e-BRIDGE Cloud Workflow

TOSHIBA

END-TO-END SECURITY

e-BRIDGE Cloud Workflow

September 2026

Revised v1.2.1

TOSHIBA

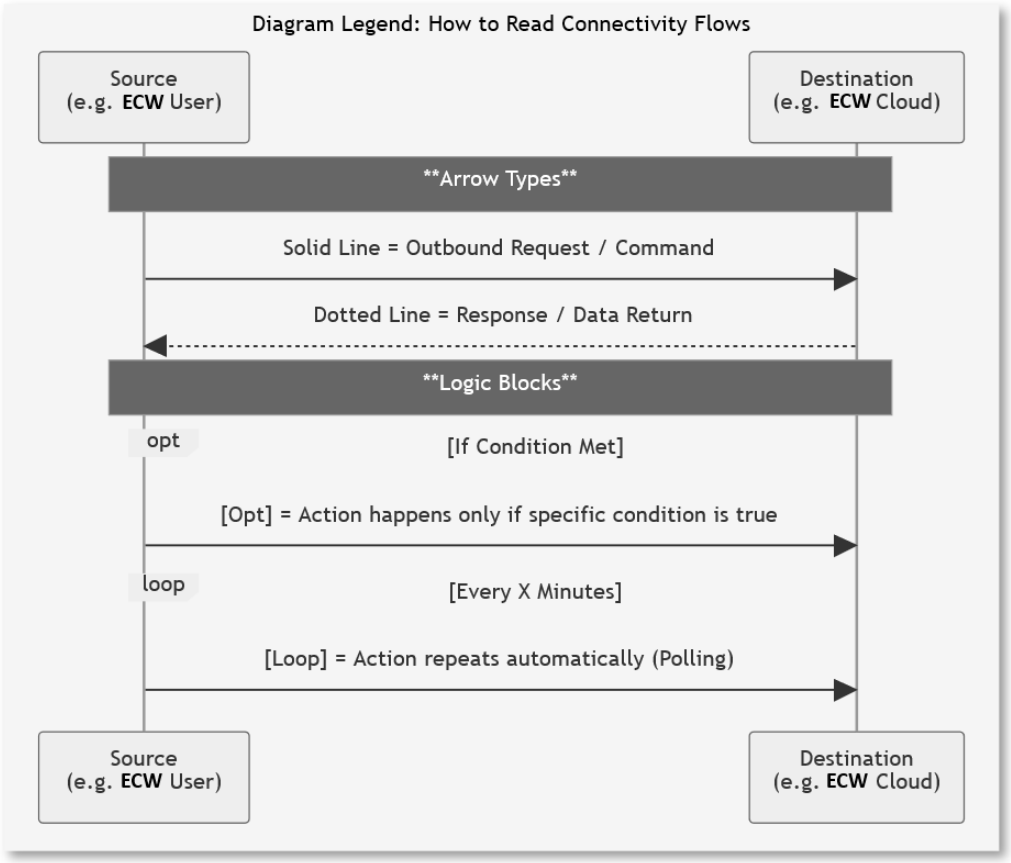
How to use this paper.

This white paper provides an overview of the security features built into Toshiba MFPs and e-BRIDGE Cloud Workflow (ECW), helping answer common IT and compliance-related questions.

Let's keep your data protected—*at every step*.

How to read security sequence diagrams in this paper.

This white paper provides detailed security data flows that depict how data is safeguarded between users sharing data artifacts, data scanned at Toshiba MFPs, and data managed within e-BRIDGE Cloud Workflow (ECW), ensuring that data is secured end-to-end. The following ledger will assist the reader in interpreting security data sequence diagrams.



Let's keep your data protected—*at every step*.

Table of Contents

Preface

Securing applications used for **data acquisition** ensures that sensitive data, including personally identifiable information (PII), remain protected from unauthorised access, breaches, and cyber threats. Strong encryption, access controls, and secure transmission protocols safeguard data both in transit and at rest, while maintaining compliance with industry standards. **For customers, secure multi-function printer (MFP) applications provide peace of mind** by preventing data leaks, ensuring document integrity, and protecting confidential business information. In general, MFP security enhances trust, reduces risk, and supports compliance, making it essential for organisations handling sensitive documents.

1.1 Before Reading This Document

Disclaimer: The information provided in this document is intended solely for informational and educational purposes. It is not designed to serve as a definitive security architecture, nor should it be relied upon for establishing formal security requirements, compliance frameworks, or risk management strategies. While every effort has been made to ensure accuracy, security best practices continuously evolve. Organisations should conduct independent assessments, consult with qualified security professionals, and tailor solutions to their specific operational and regulatory needs. The guidance presented herein does not constitute a guarantee of security and should be interpreted as a general description of features and recommendations, rather than prescriptive measures.

1.1.1 Considerations and Limitations

- Consumers of the ECW product should institute their own safeguards to further harden security.
- The utilisation and monitoring of security logs will serve as complementary best practices for ECW and any service-based application.
- ECW Administrator/User roles are implemented as Role Based Access Control (RBAC), rather than Attribute Based Access Control (ABAC) commonly applied within Identity and Access Management (IAM) implementations.
- ECW or affiliate partners such as AWS do not provide compliance guarantees. The responsibility for security best practices always resides with the customer and end-user.
- Some features described are either not available or supported in every market please check with your local Toshiba representative.

1.2 General Use Cases

ECW is designed as a hub-and-spoke architecture, with the hub representing a cloud solution and the spokes representing client-functioning embedded applications.

- An administrator manages a company within the administrative dashboard and grants access to individuals authorised to utilise ECW. The administrator may also be responsible for establishing document templates, which individuals within the company use to perform workflow activities based on template data.
- The end-user accesses ECW by entering their credentials to launch the application. Additional login options, such as PIN authentication, may be enabled at the enterprise level (rather than configured on individual MFDs). Users can update their access PIN at any time. Once logged in, the user uploads documents, triggering a data acquisition process that supports data-driven workflows.

ECW supports two primary use cases.

- In the first use case, an end-user uploads a source document directly to the MFP. A limited amount of data processing takes place on the device via the embedded ECW application and its Integrated Platform. The data is encrypted and sent to a cloud-based instance of the Integrated Platform, where full processing and job execution occur.
- In the second use case, the data originates from external connected sources rather than the MFP. Similar to the first use case, the data is encrypted and sent to the cloud-based platform for processing and job execution.

