Storage Made Easy Security White paper

SAAS HOSTED SERVICE PHYSICAL SECURITY

For the hosted SaaS service SME uses multiple data centers in USA and Europe. All data centers are Tier IV facilities and are:

USA: SSAE16 SOC1/2 compliant, have 24x7 armed security, facility surveillance, biometric + keycard access to the data floor, keycode access to the cage, plus our own surveillance on top of the facility surveillance.

Europe: The Data Centers have ISO27001:2005, ISO9001:2008 certification, plus 24x7 security, facility surveillance, biometric + keycard + mantrap access to the data floor, locking cabinets with physical key access

UK: This is a new facility, currently undergoing the iso 27001/9001 process and also has 24x7 security, facility surveillance, biometric + keycard + mantrap access to the data floor, locking cabinets with keycode access

All data centers have 24/7 physical security, facility surveillance, biometric , keycard entry authentication and mantrap access to the data floor, uninterruptible power and backup systems

Understanding Security FAQ and custom integration options

OVERVIEW

The purpose of this white paper is to:

1. Provide a Security overview of the Storage Made Easy Cloud Appliance

2. Describe an approach to security integration with the Storage Made Easy Appliance.

Ultimately there are many different security mechanisms that organizations use, and if the options provided are not relevant the please get in touch with us and we will have a direct discussion about what is possible.

The assumption for this white paper is that the Storage Made Easy platform will run on-premise as an appliance and the paper describes answers to common security questions and also discusses an approach

Understanding Storage Made Easy default Access Authentication

Storage Made Easy provides a stateless REST API to integrate with external systems. This is the same API used internally by SME and is also used to provide SME data access components.

A component needs to authenticate the user first with the SME Service before the user can use any of the SME REST services. A component authenticates a user with SME by calling a REST service with the users login name and password, after successful authentication a token is returned. This token is passed in all the subsequent REST calls to Storage Made Easy for any operation performed by the component on user's behalf.

SECURITY FAQ

On the wire Security

HTTPS (SSL / TLS) can be configured for all users of the SaaS hosted Cloud File Server and the on-premise Appliance. HTTPS is an acronym for hypertext transfer protocol secure. HTTPS is similar to the normal hypertext transfer protocol, except it is different because the "S" at the end identifies it as having a secure HTTP connection.

A HTTPS connection is used often in businesses where sensitive information, such as credit card numbers, are being passed along at point of purchase sites or other commerce sites The https protocol gives assurance that potential hackers are not able to intercept the message containing sensitive data as it is sent to its destination.

A commercial server that uses HTTPS must have a public key certificate issued that verifies the entity. The end-user can verify the entity by clicking on the HTTPS icon from the browser.

Data Security

Storage Made Easy can be used to encrypt data transmitted to any cloud that is mapped to a users personal, Cloud File Server, or Appliance account. SME uses AES-256 streamed encryption using the Rijndael cipher, with Cipher Block Chaining (CBC) where the block size is 16 bytes. The cipher Rijndael consists of:

- an initial Round Key addition
- Nr-1Rounds
- a final round.

The chaining variable goes into the "input" and the message block goes into the "Cipher Key. The likelihood of recovering a file that has been encrypted using our encryption is fairly remote. The most efficient key-recovery attack for Rijndael is exhaustive key search. The expected effort of exhaustive key search depends on the length of the Cipher Key and for a 16-byte key, 2127 applications of Rijndael.

SECURITY FAQ

Data Security Continued

Any AES-256 decryption tool that supports the Rijndael cipher with 16 byte blocksizes can be used to un-encrypt files. SME also provides free desktop decryption tools for Mac, Windows and Linux that enable the decryption of a file if you download it directly from a mapped cloud ie. without any access to the SME service.

Authentication Security

Storage Made Easy username and passwords are stored in an encrypted fashion. User login is required in order to obtain a token for a session, which allows a user to access a specific Storage Made Easy resource without using a username and password each time but in which the token is still passed on each request.

Once the token has been obtained, the user uses the token, that offers access to a Storage Made Easy resource, for up to 1 hour (it times out if there are no user interactions or is removed if the user logs out). This mechanism of authentication be complimented or replaced with other authentication systems, such as Active Directory which is available for the on-premise Cloud Appliance.

