

Go! Elephant Online Backup Service Description

Go! Elephant

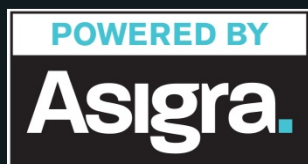


Table of Contents

1.	Go! Elephant Online Backup Service Summary	3
2.	Go! Elephant Online Backup Service Definition	4
2.1.	Go! Elephant Backup Client	4
2.1.1.	Go! Elephant Backup Client and Go! Elephant Backup User	4
2.1.2.	Encryption Keys	5
2.1.3.	Private Key	5
2.1.4.	Account Key	5
2.1.5.	Go! Elephant Backup Client SLA Monitor	6
2.2.	Go! Elephant Online Backup Service Setup	6
3.	Go! Elephant Online Backup Operations	6
3.1.	Backups	6
3.1.1.	Backup Sets	6
3.1.2.	Backup Lifecycle Management	7
3.1.3.	Backup Schedules	7
3.1.4.	Monitoring Backups	7
3.1.5.	Initial Data Collection	8
3.2.	Recoveries	8

1. Go! Elephant Online Backup Service Summary

- Go! Elephant Online Backup provides an automated and unattended backup service ensuring that data held on desktops, laptops, physical and virtual machines, and application / database servers is securely backed up and transferred offsite to be stored, encrypted in the Go! Elephant's data center.
- Go! Elephant's agentless backup and recovery solution eliminates servers disruptions and minimizes maintenance windows.
- The Go! Elephant Backup Client software needs to be installed on a physical or virtual server as a standalone or in an on-demand grid within the client's LAN. Using standard APIs, the Go! Elephant Backup Client captures requested data within the LAN and securely transfer it to the Go! Elephant's data center.
- Backed up data is transferred encrypted (FIPS 140-2 certified) from the central site, laptops and remote sites (Remote Offices/Branch Offices - ROBO) to Go! Elephant's Data Center.
- Utilizing the concept of incremental forever, Go! Elephant Online Backup leverages block-level deduplication and compression to transfer only changed data from the client's Central/ROBO to Go! Elephant's Data Center.
- Bandwidth throttling enables bandwidth optimization and backups even in cases where certain remote locations might suffer from low connection speeds.
- Go! Elephant Online Backup provides an easy to use interface that simplifies the backup and recovery process and provides detailed information about scheduled operations.
- Centralized configuration of the Go! Elephant Backup User enables a network administrator/IT manager to specify exactly what data is to be backed up ensuring investment is not wasted by backing up unauthorized or unnecessary information.
- A user-defined number of backup versions of files are retained on disk for immediate recovery.
- Service is remotely monitored 24 hours a day, seven days a week by Go! Elephant staff, and alerts are provided if scheduled backups are not completed or errors occur.
- Disk to Disk solution enables backed up data to be easily recovered without the need to locate and identify backup tapes.
- Customers can perform regular recoveries, allowing them to test the integrity of their data at any time.
- Go! Elephant Crash Response Team is on stand-by 24 hours a day, seven days a week to support major data recovery by delivering requested backup data to the customer site.
- In the event of a major customer site Disaster a portable storage media is delivered to the customer site, to a specified Disaster Recovery site or a restore to virtual environments is done at the Go! Elephant's facility with terminal access.
- Go! Elephant Backup Client can be configured with a local storage option for fast recoveries purposes. In this case if a recovery is needed, data stored locally can be quickly retrieved at LAN speed, without connecting through the IP WAN to the Go! Elephant Backup Server. Local storage can be configured for specific backup sets, especially ones containing critical data.

- 24hrs/day x 7 days/week x 365 days/year Help Desk support.

2. Go! Elephant Online Backup Service Definition

Go! Elephant Online Backup is a unique Disk to Disk alternative to traditional backup methods, replacing conventional tape-based systems with a fully automated cloud solution. It provides agentless, centralized and automated backups of desktops, laptops, physical and virtual machines, and application / database servers with secure offsite storage and immediate recovery from either a local or cloud copy.