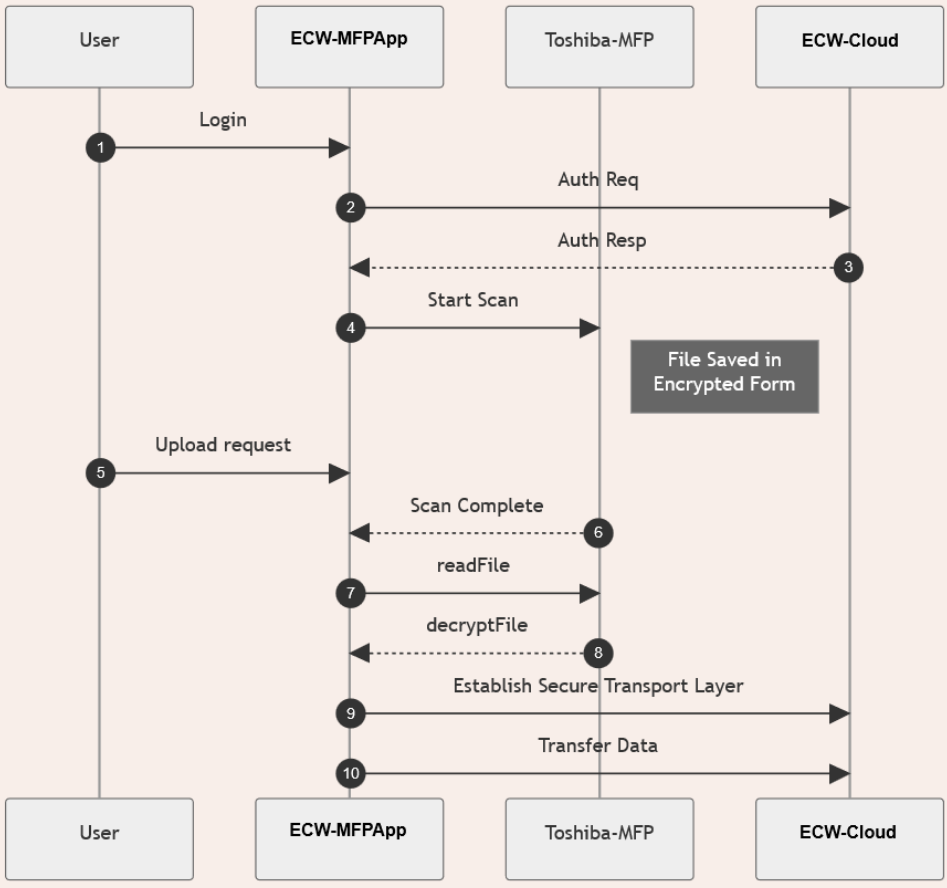


Figure 1: ECW data sequence depicting data from source to cloud

1.3 Data Chain: Data Captured at the MFP (Representative Functions)

1.3.1 Secure Data Chain at the MFP

The Toshiba MFP performs a capture function (*GetData)* in which a scan process initiates the scan of a document. Some basic functions that follow the *GetData* function include managing document lighting (*ManageDocLighting*), managing document color (*ManageDocColor),* and others before performing an analog-to-digital conversion (*ConvertToDigital*) of the source document.

Data captured at the MFP is temporarily stored in nonvolatile memory (*StoreToBuffer).* Native Toshiba MFP logic identifies the logical location (*MapLogicalAddress*) where the data is temporarily stored. The disk volume is verified (*IdentifyDisk*) as a target location where the temporary data will be stored. The available storage space is verified (*DiskSpaceValidation*) to ensure temporary storage retention.

Disk space is allocated (*DiskSpaceAllocated*) on the encrypted disk of the Toshiba MFP. The I/O controller of the Toshiba MFP transports the temporary data (*I/OdataTransport*) from nonvolatile memory to the Toshiba encrypted disk (volatile memory). The Toshiba encrypted disk automates an encrypted key retrieval (*EncryptedKeyRetrieval*) process to encrypt the data at rest. The plain text of the source document is automatically encrypted (*EncryptData*) on the Toshiba encrypted disk. Upon encryption of the data, buffers that contained the temporary data are flushed (*FlushMFPBuffer*).

The ECW app sends a transport request (*IPtransportRequest*) with the intent of moving data originating at the Toshiba MFP to the ECW cloud. The request from the ECW app begins a decryption process (*MFPosDataDecrypt*) in which the encrypted data is converted back to plain text before transport. The ECW app establishes a secure transport via Transport Layer Security (TLS) v1.2 between the Toshiba MFP and the ECW cloud, ensuring the complete security of data, while encrypting data-in-transit to the ECW cloud (*CloudDataStore*).

e-BRIDGE Cloud Workflow – Product Overview

e-BRIDGE Cloud Workflow (ECW) is a cloud service that automatically ingests documents obtained from a multi-function printer (MFP), personal computer (PC), and a mobile device with various business applications.

2.1 Operation & Management

ECW operates on AWS® (Amazon Web Services) hosted in Australia, leveraging a trusted and robust security infrastructure that complies with globally recognised standards, including ISO/IEC 27001 for Information Security Management, ISO/IEC 27017 for cloud service security, and ISO/IEC 27018 for the protection of personally identifiable information (PII) in the cloud. Additionally, AWS® meets SOC1, SOC2, and SOC3 requirements, ensuring adherence to strict controls over data confidentiality, integrity, and availability. These certifications validate that the underlying infrastructure behind ECW is designed and maintained with best-in-class security measures.

To further strengthen system security, ECW undergoes rigorous and comprehensive vulnerability audits both before release and on an ongoing basis. These assessments include automated vulnerability scans, manual penetration testing, and the remediation of any identified risks to ensure a secure operating environment. This proactive approach helps mitigate potential threats while maintaining compliance with evolving security standards, delivering a highly secure and reliable platform for users.

e-BRIDGE Cloud Workflow – Security

Ensuring security and data integrity throughout the lifecycle of a workflow is critical in any system. This document outlines key security aspects across access control, identification, data acquisition, data structuring, and data sharing, each playing a vital role in protecting sensitive information and maintaining compliance.

Access Control	Establishing and enforcing role-based and attribute-based permissions ensures that only authorised users can perform specific actions, reducing the risk of unauthorised access or privilege misuse.
Identification	Secure authentication mechanisms, including token-based verification, help validate user identities and prevent unauthorised entry.
Data Acquisition	Protecting data at the point of collection is essential; secure transmission protocols (e.g., TLS encryption) and validation processes ensure data integrity from its source.
Data Structuring	Organising and securely storing data received from scans, as well as storing data securely using encryption, access policies, and structured formats, enhances data protection and prevents unauthorised modifications.
Data Sharing	Secure integration with external services requires API security and controlled data access to prevent data leaks and unauthorised sharing.

ECW addresses security principles, utilises security-centric design to mitigate risks, ensures data confidentiality, and maintains trust by delivering a secure workflow solution.

3.1 Access Controls and Authentication

ECW enforces strong security by requiring user login, ensuring that only authorised individuals can access the ECW platform. Validation is required as part of company registration, which ensures entitlement compliance and restricts usage to legitimate users. ECW allows integration with services like Google™ and Microsoft®, while requiring separate credentials with secure authentication methods (e.g., OAuth 2.0) to ensure data ingress/egress requests are granted only to approved accounts. The ECW access controls and authentication measures uphold data integrity, prevent unauthorised access, and enable fine-grained controls tailored to ECW users.

ECW security provides safeguards in four (4) core areas of the document workflow.