If a Cloud Provider supports OAuth, which is a mechanism to connect to a Cloud Provider without revealing password details, then SME uses this delegation mechanism to access the public or private cloud resource. For Cloud Providers that don't use OAuth, authentication details are stored encrypted.

Document Security

Documents can be securely shared using the Storage Made Easy platform in a number of ways:

- Documents can be encrypted on upload using the aforementioned 256 bit AES security. The private key is not stored on the platform and only known by the user.

SECURITY FAQ

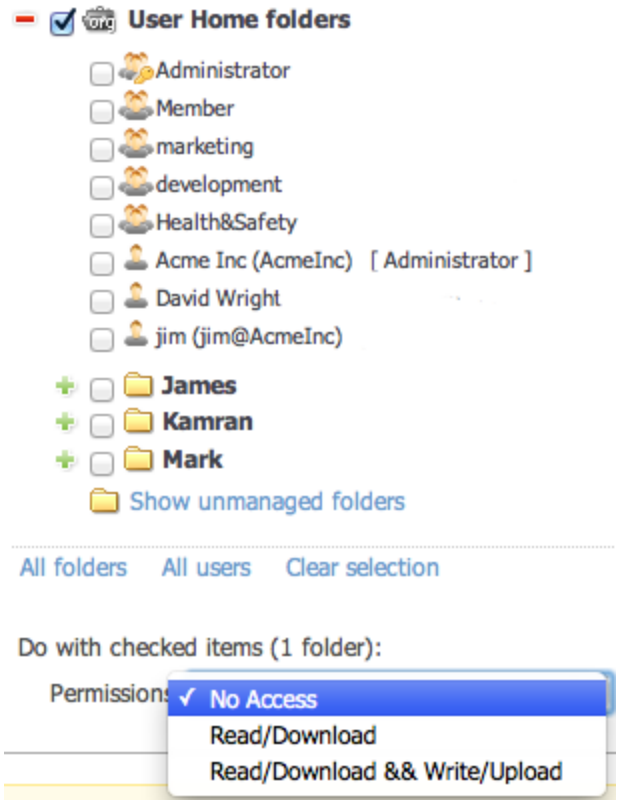
Document Security (cont)

- Private links can be created for documents and these can be combined with passwords and/or time-expiry to secure the document.

- Links can be set to be time expired and/or combined with private links and password for further additional document security.

Access Control and Permissions

Storage Made Easy supports unified Access Control Permissions across Cloud Services at a Role, User, or folder level for shared folders. The Permissions can be taken from Active Directory if single sign-on integration is being used.

