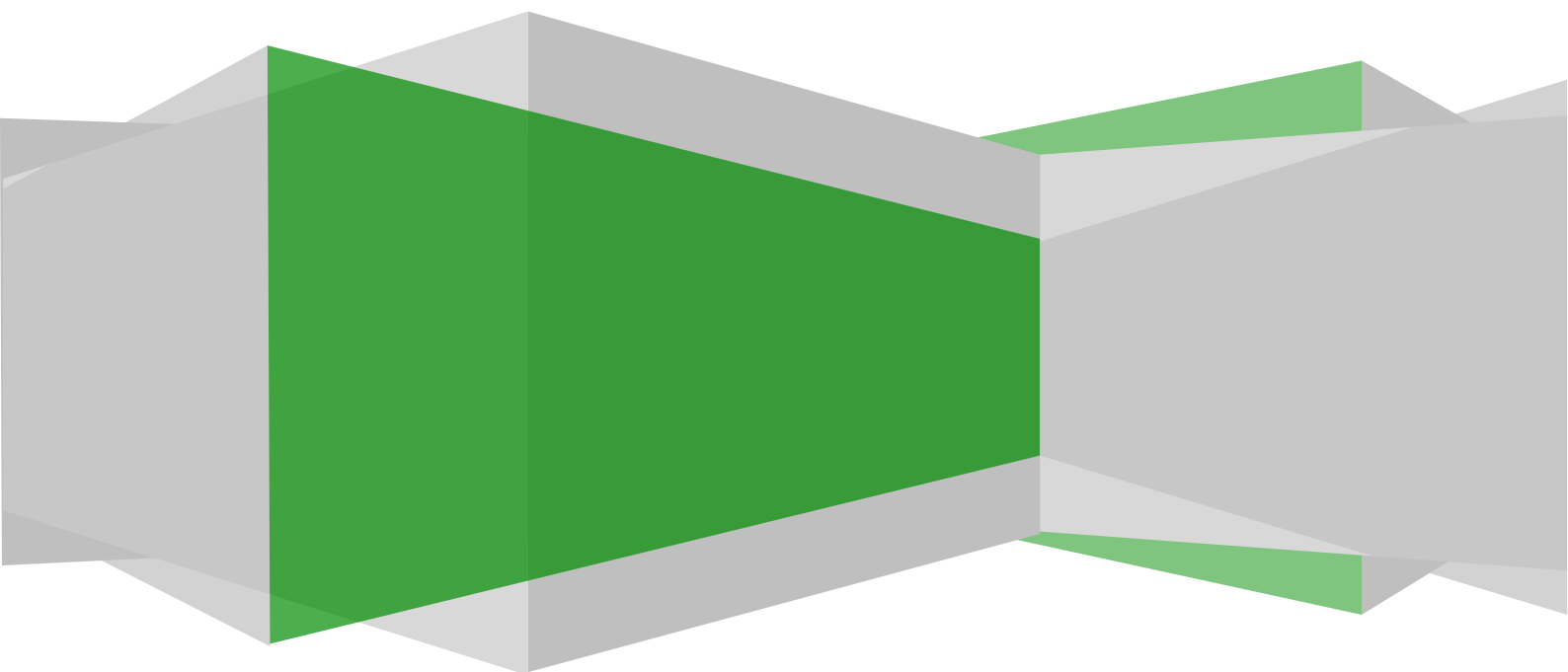




# inSync Cloud FAQ

November 2011



## FAQ List

Overview.....	3
What is inSync Cloud?.....	3
How is inSync Cloud different from other cloud-based backup solutions? .....	3
What key features does inSync Cloud offer? .....	3
How does inSync Cloud provide continuous data protection? .....	4
Infrastructure.....	4
Where is inSync Cloud hosted?.....	4
What are the key infrastructure components of inSync Cloud?.....	4
Where are the data centers located? .....	4
If additional data centers are brought online, how are customers notified before the data is allowed to backup to those locations? .....	5
What standard(s) or framework(s) does the infrastructure comply with?.....	5
What physical mechanisms are employed to protect inSync Cloud infrastructure resources and data assets? .....	5
Availability and Durability.....	6
What SLA’s does inSync Cloud offer for service availability and data durability? .....	6
Describe inSync Cloud’s business continuity plan. ....	6
Security .....	7
How are users identified and authenticated as persons that are approved to have access to the service?..	7
Can a specific password policy be specified and enforced? .....	7
Is the data leaving the customer site encrypted?.....	7
Is access to cloud encrypted? .....	7
Is Data Restore authenticated and encrypted ? .....	7
Can I restrict web-restore to particular IP addresses or users?.....	7
Can I turn off web or smartphone based restore? .....	8
How are the encryption keys managed? .....	8
What is the process for administrator’s password recovery? .....	8
Is there is security policies document for Druva employees and contractors for handling cloud data? .....	8
Virtual Private Cloud.....	8
What is a virtual private cloud and how is it applied to inSync Cloud? .....	8
How does inSync Cloud provide protection against traditional network security issues? .....	9
Monitoring.....	9
Does Druva monitor metrics on inSync Cloud? .....	9
Data Access and Restore.....	9
What methods of data restore are supported by Druva Cloud? .....	9
Is Data restore authenticated and encrypted? .....	10