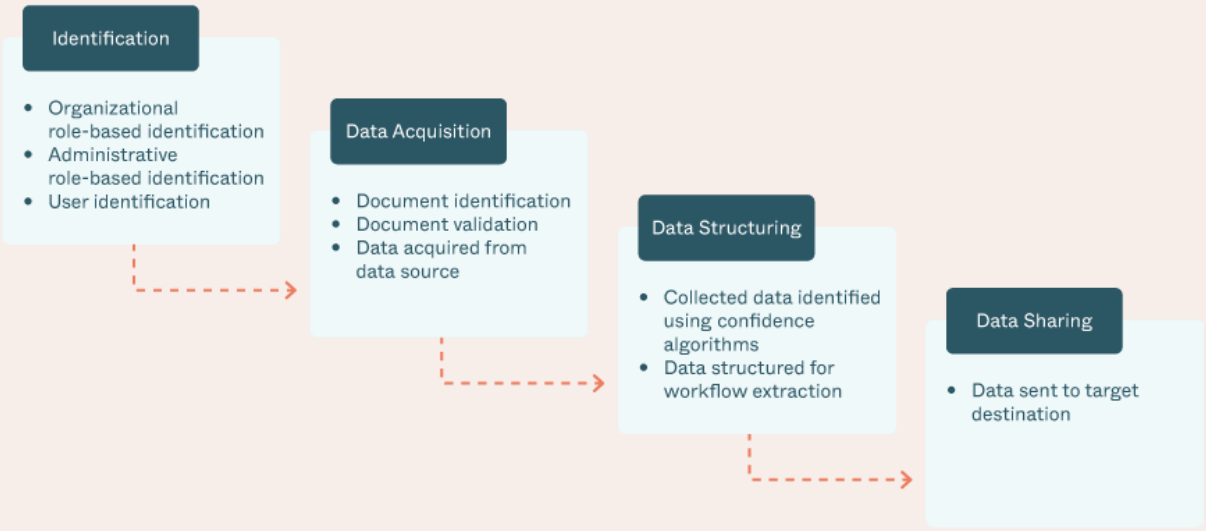


Figure 3: ECW Data Flow

3.2 Identification

ECW performs secure user interaction between the user and the ECW cloud, then verifies access using backend processing.

Secured User Interaction

ECW provides a secure web portal that enables users to manage their data workflows and gives administrators the tools to oversee business activities. Users log in through a branded, ECW- specific interface using their email and password. The connection between the user and the ECW service is established over HTTPS (Hyper Text Transfer Protocol Secure), ensuring a secure communication channel. All data transmitted is encrypted using Transport Layer Security (TLS) version 1.2, protecting it from unauthorised access, and ensuring confidentiality during transmission.

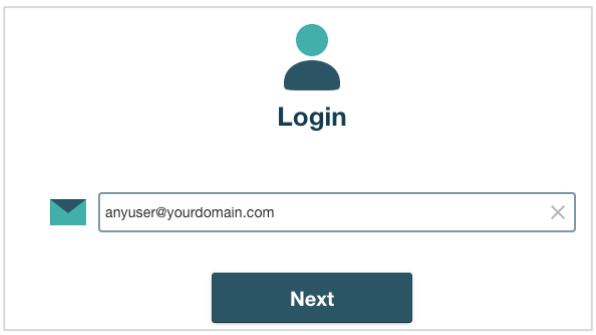


Figure 4: ECW login prompt / login data entry

3.2.1 Backend Verification

ECW leverages a robust user pool authentication system to provide secure, fine-grained access control. By utilising backend attributes and token claims, ECW ensures modern, scalable authentication that protects user data and system integrity.

- ECW user credentials are validated against a managed user pool
- Federated users are validated against the respective Identity Provider (IdP) (e.g., Microsoft®, Google™)
- ECW support for federated identities maps external identities to ECW

Credential Management

Prior to the ECW backend performing verification, ECW users provide the appropriate credentials via the web portal. The credentials provided by ECW users are hashed using hashing algorithms (e.g., bcrypt or equivalent) during the login request, then encrypted using TLS 1.2.

Token-Based Security

Upon successful authentication of the ECW user via credential management, token-based security is utilised in the form of three (3) JSON Web Tokens (JWT):

- **ID Token:** Contains ECW user information such as an email address
- **Access Token:** Used to authorise various API calls
- **Refresh Token:** Used to obtain new tokens without requiring reauthentication

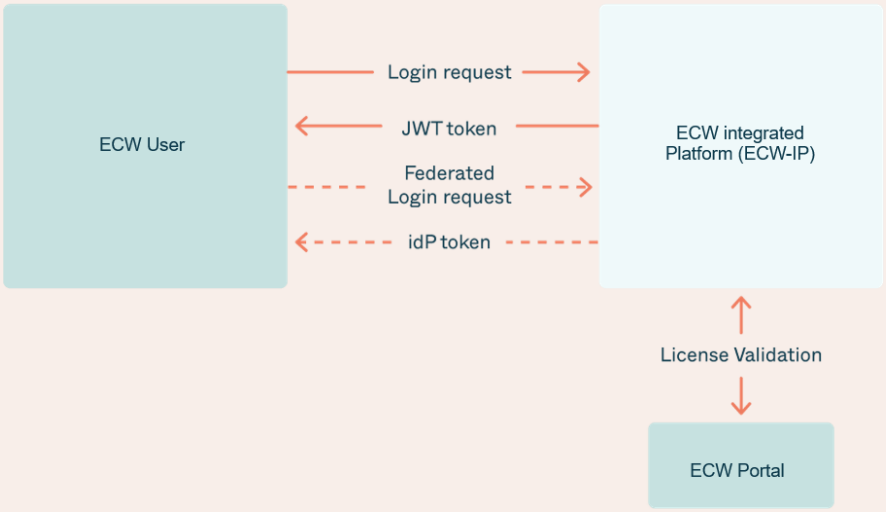


Figure 5: ECW identification & authorisation block diagram

3.3 Data Acquisition

ECW cloud services are accessed directly from Toshiba MFPs through the installed ECW embedded application. When launched from the MFP control panel, the embedded application functions as a client application of the ECW cloud. The ECW services running on the MFP, via the embedded application, securely connect to the ECW cloud using standardised protocols (e.g., HTTPS, OAuth 2.0).

Once initiated, the application facilitates data acquisition from source documents and begins data processing in the ECW cloud environment. To access the service, users must enter their unique PIN, which is authenticated against ECW's cloud-based identity service. Upon successful verification, the MFP receives an OAuth 2.0 access token, enabling the user to securely utilise ECW functionality from the device.

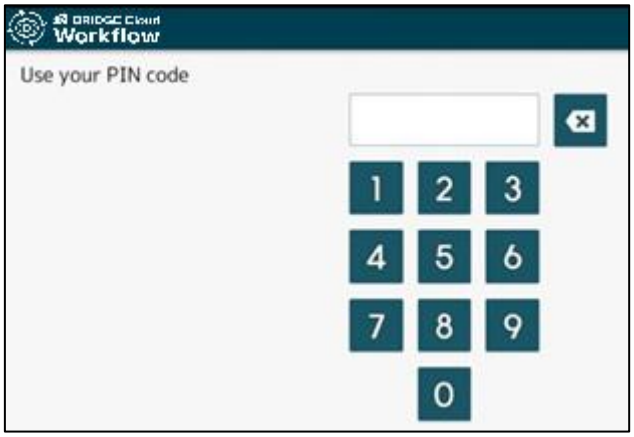


Figure 6: ECW PIN login from MFP

ECW enforces role-based access control at the MFP to ensure that only authenticated users can retrieve or manage scanned data. When a document is scanned, the acquired data is temporarily stored on the device before being securely transmitted to the ECW cloud. There, it is routed to integrated systems for OCR processing. Because OCR is not performed locally on the MFP, the risk of exposing sensitive data at the device level is significantly reduced, enhancing overall data security.