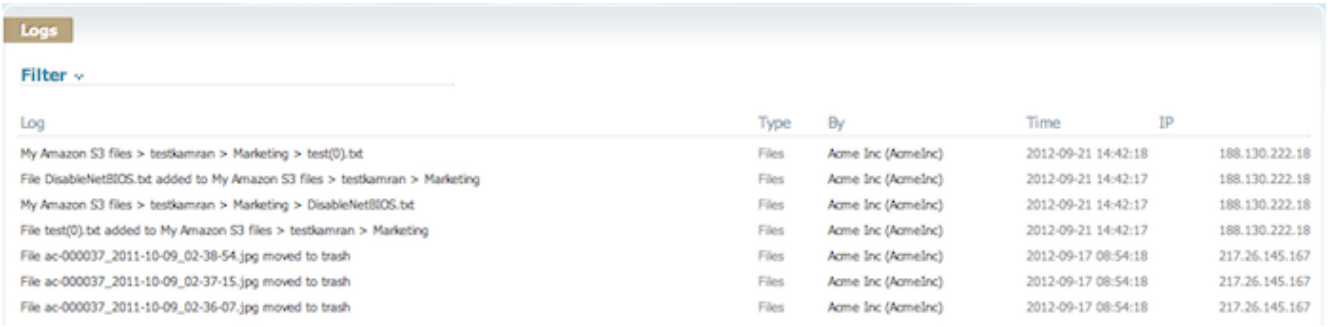


SECURITY FAQ

Audit Security

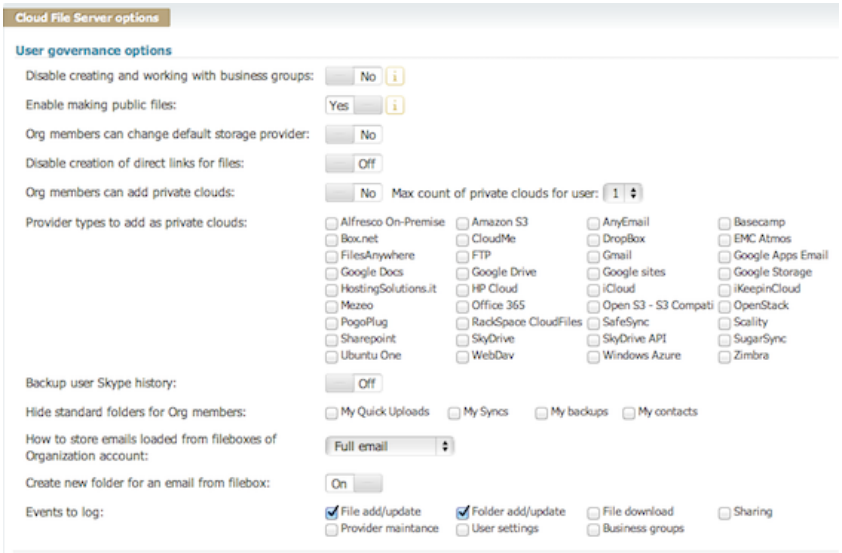
The Storage Made Easy Cloud File Server SaaS or Appliance has access to reporting abilities that can comprehensively audit all events that occur across all unified Cloud Services mapped to the account, recording any file event, including file sharing. Details logged are user (where known), event that occurred , date/time, and IP Address endpoint.

Reports can be accessed online, archived, and also exported as .cvs or excel files.



Governance / Control Options

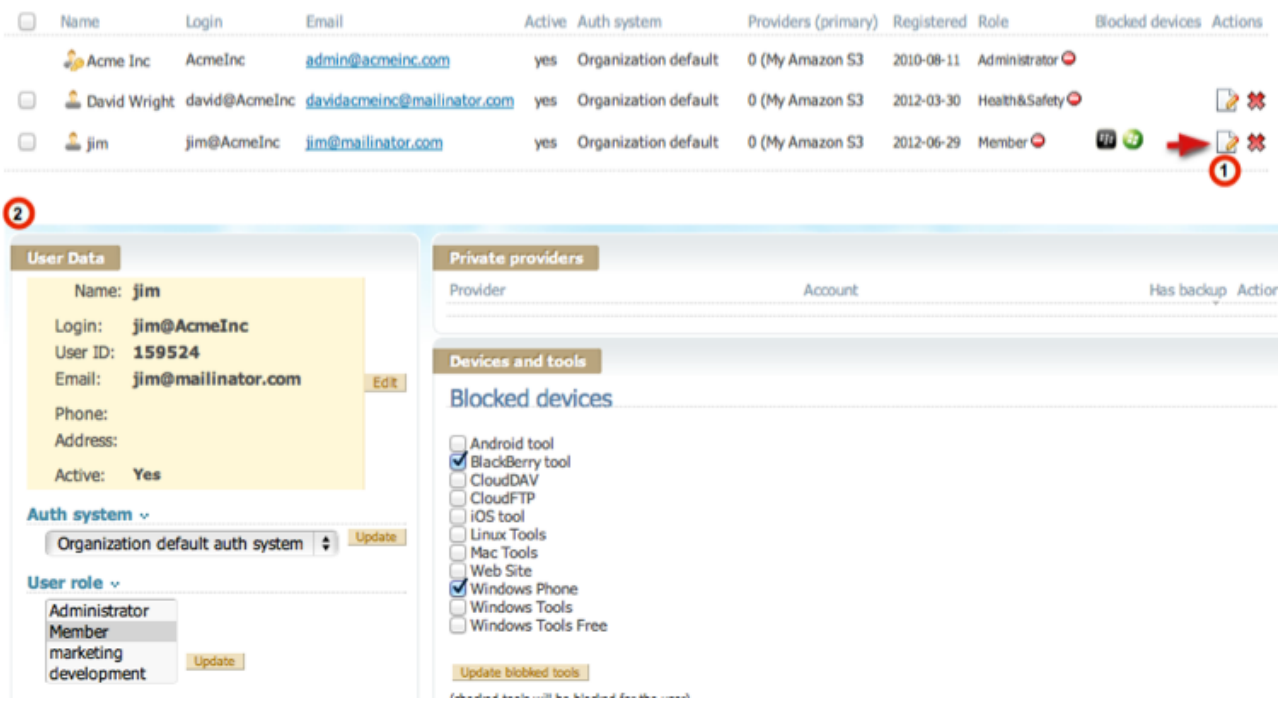
Cloud File Server Saas and Appliance users can set governance options for all users and control almost all levels of security for users, such as whether shared links can be generated, whether encryption is used, whether file versioning is turned on etc.



