



AnySecura

Secure Document Exchange

Enterprise-grade solution for secure file sharing and controlled information exchange across organizational boundaries

SECURE DOCUMENT EXCHANGE





Module Overview

AnySecura Secure Document Exchange provides enterprises with a comprehensive platform for secure file sharing and controlled information exchange. By establishing security domains, implementing approval workflows, and integrating encryption capabilities, it ensures secure document circulation while maintaining complete audit trails.



Security Domain

Divide enterprise networks into isolated security domains with clear data boundaries. Assign flexible user access permissions to control document circulation between domains.



Document Exchange

Secure cross-domain and same-domain file sharing with fine-grained permission controls. Support group sharing, external transmission via links, and comprehensive recipient permission management.



Exchange Approval

Configurable approval workflows with department-based processes. Integration with DingTalk/WeChat Work for notifications and whitelisting options for efficient processing.



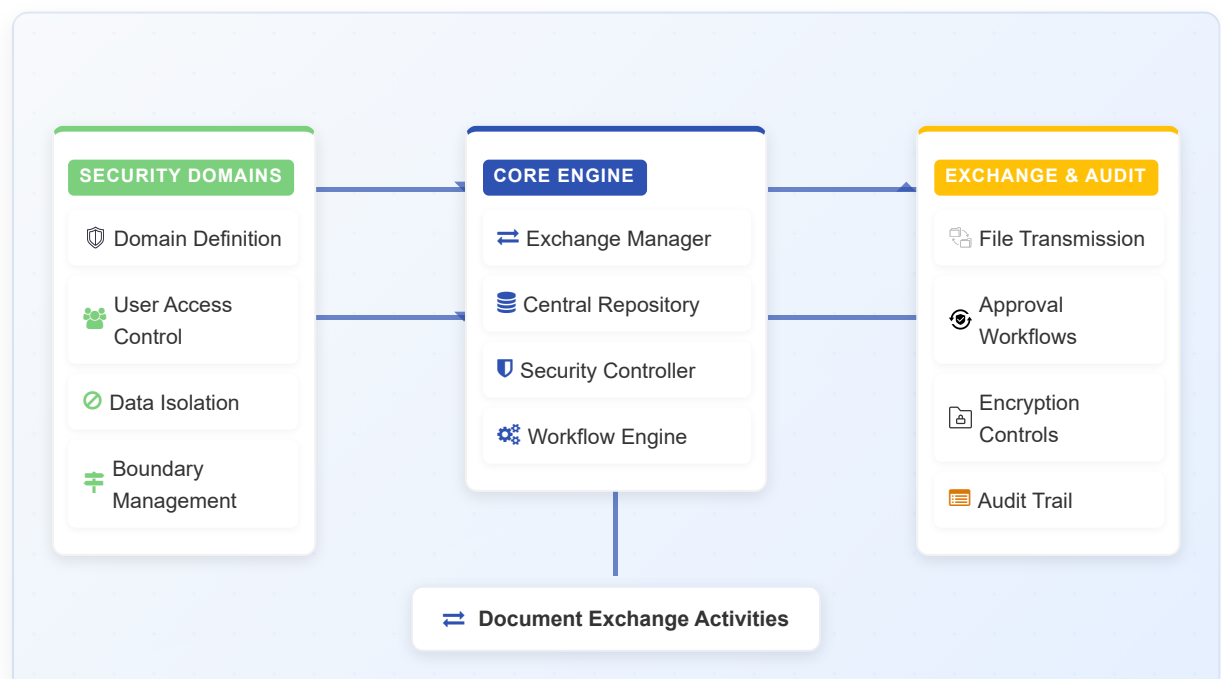
Personal Space

Managed storage space with configurable validity periods. Support for file upload/download with integrity verification, online preview, and collection of important documents.

Encryption Integration & Security Audit



Seamless integration with encryption systems for automatic decryption on upload and flexible encryption policies on download. Comprehensive logging of system operations, file exchanges, and approval processes for complete traceability.