3.3.1 Audit Logging

ECW continues to strengthen its security framework through the application of additional data acquisition features, primarily facilitated by a robust audit logging system. The importance of comprehensive audit logging cannot be overstated; audit logging is a cornerstone of a secure digital environment, creating a detailed and immutable record of all significant user and system activities. From a security perspective, the advantage of audit logging includes complete traceability, which is invaluable for forensic analysis during an incident investigation and for proactively detecting anomalous behaviour.

Figure 7: Detailed audit log of user transactions

As a best effort to ensure a comprehensive and meaningful transaction record, ECW audit logging operations capture key data points for each event, including the user's ID, email address, a precise timestamp, and the source IP address. This data creates an indisputable digital trail that answers the crucial questions of 'who, what, when, and where,' which is essential for both security and accountability. Audit logging enables organisations to rapidly investigate potential threats, while deterring policy violations by ensuring that all actions are attributable to a specific source.

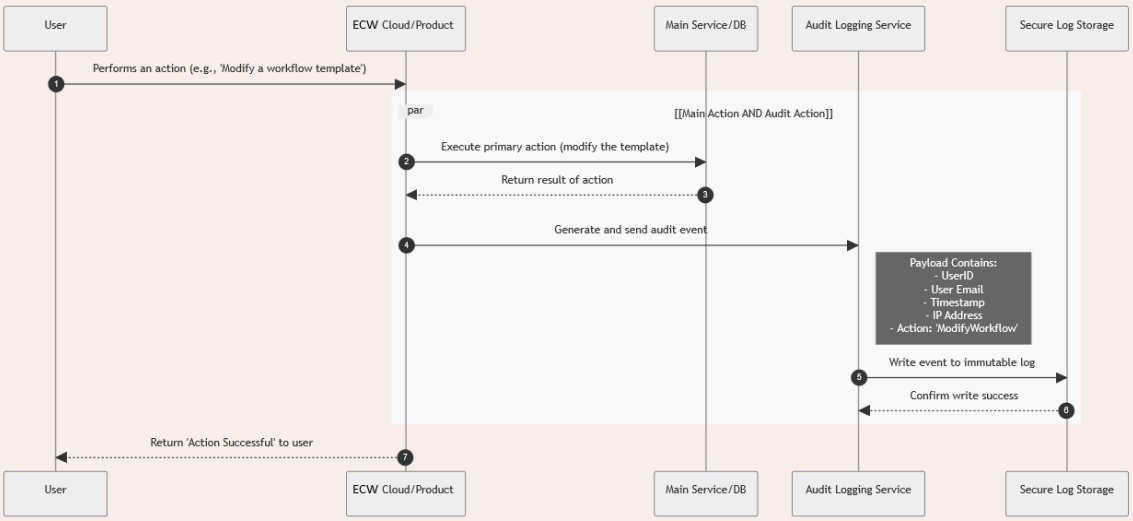


Figure 8: Data capture sequence of ECW audit logging

3.4 Data Structuring

Once data is captured through ECW, it is parsed into logical groupings and stored in secure cloud environments. Access to this data is tightly controlled, ensuring that only authorised entities can interact with it.

Within the ECW portal, only the processed and analysed OCR output—such as extracted text and confidence scores—is displayed. Fully scanned documents are not exposed, reducing the visibility of sensitive information and ensuring that only essential data is presented to the user.

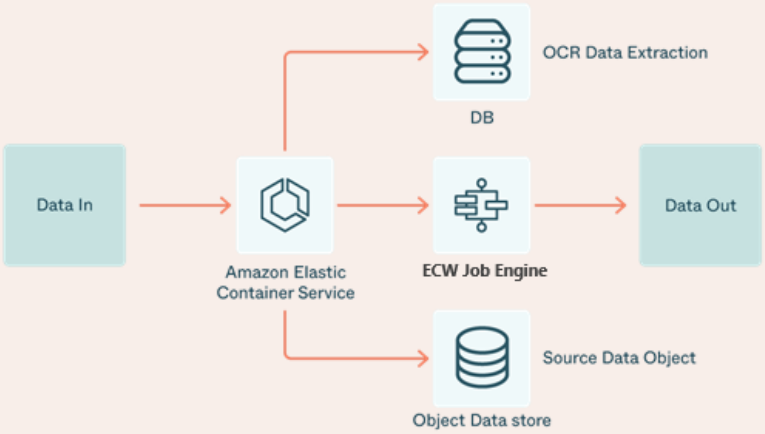


Figure 9: Abbreviated view of the ECW Data Store Environment

3.5 Data Sharing

ECW supports integration with external services through two built-in connectors: the "Popular Cloud Connector" and the "Internet Platform as a Service (iPaaS) Connector."

- The **Popular Cloud Connector** enables secure connections to widely used data storage services such as Google Drive™, Dropbox®, SharePoint®, OneDrive®, and Box™. These integrations leverage OAuth 2.0 for use cases such as document retrieval.
- Similarly, **the iPaaS Connector** supports workflow automation by connecting to services like Make.com and Zapier®, allowing seamless interaction with various third-party platforms.

Before any connection is made, ECW users must grant explicit consent for selected third-party service. Once approved, ECW retrieves access tokens—never user credentials—to authorise API calls securely, maintaining strong data protection and user privacy.

When data is shared with external services or automation platforms, ECW ensures security through robust encryption protocols—both in transit (e.g., HTTPS, TLS) and at rest. Access is restricted through strong authentication methods such as OAuth or API keys, ensuring only authorised users and systems can interact with the data. Additionally, secure integration with external services and automation tools includes endpoint validation, limiting data exposure, and applying the principle of least privilege to limit access only to data necessary for the workflow.

3.5.1 Document Classifier with Artificial Intelligence

As part of a continued focus on enhancing the user experience, ECW incorporates Artificial Intelligence (AI) in the form of backstage services that function as a cognitive layer for document workflows. This intelligence is engineered to automatically detect document types upon ingestion, interpreting content and structure to dynamically associate the correct attributes and metadata. This approach automates what is traditionally a labor-intensive process, requiring significant computational analysis given the sophistication of intelligent document classification. To achieve this, document data—including associated metadata and OCR text—is securely transmitted for processing to a specialised, top-tier external cloud service.

Uniquely, ECW utilises "Transfer Learning" to offer an optional, isolated training service. This creates a powerful, tenant-specific feedback loop. When enabled, the system uses patterns from your documents to calibrate a private custom model, enabling ECW to recognise your organisation's unique document types with increasing accuracy. This ensures that your data trains only your dedicated model instance and is **never used to retrain the global base model**.