The Go! Elephant Backup Client is installed onto the Customer network and performs the backup and recovery activity.

2.1. Go! Elephant Backup Client

The Go! Elephant Backup Client are self-contained processing units that assist in the delivery of the Go! Elephant Online Backup Service.

The Go! Elephant Online Backup is delivered through a suitably configured Go! Elephant Backup Client installed on the customer's network. The Go! Elephant Backup Client configuration will be determined by the specific requirements of each customer.

The key criteria in establishing the specification of the Go! Elephant Backup Client are the size and scope of the customer network, the number of customer servers, the mix of applications and operating systems, and the quantity of data to be managed.

2.1.1. Go! Elephant Backup Client and Go! Elephant Backup User GUI

The Go! Elephant Backup Client software runs as a service on Windows platforms or as a daemon on Linux platforms. It serves as a gateway to the Go! Elephant Backup Server. The customer's data tagged for backup flows through the Go! Elephant Backup Client, where it is deduplicated, compressed and encrypted before being sent to the Go! Elephant Backup Server

Each Go! Elephant Backup Client is connected directly to the customer's Local Area Network (LAN). The customer is responsible for providing an appropriate IP address. The Go! Elephant Backup Client supports either static or DHCP addresses.

Using standard APIs, the Go! Elephant Backup Client can remotely capture requested data and transfer data to the Go! Elephant's data center.

The Go! Elephant Backup Client comes by default with the ability to backup a wide range of applications and databases including: Windows 2000/2003/2008, Windows Vista/XP, Microsoft SQL Server, Microsoft Exchange, Oracle (including SAP-certified backup/restore), DB2, MySQL, PostgreSQL, VSS-support, System State & Services Database, Netware, AS/400, Linux/Unix, Mac OS X. In addition, Go! Elephant Backup Client integrates natively with VMware, Hyper-V and XenSource virtual machines servers.

The Go! Elephant Backup Client is configured and operated using a separate interface called Go! Elephant Backup User. The Go! Elephant Backup User GUI can be installed on one or more of the customers' Windows, Mac OSX, Linux RedHat or Suse systems.

The Go! Elephant Backup User is the customers' interface with the Go! Elephant Backup Client and can be installed on the same Go! Elephant Backup Client appliance or in a LAN workstation or laptop.

The Go! Elephant Backup User GUI is operated by the Authorized Customer Network Administrator to define backup sets and schedules, monitor backups, and perform restores.

Go! Elephant Backup User GUI access is integrated into Windows and Unix networking security. Individual user accounts, or groups of users, can be defined and granted authority to perform different levels of Go! Elephant Online Backup Service functions.

Typically, apart from the Go! Elephant Backup User GUI and the Go! Elephant Backup Client, no other Go! Elephant Online Backup software is installed on the customer's systems, making this an Agentless solution that is particularly easy to deploy and support.

2.1.2. Encryption Keys

For the security of customers' backed up data, the Go! Elephant Online Backup Client Software installed in the Go! Elephant Backup Client encrypts every file it sends with an encryption key provided by the customer. The files are stored and remain encrypted on the Go! Elephant Backup Server at all times. The decryption process occurs during recovery and is performed by the Go! Elephant Backup Client. This ensures that all backed up data transferred and stored outside the customer location is always encrypted. The Go! Elephant Backup Client uses up to 256 AES encryption and can be configured with private and account encryption keys.

Encryption is FIPS 140-2 certified.

2.1.3. Private Key

The private key is the default encryption key. It is used by the Go! Elephant Backup Client to encrypt data before it is transmitted to the [SERVICE BRAND Go! Elephant Backup Server at the Go! Elephant Data Centre. Backup files that are unique to a Go! Elephant Backup Client are encrypted using the Go! Elephant Backup Client private key and stored in the Go! Elephant Backup Client private library area on the Go! Elephant Backup Server.

