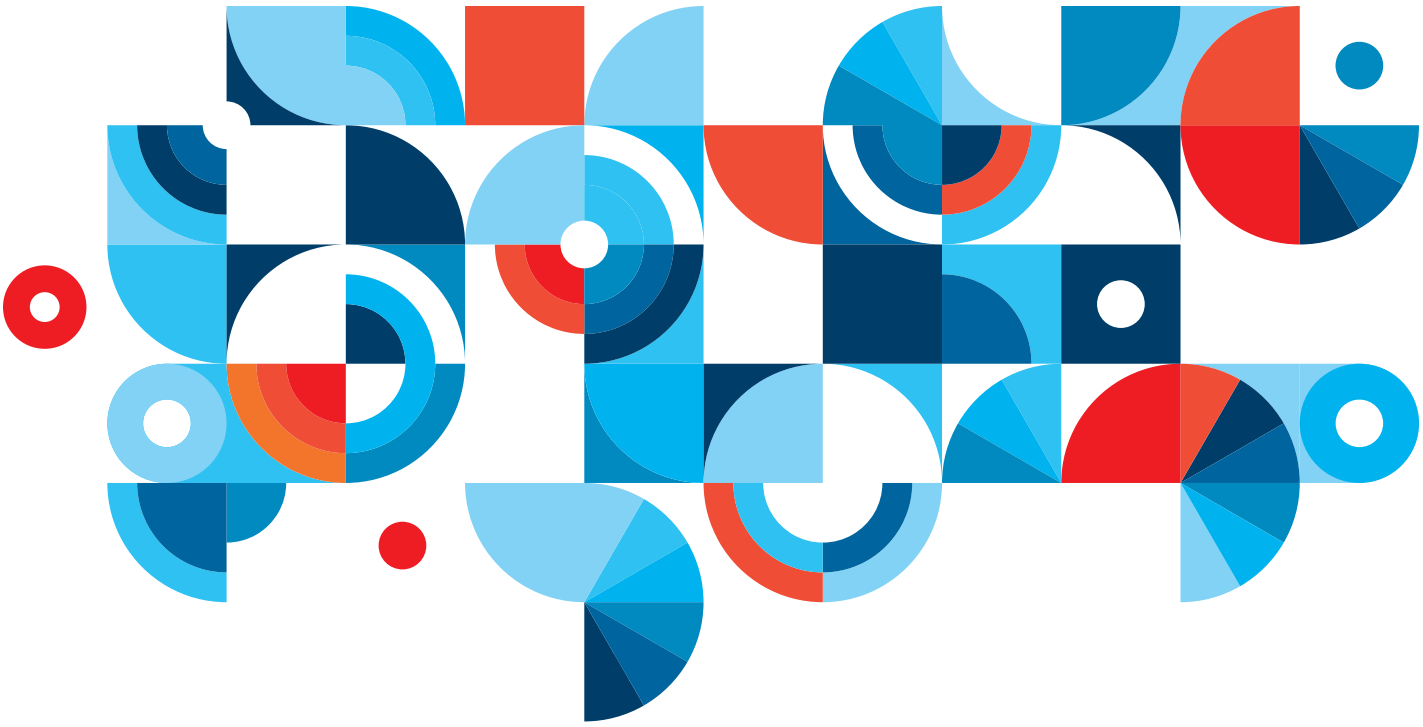
IBM Software
White Paper

September 2014

IBM SmartCloud™ Notes Security



IBM

Contents

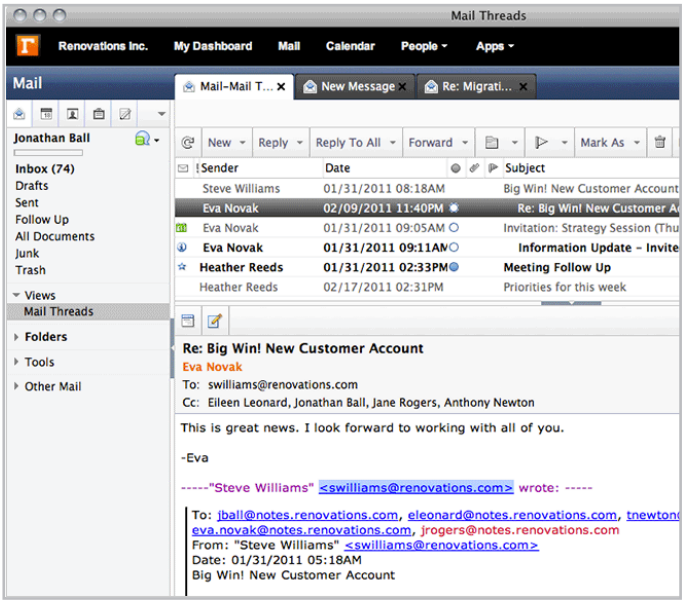
Introduction

IBM SmartCloud Notes helps to protect our customers' information through governance, tools, technology, techniques, and personnel, each of which we discuss in more detail below.