For example, if a user shares several similar documents, the AI infrastructure learns that unique structure and updates your private definition to automatically align attributes on future submissions. Security throughout this lifecycle is paramount: all data is strictly confined to your ECW subscription boundary and protected with end-to-end encryption, utilising industry-leading protocols such as TLS 1.3 for data in transit and AES-256 for data at rest.

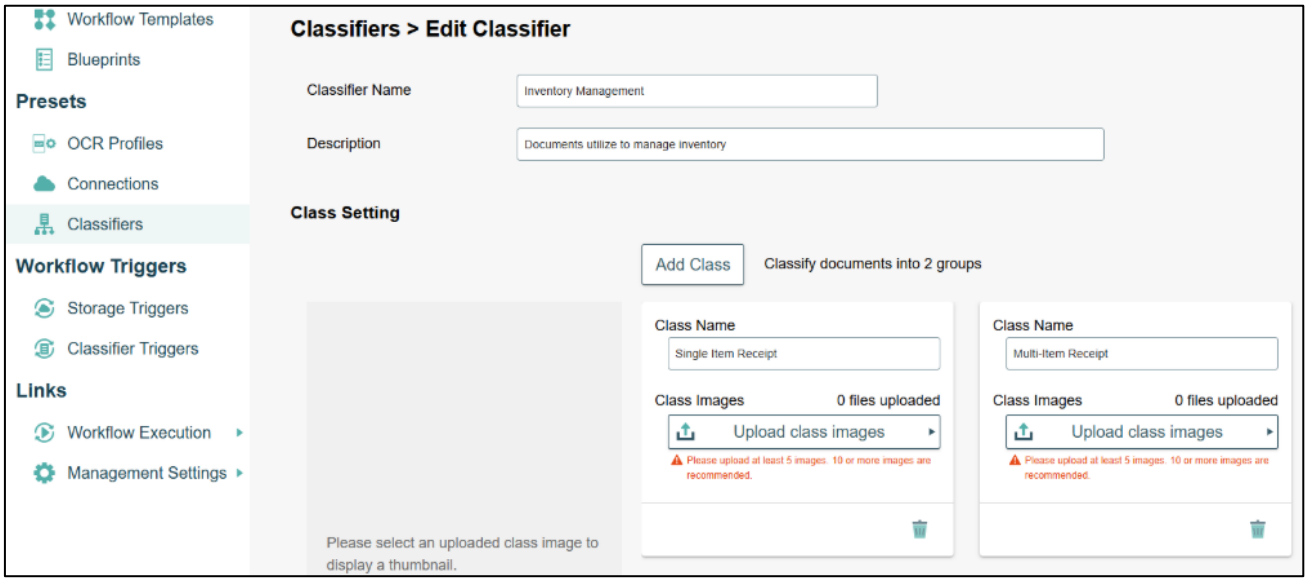


Figure 10: ECW's AI-driven classifier, data collection feature

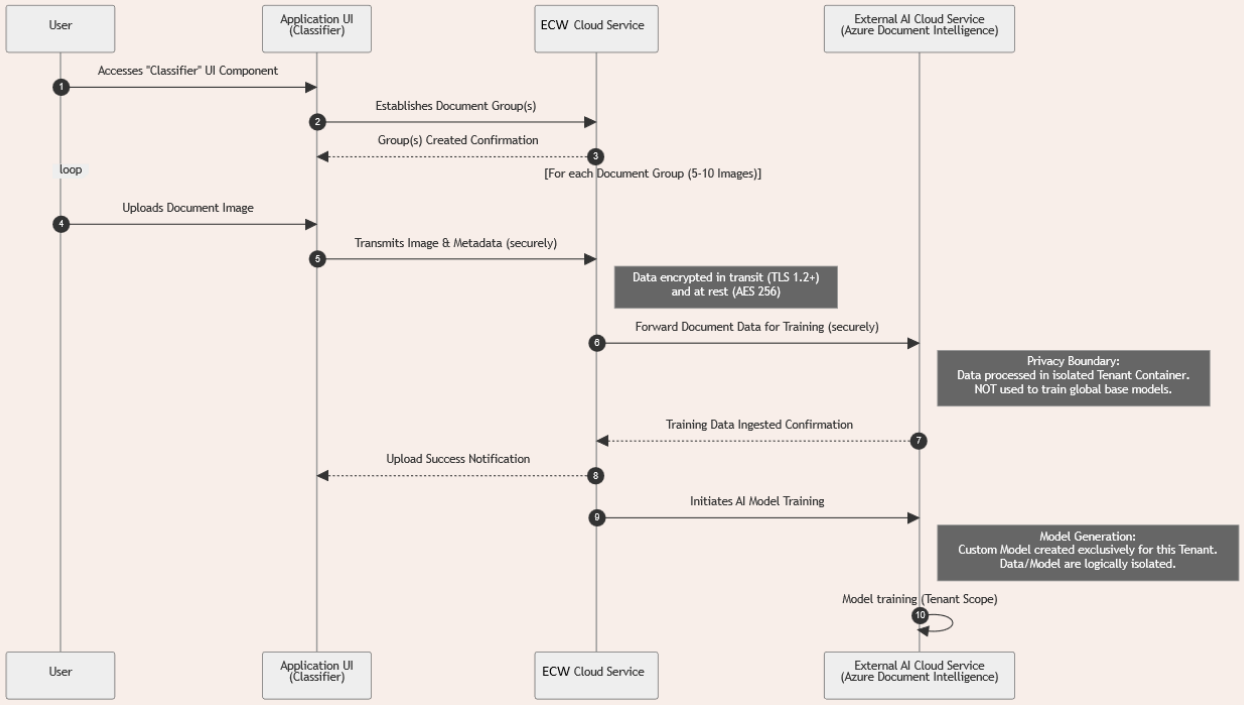


Figure 11: Secure data exchange sequence for ECW transfer learning (Classifier)

3.5.2 Configuration Sharing / Blueprinting

ECW incorporates an innovative configuration technique referred to as blueprinting. ECW's use of blueprinting utilises a configuration sharing technique that establishes a "golden standard" for workflows and deployments. Blueprinting ensures a consistent and pre-vetted security posture across an organisation. The use and application of this feature operate on the assumption of two distinct operating environments: a high-privilege administrative environment where a trusted administrator defines, tests, and deploys a master workflow template to a target company, and a lower-privilege user-facing environment connected via a REST API endpoint that allows for the instantiation of pre-approved blueprints.