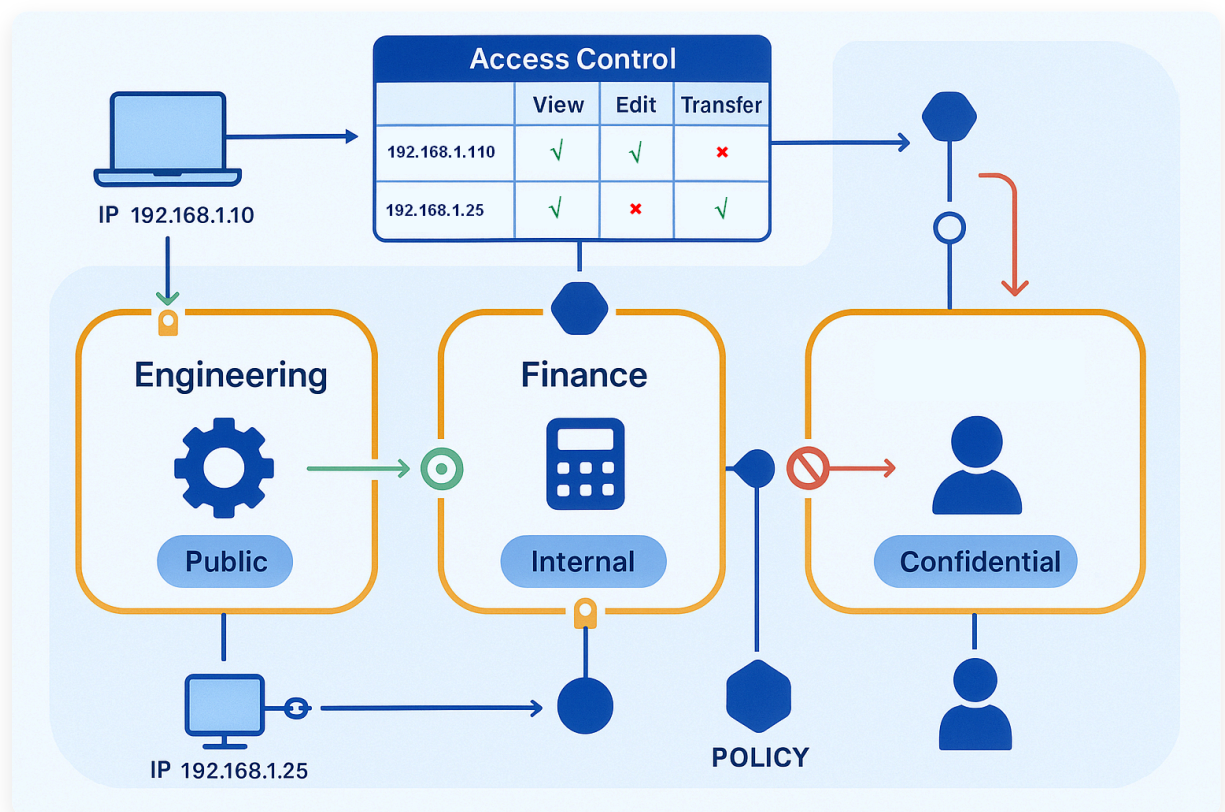




Security Domain

Establish secure boundaries for information flow within the enterprise, ensuring controlled access and preventing unauthorized data leakage between departments and network zones.

- ✓ **Security Domain Definition:** Divide enterprise networks into isolated security domains with clear boundaries for document circulation and data isolation.
- ✓ **Granular Access Control:** Assign flexible user permissions within each security domain, controlling who can access shared files and what actions they can perform.
- ✓ **Departmental Isolation:** Create independent security zones for different departments to maintain data separation and confidentiality.
- ✓ **Terminal Binding:** Restrict access to specific terminals by binding authorized IP addresses to security domains.
- ✓ **Cross-Domain Policy Management:** Define rules and restrictions for information flow between different security domains.
- ✓ **Domain Classification:** Categorize domains by sensitivity level, with appropriate security controls applied to each classification.

