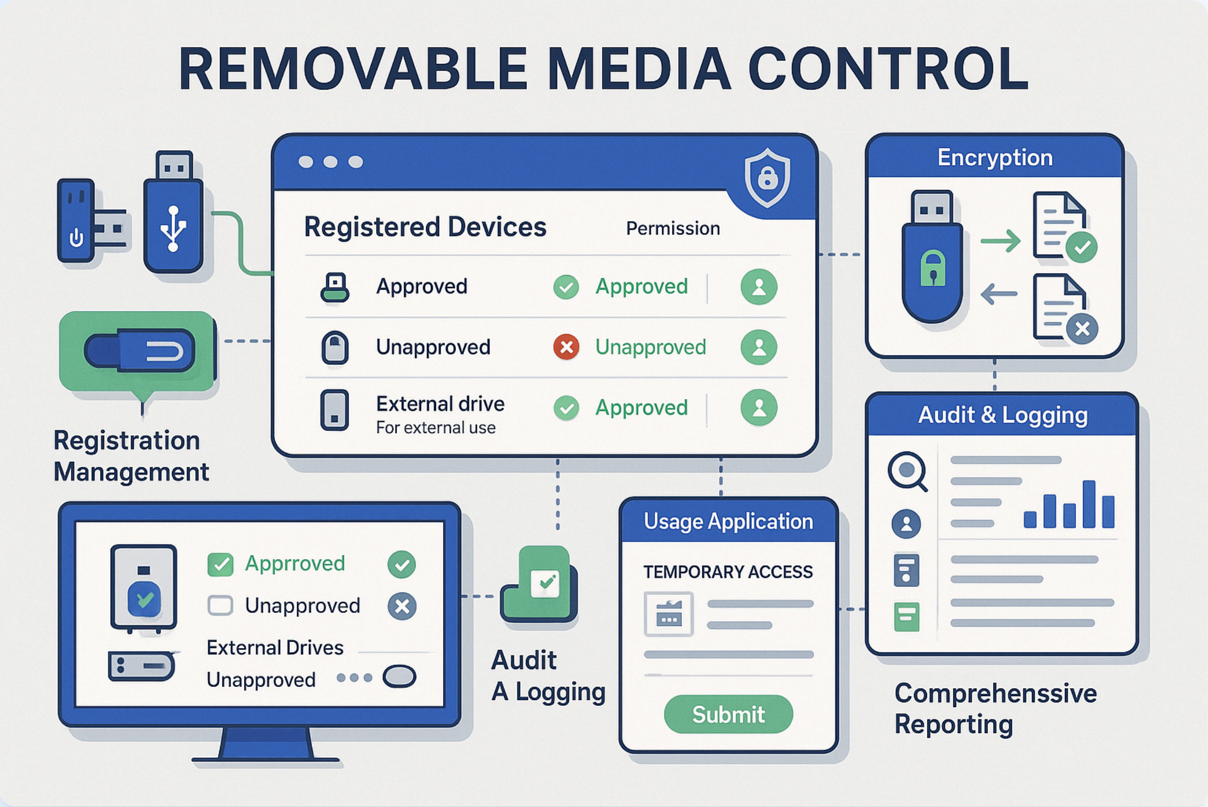
AnySecura

Removable Media Control

Comprehensive removable media security solution
Control · Encrypt · Audit · Register · Manage



Module Overview

AnySecura Removable Media Control integrates five core capabilities, providing enterprises with complete control over removable media to prevent unauthorized access and data leakage through external storage media.

Registration Management

Perform registration management for USB drives. Registered USB drives can access the internal network, while unregistered ones cannot be used, achieving "external drives for external use".

Authorization Management

Authorize the use of removable media, restricting the read, write permissions and usage scope of USB drives based on organizational policies.

