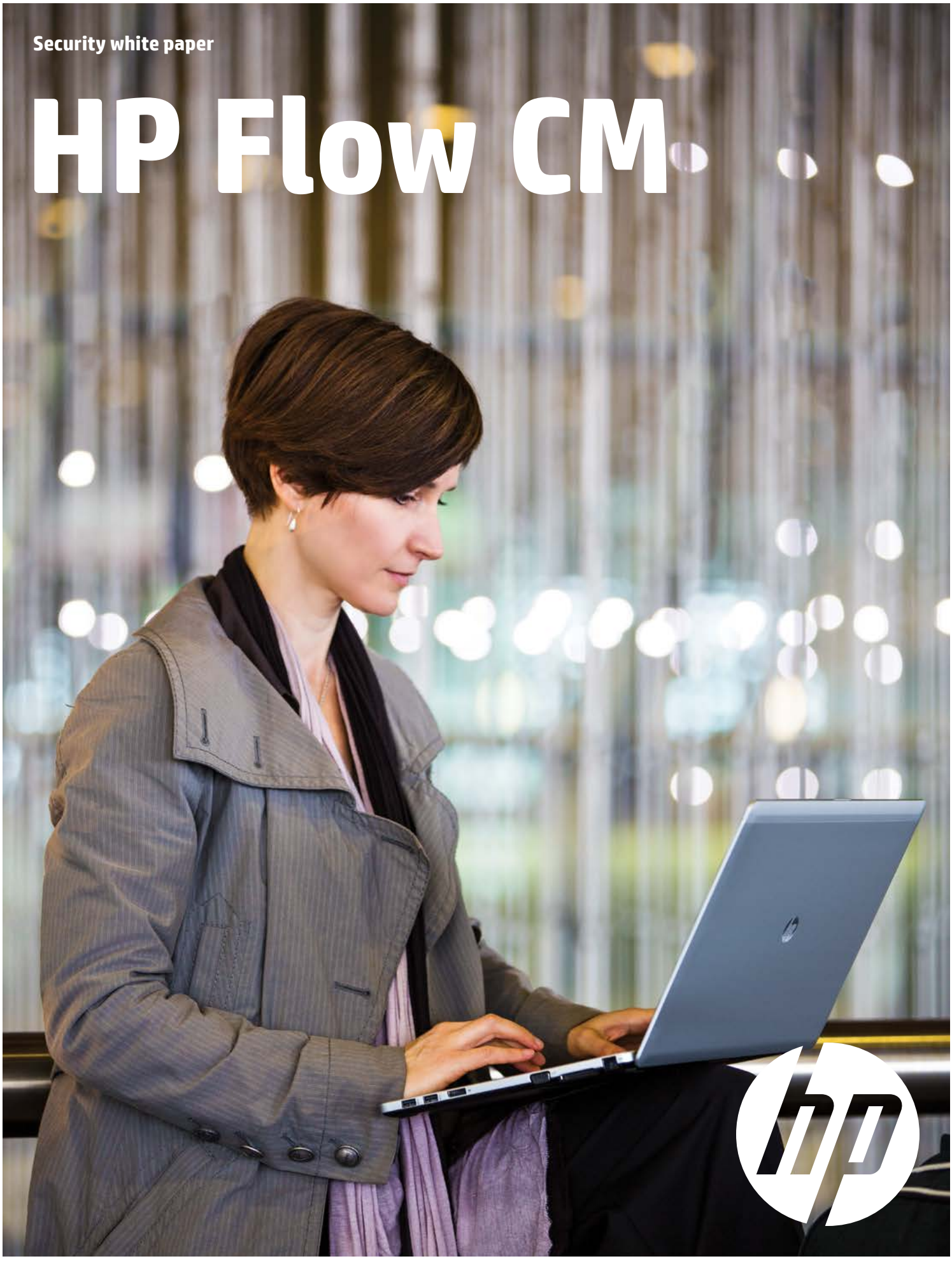
Security white paper

HP Flow CM



Content

3 Introduction
3 Systems
3 Architecture
5 Compliance and Certification
5 Physical Security
5 Security and Risk Management
5 Network Security
5 Secure Transmission and Data Protection
6 Secure Account Management and Secure Content Sharing
6 Backup and Data Recovery
6 Availability
6 Audit Log/Trail
7 Privacy
7 Deletion of Accounts
7 Safe Harbor and Binding Corporate Rules
7 Security Personnel

Introduction

HP Flow CM[1] is a cloud-based integrated solution for document capture, storage, search, retrieval, sharing, and more. HP Flow CM helps customers:

- Streamline workflows and make collaboration more convenient and productive with sharing and notification tools.
- Gain greater access to documents by storing them in the cloud.
- Safeguard sensitive business information.

This document outlines HP Flow CM's features and safeguards implemented by HP to help protect data.

Systems

HP performs security vulnerability scans for Flow CM servers regularly. Change tickets are opened to remediate high risk vulnerabilities.