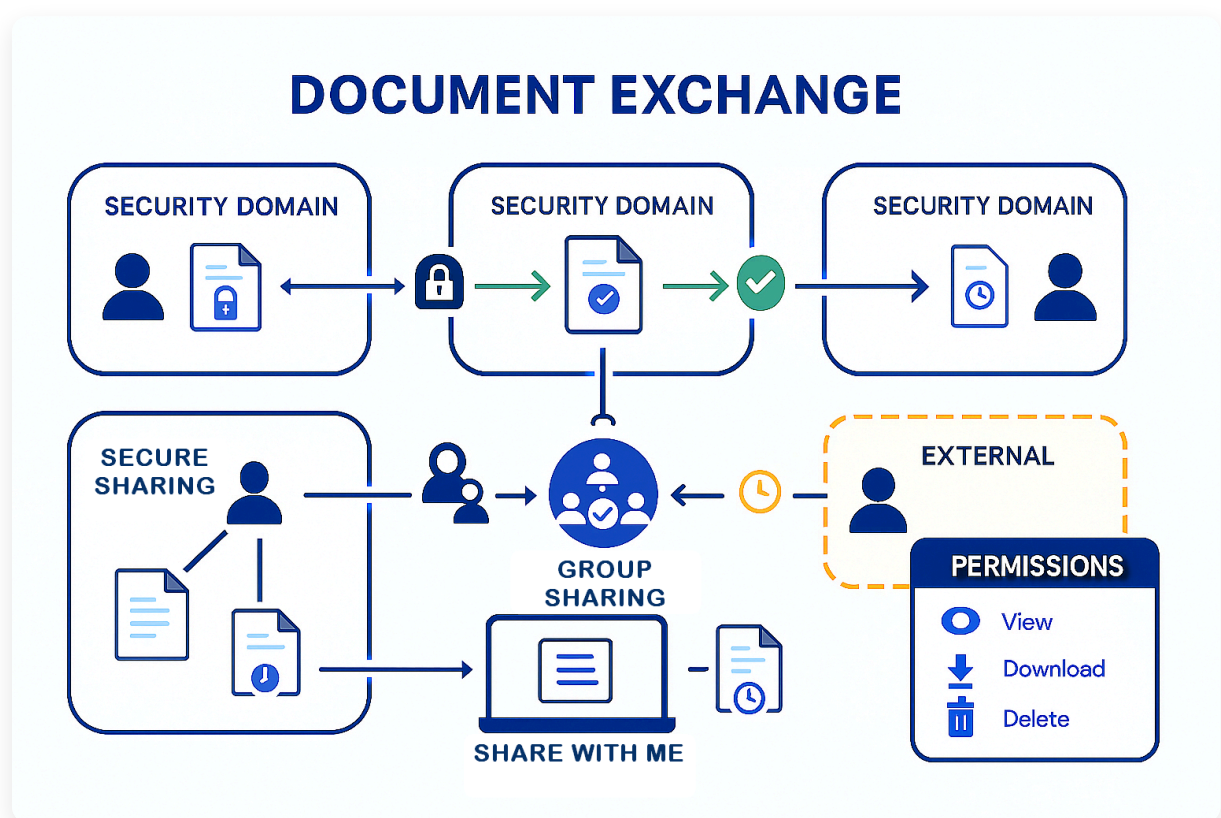




Document Exchange

Secure mechanisms for transferring files both within and between security domains, with comprehensive control over how recipients can interact with shared documents.


- ⇒ **Cross-Domain Exchange:** Securely transmit files to users in other security domains with proper authorization and tracking.
- ⇒ **Same-Domain Sharing:** Facilitate file sharing between users within the same security domain with appropriate access controls.
- 👥 **Group Sharing:** Efficiently share files with multiple users by creating groups and distributing documents in batches.
- 🔑 **External Transmission:** Share files with external parties via secure links, controlling access and document permissions.
- 🔍 **Fine-Grained Permissions:** Set detailed access rights including preview-only, downloadable, download limits, and validity periods.
- 📁 **Shared with Me:** Centralized view of all files shared by other users for easy access and management.