Encryption Management

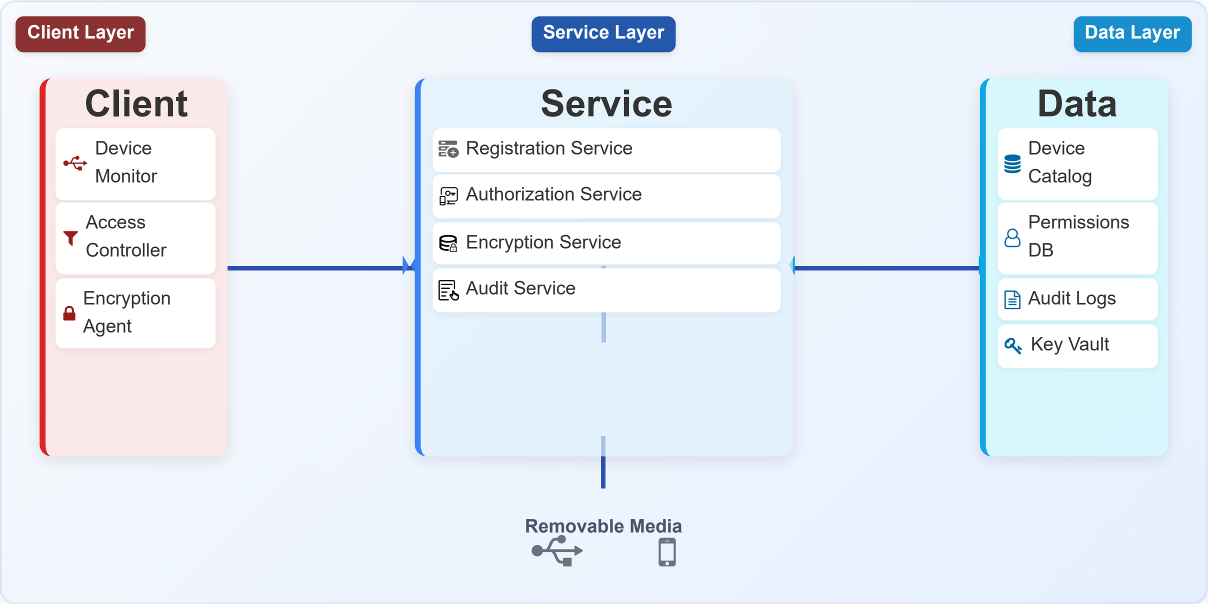
Convert ordinary USB drives into encrypted disks and perform transparent encryption/decryption for documents, ensuring secure data storage and transmission.

Audit & Logging

Automatically collect information about removable media and record in detail various document operations and connection activities for compliance.

Usage Application & Comprehensive Reporting

Allow users to submit applications for temporary use of removable media when prohibited, with approval workflows and self-filing options. The system also provides comprehensive reporting capabilities that consolidate data from all modules.