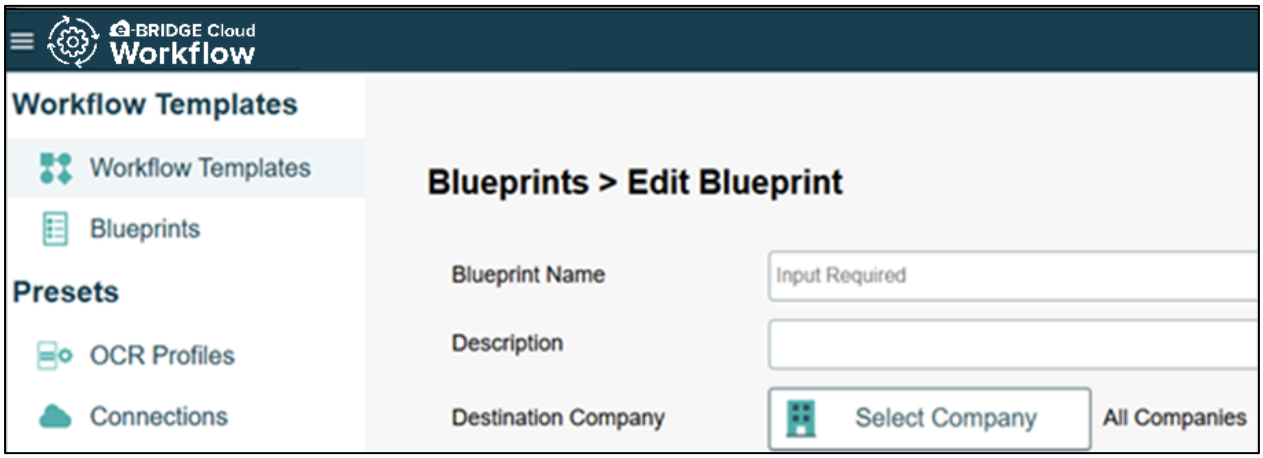


Figure 12: Professional Services and Reseller view of the blueprint Graphical User Interface (GUI)

The ECW technologies underpinning this process involve declarative configuration formats unexposed to administrators, while managed through the ECW cloud. The security advantages of blueprinting are substantial: blueprinting inherently enforces the Principle of Least Privilege (PoLP) by reducing the attack surface through the elimination of configuration drift as well as manual errors. Blueprinting streamlines compliance and auditing by focusing verification on a single, canonical blueprint rather than the sole reliance on numerous customer originated blueprints.
Administrators or end-users consuming the workflows shared from blueprinting are the recipient of its secure, pre-configured state. This model ensures that the design and execution environments are strictly segregated, with safeguards in place to protect data integrity. The only data transmitted between these environments is the abstract configuration itself. Crucially, this process involves no exchange of business data or Personally Identifiable Information (PII), ensuring that sensitive information remains isolated within its intended operational environment.

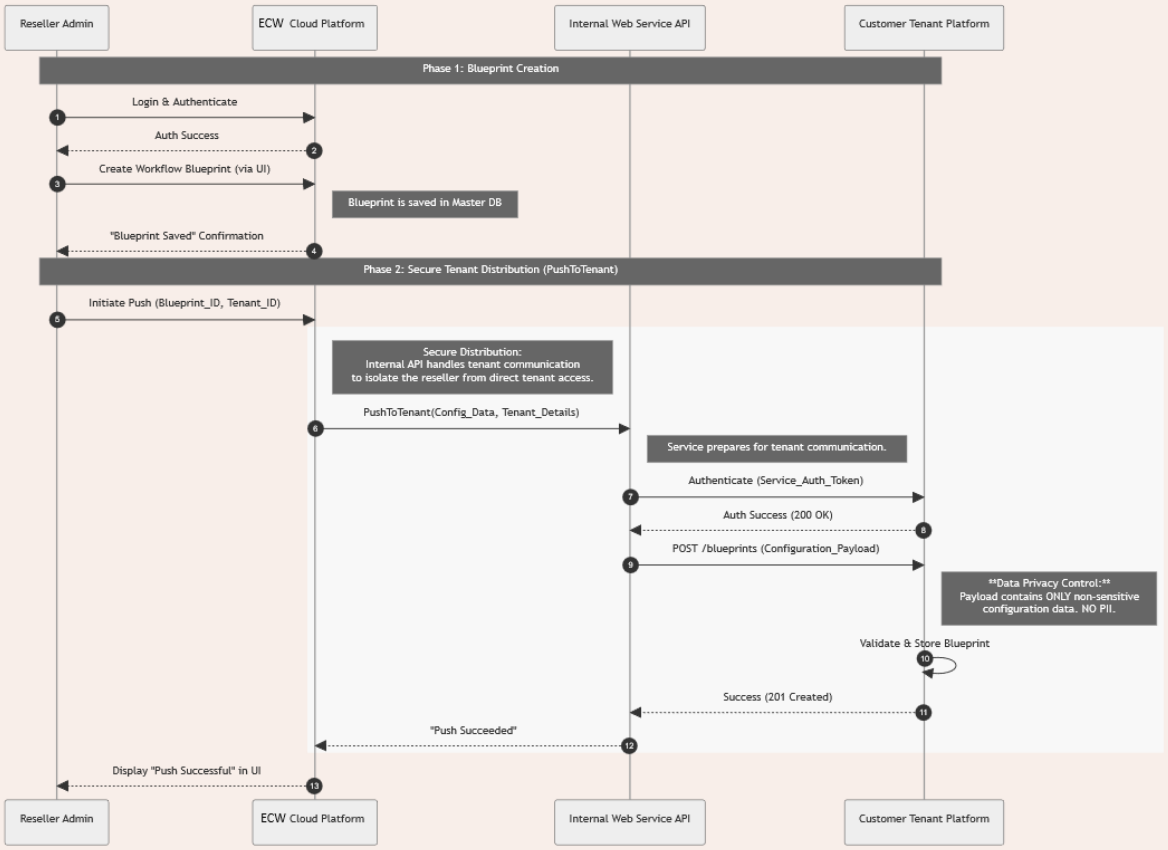


Figure 13: Data sequence diagram for secure blueprint delivery

3.6 Storage Triggers

ECW leverages an event-driven architecture to establish secure, automated workflows directly between cloud storage repositories (e.g., Google Drive, OneDrive) and ECW cloud processing engine. ECW cloud storage integration utilises provider-native webhooks and push notifications to detect file creation events in real-time, eliminating the need for constant, resource-intensive polling.

From a security perspective, this approach is superior due to the utilisation of OAuth 2.0 (IETF RFC 6749) for authorisation. Instead of sharing user credentials, ECW takes advantage of time-bound access tokens with granular scopes, ensuring that ECW detects and processes only the specific files or folders designated for triggering (e.g., an "Expenses" folder). This secure technical strategy strictly enforces the principle of Least Privilege, a core requirement of NIST SP 800-53 (Control AC-6) and ISO 27001 (Annex A.5.15). Furthermore, as data is ingested from the storage provider to an ECW workflow engine for processing (e.g., extracting receipt data for QuickBooks), all transmission is secured via TLS 1.2+ encryption, ensuring compliance with NIST SP 800-52 (Guidelines for TLS Implementations) and protecting data integrity during transit.