Can I restrict web-restore to particular IP addresses or users?.....	10
Can I turn off web or smartphone based restore? .....	10
How can data be exported in bulk from inSync Cloud service?.....	10
Pricing .....	10
How is inSync Cloud priced? .....	10
How much does data export to a physical medium cost? .....	10
What's the minimum subscription period? .....	10
About Druva.....	11

## Overview

### What is inSync Cloud?

inSync Cloud is a fully-automated enterprise laptop backup solution offered as a software-as-a-service. Offering instant backups to a virtual private cloud with advanced app-aware deduplication and WAN optimization, inSync Cloud allows immediate access to backed up files and folders across all devices.

### How is inSync Cloud different from other cloud-based backup solutions?

Unlike other cloud-based backup solutions that are mere extensions of consumer offerings, inSync Cloud offers the following enterprise features/benefits:

- An elastic, virtual private cloud (powered by Amazon Web Services 'AWS') with enterprise-scale security, availability and durability.
- Enterprise-scale SLA's for recovery point (near CDP) and recovery time (instant restore) objectives
- A solution to the bandwidth bottleneck using advanced WAN optimization and source-based, global, app-aware deduplication technologies (ensuring 10x faster backups and 100% dedupe accuracy for supported applications)
- Access to data from Web browsers and iPhone/iPad/Android devices – anytime, anywhere.

### What key features does inSync Cloud offer?

**10x Faster Backups** - App-aware, global data deduplication technology significantly reduces the amount of data to be transferred during back up, while advanced WAN optimization analyzes available networks and optimizes the data transfer for latency and packet size.

**Enterprise SLAs for RPO and RTO** - Using near-CDP, inSync Cloud maintains infinite restore points to offer one of the best Recovery Point Objectives (RPO) in the industry. Each restore

point facilitates instant access and immediate restoration of data, reducing the overall Recovery Time Objective (RTO).

**Virtual Private Cloud** – Every customer gets a virtual private cloud protected by state-of-the-art AWS. This environment is highly secure and, available with a 99.5% uptime guarantee, and protects against disasters with multiple levels of data redundancy.

**Secure backups** - Network communication between client machines and the cloud is encrypted using 256 bit SSL encryption. Backup storage at inSync Cloud is encrypted using advanced 256 bit AES encryption ensuring end-to-end security of your data.

**Instant Access and Restore** - inSync Cloud supports instant access to your data from any browser and from smartphones/tablets including iPad, iPhone and Android devices.

### How does inSync Cloud provide continuous data protection?

Druva inSync's near-Continuous Data Protection (CDP) technology creates granular and point-in-time recovery points, each of which functions as a full restore point. Users can browse through any point in the past and instantly click to restore files and folders within that point.

Based on customers' specified retention policy, old revisions (restore points) can be aggregated or deleted. A compaction routine further physically deletes data from old revisions and reclaims the space for further use.

## Infrastructure

### Where is inSync Cloud hosted?

Druva inSync Cloud is hosted at AWS, which delivers a highly scalable cloud computing platform with high availability, dependability, and flexibility. AWS provides end-to-end security and privacy of data.

### What are the key infrastructure components of inSync Cloud?

The key components of inSync Cloud in AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3). In addition, inSync Cloud uses Cassandra, which is a highly scalable second-generation distributed database that brings together Dynamo's fully distributed design and Bigtable's ColumnFamily-based data model, for metadata management.

### Where are the data centers located?

Druva inSync Cloud data centers at Amazon are located in four different geographic regions - US East, US West, Ireland & Singapore. In addition, each region offers multiple availability zones for high availability.

### If additional data centers are brought online, how are customers notified before the data is allowed to backup to those locations?