Registration & Authorization

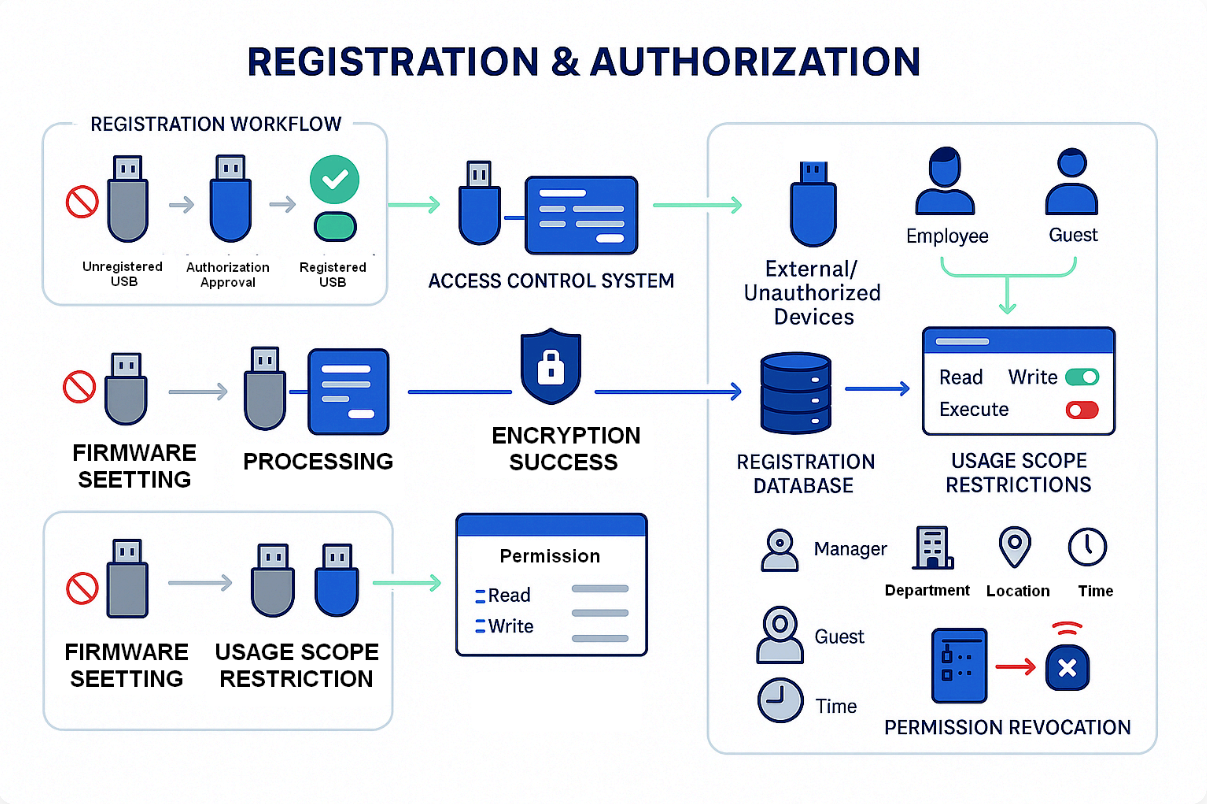
Comprehensive management of removable media access through registration and granular permission control to ensure secure data handling.

Registration Management

- **USB Registration:** Formal registration process for USB drives to establish ownership and authorization.
- **Access Control:** Registered USB drives can access the internal network, while unregistered ones are blocked.
- **External/Internal Separation:** Implement "external drives for external use" policy to prevent data leakage.
- **Unique Identification:** Assign unique identifiers to registered devices for tracking.