Exchange Approval


Configurable workflows that ensure proper authorization for sensitive document exchanges, with efficient processing and integration with common enterprise communication tools.


 **Approval Configuration:** Customize file sharing approval workflows with different processes based on file destinations and sensitivity.

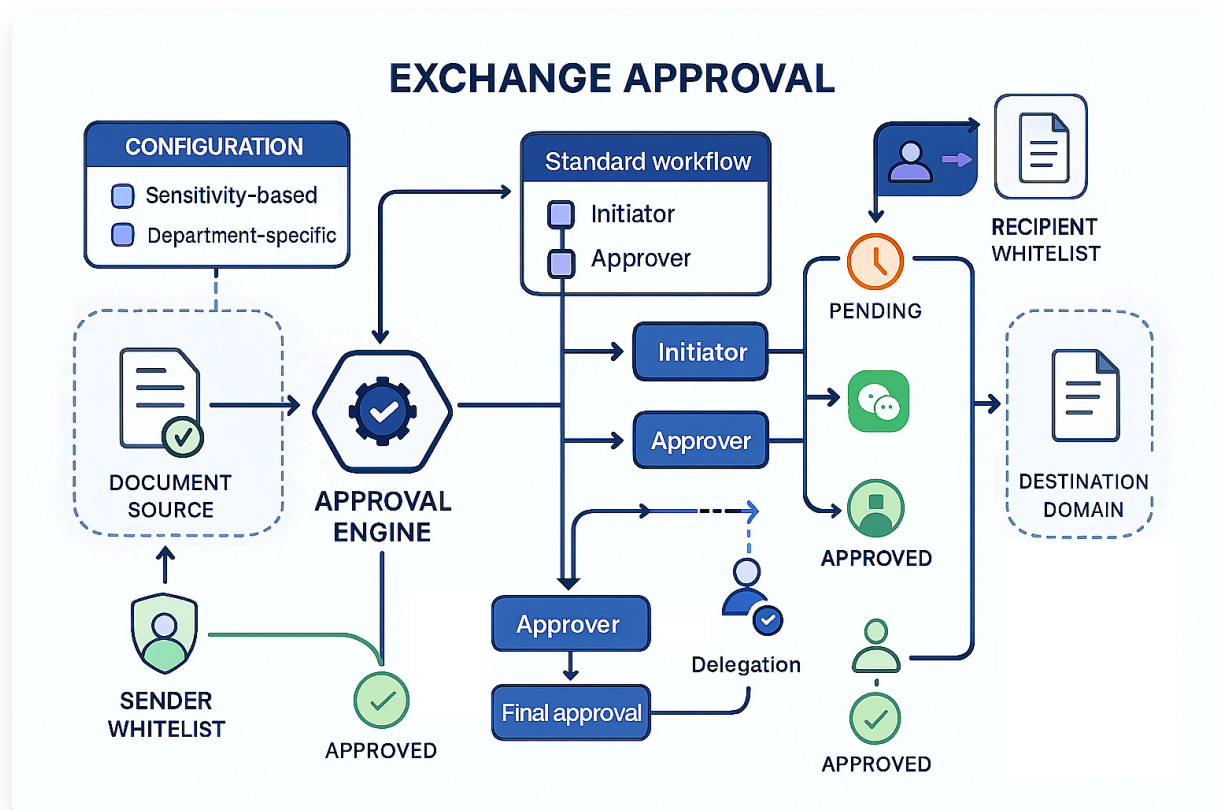
 **Organizational Workflows:** Set up approvals by department and personnel, with support for countersigning and approval delegation.

