Provider Portal

The Root Provider Admin Panel is a secure, web-based administrative interface accessible only to authorized Efflux Solutions support personnel. It is used to operate, support, and govern the Efflux Cloud Capture platform and is not accessible to dealers, partners, or end customers.

Through the Admin Panel, Efflux support staff can manage tenant lifecycle operations, including pending tenant activations, verification of new organizations, and monitoring of active tenants. The system provides visibility into instance orders and license orders, allowing support teams to review, approve, and manage provisioning and renewals in a controlled manner.

The Admin Panel also supports centralized license management, partner and dealer administration, and administrative account management. Version management features allow Efflux support to control available software versions and assign or modify organization-specific versions as required.

All administrative functions are organized within a structured interface to ensure separation of responsibilities, traceability of actions, and secure platform operation.

2.2 Provider Portal

The Provider Portal is a web-based interface designed for partners and dealers to manage their customers and commercial interactions with Efflux Cloud Capture. Access to this portal is limited to authorized partner and dealer accounts and does not provide platform-level administrative control.

Through the Provider Portal, partners and dealers can submit new tenant creation requests and license renewal orders to Efflux Solutions. The portal provides visibility into historical orders and current order status, as well as the operational status of associated tenants, including activation state and license validity.

Role-based access controls define the scope of visibility and management capabilities:

- Partners can manage their dealer network by adding dealers under their account. They have visibility into all tenants and orders associated with both their own organization and their registered dealers.
- Dealers have restricted access and can view and manage only the tenants and orders associated with their own accounts.

This role separation ensures clear responsibility boundaries while enabling partners and dealers to efficiently manage customer onboarding and licensing activities.

2.3 Tenant Owner Portal

The Tenant Owner Portal is a web-based management interface used by tenant administrators to configure and operate their own Efflux Cloud Capture environment. Access is limited to authorized users within the tenant and does not provide visibility into other tenants or platform-level controls.

Through this portal, tenant owners and tenant administrators can manage users and access control within their organization. This includes creating and managing administrator and standard user accounts, defining user groups, and assigning permissions to those groups. The portal supports integration with Microsoft Azure Entra ID, allowing tenants to connect their directory service and import users into the platform.

The Tenant Owner Portal also provides operational visibility into the tenant environment. Administrators can monitor the status of their tenant services, review system logs sourced from the Azure-hosted tenant infrastructure, and perform basic operational checks.

Temporary user accounts can be created when required to support short-term access scenarios.

These capabilities allow tenants to maintain control over user access, identity integration, and operational oversight while remaining isolated from other tenants and the underlying Efflux platform administration.

2.4 User Portal

The User Portal is a web-based interface used by end users to perform day-to-day document capture and processing activities within Efflux Cloud Capture. Access to features is governed by user roles and assigned permissions.

Through the User Portal, users can upload documents for processing and track the status of submitted documents throughout the capture workflow. Based on their permissions, users can create, update, and delete templates, connections, and picklists used for document processing and routing.

Processed documents are made available through the download section of the portal, where users can securely access and retrieve completed outputs. Visibility is restricted to documents associated with the user's tenant and permissions, ensuring isolation between users and organizations.

2.5 Desktop Client

The Efflux Desktop Client is a Windows-based application that enables users to capture and upload documents directly from their workstation. After login, the client loads and displays the templates that are accessible to the user based on their assigned permissions.

Users can select a template and upload documents for processing through the configured capture workflow. The desktop client also supports hot folder functionality, allowing users to define local folders that are continuously monitored. Documents placed into a configured hot folder are automatically uploaded and processed using predefined templates and automation rules.

This capability enables unattended or semi-automated document capture scenarios while maintaining consistent processing logic and permission enforcement.

2.6 MFP Client

The Efflux MFP Client is an embedded application installed on supported multi-functional printers (MFPs) that enables users to capture documents directly from the device panel. After user authentication, the client displays the templates that are accessible to the logged-in user based on assigned permissions.

Users can scan documents using a selected template and submit them to Efflux Cloud Capture for processing. The captured documents follow the configured workflow associated with the template, ensuring consistent processing and routing.

2.7 Cloud Storage

As third-party cloud storage, ECC supports integrations with Google Drive, Drop Box, KCIM OneDrive, and SharePoint Online. By creating a connection to your cloud storage, ECC can upload the processed document to the cloud storage automatically.

2.8 ECC Storage

Each tenant is provided with an isolated storage of 10GB that can be used to store and download the processed document.