SECURITY FAQ

Bring Your Own Device

Bring Your Own Device or BYOD as it is often referred to, is a description of a trend whereby employees use their own smartphone and tablet devices to access corporate data. This presents interesting challenges for organizations who want to embrace the cost savings of users using their own device, but also want to ensure they still have "control". The Storage Made Easy platform has built in support for controlling BYOD users.



The Cloud File Server (CFS) Admin controls which devices and access clients that each user of the Cloud File Server can connect from. By default all devices and access clients are enabled.

The CFS admin can entirely disable a user, role or department, or just choose to disable access from any of the devices/access clients from the users settings. Clicking the checkbox next to the appropriate device blocks access to that device for that user or role. This means that if a device is lost even if login details are saved login will be denied.

You can, for example, ensure that an Accounts Sub-Department can only access a certain folder from the web, on a specific IP address. and from no other access mechanism.

SECURITY FAQ

Restricting access from Physical locations

Access to the Appliance can be restricted to static IP addresses if required, for example a branch office, or individual users can have IP addresses assigned, for example a user working from home or in a home office.

GEO Location Logging

The GEO location of where a file is uploaded from and where a file is uploaded to is recorded and logged for each file, as is the IP address. Proving document location can be important for certain industries and is an important part of any audit flow.

GEO info

	Uploaded from	Stored at
IP:	86.177.176.50	72.21.215.196
Country:	United Kingdom	United States
Region:	London	WA
City:	London	Seattle
Latitude:	51.514198	47.6026000
Longitude:	-0.0931	-122.32839

File stored with:

Provider: SME

File is not locked

File Sharing Security

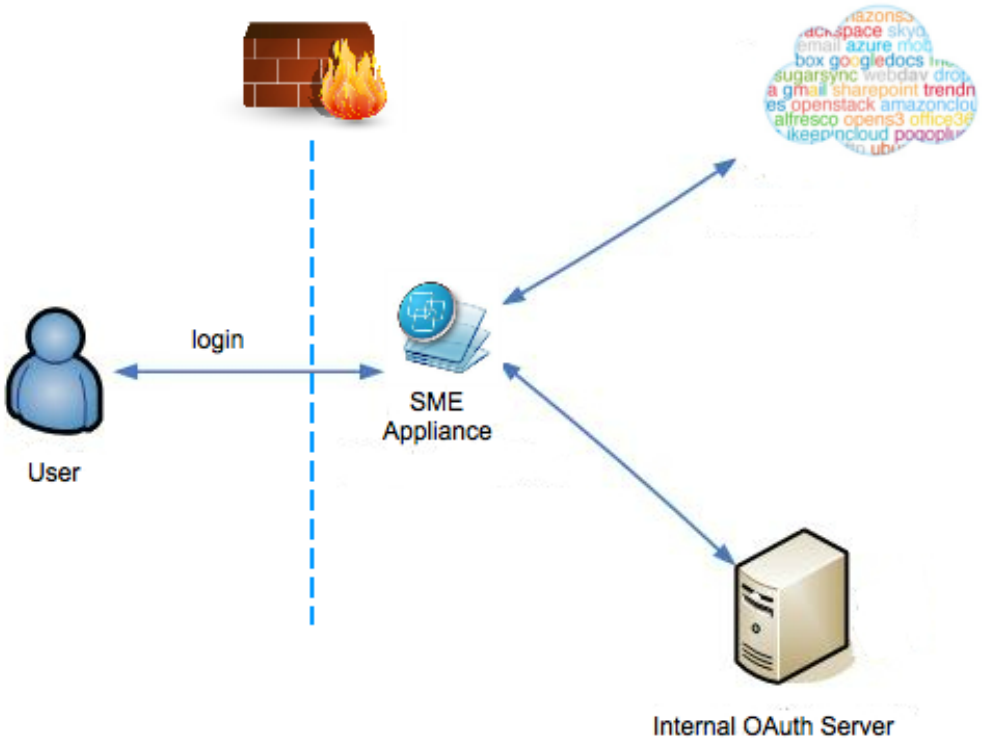
Files can be securely shared using a combination of time expiry and assigning passwords. There is also a plug-in for Microsoft Outlook that enables easy integration of this process. Any files shared either as time expired, password protected, or any link can be audited using the secure auditing options outlined elsewhere in this white paper.