When additional data centers become available, they will be handled in partnership with AWS in a way that is completely transparent to our customers. inSync Cloud will make the additional regions available in the product upon availability, so customers can create new storages in these regions and assign new users if needed.

### What standard(s) or framework(s) does the infrastructure comply with?

AWS has achieved compliance with the following standards and/or frameworks -

- **SAS 70 Type II**

AWS has successfully completed an in-depth SAS 70 audit of its controls (including control objectives and control activities), which relates to operational performance and security to safeguard customer data.

- **PCI DSS Level 1**

EC2, S3, EBS and Amazon Virtual Private Cloud (VPC) are all included in the PCI compliance validation.

- **ISO 27001**

AWS has achieved ISO 27001 Certification of its Information Security Management System (ISMS) covering its infrastructure, data centers, and services including Amazon EC2, Amazon S3 and Amazon VPC.

### What physical mechanisms are employed to protect inSync Cloud infrastructure resources and data assets?

**Redundancy** - AWS data centers are designed to anticipate and tolerate failure while maintaining service levels and are built in clusters in various global regions. inSync Cloud provides multi-zone replication of various elements of customer data including configuration, metadata and the actual data, thereby ensuring that customer data is available in multiple availability zones to handle failure of any zone.

**Fire Detection and Suppression** – AWS' automatic fire detection and suppression equipment reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action or gaseous sprinkler systems.

**Power** - The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the unlikely event of an electrical failure for critical and essential loads in the facility. Data centers are equipped with

generators to provide back-up power to the entire facility.

**Climate and Temperature** - Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems control temperature and humidity at appropriate levels.

**Management** - AWS monitors electrical, mechanical and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

## Availability and Durability

### What SLA's does inSync Cloud offer for service availability and data durability?

inSync Cloud will be available 24 hours per day, 7 days per week, excluding any scheduled (pre-determined window in a week) or unscheduled (with an email notification to the customer a few hours before the event) maintenance. inSync Cloud guarantees a 99.5% uptime SLA.

inSync's high availability is achieved by multi-zone replication of configuration data, metadata and data to multiple availability zones within each region.

Regarding data durability, inSync Cloud leverages Amazon S3's storage, which is backed with the [Amazon S3 Service Level Agreement](#), and is designed to provide 99.999999999% durability over any given year. The infrastructure is designed to sustain the concurrent loss of data in two facilities.

### Describe inSync Cloud's business continuity plan.

inSync Cloud service is designed for "continuous availability." AWS has designed its systems to tolerate systems or hardware failures without customer impact.

**Availability** - The AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. Data centers are built in clusters in various global regions. In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration.

inSync Cloud is architected to take advantage of AWS regions and availability zones. Distributing inSync Cloud instances across multiple regions and availability zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. In addition, data in all tiers of inSync Cloud (configuration, metadata and data) are **replicated synchronously across their availability zones.** **Business Continuity Plan** - AWS' Business Continuity Plan (BCP) drives standard practices to support ongoing, worldwide business and the ability to scale to the increased scope of catastrophic events. Standard practices are

supplemented with dedicated preparation for significant disruptions. AWS maintains current response plans for a series of disaster scenarios, and the response is tested in production by simulating disasters.

**Testing** - Druva tests critical systems under simulated conditions of catastrophic failure at least annually and uses routine maintenance intervals and external events as testing opportunities.

## Security

### How are users identified and authenticated as persons that are approved to have access to the service?

Client requests for backup are automatically authenticated with an authentication key, which is installed as part of the client installation.

For browser requests to access data over the Web for viewing or restore, inSync supports integration with Active Directory (both 1-time import and periodic import of users) for password authentication with the service.

### Can a specific password policy be specified and enforced?

System password policies can be implemented for Web restore passwords. In addition, Active Directory passwords, which can adhere to specific password policies, can be used.

### Is the data leaving the customer site encrypted?

Yes, data at inSync Cloud is encrypted at rest using 256-bit AES encryption. The data is encrypted during transmission using 256-bit SSL encryption.

### Is access to cloud encrypted?

Yes all protocols associated with Druva cloud are encrypted. This includes the HTTPS based web-console access and LDAPS support for Active directory integration.

### Is Data Restore authenticated and encrypted ?

Yes, the data restore is always authenticated and encrypted. The restore using the inSync application installed the user's PC is encrypted using SSL v3 256bit. The restore via web browser, smartphone or tablet is also encrypted using HTTPS.

### Can I restrict web-restore to particular IP addresses or users?

No, currently this feature is not available but being considered for future releases.