3. Multitenancy Architecture

Efflux Cloud Capture is designed using a **dedicated-tenant architecture** to ensure strong isolation between customers. Each new customer is provisioned with their **own tenant environment** hosted on Microsoft Azure.

For every tenant, a **separate server instance** is deployed with its own assigned **IP address** and **unique service URL**. All document processing, user access, and workflow execution occur exclusively within that tenant's environment.

Processing resources **are not shared between tenants**. Each tenant operates with isolated compute, storage, and application services, ensuring that performance, availability, and workload activity of one tenant cannot impact another. No document data, metadata, configuration, or system resources are accessible across tenant boundaries.

This architecture provides strong security separation, predictable performance, and simplified compliance by eliminating cross-tenant data exposure and enforcing strict tenant-level isolation at the infrastructure and application layers.

4. Role-Based Access Control (RBAC)

Efflux Cloud Capture enforces **role-based access control (RBAC)** across all portals and system components. Access to functions and data is determined by the user's assigned role, ensuring that users can only view or perform actions explicitly permitted within their scope of responsibility.

RBAC is applied consistently across tenant management, document processing, and client access to maintain security separation and accountability.

4.1 Management Access Matrix

	License Status	Tenant Status	Users	User Groups	Azure Entra
Root Provider (Efflux Support)	✓	✓	✓	✗	✗
Provider (Partner / Dealer)	✓	✓	✗	✗	✗
Tenant Owner	✓	✓	✓	✓	✓

Notes:

- Root Provider access is limited to operational and support functions only.
- Providers can view tenant and license status but cannot manage tenant users or identity configuration.
- Tenant Owners have full control within their own tenant, including identity integration and user structure management.

4.2 Functional Access Matrix

This table defines access to document capture, processing, and configuration features based on tenant roles.

Role	Upload	Status	Statistics	Resource Creation	Resource Usage	Client	Stored Documents
Owner	All templates	All users	All users	✓	All	All	All
Admin	All templates	All users	All users	✓	All	All	All
User	Assigned templates	Only own uploads	Only own statistics	If permission is granted	Assigned or created	Assigned or created	Only own document

Notes:

- Tenant Owners and Tenant Admins have equivalent operational visibility but differ in administrative authority as defined by tenant policy.
- Standard Tenant Users are restricted to their own documents and explicitly assigned resources.
- Access to templates, connections, desktop client, and MFP client is permission-based and can be controlled through user group assignments.

5. User Identification and Authentication

When accessing Efflux Cloud Capture, users must log in using a verified and active account. During user registration, a verification email is sent to the user's registered email address. The account becomes usable only after the verification link in the email has been successfully confirmed.

Only verified and active accounts are permitted to access the system. Unverified or deactivated accounts are denied authentication and cannot access any portal or service.

Tenant Owners can deactivate user accounts at any time. Once an account is deactivated, access to Efflux Cloud Capture is immediately revoked, regardless of previous authentication status.

6. Password Policy

Efflux Cloud Capture enforces a password policy to ensure a minimum level of account security. User passwords must meet the following requirements:

- Minimum length of **8 characters**
- At least **one uppercase letter (A–Z)**
- At least **one lowercase letter (a–z)**
- At least **one numeric digit (0–9)**

Passwords that do not meet these requirements are rejected during creation or password change. This policy helps reduce the risk of unauthorized access caused by weak or easily guessable credentials.

7. Automatic Logout and Session Management

Efflux Cloud Capture implements automatic logout and session management controls to reduce the risk of unauthorized access caused by unattended or persistent sessions.

Each user can view their active login sessions through the web portal. From this panel, users are able to remotely terminate active sessions, allowing immediate logout from other browsers, devices, or clients if required.

Session timeout behavior varies by client type:

MFP Client
Users are automatically logged out after a defined period of inactivity at the device. This prevents unauthorized access in shared or public printer environments.

Web Portal and Desktop Client
When **"Keep me logged in"** is enabled, the session remains active for up to **30 days** unless manually logged out or revoked.

When the option is not enabled, users are automatically logged out after **3 hours of inactivity**.

Sessions are also terminated immediately if a user account is deactivated by a tenant administrator or if the user performs a remote logout action.

These controls ensure consistent session security across all access points while balancing usability and protection for different usage scenarios.

8. PIN Authentication

Efflux Cloud Capture supports PIN-based authentication for MFP login as an alternative to standard credential entry at the device panel. PIN authentication is used exclusively for MFP access and cannot be used to log in to the web portal or desktop client.

PIN authentication must first be enabled by the Tenant Owner. Once enabled, users are allowed to generate and manage their own PINs.