CUSTOM SECURITY INTEGRATION

An example SME integration with an OAuth front-end client

Storage Made Easy can integrate with on-premise custom front end security or identity management systems, such as LDAP / Active Directory, which is provided 'out of the box'.

We will discuss in detail a user authentication integration with an company internal OAuth server with the SME Appliance.



OAuth is an open protocol that allows a user to grant a third party site access to their information stored with another third party site, without divulging their access credentials or even their identity. Designed to complement OpenID industry insiders believe OAuth will play a key role in the development of secure REST-based Web Services.

CUSTOM SECURITY INTEGRATION

An example SME integration with an OAuth front-end client (cont.)

Components Described

OAuth Proxy:

OAuth Proxy is a service that is provided by OAuth security vendors.. This service is passed a REST service URL. The OAuth Proxy adds OAuth headers for the logged in user and call the passed web or REST service and return the response.

OAuth Secure Token Service (OAuth STS):

This decrypts the headers added by OAuth Proxy and returns user attributes including the users identity.

SME Widget:

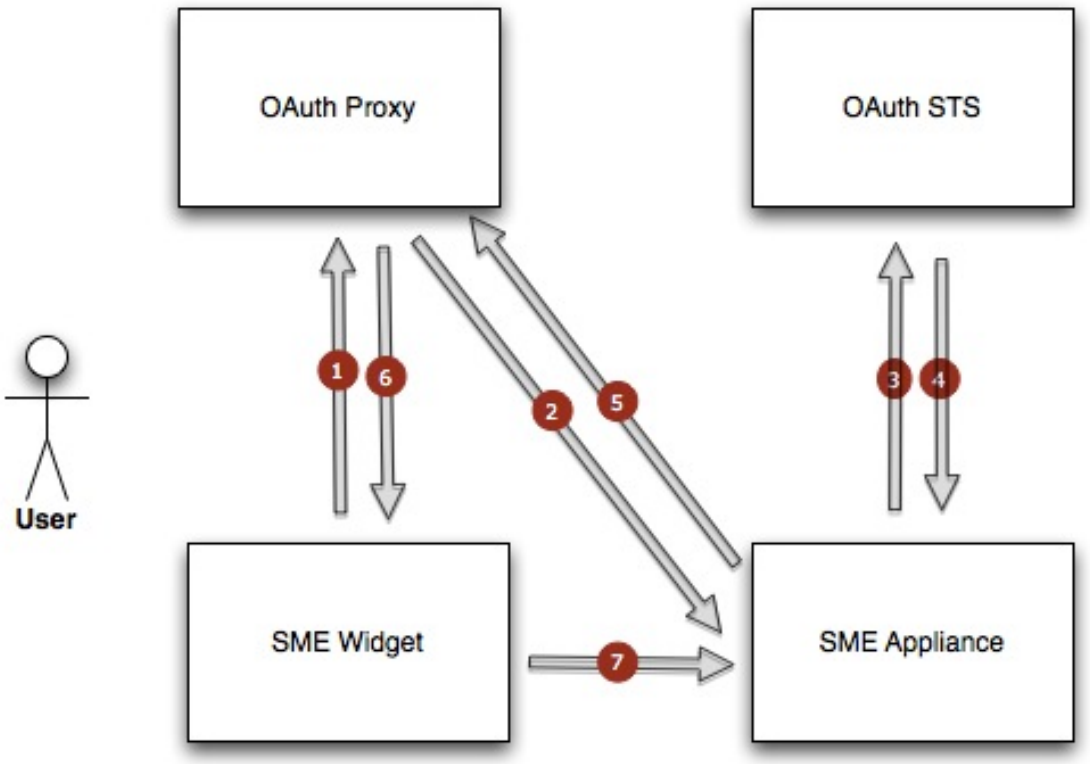
The SME Widget refers to any Storage Made Easy client.