When deploying HP Flow CM servers, HP keeps the packages up-to-date through automated configuration management tools, updated OS images, and application packages. HP's global security organization also monitors Flow CM servers for security vulnerabilities.

The HP Flow CM compliance framework has been designed to consistently address multiple certifications, regulatory requirements, and third-party attestations, rather than on a single, ad-hoc basis, allowing a structured approach to achieving compliance with HP requirements.

Security Monitoring and Management
Redundant perimeter firewalls and edge routers for the file repository help to block unwanted access to our environments, and our intrusion detection systems work around the clock, providing high levels of protection for customer data. HP regularly scan the environments for application and infrastructure vulnerabilities, and in case of an incident our incident response team engages to help resolve the situation.

Architecture

HP Flow CM is a cloud based solution with multiple client apps that enable virtually anytime, anywhere access.

[1] HP Flow CM is available in US and Canada only and through select HP partners.

Storefront
Provides provisioning and authentication to cloud services. The storefront also provides account management functions such as password recovery, deletion of accounts, addition of new users, companies, and resellers. The storefront utilizes Amazon Web Services (AWS).

File Repository
Contains user files. User files are encrypted at rest and in transit with 256-bit AES encryption. The file repository is also accessed by HP Flow CM-enabled multi-function printers (MFPs), smartphones, tablets, scanners, and personal computers.

HP Flow Sync and Scan
Allows users to print files to their HP Flow CM account, use Image Capture to scan files to HP Flow CM, send files to HP Flow CM from the Finder, and quickly view the uploaded files. HP Flow Sync and Scanis not required to use HP Flow CM, but it gives users more options for uploading files.

HP Flow CM iOS App
Enables use of Apple mobile devices (iPhone, iPad, iPod Touch) to store, manage, and view the files and folders in HP Flow CM user accounts. The HP Flow CM iOS mobile app is not required to use HP Flow CM, but it gives users more options for accessing and uploading files.

HP Flow CM Android App
Enables use of Android based mobile devices (phones and tablets) to store, manage, and view the files and folders in HP Flow CM user accounts. The HP Flow Android mobile app is not required to use HP Flow CM, but it gives users more options for accessing and uploading files.

HP Flow MFP Installer
Installs integrated MFP Application. Users can scan a hardcopy document from a MFP to a default folder or a designated folder in HP Flow CM. Users can scan a single page using the scanner glass on the MFP, or scan multiple pages at once using the MFP's Automatic Document Feeder (ADF).

HP Flow Sync
Sync files from the desktop and access Flow CM content from any device, even when offline. HP Flow Sync synchronizes files or folders across all of the user's devices so they can be widely accessed. Users can sync files between the computer and the HP Flow CM website, and view synced files on mobile devices. HP Flow Sync must be running and the user's computer must be online, or connected to a network, for files to sync automatically.

HP Flow Sync is not required to use HP Flow CM, but it gives users more options for uploading files. Once installed, HP Flow Sync is available to all users on that computer.

HP Scan to Flow CM
Allows users of WIA compliant scanning devices to scan documents and upload to HP Flow CM. Users can use HP Scan to Flow CM software to scan a hardcopy document from a MFP or scanner, and then save it in HP Flow CM. The HP Scan to Flow CM software is not required to use HP Flow CM, but it gives users more options for uploading files.

HP Universal Print PS
Users can use the Universal Printing Driver[2] (UPD) to upload any printable document to HP Flow CM as a PDF file. The UPD is not required to use HP Flow CM, but gives users more options for file types that can uploaded to HP Flow CM. The HP Universal Print PS software installs the latest version of the UPD onto the computer. If users have an outdated version of the UPD installed on their computer, the HP Universal Print PS software automatically upgrades the UPD to the latest version.

The HP Universal Print PS software also adds a 'Send to HP Flow CM' feature to the UPD, which allows users to upload any printable document to an HP Flow CM account. Documents that are uploaded through the 'Send to HP Flow CM' feature are always uploaded as a read-only PDF file.

[2] The HP Universal Print Driver is free and can be downloaded from Flow CM Downloads page.

Compliance and Certification

This section outlines the standards and certifications with which HP Flow CM complies.

Data Center
The data centers that host HP Flow CM in the United States undergo their own SSAE 16/ SOC2 audit. The SSAE 16/SOC2 audit standard is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II audit standard.

Standard	Compliance
SSAE16/SOC2 (for Data Center Hosting Infrastructure)	Yes
SAML2 authentication tokens	Yes
hpflowcm.com identity of the website has been verified by VeriSign Class 3 Secure Server CA – G3	Yes
Connection to hpflowcm.com has been verified encrypted with 256-bit encryption using AES_256_CBC with SHA1 for message authentication and RSA as the key exchange mechanism	Yes

Physical Security

Data Center / Storage
HP Flow CM 'Data at Rest' Is safeguarded with 256-bit SSL encryption and is stored in multiple secure physical locations that are protected 24/7 by onsite security including electronic access control, biometrics, dedicated cages and video monitoring. These locations undergo annual third-party audits. User 'Data in Transit' is safeguarded with 256-bit SSL encryption. This type of security is used to transmit data between HP Flow CM and all of user devices.