Authorization Management

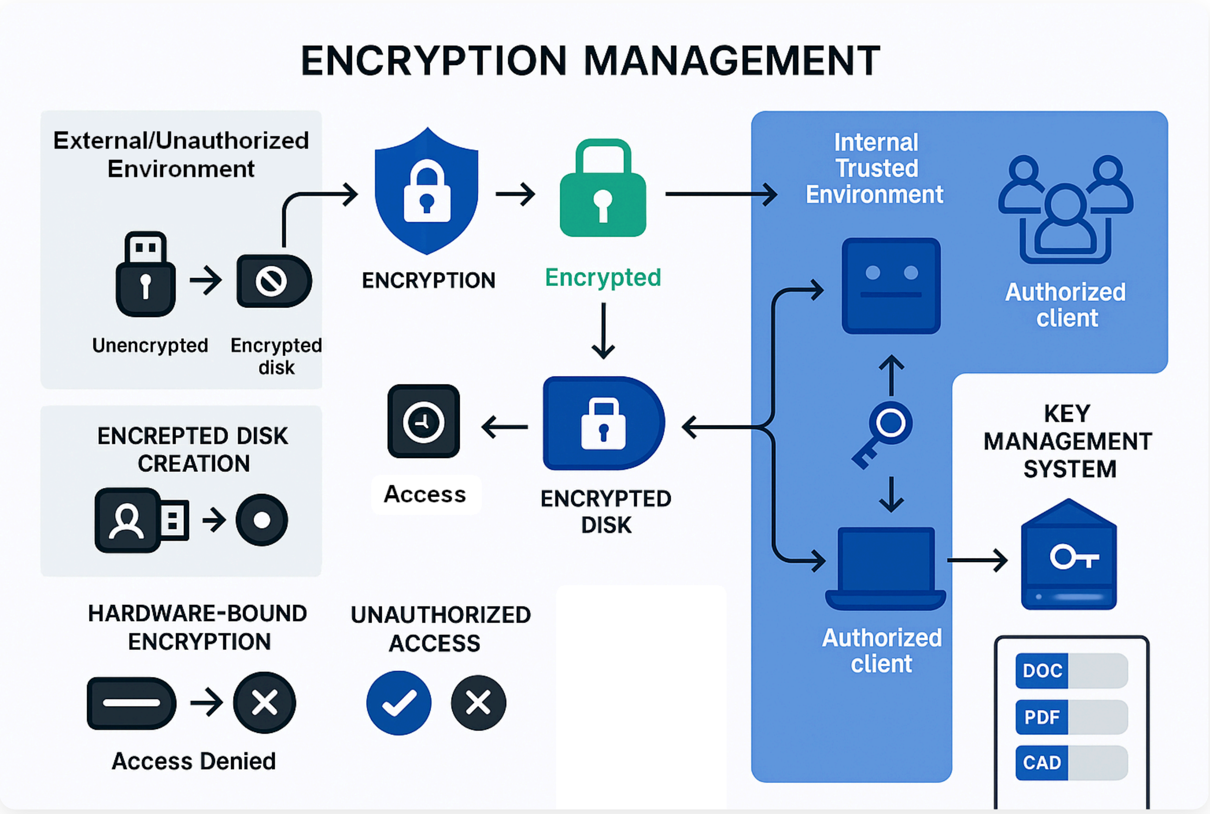
- **Permission Assignment:** Granular control over read, write, and execute permissions.
- **Role-based Access:** Define permissions based on user roles and organizational structure.
- **Usage Scope Restriction:** Limit usage to specific departments, locations, or time periods.
- **Prohibition Settings:** Completely block certain types of removable media based on policies.



Encryption Management

Advanced encryption technologies to protect sensitive data stored on removable media and prevent unauthorized access.

- **Encrypted Disk Creation:** Convert ordinary USB drives into encrypted disks that can only be recognized on internal client machines.
- **Internal Use Enforcement:** Implement "internal drives for internal use" policy through hardware-bound encryption.
- **Transparent Encryption:** Automatically encrypt and decrypt documents stored in or retrieved from designated removable media.
- **Unauthorized Access Prevention:** Ensure encrypted documents cannot be read by unauthorized clients or external computers.
- **Key Management:** Secure key storage and distribution system to ensure encryption keys remain protected.