### Can I turn off web or smartphone based restore?

Yes, you can turn off web/smartphone based access for any particular user group or for complete server.

### How are the encryption keys managed?

The storage encryption keys are uniquely generated for each customer. The key is stored in the cloud in a double-encrypted manner using the administrator's password. Double encryption of the key using the administrator's password ensures that no one, including Druva, can gain access to the customer's data without knowledge of the administrator's password.

### What is the process for administrator's password recovery?

Given the role of the administrator's password in key management, the only way to reset an administrator's password is to have another administrator within the customer's organization reset it for them. Druva cannot reset a password because it would compromise Druva's security policies and procedures that ensure the highest security standards for data access and privacy.

### Is there is security policies document for Druva employees and contractors for handling cloud data?

Yes, Druva has documented and enforced security policies for cloud. A security handbook is also incorporated for developers working on the cloud.

A copy can be obtained by the customers on request.

## Virtual Private Cloud

### What is a virtual private cloud and how is it applied to inSync Cloud?

inSync Cloud offers a virtual private cloud to customers, which means that the cloud is deployed to be (virtually) private to each customer as follows –

- Druva segregates each customer's data from data belonging to Druva's other customers. Segregation is accomplished by:
  - Compartmentalization of customer configuration based on access credentials
  - Compartmentalization of customer metadata with Cassandra keyspace
  - Compartmentalization of customer data by S3 buckets
- Druva establishes and maintains appropriate environmental, safety, facility, and data security procedures and safeguards against unauthorized access, destruction, corruption, loss, or alteration of the service and customer data.

- Druva monitors for any attempted unauthorized access to the service and promptly takes all necessary action if any such attempt is discovered.

### How does inSync Cloud provide protection against traditional network security issues?

The AWS network provides significant protection against traditional network security issues. The following are a few examples:

**Distributed Denial of Service (DDoS) Attacks** - AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that has enabled Amazon to be the world's largest online retailer. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.

**Man In The Middle (MITM) Attacks** - All of the AWS APIs are available via SSL-protected endpoints, which provide server authentication. Amazon EC2 AMIs automatically generates new SSH host certificates on first boot.

**IP Spoofing** - Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

**Port Scanning** - Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy.

**Packet sniffing by other tenants** - It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance.

## Monitoring

### Does Druva monitor metrics on inSync Cloud?

Druva inSync Cloud is extensively instrumented to monitor key operational metrics within AWS, which utilizes automated monitoring systems to provide a high level of service performance and availability.

## Data Access and Restore

### What methods of data restore are supported by Druva Cloud?

Druva inSync cloud supports secure data restores using the inSync application installed on the PC or any web-browser. The data can also be accessed remotely using any iOS or Android based smartphone or tablet.

- iPhone/iPad application can be downloaded from [Apple Apps Store](#).

- Android app can be downloaded from [Google Marketplace](#).

### **Is Data restore authenticated and encrypted?**

Yes, the restore is always authenticated and encrypted. The PC restore is encrypted using SSL v2 256bit encryption and web-browser or smartphone/tablet access is encrypted using HTTPS.

### **Can I restrict web-restore to particular IP addresses or users?**

No, currently this feature is not available but being considered for future releases.

### **Can I turn off web or smartphone based restore?**

Yes, you can turn off web/smartphone based access for any particular user group or for complete server.

### **How can data be exported in bulk from inSync Cloud service?**

In addition to a normal restore process, an administrator could also request a bulk export from inSync Cloud to a physical device. Druva will ship the physical device to the customer at an additional cost. See pricing section for more details.

## **Pricing**

### **How is inSync Cloud priced?**

InSync Cloud is priced at \$2 per user per month. A user corresponds to a machine.

In addition, there's a \$1 per GB cost per month for the cumulative deduplicated storage consumed, which on an average is 75% lower than the total raw storage. To estimate the deduped storage for your organization, check <http://www.druva.com/insync/cloud/buy-insync-cloud/>

### **How much does data export to a physical medium cost?**

Bulk data export to a physical medium, if needed, costs \$50 per 100GB and a \$150 shipping and administration fee.

### **What's the minimum subscription period?**

The minimum subscription period for inSync Cloud is 1 year.

## About Druva

Druva provides premium enterprise-class solutions for data protection and disaster recovery. Our products - powered by our patented App-aware Deduplication and WAN Optimization technologies - are changing the way enterprises manage and protect their endpoint data. For more information about Druva, please visit [www.druva.com](http://www.druva.com)