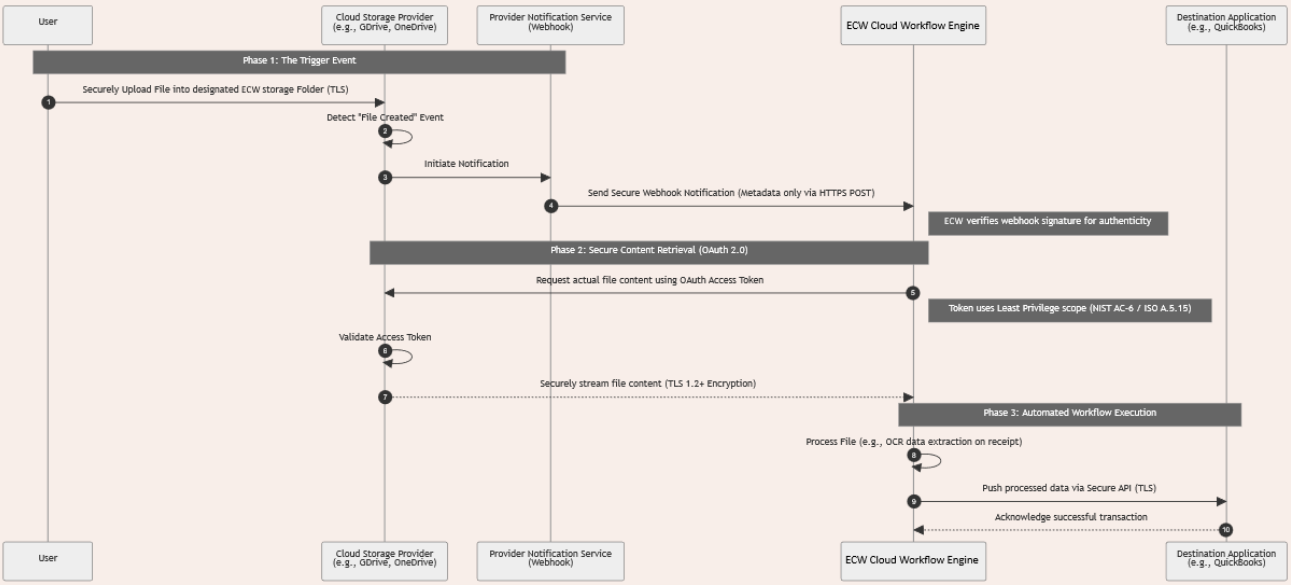


Figure 14: Example of a secure storage triggered workflow from a receipts folder to QuickBooks

3.6.1 Re-Subscribing to Storage Triggers

ECW's connection lifecycle & token expiry policy employs strict token lifecycle management for all external storage integrations. ECW storage connections are not permanent; storage connections utilise standard OAuth 2.0 refresh token policies which respect the Time-to-Live (TTL) constraints enforced by the cloud provider (e.g. Google, Microsoft).

In the event of a credential expiry or token revocation, ECW automatically enters a Fail-Secure state, de-activating the associated storage trigger immediately. This secure methodology ensures that no unauthorised attempts are made using stale credentials. Service restoration requires explicit administrative re-authorisation, ensuring that third-party access permissions are periodically reviewed and re-validated by a privileged user, preventing the security risk of "orphaned" or forgotten access keys.

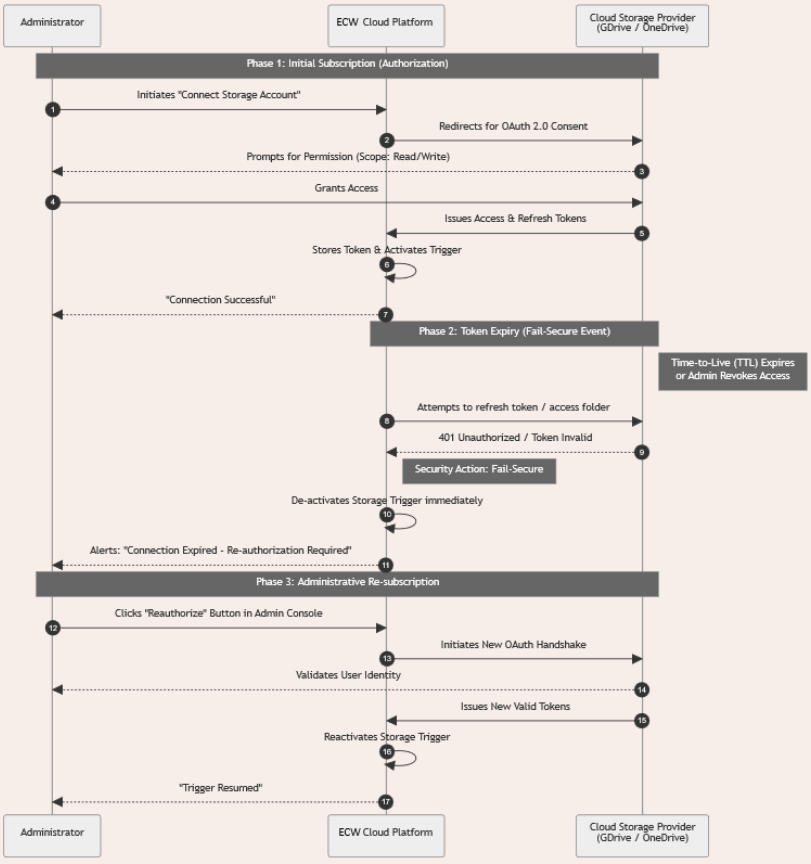


Figure 15: ECW storage trigger subscribe and resubscribe secure data flow

3.7 Browse and Upload

ECW allows end-users to authenticate with and transfer data to external cloud storage providers (OneDrive, SharePoint Online, Google Drive, Box, and Dropbox) via the "Browse and Upload" interface. To prevent data leakage and align with corporate security policies, Browse & Upload is governed by a centralised administrative control Layer. Administrators can enforce service-level whitelisting, granularly enabling or disabling specific storage providers at the company level. For instance, an administrator can permit "OneDrive" and "SharePoint" for corporate use while strictly disabling "Dropbox" and "Google Drive" to prevent unauthorised data exfiltration to personal accounts.

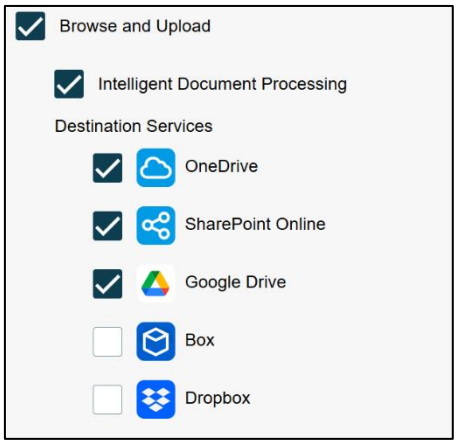


Figure 16: Secure destination services utilised by Browse and Upload

The following diagram illustrates a two-phase process: first, an Administrator can define their corporate policy (i.e....enabling or disabling a provider as illustrated by unchecking a provider such as Box and Dropbox in the figure above), and second, ECW enforces that policy dynamically when a user launches the Browse & Upload interface within the ECW Management Settings UI, ensuring that users only utilise approved options.