 **Mobile Integration:** Receive and process approvals via DingTalk or WeChat Work for timely decision-making.

 **Sender Whitelists:** Pre-authorize trusted users whose file sharing can bypass approval processes for efficiency.







 **Recipient Whitelists:** Allow direct sharing to pre-approved recipients without formal approval procedures.

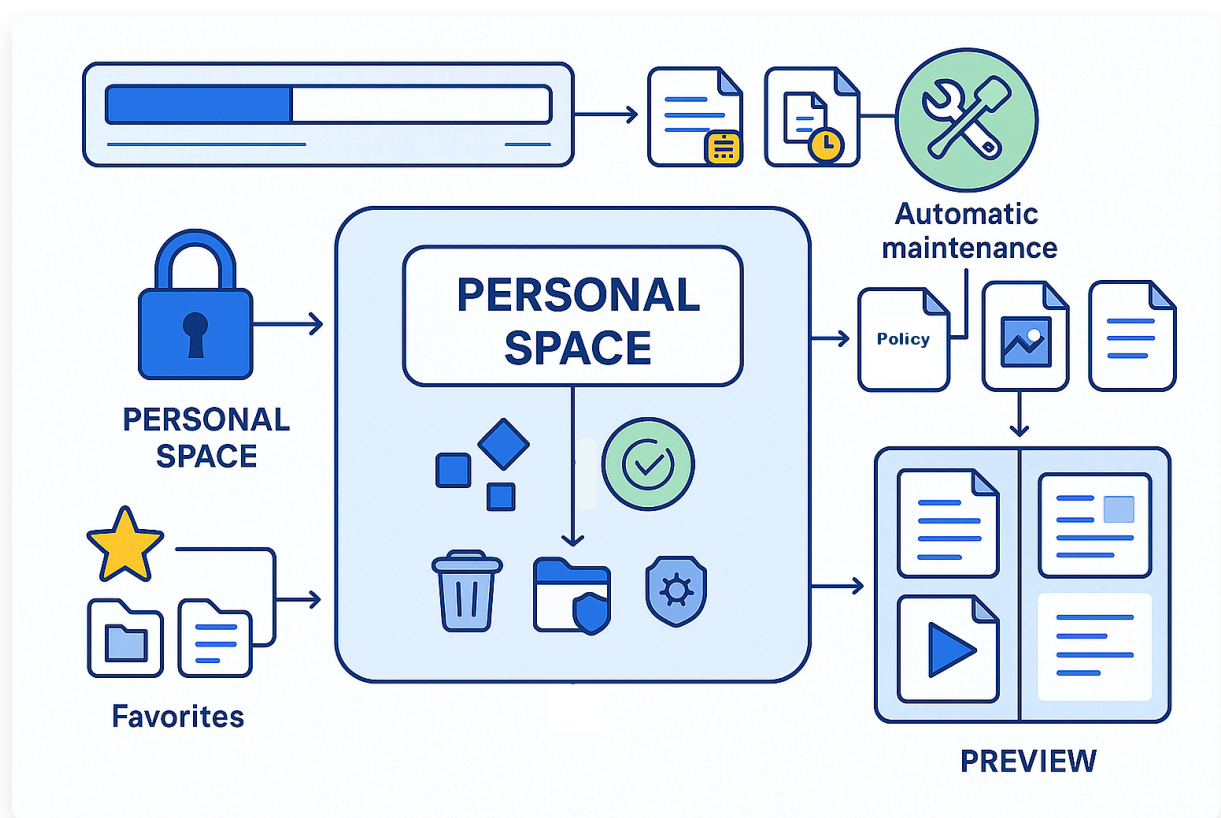
 **Leader Exception Handling:** Special workflows for department leaders to avoid self-approval situations.



Personal Space

Secure storage and management of personal documents with controlled access, automated maintenance, and comprehensive file handling capabilities.

-  **Storage Management:** Allocate personal storage space with configurable limits and automatic expiration for efficient disk usage.
-  **Comprehensive File Management:** Complete upload, download, and deletion functions with support for large files via chunked and resumable transfers.
-  **Online Preview:** View common file types directly in the system including documents, spreadsheets, presentations, PDFs, and images.
-  **File Collection:** Mark important or frequently used files as favorites for quick access and organization.
-  **Integrity Verification:** Ensure data correctness during upload and download with built-in verification mechanisms.
-  **Automatic Maintenance:** Files are automatically cleared after their configured validity period to optimize storage.