SmartCloud Notes (https://www.ibmcloud.com/social) is a full-featured email, calendar, contact management and instant messaging service in the IBM cloud.

At IBM we strive to implement security and privacy best practices.

The SmartCloud Notes security controls provide a range of protection of e-mail while enabling business operations.



Service Access

Physical access to service

SmartCloud Notes is deployed in a data center which provides physical protection to systems and data. Two sets of paired (for disaster recovery) data centers are located on the east and west coasts of the United States and in two locations in Japan. The data centers use multiple layers of security controls designed to help eliminate or prevent physical access to our systems. Biometric controls are utilized on all physical access points to help ensure that only authorized persons can acquire physical access to hardware. The data center is actively monitored via CCTV, which also provides logging of staff activities. Security officers are on premises 24 hours a day, 7 days a week.

High Availability

The data center was built with solid construction practices and includes fire prevention systems and electrical monitoring systems designed to help minimize the probability of natural disasters interrupting our services. The data center is connected to multiple power providers via multiple points in the public power grid and emergency power is provided by redundant generators and UPSs. It also possesses redundant network connection providers. Each logical component of the service is redundantly implemented by multiple physical systems designed to prevent the loss of any single CPU or hard drive from disabling any portion of the service. All customer data is stored redundantly in an active configuration of Domino replicas across multiple servers. All SmartCloud Notes

Domino servers are restarted daily to help ensure clean operations and failover. Multiple levels of monitoring, both external and internal, provide feedback on configuration health and service activity. Legal archiving and E-discovery is also available as an optional service (IBM Connections Archive Essentials Cloud). Daily reports provide system health and performance metrics information to operational and development staff. Sanitized crash data is also reported to the development team.

Network access to service

SmartCloud Notes utilizes a defense-in-depth strategy to protect against unauthorized access. We use a well recognized topology of multiple levels of firewalls designed to provide enhanced network protection. All user authentication occurs in a Yellow Zone (DMZ) and only authenticated connections are routed into the Green Zone (i.e. past the firewalls). All web traffic to the SmartCloud Notes data center is encrypted using SSL/TLS. Web servers use higher assurance extended validation (EV) certificates designed to provide stronger user visible authentication of SmartCloud Notes and enable users to avoid common spoofing and phishing server impersonation attacks. All SSL ciphers below 128 bits are disabled. All Notes client traffic in transit to SmartCloud Notes uses Notes port encryption with 128 bit keys. Incoming and outgoing SMTP traffic utilizes opportunistic TLS encryption, if the external SMTP server also supports STARTTLS. All internal Domino to Domino server traffic utilizes NRPC port encryption

Server Security

IBM has deployed real time antivirus support services on the SmartCloud Notes operating systems environment with a commercially available antivirus product. Security audit logs are produced, retained and secured to help enable analysis of the appropriate access and activities of provider system administrators.

People, Processes, and Compliance

Compliance

IBM strives to ensure that the data center and operational processes are consistent with SSAE 16 (formerly SAS70) Type II controls, and are audited annually by an independent outside auditor. IBM also requires that all third party service providers are SAS70 Type II certified. IBM compliance programs mandate periodic self-assessments and production scanning and reporting of compliance posture. Business process-based reviews are conducted through the project cycles. Privacy reviews align IBM Connections Cloud with IBM's comprehensive policies on privacy and client data protection, which can be found at http://www.ibm.com/privacy/us/en/.

Administrators

Access is restricted by role and task to conform to the principle of least privilege and SmartCloud Notes' separation of duties matrix. Operations personnel are required to use specific administrative credentials to access the service when performing administrative duties. IBM personnel do not have the ability to reset user passwords or to extract user ID files or customers' certifier ID files. Personnel also do not have read access to customer mail files. All provider access is evaluated quarterly. Security audit logs are produced, retained and secured to help enable analysis of the appropriate access and activities of provider system administrators.