SME Cloud Appliance:

An onsite appliance that provides an application which encompasses a users access to the unified cloud services.

CUSTOM SECURITY INTEGRATION

Call flow



A user logs into an Single Sign On system and is authenticated. The user role is authorized to use the Storage Made Easy widgets/clients.

CUSTOM SECURITY INTEGRATION

Lets looks at the flow for such an interaction in more detail:

1. The SME widget is invoked and calls the OAuth Proxy by passing the SME login service URL

2. The OAuth proxy service will automatically add the OAuth headers for the logged in user and will call the http://smeloginurl hosted on the SME appliance.

3. The SME appliance will call the OAuth STS with the received OAuth headers. This will involve just copying the headers and calling OAuth STS service.

4. The OAuth STS service will parse the headers and return user attributes to the SME appliance including the users identity.

5. If the response from STS was successful the SME Appliance will generate the SME token using the user identity, map it to the SME user and return the token.

6. The user is authenticated and mapped, SME has generated the token and returned the token to the widget.

7. All the subsequent REST calls to SME appliance from the SME widget will use the returned token for authentication and authorization.

Time Estimate

For SME to do a custom integration into such an OAuth identity management system the bulk of the time will be taken in setting up the environment and testing. We are confident that such a custom integration can be completed and tested in 5-10 working days having had experience of doing this previously.

Additional to this we may also need to change some authentication details on the SME clients. The time required for this depends on the number of SME clients required but should not take longer than 5-8 days.

CUSTOM SECURITY INTEGRATION

Other Security Models

Other Security models can also be embraced, such as OpenID and Kerberos.

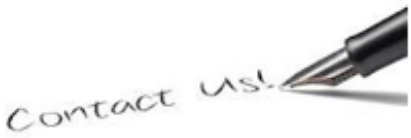
OpenID is an open identity federation standard originally designed to allow consumers to register with one OpenID provider, then use that same identity to log into a variety of Websites. While currently there are a number of barriers preventing widespread corporate adoption of OpenID, security being a primary concern, enterprise adoption of OpenID is expected to expand in the future.

Kerberos is a secure method for authenticating a request for a service in a computer network. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server.

There are a variety of ways that Storage Made Easy could work with a Kerberos based Architecture.

Storage Made Easy can work with NTLM authentication and can already be setup to enable SME to authenticate users on Active Directory to enable federated single sign on (SSO). The time taken to set up the SME Cloud Appliance, integrate with Active Directory and test end-to-end can easily be achieved with a day.

Storage Made Easy Cloud Appliance
White Label and OEM options



UK OFFICE
Vehera Ltd
First Floor Unit 1
Mulgrave Chambers
26-28 Mulgrave Road
Sutton
Surrey
SM2 6LE

TELEPHONE:
+448006899094 ext. 1 for Sales

US OFFICE
40 Richards Ave.,
3rd Floor,
Norwalk, CT 06854,
USA

TELEPHONE:
+1.203.604.6860

EUROPEAN OFFICE
Imbisbuehlstrasse 108
CH-8049 Zurich
Switzerland

TELEPHONE :
+41 (0) 43 818 46 74

OTHER METHODS OF CONTACT

Email: Sales@StorageMadeEasy.com

Skype: StorageMadeEasy

Website: Live Sales feature. Just click to chat

UK HEAD OFFICE ADDRESS AND LOCATION