GoodSync

GoodSync Control Center

Data and Security

GoodSync Control Center Centralized management over data backup and synchronization jobs.

Compatible with:

Windows

Windows Server 2003, 2008, 2012, 2016

Windows XP, 7, 8, 8.1, 10

Mac

OSXServer

Linux

GoodSync is compatible with the majority of Linux Oss; for details on the specific versions, please contact our technical support.

NAS

GoodSync Enterprise installer for NAS devices is compatible with the majority of Western Digital, Synology, QNAP, and other Linux based NAS devices.

GoodSync can be run on Windows, Mac, and Linux operating systems hosted in virtualization software such as VMWare, Virtual Box, Hyper-V, etc. Each virtual machine involved inthe synchronization / replication requires appropriate licensing.

Contact Information

For more information on GoodSync Control Center please contact our support or sales team.

Syber Sistems, Inc.
11781 Lee Jackson Hwy, Suite 380
Fairfax, VA 22033USA
Phone: +1-703-218-1851 Option-4
Contact e-mail: enterprise@goodsync.com

Technical support is available between 8:30AM and 5:30PM EST Monday - Friday

What Data is stored on the GoodSync Control Center?

A limited amount of data is stored within the Control Center about your Users, Computers, GoodSync Jobs, and Job Runs. This data is stored securely within our SQL database in our Tier One Data Center.

The following is all of the Data shared between the Client (GoodSync running on your Workstation or Server) and the Server (the Control Center).

Users and Computers are the two primary points of Job Distribution within the Control Center. GoodSync Jobs are assigned to a User and/or Computer, and when a Runner Service requests Jobs, it requests for both the User the Runner is running as, and the Computer the Runner is running on. The information stored is:

- User OS Name – The User Name of the Account running the GoodSync Service
- Computer Name – The PC Name of the device running the Service
- Runner Name – Combination of UserName@ComputerName
- Runner Password – Random Password, assigned to Runner on initial connection; generated by Control Center Server
- User Full Name and Email Address are optionally provided, but not required

The GoodSync Job in the Control Center has all of the same options and functionality as a GoodSync Job created in the core product itself.

- GoodSync Job Command Line – This contains the same information as a standard GoodSync Job, including Left Folder, Right Folder, and all Job Options

A Job Run corresponds to an individual GoodSync Job doing an instance of a backup or synchronization from a Computer. This consists of the basic summary of the current stats of the GoodSync Job:

- Date/Time Started – Date Time the current Run of the Job began
- Job Name – The name you have provided for the Job within the Control Center
- Computer / User – The same User / Computer Names from within the Control Center
- State – Analyzing, Syncing, Synced, Analyzed
- Progress – The estimated percentage complete of the current State
- Return Code – In Progress, Ok, Terminal Errors, etc.
- Terminal Error – If there is an error that causes the Job to not complete, the error message from GoodSync

- # Files Synced – Upon completion of the Job, the total number of files synchronized
- # Errors – Upon completion of the Job, the total number of Errors encounters Note: not all errors are Terminal Errors
- # Conflicts – Upon completion of the Job, the total number of Conflicts (a Conflict is a File Changed on both Sides of a synchronization, since the last run of the Job)
- Log Lines – A line by line copy of the log generated by GoodSync when the Job runs. Aspects of these log lines are parsed to populate the other Job Run details described here

How is Communication done with GoodSync Control Center?

All communication with the Control Center is done via HTTPS over port 443. For those hosted on our Control Center, this means establishing a connection to https://jobs.goodsync.com. For those hosting their own control center, this means establishing a connection to that server via its IP, Computer Name, or DNS. In either case, as long as the client can view the Control Center through a web browser, GoodSync will be able to communicate as well.

Requests are begun on the client side, by the GoodSync Runner Service. The client is configured (Windows through Registry, Mac/Linux through a configuration file) to look for Jobs on a specifific Control Center Server (URL) and CompanyID (unique numeric identifier for each Company).

On first launch, the client sends its information (User Name and Computer Name) to the Control Center Server. The Server creates a Runner (combination UserName@ComputerName), generates a random password, and sends these back to the client via https response.

All subsequent communication between Client and Control Center Server send User Name, Computer Name, and the assigned Password. As the GoodSync Job runs, the Logs are sent back, line by line, to the Control Center, and written to the SQL database for reporting purposes.

How is Data on GoodSync Control Center Secured?

Data Center Security

All data is stored securely within our SQL database in our Tier One Data Center. In-house physical security is on-site 24x7x365 in addition to key card access, biometric scanners, mantrap entries, IP-DVR cameras and controlled site access. Security systems and protocols are tested regularly to ensure exceptional response rates.

http://www.coresite.com/data-centers/locations/northern-virginia-washington-dc

Server Security

All of GoodSync's internal servers use the most up to date security patches and GoodSync uses best practices for system access.

The GoodSync Control Center application is built on a proprietary web server software, making it difficult to use known vulnerabilities of typical web servers like Apache or application platforms like PHP.

The web server itself is designed to fight off DDOS (distributed denial-of-service) attacks, by collecting extensive statistics, to track users and automatically block suspicious connections.

Communication Security

All communication with the Control Center is done via HTTPS over port 443.

Application Security

The GoodSync Control Center application blocks all attempts at SQL injection to ensure all data is validated before being used as the basis for database queries.

Additionally we block all XSS (Cross-Site Scripting) attacks, and use anti-CSRF (Cross-Site Request Forgery) tokens within all forms and requests to prevent any attacks, or data sniffing.

Optionally, on a Company by Company basis, Administrators can enable logins for only accounts that have been confirmed through email verification.

Data Security

All potentially sensitive data (Administrator passwords, File system credentials, etc.) stored in the SQL database is stored in encrypted form and only decrypted in memory on an as-needed basis.