

HP Capture and Route Data Loss Prevention Module



In today's business climate, data security and compliance are more critical than ever. HP's enterprise-class secure document capture and fax solution, Capture and Route, includes robust and intuitive security features designed to safeguard customer data and facilitate data loss detection and prevention.

Benefits

- **Protect** sensitive organization, customer, and vendor data
- **Facilitate** data loss detection and prevention
- **Prevent** both intentional and unintentional data leaks
- **Reduce** time spent hunting for data or correcting errors
- **Perform** secure scans to detect data loss

Overview

HP Capture and Route Data Loss Prevention (DLP) allows organizations to easily monitor documents traveling through their enterprise for sensitive or confidential information. By using specific rule sets, HP CR DLP can execute workflows based on the information it finds to protect sensitive information from leaving the organization—or at a minimum, the ability to trace that information. This robust solution gives users the ability to:

- **Search and detect** key terms or sequences in scanned, faxed, or printed (if they pass through HP CR) documents that may indicate the presence of confidential information or sensitive data
- **Configure** specific workflow rules for each flagged term
- **Review** flagged documents and related rule sets
- **Create** gated security blocks for sensitive data

DLP profiles

To protect data from theft and accidental disclosure, you first need the ability to differentiate day-to-day communications from those that contain sensitive data (for example, a marketing datasheet versus a confidential financial document). HP CR DLP transforms the content of documents to text-searchable information, where it then is able to detect key terms or numeric patterns that may indicate the presence of confidential or sensitive data. HP CR DLP:

- **Can detect distinct words and phrases** (such as “secure,” “private,” or “confidential”), and specific character patterns, such as credit card numbers or social security numbers.
- **Supports “fuzzy logic” functionality**, meaning it can detect data whether it's uppercase, lowercase, or substitutes numbers or symbols for characters (for example, “s3cure” rather than “secure”).
- **Is built around the Optical Character Recognition (OCR) engine** already embedded in the HP CR platform, which allows for enhanced scalability depending on the organization's needs and requirements.
- **Can detect any supported languages** which have been added to the HP CR server by the organization (using OCR).

Security station

The system administrator oversees much of the functionality of HP CR DLP; however, delegated content auditors or (potentially) end-users are also able to intuitively interact with the module via the Security Station (found in HP CR WebApps).

This simple dashboard platform allows users to:

- Easily locate sensitive data that has been flagged
- Quickly approve or reject flagged data
- Communicate specifics by adding a note

The screenshot shows the HP Security Station interface. At the top, there's a navigation bar with the HP logo, 'Capture and Route > Security Station', and a user profile 'VMAD700\Administrator'. Below the navigation bar are buttons for 'Approve', 'Reject', 'Download', and 'Preview'. The main area contains a table with columns: Job ID, Sender, Destination, Profile ID, Matches, and Summary. The table lists several items, with Job ID 4299 highlighted. Below the table, there are 'Matches' and 'Notes' sections. The 'Matches' section shows a rule named 'CONSENT' with the text 'CONSENT'. The 'Notes' section is empty. At the bottom of the table area are 'Approve' and 'Reject' buttons. On the right side, there's a preview of a consent form titled 'Healthcare Provider CONSENT FOR DISCLOSURE OF INDIVIDUALLY IDENTIFYING HEALTH INFORMATION'. The form includes fields for Client Name, Date of Birth, Phone, Address, Health Number, and a section for authorization: 'I authorize _____ for the purpose of _____'. Below this, there's a section for 'Information is required for the purpose(s) of _____' and 'Disclose information to _____'. At the bottom of the form, there are fields for Client Signature, Date, Witness Signature, and Authorized.

HP Capture and Route preview and self-policing

Exposure to sensitive data varies depending on an employee's roles and responsibilities. Though some staff encounter sensitive data on a regular basis, not every employee needs strict standard processes set for them as they may not deal with sensitive data often. Introducing HP CR Preview! When paired with HP CR DLP, HP CR Preview allows the system administrator to provide access to sensitive data to users on an as-needed basis. HP CR Preview gives users the ability to:



Quickly confirm

the quality of the image



Simply view

the scan—no metadata entry or editing needed



Note

any flagged data highlighted in preview



Immediately approve

or reject data



Work in conjunction

with HP CR DLP to create a self-policing workflow for Data Loss Detection

Learn more at hp.com/go/hpccr.