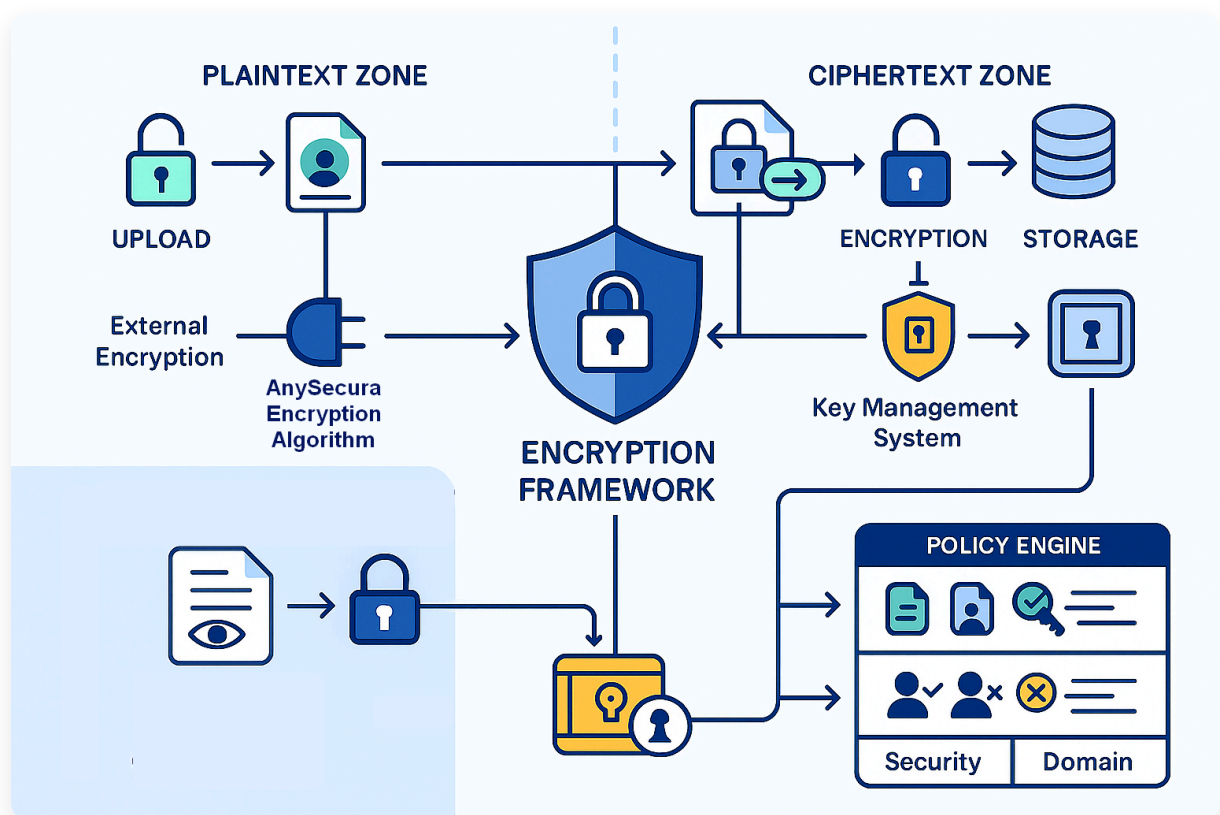




Encryption Integration







Seamless integration with encryption systems to ensure secure handling of sensitive documents during upload, storage, and download processes.