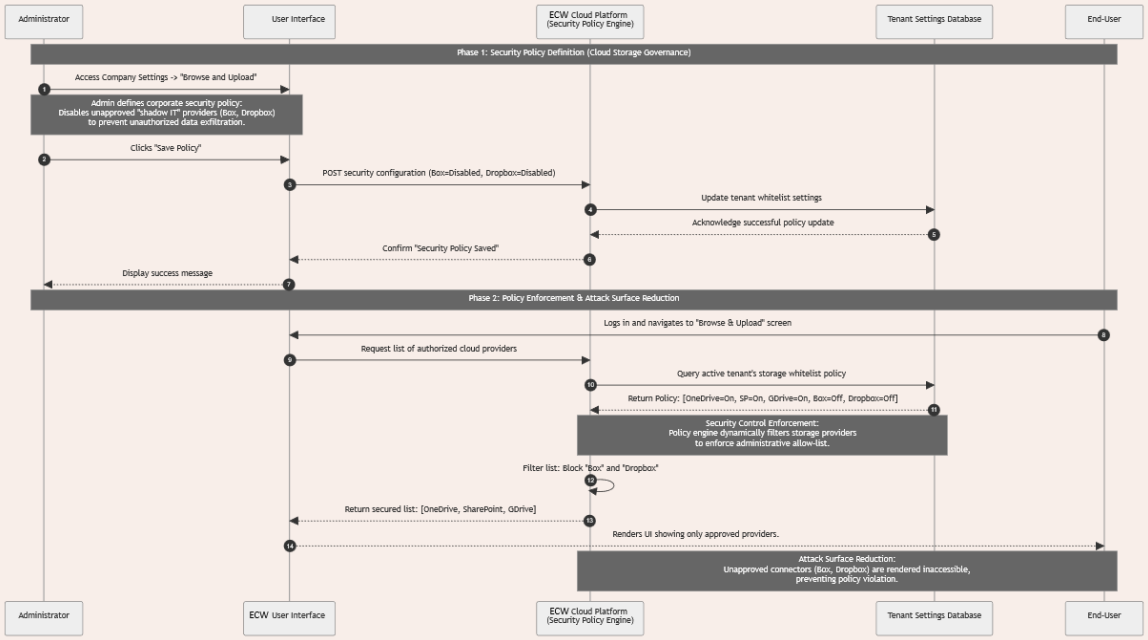


Figure 17: Secure illustration of security policy implementation, managing shadow IT

3.7.1 Browse & Upload Benefits & Advantages

- **Mitigation of Shadow IT Occurrence**: By technically enforcing which storage services are accessible, ECW prevents users from bypassing corporate policy using unauthorised "Shadow IT" tools. This ensures all data outflows remain within the organisation's approved ecosystem.
- **Data Loss Prevention (DLP) Alignment**: Restricting upload destinations reduces the risk of sensitive intellectual property being transferred to unmonitored or insecure personal repositories.
- **Attack Surface Reduction**: Disabling unused integrations closes potential API vectors. If an organisation does not use Box, disabling the Box connector ensures that no dormant tokens or API pathways exist that could be exploited

3.7.2 Browse & Upload Alignment with Industry Security Standards

- NIST SP 800-53 (Control AC-3 - Access Enforcement): This feature satisfies requirements to enforce approved authorisations for logical access to information and system resources.
- ISO/IEC 27001 (Annex A.13.1 - Network Security Management): Supports the management and control of network services and data transfer mechanisms to ensure information security.
- CIS Controls (Control 3 - Data Protection): Helps establish data protection boundaries by limiting the technical ability to move data to untrusted storage networks.

3.8 Data Encryption

ECW cloud data storage is secured using server-side encryption, which automatically encrypts data at rest using keys managed by the AWS Key Management Service (KMS). The AWS KMS service ensures that data is protected without requiring any action from the ECW user. ECW's integration with AWS offers scalability, compliance with global security standards, and seamless integration with various AWS services, making it a robust solution for secure data storage.

Key Security Aspects of ECW Data Encryption

- Automatic encryption for data at rest and in transit
- Encryption algorithms such as AES-256
- Compliance with standards such as GDPR, HIPAA, and SOC

3.9 Data Retention

ECW follows a strict data retention policy to enhance security and reduce the risk of unauthorised access. Sensitive OCR-processed data is retained only as long as necessary to support system functions, minimising exposure to potential breaches and unauthorised access. Through its integration with AWS, ECW leverages native data lifecycle and retention policies within AWS S3 and AWS DynamoDB. These capabilities help automate data deletion, reduce reliance on manual processes, and improve overall security posture. Additionally, ECW's use of AWS S3 lifecycle rules supports automatic archiving or deletion based on predefined conditions, while AWS DynamoDB utilises Time to Live (TTL) functionality, which automatically removes expired data to maintain optimal performance and efficiency. Together, these tools ensure that data is only stored for as long as it is needed, supporting a balance between security, compliance, and cost optimisation.

3.9.1 Job Data Retention

To maintain performance and keep stored data relevant, ECW enforces short retention periods for job-related data. This prevents data accumulation, improves system efficiency, and ensures operational focus. Once an ECW job is completed, the data is deleted after the following conditions are met:

Job State	Retention Period
Incomplete job	Data removed after 7 days
Jobs uploaded successfully	Data removed after 14 days
Jobs uploaded unsuccessful	Data removed after 14 days
Job execution log data	Data removed after 90 days

Table 1: ECW job data retention lifecycle

3.9.2 Company Data Deletion Actions

To further enhance security and ensure compliance, ECW automatically decommissions associated AWS systems after the license expiration period. This process helps prevent unauthorised access, minimises the risk of data breaches, and aligns with licensing agreement requirements. All company-related data is scheduled for removal two months after the official license expiry date, including:

Data Type	Data Resource Removed **(Purged / Unallocated)**
User data	AWS Cognito
Company data (and workflow template data)	AWS Cognito & AWS Dynamo DB
User group data	AWS Cognito & AWS Dynamo DB
Device data	AWS Dynamo DB
Company connection data	AWS Dynamo DB

Table 2: ECW company data deletion actions performed after expiry period

Classifier Status	Retention Period
Active Classifier	Perpetual Retention
Deleted Classifier / Deleted Company	Deleted Immediately

Table 3: ECW classifier data deletion action

3.9.3 User Data Retention

When a user is removed from ECW, all associated data is immediately deleted to maintain security and ensure data hygiene. This includes:

- User connection data
- User PIN code

User audit logs are retained for security and audit policy. This includes:

- Log retention for 18 months
- Log deletion after the user's associated company is deleted

3.10 Network Security

ECW employs a multi-layered network security strategy to protect against unauthorised access, data breaches, and cyber threats.

A Web Application Firewall (WAF) is implemented to monitor, filter, and block malicious traffic in real time. The WAF helps prevent common web-based threats such as SQL injection, cross-site scripting (XSS), and denial-of-service (DoS), ensuring that only legitimate traffic reaches the ECW platform.

All communication between ECW and connected devices, including MFPs, PCs, mobile devices, and integrated business applications, is encrypted using HTTPS with TLS v1.2 encryption, providing end-to-end protection. This ensures data confidentiality and integrity during transmission, safeguarding against interception or tampering.

ECW also enforces strict certificate validation and secure handshakes to authenticate all endpoints before any data exchange occurs. This robust encryption framework aligns with industry best practices and helps protect sensitive information in transit.

Additional Information

Toshiba is committed to the ongoing security and reliability of the e-BRIDGE Cloud Workflow platform. If you have any questions not covered in this document, or if you believe you have identified a potential security issue, please contact us at privacyofficer@toshiba-tap.com