How Will SkySync Impact My Existing Security?

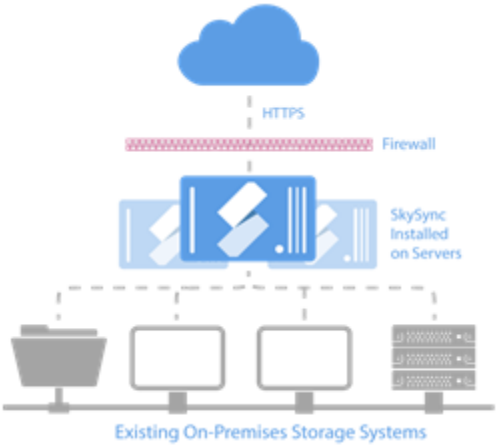
Overview

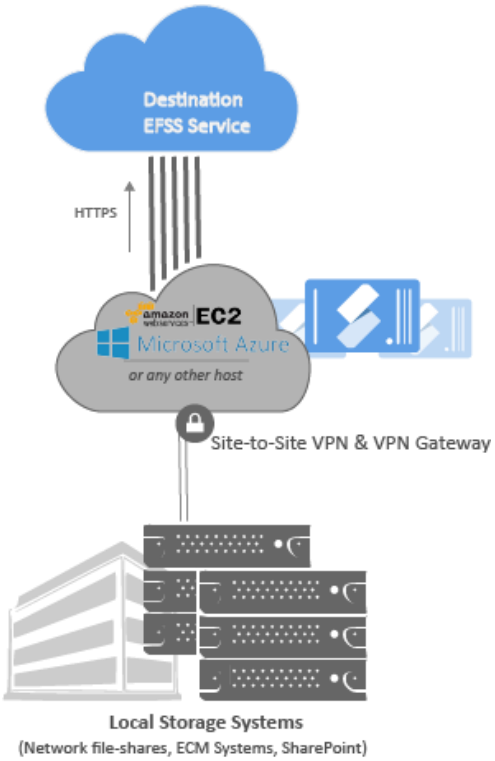
This document outlines information about how SkySync interacts with your existing security IT infrastructure. Portal Architects recommends that you contact SkySync Professional Services to assist you with your specific security configuration requirements.

On-Premises Deployment

SkySync is client-downloadable software that is installed on-premises on a Windows Machine (Server 2008-R2, Server 2012, Windows 7/8/10 and SQL Database). SkySync runs within your existing security infrastructure without requiring modification, leaving you in complete control of security.

- Deploys on client hardware.
- Sits behind the client's firewall.
- Fully under the Admin's control.
- Does not save or cache files.
- Rides "on top" of existing security.
- Has no impact upon existing security.



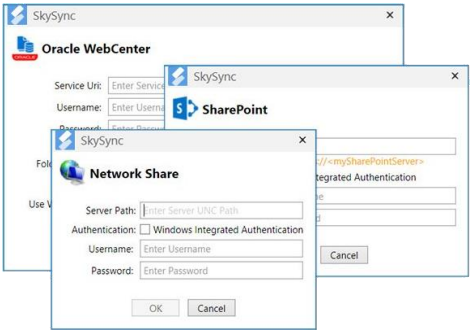


Cloud Compute Deployment

SkySync is certified by Microsoft Azure and Amazon Web Services and may be purchased and provisioned via the Microsoft Azure and AWS Marketplaces. It can also be deployed in any other private cloud. SkySync is deployed as a virtual machine and remains under the domain and complete ownership of the client.

SkySync Connections

SkySync uses a concept of “Connections” to tie various platforms together. A connection can be either a source or a destination. SkySync stores connection information (for example, user name, password, URL, UNC, etc.) encrypted within its database. This makes it important to secure the server running SkySync’s local file system to add additional protection to this information. SkySync uses all the default ports based upon the platform’s required communication protocol.



Security Impact

SkySync does not control, edit, move, or modify existing security constructs. SkySync acts as an external user to storage systems, interacting with them via their public API’s or via the credentials utilized for Network-based (NFS/SAN/NAS) file systems.

The connection identity and credentials used during the Add New Connection process directly controls how and what SkySync can access and modify. SkySync completely respects the permissions set with any platform, and will receive access denied or other related permissions errors if requested to perform operations where underlying credentials do not have access.

As such, the connection identity determines what SkySync can access on each underlying platform and has several implications:

- SkySync cannot access folders, drives, or any content areas where its connection identity does not have access.
- SkySync is most efficiently configured when the connection identity has permissions to all desired sync locations.
- Content Ownership information (created by, last modified by, etc.) may be tagged with the connection identity when SkySync operates on content, depending upon platform support.
- SkySync can be configured on a “user by user” basis to solve content ownership issues, however this will require additional administrator maintenance and the sheer number of connections would not easily scale.

Security Best Practices

Principle of Least Privilege

SkySync is an Administrator utility and is not intended to be operated by anyone from the general user community. It's highly recommended to follow the "Principle of Least Privilege" (PoLP; also known as the Principle of Least Authority). This computer security concept promotes minimal user profile privileges on computers, based upon the SkySync connector's necessities.

Following PoLP, the System Administrator will need to create Service Accounts for all platform connections and it's recommended that the SkySync Service password(s) are set with no expiration. Note that if a password expires, SkySync will fail to connect to the platform.

Memory Management

Vulnerabilities such as the Heartbleed bug which expose data in memory are a major concern for IT organizations. Minimizing the exposure of files in memory is imperative for secure file transfer. As SkySync downloads from the source and reads a file, only a small portion of the file is available and decrypted in memory at any given time. Once the chunk is read into memory, it is pushed up to the destination and then the same block of memory is used to read the next chunk. After the file is uploaded in its entirety, the memory is zeroed out.

Checksums and Data Integrity

SkySync also supports the use and validation of checksum values for platforms that support it. While this does not specifically provide for data security, it does ensure data integrity, the lack of which could signal a breach in data security.

Auditing & Custom Reporting

If activated, SkySync provides a full array of auditing capabilities where every action is logged within the SkySync database. If any potential issues arise during the transfer, it will be logged in the audit and administrators will be notified.

Security-Safe

SkySync is "security-safe," making no impact on your existing security measures and leaving you in complete control of your content and user access. If you have specific questions about how SkySync may interact with your security environment, contact us.