2.1.4. Account Key

For customers with more than one Go! Elephant Backup Client, an account encryption key is also defined. The account key is used to encrypt customer files that are common to multiple Go! Elephant Backup Client to the same Go! Elephant Backup Server. These common backup files are encrypted with the account key and stored in the account library area on the Go! Elephant Backup Server. Go! Elephant Backup Clients that share a Go! Elephant Backup Server must be configured with the same account key.

The Go! Elephant Backup Server uses encryption cookies to verify every connection by the Go! Elephant Backup Client. Cookies are a piece of code generated using the encryption key. The Go! Elephant Backup Client sends its cookie on every connection request. The Go! Elephant Backup Server compares it with the cookie originally received during the initial Go! Elephant Backup Client configuration. This verification process ensures integrity of both private and account keys. After initial configuration the authentication between the Go! Elephant Backup Client and the Go! Elephant Backup Server is transparent.

Both private and account encryption keys can be up to 32 alpha/numeric characters and are configured during Go! Elephant Backup Client installation. Encryption keys are stored in the Database in encrypted form, so even if you have full access to the Go! Elephant Backup Client (such as Go! Elephant Customer Support) they cannot be read. Intentional or unintentional changes to the encryption keys will make data stored on the Go! Elephant Backup Server unusable.

It is the responsibility of the customer to supply appropriate values for the private and account encryption keys.

IMPORTANT: The customer is responsible for storing their original encryption keys in a secure location. Loss of the keys will prevent recovery of the Go! Elephant Backup Client and the customer's backup data. Go! Elephant has no knowledge of the customer's encryption keys and is unable to recover them. The encryption keys can be sent to the Go! Elephant Backup Server in an encrypted format, and through the DS-Operator a file can be generated to restore the Go! Elephant Backup Client.

2.1.5. Go! Elephant Backup Client SLA Monitor

The Go! Elephant has an SLA Monitor for monitoring Go! Elephant Backup Client backup and recovery related service levels agreed between the parties. It is HTML-based and accessed from customer machines running TCP/IP and an appropriate Web browser (Microsoft Internet Explorer, Mozilla Firefox or equivalent).

The SLA Monitor graphical user interface provides status information about the Go! Elephant Online Backup Service (and reference information about Go! Elephant customer services). The Go! Elephant Online Backup Status Report displays the current status of all Go! Elephant Online Backup backup activity. It includes backup start and completion times, backup results, a list of backed up data and information on any open files that failed to back up.

2.2. Go! Elephant Online Backup Service Setup

Go! Elephant will arrange a convenient time to perform the installation and configuration of the Go! Elephant Backup Client. Once the Go! Elephant Backup Client has been installed, Go! Elephant will work with the customer to configure the Go! Elephant Online Backup Client Software. This will involve configuration of the Go! Elephant Backup Client settings, definition of the customers' encryption keys, installation of the Go! Elephant Backup User GUI and demonstration of the Go! Elephant Online Backup functionality.

One day of onsite support for this initial configuration is included within the standard Go! Elephant Online Backup Service offering. The customer can purchase additional onsite support at a fixed daily rate.

3. Go! Elephant Online Backup Operations

All Go! Elephant Online Backup operations are performed using the Go! Elephant Backup User GUI. Authority to perform Go! Elephant Online Backup operations can be controlled by defining access to authorized users or groups of users, thus preventing backup and restoration of data by unauthorized personnel.

3.1. Backups

Go! Elephant Online Backup backups are based on backup sets that define the scope of the backup operation to be performed. Backup sets perform the specified backup operation and can be executed manually or scheduled automatically.

3.1.1. Backup Sets

A backup set defines the files or databases that are to be backed up. They can include or exclude files and databases by directories, or by filtering the file type. This allows the Customer Administrator to define backup sets that meet the customer's precise requirements, thus eliminating the backup of unnecessary data.