Audit & Logging

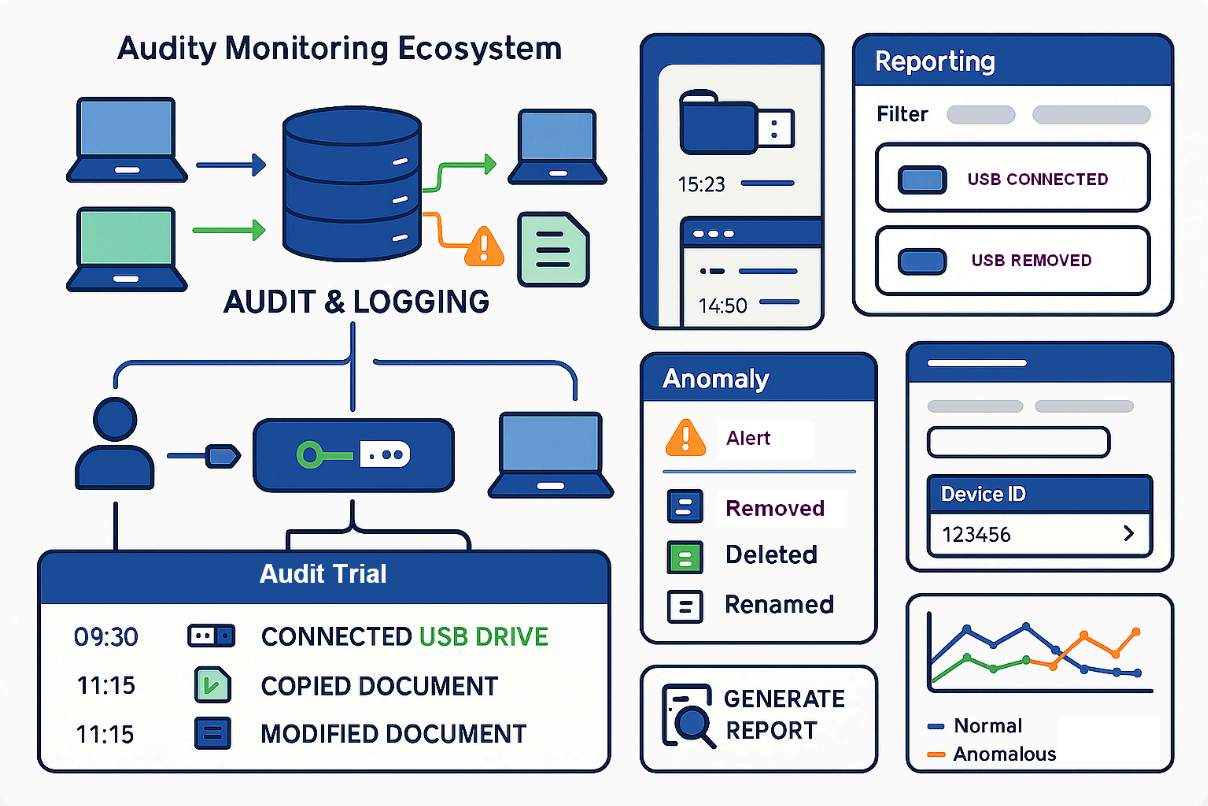
Comprehensive tracking and documentation of all removable media activities to ensure compliance and enable security investigations.

Activity Monitoring

- **Connection Tracking:** Record all plug-in and plug-out events of removable media across the enterprise.
- **File Operation Logging:** Detailed records of document copying, modifying, deleting, and renaming activities.
- **Timestamps:** Accurate time recording for all activities to establish a complete audit trail.
- **User Identification:** Link all activities to specific users for accountability and investigation.

Audit Capabilities

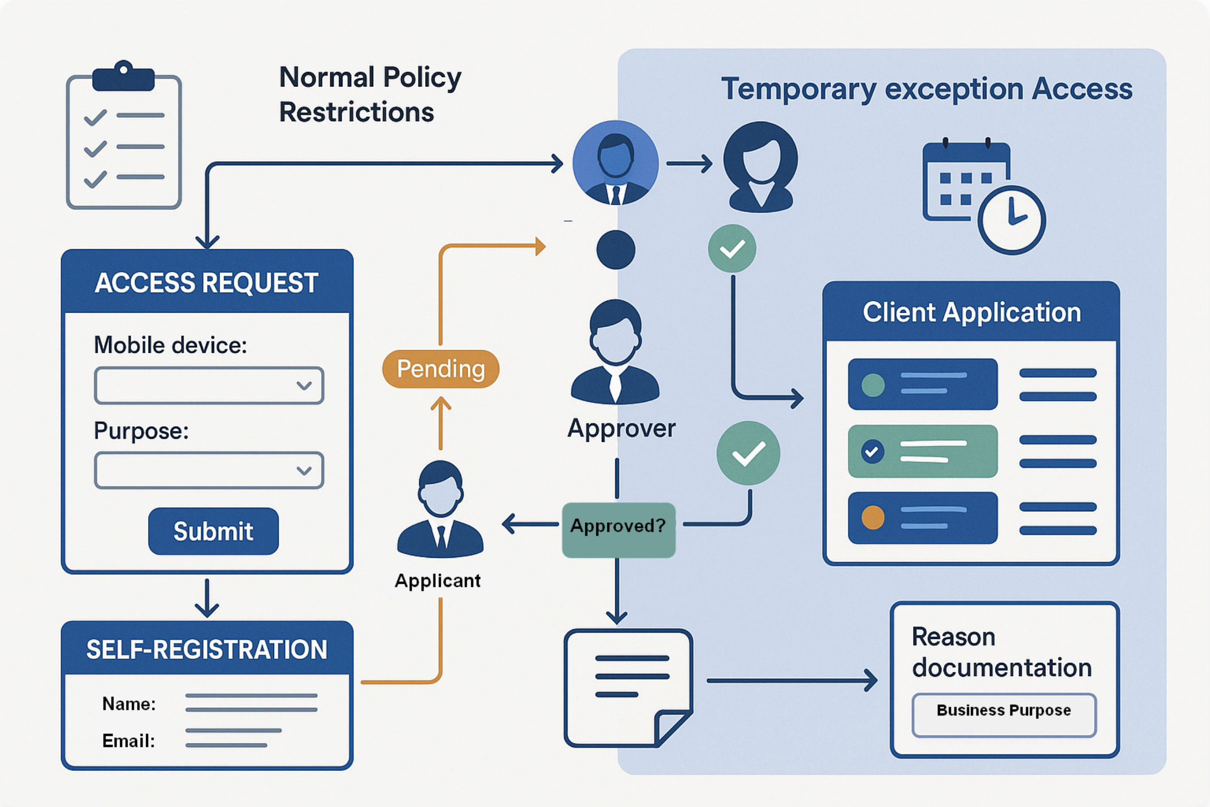
- **USB-specific Query:** Query activities of a specific USB drive across various computers in the network.
- **Filtered Reporting:** Generate reports based on time periods, users, device types, or specific activities.
- **Trend Analysis:** Identify patterns in removable media usage to optimize security policies.
- **Compliance Reporting:** Generate audit reports for regulatory compliance and internal audits.