The following rules apply to PIN authentication:

- PINs can contain **6 to 10 numeric digits**
- PINs are valid for **three (3) months** and must be regenerated after expiration
- Users may delete their PIN at any time, immediately disabling PIN-based login
- Tenant Owners can disable PIN authentication globally or revoke PIN usage at any time
- PIN-based login sessions are configured with a shorter session duration to reduce exposure risk on shared MFP devices

PIN authentication is designed to provide fast and convenient access at MFPs while maintaining appropriate security controls for shared-device environments.

9. Microsoft Entra ID Integration

Efflux Cloud Capture supports integration with **Microsoft Entra ID** to enable centralized identity management and single sign-on (SSO) for tenant users.

To enable this integration, the **Tenant Owner must first provide consent** for Efflux Cloud Capture to access their organization's Microsoft Entra ID environment. This consent allows Efflux Cloud Capture to interact with Entra ID for identity federation purposes only.

After consent is granted, the Tenant Owner can **import selected users** from Microsoft Entra ID into Efflux Cloud Capture. When an imported user belongs to one or more user groups in Entra ID, the same groups are automatically created within Efflux Cloud Capture and the user is assigned accordingly.

Once added, users receive an email notification and can log in to Efflux Cloud Capture using the **"Sign in with Azure"** single sign-on option.

Efflux Cloud Capture **does not access, store, or manage Microsoft Entra ID credentials**. Authentication is performed using secure identity tokens issued by Microsoft Entra ID. At no time are user passwords or directory credentials stored within the Efflux Cloud Capture platform.

The Tenant Owner may **revoke Entra ID consent at any time**. Once consent is revoked, users will no longer be able to authenticate using Azure single sign-on.

10. Authentication Flow and Token Management

Efflux Cloud Capture uses a **token-based authentication architecture** to securely manage user sessions.

When users authenticate using local credentials, Efflux Cloud Capture issues a **JSON Web Token (JWT)** after successful authentication. This token contains user identity and authorization claims and is required for subsequent requests.

When Microsoft Entra ID authentication is used:

- The user is redirected to a Microsoft-controlled login page.
- Authentication is performed entirely by Microsoft Entra ID.
- Microsoft Entra ID returns an identity token to Efflux Cloud Capture.
- Efflux Cloud Capture validates the received token.

A short-lived ECC access token (JWT) is generated and issued to the user.

Efflux Cloud Capture does not store Microsoft Entra ID credentials. All authentication is performed using secure identity tokens.

Access tokens are issued with a **limited validity period**. When an access token expires, a **refresh mechanism** is used to obtain a new token without requiring the user to re-enter credentials, unless the session has been revoked or expired.

All tokens are validated on every request. Expired or invalid tokens are rejected, preventing unauthorized access.

This token-based model reduces exposure risk, limits session misuse, and ensures secure authentication across all system components.

11. Network Security and Service Isolation

Efflux Cloud Capture is deployed on Microsoft Azure using a container-based architecture.

Each tenant is provisioned with a dedicated Kubernetes environment, isolated from other tenants at the network and application levels.

Within a tenant environment:

- The **Web UI service** is exposed through a secured public endpoint for user access.
- The **Processing Engine service** is not publicly accessible and can only be reached internally by the Web UI.
- Databases and document storage are deployed within the tenant's private network and are not exposed to external networks.
- All inter-service communication occurs over **private internal networks** and is not reachable from the public internet.

This design ensures that sensitive components such as document processing services and storage systems remain protected from external access.

12. Data Protection and Tenant Isolation

All customer data processed by Efflux Cloud Capture is stored within the tenant's dedicated Azure environment.

Documents, metadata, and system logs are maintained in **tenant-isolated storage** and are not shared between tenants.

Access to databases and document storage is restricted to internal services within the tenant environment. No external systems or users can directly access stored data.

All communication between services is secured using encrypted channels. Access to data is controlled through application-level authorization and role-based access control.

This architecture ensures confidentiality, integrity, and isolation of customer information.

13. Logging and Audit Records

Efflux Cloud Capture provides logging capabilities to support auditing, troubleshooting, and operational monitoring.

The following logs are available:

- **Job logs** recording document processing activities are retained for **30 days**.
- **Processing engine logs** can be enabled by the Tenant Administrator. The logging level can be configured based on operational requirements.
- Processing logs are retained for up to **one (1) year** and stored securely within the tenant's isolated storage.

Only authorized tenant administrators can access and download logs. Logs are not shared across tenants and cannot be accessed by other organizations.

These logs provide traceability of system activity while maintaining strict tenant isolation.

efflux solutions

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

Europe
South Africa
Asia