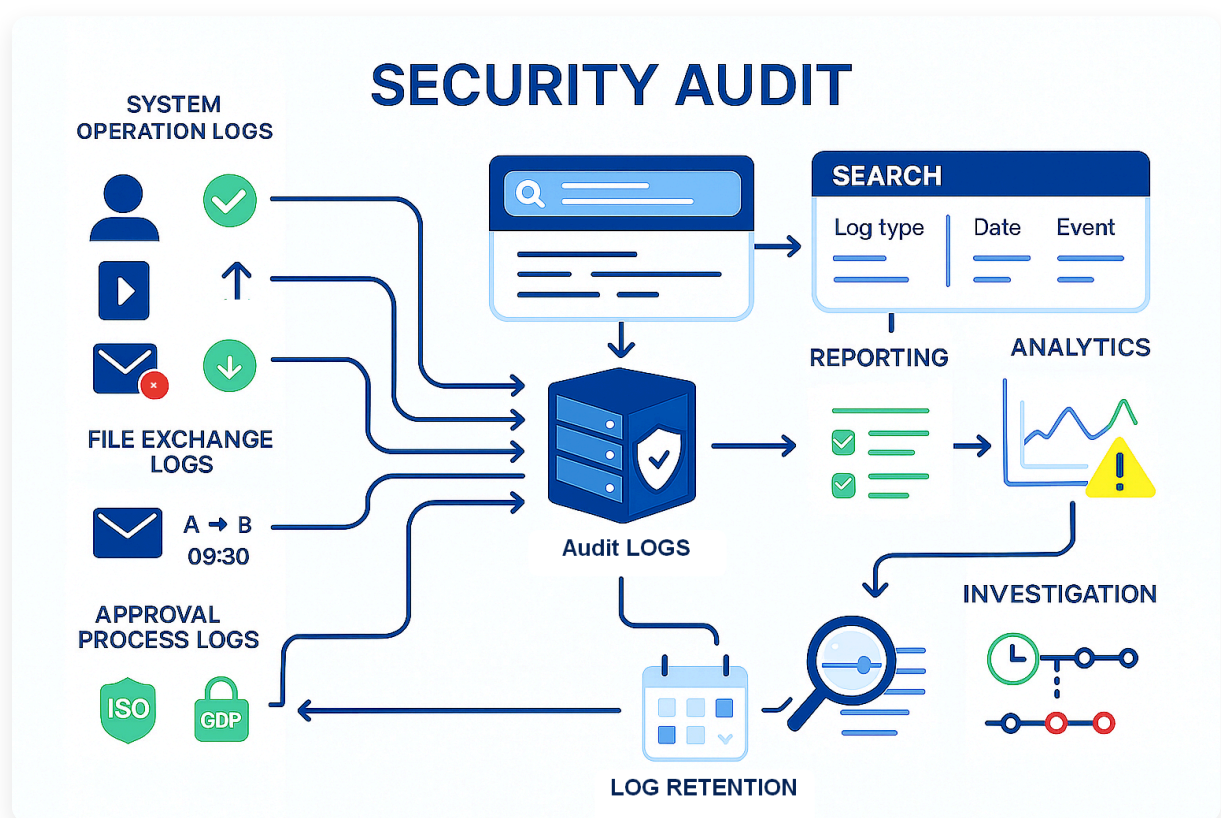
- Upload Decryption:** Automatically decrypt encrypted documents upon upload to enable online preview and processing.
- Download Encryption:** Apply flexible encryption policies based on security domains, including options for unencrypted, enterprise-internal, or user-specific encryption.
- Cross-Zone Encryption:** Automatic encryption/decryption when transferring files between plaintext and ciphertext areas.
- Third-Party Integration:** Seamless connection with IP-guard and other enterprise encryption systems.
- Key Management:** Secure handling of encryption keys with appropriate access controls and rotation policies.
- Policy-Based Encryption:** Apply encryption rules based on document sensitivity, user roles, and security domains.



Security Audit

Comprehensive logging and monitoring of all system activities to ensure compliance, enable investigation, and maintain security oversight.

-  **System Operation Logs:** Detailed records of account synchronization, user login/logout, and file operations including uploads, downloads, and deletions.
-  **File Exchange Logs:** Complete documentation of all file sharing activities with information about senders, recipients, and timestamps.
-  **Approval Process Logs:** Detailed tracking of all approval workflows including initiators, timestamps, file information, and status changes.
-  **Query and Reporting:** Powerful search capabilities and report generation for audit trails and compliance documentation.
-  **Audit Analytics:** Tools for analyzing audit data to identify patterns, anomalies, and potential security issues.
-  **Log Retention:** Configurable storage periods for audit logs to meet compliance requirements and business needs.