Usage Application

Flexible mechanisms for requesting temporary removable media access while maintaining security controls and accountability.

- **Access Request:** Allow users to submit formal applications for temporary use of removable media when prohibited by policy.
- **Time-bound Permissions:** Grant access for specific time periods with automatic expiration to minimize risk.
- **Self-filing Option:** Enable usage through self-registration and filing processes for lower-risk scenarios.
- **Approval Workflows:** Configurable multi-level approval processes based on data sensitivity and user roles.
- **Client-based Application:** User-friendly client interface for submitting and tracking access requests.



Application Scenarios

1. External Drive for External Use

⚠ The Challenge

A large corporation faces significant data leakage risks as employees frequently use personal USB drives to copy sensitive company data. This creates unauthorized data exfiltration channels that bypass security controls.

The Solution with AnySecura

Implementing strict **Registration Management** and access controls:

1. Prohibit all unregistered USB drives from connecting to internal systems
2. Create a formal registration process for any USB drive requiring network access
3. Enforce "external drives for external use" policy through device recognition
4. Log all attempts to use unregistered devices for security auditing

2. Internal Drive for Internal Use

⚠ The Challenge

A research organization needs to distribute sensitive data internally via USB drives but is concerned about drives being lost or used outside the organization, potentially exposing confidential research data.

The Solution with AnySecura

Leveraging powerful **Encryption Management** capabilities:

1. Convert company USB drives into encrypted disks using hardware-bound encryption
2. Ensure encrypted drives can only be recognized and accessed on internal systems
3. Implement transparent encryption for all files stored on these drives
4. Maintain central control over encryption keys for complete security

Results Achieved

- ✓ Secure internal data distribution while preventing external access
- ✓ Protection against data exposure even if drives are lost or stolen
- ✓ Maintained operational efficiency while enhancing security

Core Values & Benefits

Data Leakage Prevention

Prevent unauthorized data transfer through removable media with comprehensive control mechanisms and encryption technologies.

Complete Visibility

Full visibility into all removable media activities with detailed logging and auditing capabilities across the enterprise.

Compliance Assurance

Meet regulatory requirements with comprehensive audit trails, access controls, and data protection mechanisms.

Flexible Security

Balance security needs with operational efficiency through flexible access policies and temporary usage mechanisms.

Ready to Secure Your Removable Media?

Learn More About Solutions

Contact Our Experts

www.anysecura.com

support@anysecura.com