Code Controls

Periodic vulnerability scanning is performed on the network and servers, and there are regular independent application and infrastructure reviews. Use of IBM Rational AppScan testing checks for common web exposures such as cross site scripting (XSS), cross site request forgery (CSRF), and SQL injection. Manual ethical hacking supplements the award winning AppScan tool set and targets the specific application and infrastructure configuration in SmartCloud Notes. Regular application testing covers common security exposures. Security testing is also integrated into the development cycle and automated regression testing. IBM has a dedicated security organization working across all IBM Connections Cloud services that provides security management activities surrounding the network, infrastructure, applications, and supporting services. The SmartCloud Notes security organization is responsible for the delivery of security capabilities, security architecture, infrastructure security design and compliance management process and technologies. It also has responsibilities within the system development lifecycle, which includes application and service product security requirements development, code security, security feature development and security testing activities. Security related functionality undergoes specific security design reviews by the cross-IBM Connections Cloud security organization. All code updates are peer reviewed, then approved by a development

architect before being merged into the code base. Each update is associated with an escalated problem report or approved work item. All code updates associated with a single problem report or work item are tested and verified. Code updates are rolled up into a full system build in preparation for deployment. After internal system verification testing, the development team stages the build for handoff to operations staff on a designated server. Operations does not have access to source code and their access to builds is restricted to this server. Operations staff then deploys the system to their staging and testing systems for another round of system verification testing. The system update is deployed in production only after those tests are successful.

Service Security

Identity and Authentication Notes clients authenticate into SmartCloud Notes using the same ID files they use to authenticate to on-premises Domino servers. All customers' Notes clients authenticate transparently against the SmartCloud Notes authentication servers in the Yellow Zone before connecting to any Green Zone servers that contain customer data. From the point of view of the Notes client and the end user, those servers are part of the customer's naming and certification hierarchies. For customers without an existing on premises Domino infrastructure, the root Certificate Authority (CA) and all related PKI and naming information (user ID files, server certificates) are generated and managed by the SmartCloud Notes team. Existing Notes customers will give a top level or OU level certifier ID file to SmartCloud Notes, and that will be used to generate the virtual server ID files for the virtual mail servers. User ID files for those customers are generated by their Domino administrators in the same fashion as existing user ID files. Critical portions of a customer's on-premises Domino directory are synchronized into the SmartCloud Notes hosted environment in a manner designed to allow SmartCloud Notes users to interoperate seamlessly with the organization's on-premises Domino users.

The SmartCloud Notes service will automatically and transparently provide ID file backup and ID file password reset services through a hosted Notes ID vault for each customer. Customers' administrators can reset Notes ID file passwords for their users with the SmartCloud Notes web administration interface. SmartCloud Notes users transparently authenticate to other SmartCloud Notes services from within the Notes 8.5.2+ standard client by way of a Domino- based SAML Identity Provider provided by SmartCloud Notes. SmartCloud Notes Web and SmartCloud Notes Administration are integrated with the single sign-on login and log-out mechanisms supported by other web based Connections Cloud services. Customers who wish to manage the web passwords and authentication experience of their subscribers to SmartCloud Notes can deploy a SAML Identity Provider on-premise for their SmartCloud Notes organization.

Mail Security

SmartCloud Notes supports both Notes and S/MIME signing, and encryption of e-mail through the supported Notes, web browser, and mobile clients. All SMTP mail entering or leaving the SmartCloud Notes service is scanned for viruses and spam by Lotus Protector for E-mail Security. All NRPC mail internal to SmartCloud Notes is also virus scanned. SmartCloud Notes messages are protected from potentially malicious active content in emails by the Notes client Execution Control List (ECL) mechanism when viewed with Notes, and by an active content filter which is designed to strip out active content such as Java and Javascript when viewed with a browser. Remote images inserted in e-mail, which can be used to track users, are not automatically fetched. The user may choose to show such images in an e-mail on a per email basis. SmartCloud Notes Web returns all message data retrieved from the Domino mail file to the browser with the Cache-Control: no-store HTTP header (and Cache-control: no-cache for IE 6) to help facilitate the browser not leaving behind any e-mail information within the browser cache.

IBM Corporation
IBM Software Group
Somers, NY

Produced in the United States of America
September 2014

Please Recycle

LOW14029-USEN-01