Application Scenarios



1. Departmental Data Isolation



The Challenge

A large enterprise with multiple departments needs to prevent unauthorized access to sensitive information while allowing legitimate cross-departmental collaboration. Without proper controls, confidential data from R&D and finance departments is at risk of exposure to other departments.



The Solution with AnySecura

Implementing **Security Domain** and **Document Exchange** capabilities:

1. Create separate security domains for each department with strict access controls
2. Bind authorized terminals and IP addresses to each security domain
3. Implement controlled cross-domain document exchange with approval workflows
4. Apply appropriate encryption based on domain classification and document sensitivity

Results Achieved

- ✓ Complete isolation of sensitive departmental information
- ✓ 95% reduction in unauthorized data access attempts
- ✓ Streamlined legitimate cross-departmental collaboration



2. Secure Cross-Network Exchange



The Challenge

An enterprise with isolated network zones needs to share documents between these networks while maintaining security. Without proper controls, sensitive information could leak between networks or unauthorized users might access confidential data.



The Solution with AnySecura

Leveraging **Cross-Domain Exchange** and **Encryption Integration**:

1. Establish security domains for each isolated network with clear boundaries
2. Package files with recipient information, security domain details, and access permissions
3. Implement precise cross-domain delivery with encryption based on domain classification
4. Ensure only authorized users from the receiving domain can access the files
5. Maintain complete audit trails of all cross-domain activities

Results Achieved

- ✓ Secure information flow between isolated network zones
- ✓ 100% compliance with network isolation policies
- ✓ Reduced operational costs by 35% compared to manual processes

Application Scenarios

3. Supply Chain Collaboration

The Challenge

A manufacturing company needs to securely exchange design documents and specifications with suppliers and partners while maintaining intellectual property protection. Traditional email and file transfer methods create security risks and lack proper controls.

The Solution with AnySecura

Utilizing **External Transmission** and **Exchange Approval**:

1. Create separate security domains for internal network and external partners
2. Implement cross-domain exchange model with approval workflows for external sharing
3. Share files via secure links with configurable access permissions and passwords
4. Set download limits and validity periods for external access
5. Maintain comprehensive logs of all external exchanges for audit purposes

Results Achieved

- ✓ Secure collaboration with external partners while protecting IP
- ✓ 40% faster time-to-market through improved supply chain communication
- ✓ Complete visibility and control over external document sharing

4. Secure Personal Data Management

The Challenge

Employees need a secure space to manage personal work documents while ensuring enterprise data governance policies are enforced. Without proper controls, sensitive information may be stored in unauthorized locations or shared inappropriately.

The Solution with AnySecura

Using **Personal Space** and **Security Audit**:

1. Provide each employee with a secure personal storage space with defined quotas
2. Implement automatic document classification and encryption based on content
3. Enforce data retention policies with automatic cleanup of expired documents
4. Maintain comprehensive audit logs of all personal space activities
5. Enable secure sharing of personal documents through defined approval workflows

Results Achieved

- ✓ Reduced data sprawl through centralized personal document management
- ✓ 75% reduction in unauthorized personal storage of company data
- ✓ Improved employee productivity with secure access to personal work files

Core Values & Benefits



Enhanced Data Security

Security domains and encryption integration ensure sensitive information remains protected while enabling legitimate business exchanges.



Controlled Collaboration

Secure cross-departmental and external collaboration with appropriate access controls and approval workflows.



Complete Audit Trails

Comprehensive logging of all document exchanges and system activities for compliance verification and incident investigation.



Operational Efficiency

Streamlined document exchange processes with whitelisting options and mobile approval integration to balance security and productivity.

Ready to Secure Your Document Exchanges?

 [Learn More About Solutions](#)

 [Contact Our Experts](#)



www.anysecura.com



support@anysecura.com

© 2025 AnySecura SOFTWARE PTE. LTD. All rights reserved. Enterprise-grade security solutions.