In addition, these backup sets define the number of retained generations, or versions, of files and databases that have been backed up. This enables the customer to selectively restore any of the previous versions of files that have been backed up. The default number of generations is set during installation.

Multiple backup sets can be defined for the same customer system. This feature enables the customer to define separate backups of different types of data on the same system. Multiple backup sets for the same system can also be setup independently.

Backup sets are defined in a similar manner regardless of the type of system to be backed up. A single interface enables efficient administration of the Go! Elephant Online Backup Service.

Authorized administrators can manually execute ad-hoc backups. However, under normal conditions execution of backup sets are scheduled and performed automatically.

3.1.2. Backup Lifecycle Management

Go! Elephant Online Backup provides for the long-term storage of non-critical backup data. This is typically backup data no longer required for day-to-day operations, but required for peripheral business concerns, such as legal, compliance or audit purposes.

The long-term retention of backup files, also known as Backup Lifecycle Management (BLM), is performed by defining and executing additional backup sets for the appropriate customer file or database systems. These long-term storage backup sets are typically executed on a monthly or quarterly cycle and complement the regular day-to-day backups.

Backup data generated by these long-term storage sets is stored in a separate disk area on the Go! Elephant Backup Server and copied to cheaper storage after a customer-defined interval.

3.1.3 Backup Schedules

Go! Elephant Online Backup has an extensive, calendar-based scheduler for automatically executing backup sets. Schedules can be defined to execute backups daily, weekly, monthly, or at a more randomly defined frequency.

Multiple schedules can be defined, and multiple backup sets can run on a single schedule. Where multiple backup sets are run on the same schedule, the customer network administrator can define the number of concurrent backup sets to be executed, and the priority in which they should be executed.

The Go! Elephant Backup User GUI provides a graphical view of the backup schedules. This allows the customer network administrator to quickly view the status of the backups and identify any conflicting or overlapping schedules.

3.1.4 Monitoring Backups

In addition to the Go! Elephant Backup User GUI, a web-based interface from the Go! Elephant Backup Client presents daily management reports on the status of the Go! Elephant Online Backup Service. This web interface includes a summary of scheduled backups, highlights of any errors that may have occurred and statistical information detailing the quantity of data backed up.

The Go! Elephant Backup User GUI provides extensive monitoring and reporting capabilities for customer administrators. This includes detailed logs of backup activity, details of all files backed up, error reports, and audit trails for all backup and restore activity.

3.1.5 Initial Data Collection

The primary method of backup is over the WAN line between the Go! Elephant Backup Client and the Go! Elephant Backup Server at Go! Elephant's Data Centre. However, in situations where the initial backup volume makes a network transfer impractical, Go! Elephant will perform an initial backup through a portable drive and transport it to the Data Centre.

Where it is appropriate for Go! Elephant to manually transport the initial backup data, the process will involve connecting a removable/portable hard-disk location on the customer premises to the Go! Elephant Backup Client via a LAN connection. Initial backups are performed to this removable/portable hard-disk location until an agreed time when the removable/portable hard-disk device is disconnected from the LAN and transported back to the Data Centre. Once at the Data Centre, the data residing on the removable/portable hard-disk device is imported into the Go! Elephant Backup Server and incremental backups between the Go! Elephant Backup Server and the Go! Elephant Backup Client can occur on a regular basis (either scheduled or on-demand).

The initial backup is the only circumstance where a full backup is done, after which, all other backups are incremental (incremental forever).

3.2. Recoveries

The Go! Elephant Backup User GUI allows the authorized customer network administrator to quickly and easily select and recover data. The administrator can restore data to a remote system by using their desktop/laptop.

There are four methods in which data can be restored.

- Data is restored at LAN speed from Local Storage.
- Data is restored across the WAN link.
- Restore data is delivered via a portable disk.
- A Go! Elephant Backup Server with replicated data can be delivered to the customer's site or alternative disaster recovery location or hot-site in the event of a major DR effort.