HP minimizes single points of failure in our computing environment by implementing controls such as component redundancy, real-time monitoring & backup, transaction recovery, replacement equipment, high availability hardware and redundant power sources.

Security and Risk Management

HP has dedicated functional teams each responsible for security, privacy, operations, standards, architecture, incident management, application security, information risk management, compliance and business continuity.

At the local level, HP has a 24x7 operations team that includes a security incident triage process to the various security and legal teams globally within the company that are responsible for handling security issues.

Network Security

All ports are blocked by default. All communication with our servers occurs over secure ports. Unsecured ports are redirected to secure ports.

Wireless Access
Wireless access to the HP Flow CM physical production environment is not allowed.

Secure Transmission and Data Protection

Encryption used to protect the confidentiality of transmitted information. Client connections use 256- Bit AES encryption for "Data in Motion". Client applications are certified through various distribution methods so that customers can maintain maximum control of their content.

[2] The HP Universal Print Driver is free and can be downloaded from Flow CM Downloads page.

Password Protection
HP requires strong authentication to access HP Flow CM. Passwords are stored as a hash based on industry best practices.

Encryption Keys
Encryption keys are managed according to security best practices, including policies for who has access to decrypt, protection of private keys, and periodic key rotation. HP limits access to the encryption keys to only those authorized individuals who have a business need.

Secure Account Management and Secure Content Sharing

Access to customer data is protected via authentication, authorization, account management and audit logging. HP Flow CM enables administrators to decide what content could be shared with other users in the customer environment, and the HP Flow CM platform is based on industry standards such as SAML2 authentication tokens to seamlessly enable access to business data.

Personally Identifiable Information (PII)
Encryption is used to help protect the confidentiality of personal information. User data is encrypted in HP's databases using AES-256.

Backup and Data Recovery

Backups for the HP Flow CM file repository are implemented via an enterprise HP server backup product providing AES 256 encryption. We utilize highly scalable and available enterprise storage environments along with automated data replication and backups. HP Flow CM is running in an enterprise-class datacenter on an industry leading cloud design, providing physical and logical redundancy at every layer.

The HP Flow CM database is backed up on a scheduled basis and encrypted at rest. This backup process can help maximize data recovery.

Availability

HP strives to provide customers with persistent availability to their solutions and data. Our goal for HP Flow CM application availability consists of site availability of no less than 99.95%.

As with any SaaS application, HP will occasionally have planned downtime for maintenance or to improve, add or remove features or capabilities we believe are right for our business and customers. Planned downtime for these reasons is not included in the calculation of HP Flow CM application availability.

HP Flow CM application availability also does not include unavailability of the service caused by circumstances beyond the control of HP or because of defects in materials or services located outside of HP Flow premises. These exceptions include, but are not limited to, failure of computer infrastructure systems at a customer's place of business or defects in the transmission of any information by acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving HP Flow employees).

HP will use commercially reasonable efforts to schedule all planned downtime.

Audit Log/Trail

HP maintains detailed audit logs that capture such data elements as account name, date and time stamp, activity performed, and source network address. Access to the database is limited to authorized personnel. HP maintains an audit stream that includes a Hash Message Authentication Code (HMAC) so if any modification occurs to the audit log, HP would be made aware. Audit logs are backed up and maintained.

Privacy

HP has a documented and published privacy statement that strictly prohibits the sale, rental, transfer, trading, or disclosure of personal information to third parties. The global HP privacy standards and statement can be found on the HP Flow CM support website or go to hp.com/go/privacy.

HP provides and requires security and privacy training for HP employees who handle confidential or personal information. HP adheres to global PII standards and processes.

HP provides administrative, technical and physical safeguards for customer environments and leverages industry programs such as Safe Harbor, ISO and others to keep information confidential.

Deletion of Accounts

HP implements a documented process for handling deletion of accounts and user data in the event customers choose to end their service.

Safe Harbor and Binding Corporate Rules

HP complies with the U.S. – E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. HP has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view HP's certification, please visit export.gov/safeharbor/

HP has also established a set of binding corporate rules ("BCR"), which have been approved by all Data Protection Regulators in the EEA and Switzerland, effective June 2011. The BCR ensure that personal data of covered individuals in the EEA is adequately protected while being processed by any of HP's global entities.

Security Personnel

HP requires background screenings for all new hires and contractors that have access to HP Flow CM infrastructure components.

Learn more at
hp.com/go/flowcm

Get connected
hp.com/go/getconnected

Share with colleagues

Rate this document

4AA4-9455ENUC, May 2014, Rev. 1