The following table maps the 4 different categories of data restoration methods.

Restore category	Description	Volume of customer data	Restore method	RTO (hours)
1	<u>Local Recovery</u> Fast recovery from local storage	N/A	Local Storage	y
2	<u>Moderate Data Loss</u> Single/small number of files; small/medium server	Up to X GB	Cloud Restore	y

3	<u>Major Data Loss</u> Major database server or multiple servers	From X GB to X TB	Portable Disk Restore	y
4	<u>Disaster Recovery</u> Multiple server loss or complete site	X TB +	DS-System Restore	y

Local Restore

Local Restore addresses fast recovery requirements by saving copies of the backup files at a local storage location. If a recovery is needed, the file can be restored quickly from local storage, at LAN speed, without connecting through the IP WAN to the Go! Elephant Backup Server. Local storage can be configured for specific backup sets, typically ones containing critical data. On the first regular backup, the whole backup set is stored in the local storage.

When a file in a backup set identified for local storage is created or modified, it is sent by the backup process to both the Go! Elephant Backup Server and to local storage. Data stored on locally is compressed but not encrypted, and stored as regular generations, without elimination of common files or delta processing. However, delta processing is performed to the data before it is sent to the Go! Elephant Backup Server. Any backup sets marked for local storage are also sent to the DS-System to be stored encrypted and compressed with master/delta online generations and common file elimination.

Requests to recover data will attempt to retrieve data from local Storage first. If the requested files are not available locally, data will be retrieved from the Go! Elephant Backup Server storage.

Utilizing local storage on DS-Clients speeds up the recovery process thus increasing SLA compliance. In addition, local storage facilitates backup windows to be met regardless of WAN connection bottlenecks.

Cloud Restore

(Normally conducted by the customer without SP intervention)

The Go! Elephant Backup User GUI provides a Restore Wizard that guides the customer administrator/end user through the process of selecting and restoring data. The Restore Wizard allows the administrator to search and select files for restore, select the version of the files and choose the target destination for delivery.

Having selected the data to be restored, the Go! Elephant Backup Client retrieves the data across the WAN from the Go! Elephant Backup Server at the Go! Elephant data center facility. The Go! Elephant Backup Client then sends the data to the specified system on the customer network. As part of the operation, all associated security permissions for the data are restored.

In case backup data is available in the Go! Elephant Backup Client Local Storage, data will be restored by Go! Elephant Backup Client at LAN speed. The Go! Elephant Backup Client then sends the data to the specified system on the customer network

Portable Disk Restore

(Normally conducted by both the Customer and SP)

For larger quantities of data, the customer administrator can invoke the Disaster Recovery Wizard to request that a copy of the backup data be copied to a portable disk device.

The Disaster Recovery Wizard provides the same level of restore granularity as the Restore Wizard, but rather than restoring the data across the network it is copied to a portable disk device, which is then transported to the

customer site. The customer network administrator can then use the Go! Elephant Backup User GUI to restore the requested data directly from the Go! Elephant Backup Client to the system being restored.

The only data that can be restored from the portable disk device is that which was specified when initially requested. If additional backup data is required then this can be restored either online or by initiating a new request for a portable disk device.

Restore from a new replicated Go! Elephant Backup Server

(Normally conducted by both the Customer and SP)

The third restore scenario refers to shipping a new Go! Elephant Backup Server with replicated data to the customer's site. This could be used as an alternative to the portable disk device or in a major disaster situation where complete backup data is required.

Go! Elephant will replicate the production Go! Elephant Backup Server entirely to a new Go! Elephant Backup Server and ship it to either the customer's primary work site or an alternate disaster recovery location. The replicated Go! Elephant Backup Server is then connected to the customer's private LAN connection. Data can then be restored in the same way as would an online restore but with the performance benefit of the replicated Go! Elephant Backup Server being on an internal LAN at native Ethernet speeds.